BULL. AUSTRAL. MATH. SOC. 11D41, 11F80, 11F11, 11G05
VOL. 76 (2007) [161–194]

ÉQUATIONS DE FERMAT DE TYPE $(5, 5, p)$

NICOLAS BILLEREY

Soient p un nombre premier $\geqslant 7$ et d un entier naturel sans puissances cinquièmes. Nous mettons en œuvre les différentes méthodes modulaires connues pour l'étude de l'équation diophantienne $x^5+y^5 = dz^p$. Nous montrons en particulier qu'elle n'admet aucune solution propre et non triviale pour $p \geqslant 7$ ou pour une infinité de nombres premiers, dans certains cas où d est de la forme $2^\alpha \cdot 3^\beta \cdot 5^\gamma$. Pour $d = 3$, on énonce un critère permettant de vérifier, notamment, que tel est le cas lorsque p est $\leqslant 10^6$.

Let p be a prime number $\geqslant 7$ and d be a positive integer fifth power free. We use the known modular methods for the study of the diophantine equation $x^5+y^5 = dz^p$. We prove that this equation has no non trivial proper solution for $p \geqslant 7$ or for infinitely many prime numbers, in some cases where d is of the form $2^\alpha \cdot 3^\beta \cdot 5^\gamma$. For $d = 3$, we give a criterion which allows us to verify that this holds if p is less than 10^6.

INTRODUCTION

Soient d un entier naturel sans puissances cinquièmes et p un nombre premier $\geqslant 7$. On s'intéresse dans cet article à l'équation diophantienne suivante:

$$x^5 + y^5 = dz^p. \tag{1}$$

Suivant la terminologie de Darmon et Granville ([5]), on dira qu'un triplet d'entiers $(a, b, c) \in \mathbb{Z}^3$ est une solution de l'équation (1) si l'on a $a^5 + b^5 = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Notons $S_p(d)$ l'ensemble des solutions propres et non triviales de l'équation (1). On se propose dans cet article de démontrer quelques résultats concernant l'ensemble $S_p(d)$. Une conséquence de la conjecture *abc* est la suivante:

CONJECTURE 1. *Supposons que d ne soit pas la somme de deux puissances cinquièmes d'entiers relatifs non nuls. Alors, il existe une constante $c(d)$, qui ne dépend que de d, telle que si l'on a $p > c(d)$, alors l'équation (1) n'admet aucune solution propre et non triviale.*

Received 20th November, 2006
Je remercie Kraus pour ses nombreux conseils et Bernardi pour son aide sur le logiciel de calculs PARI.

Les travaux de Frey, Ribet, Serre et Wiles sur les représentations modulaires, permettent parfois d'aborder ce type de problèmes (voir [**7, 17, 19**] et [**22**]). La méthode maintenant fréquemment utilisée à ce sujet est souvent appelée la méthode modulaire. Elle exploite les propriétés modulaires de certaines courbes elliptiques ainsi que les propriétés galoisiennes de leurs points de p-torsion. Plus précisément, à une hypothétique solution de l'équation (1), on associe ici une courbe elliptique sur $\mathbb{Q}$, dont la construction est dûe à Darmon ([**4**]), dite *courbe de Frey* ou *courbe de Hellegouarch-Frey* et dont la représentation galoisienne dans ses points de p-torsion est liée à l'existence d'une forme modulaire de poids et de niveau précis, qui ≪essentiellement≫ ne dépendent pas de la solution considérée. On est alors confronté au problème de démontrer que l'existence d'une telle forme modulaire conduit à une contradiction. Une étude de la ramification du corps des points de p-torsion de la courbe de Frey permet parfois d'y parvenir.

Signalons qu'un résultat figurant dans [**13**] entraîne que, p étant donné, l'ensemble des entiers d sans puissances cinquièmes et sans diviseurs premiers congrus à 1 modulo 5, pour lesquels $S_p(d)$ soit non vide, est fini. Dans cet article, nous mettons en œuvre la méthode modulaire et certaines de ses variantes pour l'étude de l'équation (1). Elle permet de montrer que $S_p(d)$ est vide pour $p \geqslant 7$, ou seulement pour une infinité de p, dans certains cas où d est de la forme $2^\alpha \cdot 3^\beta \cdot 5^\gamma$ avec $0 \leqslant \alpha, \beta, \gamma \leqslant 4$.

On énonce par ailleurs un critère, analogue à celui obtenu par Kraus concernant l'équation $x^3 + y^3 = z^p$ (voir [**12**]), permettant souvent de montrer que $S_p(3)$ est vide pour un nombre premier p fixé. On démontre qu'il s'applique également aux petites valeurs de p (notamment $p = 7$). On le vérifie numériquement, à l'aide d'un programme PARI pour tous les nombres premiers p compris entre 7 et 10^6.

1. Énoncés des résultats

Soit p un nombre premier $\geqslant 7$. Les résultats décrits ici concernent les entiers d de la forme

$$d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma, \quad \text{avec} \quad 0 \leqslant \alpha, \beta, \gamma \leqslant 4.$$

Dans le cas particulier où $d = 1$, en utilisant la méthode modulaire classique, on obtient l'énoncé suivant:

Théorème 1.1. *Soit (a, b, c) un élément de $S_p(1)$. Alors c est impair. Autrement dit, la puissance p-ième d'un entier pair non nul ne peut s'écrire comme la somme de deux puissances cinquièmes d'entiers premiers entre eux.*

Pour quinze valeurs de d sur les cent vingt-cinq envisagées ci-dessus, par la même méthode que celle utilisée dans le Théorème 1.1, on obtient une réponse complète quant à la description de $S_p(d)$:

Théorème 1.2. *Supposons que d soit de la forme*

$$d = 2^\alpha \cdot 5^\gamma \quad \textit{avec } \alpha \in \{2, 3, 4\} \quad \textit{et} \quad 0 \leqslant \gamma \leqslant 4.$$

Alors, $S_p(d)$ est vide.

Pour certaines valeurs de d, nous obtenons une réponse partielle en démontrant que $S_p(d)$ est vide seulement pour un ensemble de nombres premiers p de densité > 0. En utilisant la méthode symplectique, décrite dans [8], on obtient à ce sujet l'énoncé suivant:

THÉORÈME 1.3. *Posons $d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$ et supposons que l'on soit dans l'un des cas ci-dessous:*

1. $(\alpha, \beta, \gamma) \in \{(3,1,\geqslant 1), (3,4,\geqslant 1), (4,2,\geqslant 1)\}$ *et* $p \equiv 5$ *ou* $7 \pmod{12}$;
2. $(\alpha, \beta, \gamma) \in \{(3,2,\geqslant 1), (4,1,\geqslant 1), (4,4,\geqslant 1)\}$ *et* $p \equiv 7, 11, 13$ *ou* $17 \pmod{24}$;
3. $(\alpha, \beta, \gamma) \in \{(3,1,0), (3,4,0), (4,2,0), (4,3,0)\}$ *et* $p \equiv 5$ *ou* $19 \pmod{24}$;
4. $(\alpha, \beta, \gamma) = (4,3,\geqslant 1)$ *et* $p \equiv 3$ *ou* $5 \pmod{8}$.

Alors, $S_p(d)$ est vide.

Énonçons maintenant les résultats obtenus concernant le cas où $d = 3$. Pour tout nombre premier $p \geqslant 7$, on démontre un critère qui permet souvent de prouver que $S_p(3)$ est vide. Considérons pour cela un nombre premier q congru à 1 modulo p. Posons $q = np + 1$. Le groupe $\mu_n(\mathbb{F}_q)$ des racines n-ièmes de l'unité de $\mathbb{F}_q$ est d'ordre n. On définit deux sous-ensembles $A(n,q)$ et $B(n,q)$ de $\mu_n(\mathbb{F}_q)$ de la façon suivante.

1. Soit $\widetilde{A}(n,q)$ le sous-ensemble de $\mu_n(\mathbb{F}_q)$ formé des éléments ζ pour lesquels:

$$405 + 62500\zeta \text{ est un carré dans } \mathbb{F}_q.$$

À un tel élément ζ, on associe le plus petit entier $\delta_{1,\zeta} \geqslant 0$ tel que

$$\delta_{1,\zeta}^2 \pmod{q} = 405 + 62500\zeta.$$

On définit $A(n,q)$ comme étant le sous-ensemble de $\widetilde{A}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

$$-225 + 10\delta_{1,\zeta} \quad \text{et} \quad -225 - 10\delta_{1,\zeta}$$

est un carré modulo q. À tout élément $\zeta \in A(n,q)$, on associe alors la cubique sur $\mathbb{F}_q$ suivante:

$$F_{1,\zeta} : y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{2}$$

Son discriminant vaut $6480\zeta^2 = 2^4 \cdot 3^4 \cdot 5\zeta^2$, qui est non nul car on a $q \geqslant 7$. Par suite, $F_{1,\zeta}$ est une courbe elliptique sur $\mathbb{F}_q$. On note $n_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F_{1,\zeta}$ et l'on pose

$$a_q(\zeta) = q + 1 - n_{1,q}(\zeta). \tag{3}$$

2. Soit $\widetilde{B}(n,q)$ le sous-ensemble de $\mu_n(\mathbb{F}_q)$ formé des éléments ζ pour lesquels:

$$405+20\zeta \text{ est un carré dans } \mathbb{F}_q.$$

À un tel élément ζ, on associe le plus petit entier $\delta_{2,\zeta} \geqslant 0$ tel que

$$\delta_{2,\zeta}^2 \pmod q = 405+20\zeta.$$

On définit $B(n,q)$ comme étant le sous-ensemble de $\widetilde{B}(n,q)$ constitué des éléments ζ pour lesquels l'un au moins des entiers

$$-225+10\delta_{2,\zeta} \quad \text{et} \quad -225-10\delta_{2,\zeta}$$

est un carré modulo q. À tout élément $\zeta \in B(n,q)$, on associe alors la cubique sur $\mathbb{F}_q$ suivante:

$$F_{2,\zeta} : y^2 = x^3+\delta_{2,\zeta}x^2+5\zeta x. \tag{4}$$

Son discriminant $2^4\cdot 3^4\cdot 5^3\zeta^2$ est non nul car on a $q \geqslant 7$. Par suite, $F_{2,\zeta}$ définit une courbe elliptique sur $\mathbb{F}_q$. On note $n_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F_{2,\zeta}$ et l'on pose

$$b_q(\zeta) = q+1-n_{2,q}(\zeta). \tag{5}$$

Les notations étant celles utilisées dans les tables de [3] (à ceci près que les lettres minuscules ont été remplacées ici par des lettres majuscules), on considère les trois ensembles de courbes elliptiques suivants:

$$\mathcal{E}_1 = \{150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{J1}\};$$
$$\mathcal{E}_2 = \{150\text{A1}, 600\text{C1}, 1200\text{N1}\}.$$

Si F est l'une des courbes des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ et si ℓ est un nombre premier $\geqslant 7$, alors F a bonne réduction en ℓ. On pose

$$a_\ell(F) = \ell+1-\left|\widetilde{F}(\mathbb{F}_\ell)\right|,$$

où $\left|\widetilde{F}(\mathbb{F}_\ell)\right|$ est le nombre de points rationnels de la courbe $\widetilde{F}$ sur $\mathbb{F}_\ell$ déduite de F par réduction modulo ℓ.

Le critère que l'on obtient est le suivant:

THÉORÈME 1.4. *Soit p un nombre premier $\geqslant 7$. Supposons que les deux conditions suivantes soient satisfaites:*

1. *Pour toute courbe elliptique F appartenant à $\mathcal{E}_1$, il existe un entier $n \geqslant 2$ tel que:*

   (a) *l'entier $q = np+1$ est premier.*

(b) *On a* $a_q(F)^2 \not\equiv 4 \pmod{p}$.

(c) *Pour tout* ζ *dans* $A(n,q)$, *on a*

$$a_q(\zeta)^2 \not\equiv a_q(F)^2 \pmod{p}.$$

2. *Pour toute courbe elliptique* F *appartenant à* $\mathcal{E}_2$, *il existe un entier* $n \geqslant 2$ *tel que:*

(1) *l'entier* $q = np + 1$ *est premier.*

(b) *On a* $a_q(F)^2 \not\equiv 4 \pmod{p}$.

(c) *Pour tout* ζ *dans* $B(n,q)$, *on a*

$$b_q(\zeta)^2 \not\equiv a_q(F)^2 \pmod{p}.$$

Alors, $S_p(3)$ *est vide.*

En utilisant ce critère et un résultat de L. Dirichlet concernant le cas où $p = 5$ ([**6**]), on obtient l'énoncé suivant:

PROPOSITION 1.1. *Si l'on a* $5 \leqslant p \leqslant 10^6$, *alors* $S_p(3)$ *est vide.*

Le critère du Théorème 1.1 s'applique pour des valeurs de p considérablement plus grandes que 10^6. Ainsi $S_p(3)$ est vide lorsque $p = 15485863$ qui est le millionième nombre premier: on vérifie en effet que $n = 10$ satisfait aux conditions du Théorème 1.1 (pour toute courbe F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$). De même, $S_p(3)$ est vide pour $p = 1000000007$. Il suffit de prendre $n = 44$.

On donne en Appendice un tableau de valeurs d'entiers n satisfaisant aux conditions du Théorème 1.1 pour les nombres premiers compris entre 11 et 150, ainsi que quelques explications heuristiques sur l'efficacité de ce critère pour les ≪grands≫ nombres premiers.

2. La courbe elliptique E

On considère un élément (a,b,c) de $S_p(d)$. À un tel triplet on associe l'équation de Weierstrass E définie sur $\mathbb{Q}$:

$$y^2 = x^3 - 5(a^2+b^2)x^2 + 5\Big(\frac{a^5+b^5}{a+b}\Big)x. \tag{6}$$

Ses invariants standard (c_4, c_6, Δ) sont les suivants (voir [**21**]):

$$\begin{cases} c_4 &= 2^4 \cdot 5\Big(5(a^2+b^2)^2 - 3\dfrac{a^5+b^5}{a+b}\Big) = 2^4 \cdot 5(2a^4 + 3ba^3 + 7a^2b^2 + 3ab^3 + 2b^4), \\ c_6 &= 2^5 \cdot 5^2(a^2+b^2)\Big(2 \cdot 5(a^2+b^2)^2 - 3^2\dfrac{a^5+b^5}{a+b}\Big) \\ &= 2^5 \cdot 5^2(a^6 + 9a^5b + 12a^4b^2 + 18a^3b^3 + 12a^2b^4 + 9ab^5 + b^6), \\ \Delta &= 2^4 \cdot 5^3(a+b)^2(a^5+b^5)^2. \end{cases}$$

Puisque (a,b,c) appartient à $S_p(d)$, E est une courbe elliptique définie sur $\mathbb{Q}$.

NOTATIONS 1.

1. On pose
$$r = \prod_{\ell \mid cd, \ell \neq 2,5} \ell,$$
où ℓ parcourt l'ensemble des diviseurs premiers de cd autres que 2 et 5.
2. Si ℓ est un nombre premier, on note v_ℓ la valuation ℓ-adique de $\mathbb{Q}$.
3. On pose
$$\phi(a,b) = \frac{a^5+b^5}{a+b} = a^4 - a^3b + a^2b^2 - ab^3 + b^4. \tag{7}$$
4. On note Δ_m le discriminant minimal de E.

REMARQUES PRÉLIMINAIRES.

1. Les entiers a, b et c sont premiers entre eux deux à deux: cela résulte du fait que a, b et c sont premiers entre eux dans leur ensemble et que d est sans puissances cinquièmes.

2. Supposons d impair. Si a ou b est pair (mais pas les deux), alors c est impair. Si a et b sont impairs, alors c est pair.

3. Si d est pair, alors ab est impair.

4. Compte tenu des deux remarques précédentes, on peut supposer, ce que l'on fera dans toute la suite, que l'on est dans l'un des cas suivants:
   (a) d est impair et ac est pair: si c est impair, alors ab est pair et l'on suppose que c'est a qui est pair.
   (b) d est pair et ab impair.

PROPOSITION 2.1. *L'équation* (6) *est minimale en dehors de* 2. *Elle est minimale en* 2, *auquel cas on a* $\Delta_m = \Delta$, *sauf dans les trois cas suivants:*

1. *les entiers d et a sont impairs (et c est pair);*
2. *les entiers d et c sont pairs;*
3. *l'entier c est impair et l'on a* $v_2(d) = 2$, 3 *ou* 4.

Dans chacun de ces trois cas, on a alors:
$$\Delta_m = \frac{\Delta}{2^{12}}.$$

Soit N_E le conducteur de E.

PROPOSITION 2.2. *Supposons d impair. On a:*

1. $N_E = 2^4 \cdot 5^2 r$ *si* $v_2(a) = 1$;
2. $N_E = 2^3 \cdot 5^2 r$ *si* $v_2(a) \geqslant 2$;
3. $N_E = 2 \cdot 5^2 r$ *si a est impair.*

PROPOSITION 2.3. *Supposons d pair.*

1. *Si c est* pair, *on a* $N_E = 2 \cdot 5^2 r$.
2. *Si c est* impair, *alors:*
   (a) *si* $v_2(d) = 2$, *on a* $N_E = 5^2 r$;
   (b) *si* $v_2(d) = 3$ *ou* 4, *on a* $N_E = 2 \cdot 5^2 r$;
   (c) *si* $v_2(d) = 1$, *on a* $N_E = 2^4 \cdot 5^2 r$.

Les démonstrations de ces propositions font l'objet des paragraphes 2.1 à 2.5.

2.1. LEMMES PRÉLIMINAIRES. Les trois lemmes suivants interviennent dans la suite à plusieurs reprises.

LEMME 2.4. *Soit* ℓ *un nombre premier divisant* $a + b$. *On a alors*

$$\phi(a,b) \equiv 5a^2b^2 \pmod{\ell^2}. \tag{8}$$

DÉMONSTRATION: Si ℓ un nombre premier divisant $a + b$, on a

$$a^2 + b^2 \equiv -2ab \pmod{\ell^2}.$$

Or

$$\phi(a,b) = (a^2 + b^2)^2 - ab(a^2 + b^2 + ab), \tag{9}$$

d'où

$$\phi(a,b) \equiv 5a^2b^2 \pmod{\ell^2}$$

et le Lemme 2.4.

LEMME 2.5. *Les entiers* $a + b$ *et* $\phi(a,b)$ *sont premiers entre eux en dehors de* 5. *De plus, si* 5 *divise* $a + b$, *alors* $v_5\big(\phi(a,b)\big) = 1$ *et* $v_5(a+b) = v_5(d) + pv_5(c) - 1$.

DÉMONSTRATION: Soit ℓ un nombre premier divisant $a + b$ et $\phi(a,b)$. Si $\ell \neq 5$, on a $5a^2b^2 \not\equiv 0 \pmod{\ell}$ car ℓ ne divise pas ab. Donc ℓ ne divise pas $\phi(a,b)$ (Lemme 2.4). Si $\ell = 5$, la congruence (8) ci-dessus implique $v_5\big(\phi(a,b)\big) = 1$. L'égalité $(a+b)\phi(a,b) = dc^p$ entraîne alors le lemme.

LEMME 2.6. *Soit* ℓ *un nombre premier non congru à* 1 *modulo* 5 *et divisant* $a^5 + b^5$. *Alors,* ℓ *divise* $a + b$.

DÉMONSTRATION: Puisque ℓ divise $a^5 + b^5$, ℓ ne divise pas ab. Soit b' l'inverse de $-b$ modulo ℓ. On a $a^5 \equiv (-b)^5 \pmod{\ell}$, d'où $(ab')^5 \equiv 1 \pmod{\ell}$. Par suite, l'ordre de ab' dans le groupe multiplicatif $\mathbf{F}_\ell^*$ est 1 ou 5. La congruence $ab' \equiv 1 \pmod{\ell}$ conduit à $a + b \equiv 0 \pmod{\ell}$. Si ℓ ne divise pas $a + b$, on en déduit donc que l'ordre de ab' dans $\mathbf{F}_\ell^*$ est 5 puis $\ell \equiv 1 \pmod{5}$. D'où le lemme.

2.2. ÉTUDE DE LA RÉDUCTION DE E EN DEHORS DE $\{2,5\}$. On démontre le résultat suivant:

LEMME 2.7. *Soit ℓ un nombre premier distinct de 2 et 5. La courbe E est semi-stable en ℓ et l'on a*

$$v_\ell(N_E) = \begin{cases} 1 & \text{si } \ell \text{ divise } cd, \\ 0 & \text{sinon.} \end{cases}$$

L'équation (6) *définit un modèle minimal en ℓ de E et $\Delta_m = \Delta$. On a de plus,*

$$v_\ell(\Delta_m) \equiv \begin{cases} 4v_\ell(d) \pmod p & \text{si } \ell \text{ divise } a+b, \\ 2v_\ell(d) \pmod p & \text{si } \ell \text{ ne divise pas } a+b. \end{cases} \tag{10}$$

En particulier,

$$p \text{ divise } v_\ell(\Delta_m) \Longleftrightarrow \ell \text{ ne divise pas } d. \tag{11}$$

DÉMONSTRATION: D'après l'égalité,

$$\Delta = 2^4.5^3(a+b)^2(a^5+b^5)^2,$$

on a $v_\ell(\Delta) = 2v_\ell(a+b) + 2v_\ell(a^5+b^5)$. Or

$$a^5 + b^5 = dc^p,$$

donc $v_\ell(a^5+b^5) = v_\ell(d) + pv_\ell(c)$. D'où

$$v_\ell(\Delta) \equiv 2v_\ell(a+b) + 2v_\ell(d) \pmod p. \tag{12}$$

Si ℓ ne divise pas cd, alors d'après l'égalité $a^5+b^5 = dc^p$ et le fait que $a+b$ divise a^5+b^5, ℓ ne divise pas Δ et E a donc bonne réduction en ℓ.

Supposons que ℓ divise cd. Dans ce cas, ℓ divise a^5+b^5. On distingue alors deux cas suivant que $a+b$ est ou non divisible par ℓ.

1. Supposons que ℓ divise $a+b$. Alors, $\phi(a,b) \equiv 5a^4 \pmod \ell$, d'après le Lemme 2.4. On en déduit

$$c_4 \equiv 2^4.5^2a^4 \pmod \ell$$

d'où $v_\ell(c_4) = 0$. L'équation (6) est donc minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$ et $v_\ell(\Delta_m) = v_\ell(\Delta)$.

Puisque ℓ divise $a+b$, ℓ ne divise pas $\phi(a,b)$ (Lemme 2.5). On en déduit

$$v_\ell(a+b) \equiv v_\ell(d) \pmod p.$$

La congruence (12) entraîne alors la condition (10). L'équivalence (11) en résulte vu que l'on a $0 \leqslant v_\ell(d) \leqslant 4$.

2. Supposons que ℓ ne divise pas $a+b$. On a $\phi(a,b) \equiv 0 \pmod{\ell}$ car ℓ divise a^5+b^5 sans diviser $a+b$. D'après l'égalité (9), ℓ ne divise pas a^2+b^2 car ℓ ne divise pas ab. On en déduit que $v_\ell(c_4) = 0$. Par suite, l'équation (6) est minimale en ℓ et E a réduction multiplicative en ℓ, d'où $v_\ell(N_E) = 1$. D'après la congruence (12), on a $v_\ell(\Delta_m) \equiv 2v_\ell(d) \pmod{p}$ et l'on conclut comme ci-dessus.

2.3. ÉTUDE DE LA RÉDUCTION DE E EN 5. On démontre le résultat suivant:

LEMME 2.8. *La courbe E a mauvaise réduction de type additif en 5 et l'on a $v_5(N_E) = 2$. L'équation (6) est minimale en 5. L'invariant modulaire j de E est entier en 5 si et seulement si 5 ne divise pas $a+b$.*

De plus, p divise $v_5(j)$ si et seulement si l'une des deux conditions suivantes est satisfaite:

1. *on a $a+b \not\equiv 0 \pmod{5}$,*
2. *on a $a+b \equiv 0 \pmod{5}$ et $\big(p, v_5(d)\big) \in \big\{(7,3),(11,4)\big\}$.*

DÉMONSTRATION: On distingue deux cas.

1. Supposons que 5 ne divise pas $a+b$. Dans ce cas, $\phi(a,b) \equiv 1 \pmod{5}$ car $a^5+b^5 \equiv a+b \pmod{5}$, d'où:

$$\big(v_5(c_4), v_5(c_6), v_5(\Delta)\big) = (1, \geqslant 2, 3).$$

Le type de Kodaira de E est donc III (voir [**16**, tableau I, p. 126]) et l'on a ainsi $v_5(N_E) = 2$. L'égalité $j = c_4^3/\Delta$ entraîne alors $v_5(j) = 0$.

2. Supposons que 5 divise $a+b$. On a alors (Lemme 2.4)

$$a^2+b^2 \equiv -2ab \pmod{25} \quad \text{et} \quad \phi(a,b) \equiv 5a^2b^2 \pmod{25}.$$

On a donc:

$$\frac{c_4}{5} \equiv 2^4.5a^2b^2 \pmod{25} \quad \text{et} \quad \frac{c_6}{5^2} \equiv 2^6.5(ab)^3 \pmod{25},$$

d'où les égalités:

$$v_5(c_4) = 2 \quad \text{et} \quad v_5(c_6) = 3.$$

On en conclut que la courbe E a mauvaise réduction de type additif en 5 et que l'équation (6) est minimale en 5. Le type de Kodaira de E est donc I_ν^* où $\nu = 4v_5(a+b) - 1$ et l'on obtient $v_5(N_E) = 2$ (voir *loco citato*).

D'après le Lemme 2.5, on a:

$$v_5(a^5+b^5) = v_5(a+b) + 1,$$

d'où $v_5(\Delta) = 5 + 4v_5(a+b) \geqslant 9$ et l'inégalité $v_5(j) < 0$.

De l'égalité

$$v_5(\Delta) = 5 + 4(v_5(d) + pv_5(c) - 1),$$

il vient:

$$v_5(j) = 6 - v_5(\Delta) \equiv 5 - 4v_5(d) \pmod{p}.$$

Autrement dit,

$$v_5(j) \equiv \begin{cases} 5 \pmod{p} & \text{si } v_5(d) = 0, \\ 1 \pmod{p} & \text{si } v_5(d) = 1, \\ -3 \pmod{p} & \text{si } v_5(d) = 2, \\ -7 \pmod{p} & \text{si } v_5(d) = 3, \\ -11 \pmod{p} & \text{si } v_5(d) = 4. \end{cases}$$

Cela établit le lemme.

2.4. ÉTUDE DE LA RÉDUCTION DE E EN 2 SI d EST IMPAIR. On démontre le résultat suivant:

LEMME 2.9. *Supposons d impair. La courbe E a mauvaise réduction en 2.*

1. *Si a est pair, E a réduction de type additif en 2. On a*

$$v_2(N_E) = \begin{cases} 4 & \text{si } v_2(a) = 1, \\ 3 & \text{si } v_2(a) \geqslant 2. \end{cases}$$

2. *Si a est impair, E a réduction de type multiplicatif en 2 et l'on a alors $v_2(N_E) = 1$.*

L'équation (6) *est minimale en 2 si et seulement si a est pair.*

DÉMONSTRATION: On est amené à distinguer deux cas suivant la parité de a.

1. Supposons a pair. On a alors:

$$v_2(c_4) \geqslant 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

En fait, on a plus précisément $\big(v_2(a), v_2(c_4)\big) \in \big\{(1, \geqslant 6), (\geqslant 2, 5)\big\}$. En effet, on a

$$\frac{c_4}{2^4} \equiv 2 + 3ab^3 \equiv 2 + 3ab \pmod{4}$$

$$\equiv \begin{cases} 0 \pmod{4} & \text{si } v_2(a) = 1 \\ 2 \pmod{4} & \text{si } v_2(a) \geqslant 2. \end{cases} \tag{13}$$

Il convient donc de séparer les cas où $v_2(a) = 1$ et $v_2(a) \geqslant 2$.

(a) Supposons $v_2(a) = 1$. On est dans le cas 3 ou 5 de Tate (voir [**16**, tableau IV, p. 129]). D'après la Proposition 1, p. 124 de *loco citato* appliquée avec $r = t = 1$, on est dans un cas $\geqslant 4$ si et seulement si

$$5\Big(\frac{a^5 + b^5}{a + b}\Big) - 5(a^2 + b^2) \equiv 0 \pmod{4},$$

ce qui équivaut à

$$a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv 0 \pmod 4.$$

Or on a $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv -ab \pmod 4$ et comme $v_2(a) = 1$, l'entier ab n'est pas multiple de 4. On est donc dans le cas 3 de Tate et l'on a $v_2(N_E) = 4$.

(b) Supposons $v_2(a) \geqslant 2$. On a alors:

$$v_2(c_4) = 5, \quad v_2(c_6) = 5, \quad v_2(\Delta) = 4.$$

On est donc dans le cas 3 ou 4 de Tate. On déduit alors de la congruence $a^4 - a^3b + a^2b^2 - ab^3 + b^4 - (a^2 + b^2) \equiv -ab \pmod 4$, que l'on est dans le cas 4 de Tate et l'on a $v_2(N_E) = 3$.

2. Supposons a impair. Dans ce cas, d'après la remarque préliminaire 4, b est impair et c est pair. On a ainsi $\phi(a, b) \equiv 1 \pmod 2$, $a^2 + b^2 \equiv 2 \pmod 4$ et l'égalité $v_2(a^5 + b^5) = v_2(a + b)$. Compte tenu de l'égalité (1), il en résulte que l'on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, \geqslant 32).$$

Vérifions que l'équation (6) n'est pas minimale en 2. On étudie pour cela la congruence de $c_6/2^6$ modulo 4 ([**10**, p. 77]). On constate que l'on a

$$\frac{c_6}{2^6} \equiv 2ab + 1 \pmod 4.$$

Puisque ab est impair, on a $ab \equiv \pm 1 \pmod 4$, et l'on obtient la congruence $c_6/2^6 \equiv -1 \pmod 4$. Notre assertion résulte alors du corollaire du Théorème 2 de *loco citato*. On en déduit que E a réduction multiplicative en 2 et l'on a donc $v_2(N_E) = 1$.

Cela termine la démonstration du Lemme 2.9.

2.5. ÉTUDE DE LA RÉDUCTION DE E EN 2 SI d EST PAIR. On démontre le résultat suivant:

LEMME 2.10. *Supposons d pair.*

1. *Si c est impair et si $v_2(d) = 2$, E a bonne réduction en 2, auquel cas on a $v_2(N_E) = 0$.*
2. *Si c est impair et si $v_2(d) = 1$, E a mauvaise réduction de type additif en 2 et l'on a $v_2(N_E) = 4$.*
3. *Supposons c pair ou bien que l'on ait $v_2(d) = 3$ ou 4. Alors E a réduction de type multiplicatif en 2 et l'on a $v_2(N_E) = 1$.*

L'équation (6) *est minimale en 2 si et seulement si c est impair et $v_2(d) = 2$.*

DÉMONSTRATION: Puisque d est pair, les entiers a et b sont impairs. On a donc $\phi(a,b) \equiv 1 \pmod 2$ et $v_2(a+b) = v_2(a^5+b^5)$. Il en résulte que l'on a

$$v_2(c_4) = 4, \quad v_2(c_6) = 6, \quad v_2(\Delta) = 4\big(1 + v_2(d) + pv_2(c)\big).$$

En particulier, on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, \geqslant 8).$$

Plus précisément, on a

$$\begin{cases} v_2(\Delta) = 8 & \text{si } v_2(d) = 1 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) = 12 & \text{si } v_2(d) = 2 \text{ et si } c \text{ est impair,} \\ v_2(\Delta) > 12 & \text{si } v_2(d) = 3 \text{ ou } 4, \text{ ou bien si } c \text{ est pair.} \end{cases}$$

On distingue donc les cas où $v_2(\Delta) = 8$ et $v_2(\Delta) \geqslant 12$.

1. Supposons $v_2(\Delta) \geqslant 12$. On a comme ci-dessus les congruences

$$\frac{c_6}{2^6} \equiv 2ab + 1 \equiv -1 \pmod 4.$$

Par suite, l'équation (6) n'est pas minimale en 2. Si l'on a $v_2(d) = 2$ et si c est impair, la courbe E a donc bonne réduction en 2, c'est-à-dire $v_2(N_E) = 0$. Par ailleurs, si $v_2(d) = 3$ ou 4, ou bien si c est pair, E a réduction multiplicative en 2 et l'on a $v_2(N_E) = 1$.

2. Supposons $v_2(\Delta) = 8$. On a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (4, 6, 8)$$

et l'on est dans le cas 6, 7 ou 8 de Tate. D'après [**16**, Proposition 3, p. 124], on est amené à déterminer si la congruence

$$-5^2\Big(\frac{a^5+b^5}{a+b}\Big)^2 + 2.3.5r^2\Big(\frac{a^5+b^5}{a+b}\Big) - 2^2.5r^3(a^2+b^2) + 3r^4 \equiv 0 \pmod{32}$$

a ou non une solution $r \in \mathbb{Z}$. On vérifie que $r = 1$ convient. D'après la proposition 3 de *loco citato*, il existe $t \in \mathbb{Z}$ tel que

$$5\Big(\frac{a^5+b^5}{a+b}\Big) - 5(a^2+b^2) + 1 \equiv t^2 \pmod 8,$$

et l'on vérifie que $t = 2$ convient. Posons

$$u = 5\Big(\frac{a^5+b^5}{a+b}\Big) - 5(a^2+b^2) - 3.$$

Vérifions que l'on a $v_2(u) = 3$. Les entiers a^2 et b^2 sont congrus à 1 ou 9 modulo 16, de sorte que l'on a $a^2 \equiv b^2 \pmod{16}$ ou $b^2 \equiv 9a^2 \pmod{16}$. Par ailleurs, on a $v_2(d) = 1$ et c est impair. D'après l'égalité (1), on a donc la congruence $a \equiv b \pmod 4$, autrement dit, on a $ab \equiv 1$ ou $5 \pmod 8$.

(a) Supposons $a^2 \equiv b^2 \pmod{16}$. Dans ce cas, on vérifie que l'on a

$$u \equiv 2 + 6ab \pmod{16}.$$

D'après l'hypothèse faite, on a $ab \equiv 1 \pmod{8}$, ce qui entraîne notre assertion.

(b) Supposons $b^2 \equiv 9a^2 \pmod{16}$. On obtient alors

$$u \equiv 2(1 - ab) \pmod{16}.$$

Par ailleurs, on a dans ce cas $ab \equiv 5 \pmod{8}$, d'où l'assertion.

Il en résulte que l'on est dans le cas 6 de Tate, puis que $v_2(N_E) = 4$. D'où le lemme 2.10.

Les propositions 2.1, 2.2 et 2.3 résultent alors des Lemmes 2.7 à 2.10.

3. La représentation ρ_p^E

Soit p un nombre premier $\geqslant 7$ et (a, b, c) un élément de $S_p(d)$. Notons $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$. Soit $E[p]$ le sous-groupe de $E(\overline{\mathbb{Q}})$ constitué des points de p-torsion de la courbe elliptique E. C'est un $\mathbb{F}_p$-espace vectoriel de dimension 2 sur lequel $G_{\mathbb{Q}}$ opère continûment. Par le choix d'une base de $E[p]$ sur $\mathbb{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^E : G_{\mathbb{Q}} \longrightarrow \mathbf{GL}_2(\mathbb{F}_p).$$

À une telle représentation J.-P. Serre associe un poids k qui est un entier $\geqslant 2$ et un conducteur $N(\rho_p^E)$ qui est un entier $\geqslant 1$, premier à p, qui divise le conducteur N_E de E (voir [19]).

Proposition 3.1. *La représentation ρ_p^E est irréductible.*

Démonstration: La courbe E a un point d'ordre deux rationnel sur $\mathbb{Q}$. Par suite, si ρ_p^E était réductible, le groupe $E(\overline{\mathbb{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $G_{\mathbb{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbb{Q}$. Or, si $p \geqslant 11$, B. Mazur et M. A. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbb{Q})$ est vide (voir [9]). D'où le résultat dans ce cas.

Supposons maintenant $p = 7$ et ρ_7^E réductible. La courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [3] ([15, p. 45]). Elle possède exactement deux points rationnels sur $\mathbb{Q}$ qui correspondent aux deux classes de $\overline{\mathbb{Q}}$-isomorphisme de courbes elliptiques d'invariants $j = -15^3$ et 255^3. Ce sont en effet les invariants modulaires des courbes notées 49A1 et 49A2 dans les tables de [3] et elles ont bien un sous-groupe d'ordre 14 stable par $G_{\mathbb{Q}}$. La courbe elliptique E correspond donc à un point rationnel sur $\mathbb{Q}$ de la courbe modulaire $Y_0(14)$. En particulier, on a $j = -15^3$ ou 255^3. En posant $t = a/b$, on en déduit que t est une solution rationnelle de l'équation:

$$2^8 \frac{(2t^4 + 3t^3 + 7t^2 + 3t + 2)^3}{(t+1)^2(t^5+1)^2} = -15^3 \quad \text{ou} \quad 255^3.$$

On vérifie que cela conduit à une contradiction. D'où la proposition.

PROPOSITION 3.2. *On a $k = 2$ si p ne divise pas d et $k = p + 1$ sinon.*

DÉMONSTRATION: Supposons que p ne divise pas d. Si p ne divise pas c, alors E a bonne réduction en p (Lemme 2.7) et l'on a $k = 2$ d'après [**19**, Proposition 5, p. 191]. Si p divise c, puisque l'on a $p \geqslant 7$, la courbe E a réduction multiplicative en p (*loco citato*). Par ailleurs, p divise $v_p(\Delta_m)$ (*loco citato*), ce qui entraîne de nouveau $k = 2$.

Supposons que p divise d. D'après le Lemme 2.7, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_m)$. Cela conduit à $k = p + 1$, d'où le résultat.

Calcul de $N(\rho_p^E)$. Posons

$$r' = \prod_{\substack{\ell \neq 2,5,p \\ \ell | d}} \ell,$$

où ℓ parcourt les diviseurs premiers de d distincts de $2, 5$ et p. Le conducteur $N(\rho_p^E)$ de ρ_p^E est donné dans les deux énoncés suivants:

PROPOSITION 3.3. *Supposons d* impair. *Alors:*

1. $N(\rho_p^E) = 2^4.5^2r'$, *si* $v_2(a) = 1$;
2. $N(\rho_p^E) = 2^3.5^2r'$, *si* $v_2(a) \geqslant 2$;
3. $N(\rho_p^E) = 2.5^2r'$, *si a est impair.*

PROPOSITION 3.4. *Supposons d* pair. *Alors:*

1. $N(\rho_p^E) = 2.5^2r'$, *si* $v_2(d) = 3$ *ou* 4;
2. $N(\rho_p^E) = 5^2r'$, *si* $v_2(d) = 2$;
3. $N(\rho_p^E) = 2.5^2r'$, *si* $v_2(d) = 1$ *et c est pair.*
4. $N(\rho_p^E) = 2^4.5^2r'$, *si* $v_2(d) = 1$ *et c est impair.*

Avant de démontrer ces propositions, on commence par le résultat suivant.

LEMME 3.5. *Supposons que E ait réduction de type multiplicatif en 2. Alors,*

$$v_2(\Delta_m) \equiv -8 + 4v_2(d) \pmod{p}. \tag{14}$$

En particulier, p divise $v_2(\Delta_m)$ si et seulement si c est pair et $v_2(d) = 2$.

DÉMONSTRATION: Puisque E a réduction de type multiplicatif en 2, on est dans l'un des cas suivants (Lemmes 2.9 et 2.10):

1. les entiers d et a sont impairs (et c est pair);
2. les entiers d et c sont pairs;
3. l'entier c est impair et l'on a $v_2(d) = 3$ ou 4.

Dans chacun des trois cas ci-dessus, l'entier ab est impair donc

$$v_2(a+b) = v_2(a^5+b^5).$$

D'après la proposition 2.1, on a:

$$\Delta_m = \frac{\Delta}{2^{12}}.$$

On en déduit

$$v_2(\Delta_m) = 4 + 4v_2(a^5+b^5) - 12.$$

Or $v_2(a^5+b^5) = v_2(d) + pv_2(c) \equiv v_2(d) \pmod{p}$. D'où la congruence (14). L'équivalence du lemme s'en déduit immédiatement car on a $0 \leqslant v_2(d) \leqslant 4$.

Démontrons à présent les propositions 3.3 et 3.4. Puisque $N(\rho_p^E)$ divise N_E, pour tout nombre premier ℓ qui ne divise pas $10r$, on a $v_\ell\big(N(\rho_p^E)\big) = 0$.

Considérons un diviseur premier ℓ de N_E distinct de $2, 5$ et p. D'après le Lemme 2.7 et [**11**, p. 28], on a

$$v_\ell\big(N(\rho_p^E)\big) = \begin{cases} 1 & \text{si } \ell \text{ divise } d, \\ 0 & \text{sinon.} \end{cases}$$

La courbe E ayant réduction de type additif en 5, on a $v_5\big(N(\rho_p^E)\big) = 2$ (*loco citato*).

Il reste à déterminer l'exposant de 2 dans $N(\rho_p^E)$. La valeur de l'exposant de 2 dans le conducteur N_E est donnée dans les propositions 2.2 et 2.3. Dans le cas où E a réduction de type additif en 2, c'est-à-dire, si $v_2(N_E) \geqslant 2$, on a $v_2\big(N(\rho_p^E)\big) = v_2(N_E)$ (*loco citato*). Si E a réduction multiplicative en 2, alors d'après le Lemme 3.5, $v_2\big(N(\rho_p^E)\big) = v_2(N_E)$ sauf si c est pair et $v_2(d) = 2$ auquel cas on a $v_2\big(N(\rho_p^E)\big) = v_2(N_E) - 1$, c'est-à-dire, $v_2\big(N(\rho_p^E)\big) = 0$.

Compte tenu du fait que $N(\rho_p^E)$ est premier à p, cela termine la démonstration des propositions 3.3 et 3.4.

4. Démonstrations des résultats

On suppose pour toute la suite qu'il existe un élément $(a, b, c) \in S_p(d)$ où p est un nombre premier $\geqslant 7$. Soit E la courbe d'équation (6) attachée à la solution (a, b, c).

Notations 2. Si n est un entier $\geqslant 1$, on note $\mathcal{S}_2^+(n)$ le $\mathbb{C}$-espace vectoriel formé des newforms paraboliques de poids 2 pour le sous-groupe $\Gamma_0(n)$ au sens de [**1**].

La représentation ρ_p^E est irréductible, de poids 2 et de conducteur $N(\rho_p^E)$. D'après les travaux de Ribet (voir [**17**]), il existe alors une newform

$$f = q + \sum_{n \geqslant 2} a_n(f) q^n \in \mathcal{S}_2^+\big(N(\rho_p^E)\big) \quad \text{avec} \quad q = e^{2i\pi\tau},$$

et une place $\mathfrak{P}$ de $\overline{\mathbb{Q}}$ de caractéristique résiduelle p telles que, pour tout nombre premier ℓ, on ait:

$$(15)\qquad \begin{cases} a_\ell(f) \equiv a_\ell(E) \pmod{\mathfrak{P}} & \text{si } \ell \text{ ne divise pas } pN_E, \\ a_\ell(f) \equiv \pm(\ell+1) \pmod{\mathfrak{P}} & \text{si } \ell \text{ divise } N_E \text{ et ne divise pas } pN(\rho_p^E). \end{cases}$$

Par ailleurs, dans le cas où les coefficients $a_n(f)$ sont dans $\mathbb{Z}$, la newform f correspond à une courbe elliptique $A/\mathbb{Q}$ de conducteur $N(\rho_p^E)$ unique à isogénie près. Notons respectivement

$$L_E(s) = \sum_{n\geqslant 1} a_n(E)n^{-s} \quad \text{et} \quad L_A(s) = \sum_{n\geqslant 1} a_n(A)n^{-s}$$

les fonctions L de Hasse - Weil de E et A.

Les représentations ρ_p^E et ρ_p^A sont alors isomorphes et l'on a en particulier:

$$(16)\qquad a_\ell(E) \equiv a_\ell(A) \pmod{p},$$

pour tout nombre premier ℓ ne divisant pas N_E (voir [14]). Il s'agit de contredire l'existence de f.

Soit $\mathbb{Q}(E[p])/\mathbb{Q}$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbb{Q}$. On note e son indice de ramification en 5.

Le lemme suivant intervient dans les paragraphes 4.3 et 4.4.

LEMME 4.1. *1. Si 5 divise $a+b$, on a:*

$$(17)\qquad e = \begin{cases} 2 & \text{si } \big(p, v_5(d)\big) = (7,3) \text{ ou } (11,4), \\ 2p & \text{sinon.} \end{cases}$$

2. Si 5 ne divise pas $a+b$, on a $e=4$.

DÉMONSTRATION: Si 5 divise $a+b$, la courbe E a potentiellement réduction multiplicative en 5, autrement dit, E a réduction additive en 5 et son invariant modulaire n'est pas entier en 5 (Lemme 2.8). L'égalité (17) résulte alors du Lemme 2.8 et de [2, p. 7].

Si 5 ne divise pas $a+b$, l'invariant modulaire j de E est entier en 5 (Lemme 2.8). La courbe E a donc potentiellement bonne réduction en 5. La valuation en 5 de son discriminant minimal vaut 3 (voir Section 2.3). Le défaut de semi-stabilité en 5 de E (qui est mesuré par l'ordre d'un certain groupe fini Φ_5) est donc d'ordre 4 ([18, p. 312]), d'où le résultat.

4.1. DÉMONSTRATION DU THÉORÈME 1.1. On suppose ici que l'on a $d=1$ et que c est pair. L'entier a est impair. D'après l'étude faite dans la partie 3, la représentation ρ_p^E est irréductible de poids 2 et de conducteur 50. Or une base du $\mathbb{C}$-espace vectoriel

$\mathcal{S}_2^+(50)$ correspond aux deux courbes elliptiques sur $\mathbb{Q}$ de conducteur 50 notées 50A1 et 50B1 dans [3] et d'équations respectives:

$$50\text{A1} : y^2 + xy + y = x^3 - x - 2,$$
$$50\text{B1} : y^2 + xy + y = x^3 + x^2 - 3x + 1.$$

On va alors contredire les congruences (15) avec le nombre premier $\ell = 3$. On remarque pour cela que l'on a

$$\begin{cases} a_3(50\text{A1}) & = +1, \\ a_3(50\text{B1}) & = -1. \end{cases}$$

Par ailleurs, la courbe elliptique E a réduction semi-stable en 3 (Lemme 2.7). Supposons que E ait réduction multiplicative en 3. Puisque 3 divise N_E, mais pas $50p = pN(\rho_p^E)$, on déduit des congruences (15) que l'on a

$$\pm 1 \equiv \pm 4 \pmod{p},$$

ce qui conduit à une contradiction car $p \geqslant 7$. La courbe E a donc bonne réduction en 3. Puisque E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, $a_3(E)$ est pair et l'inégalité $|a_3(E)| < 2\sqrt{3}$ ([**20**, Théorème 1.1, p.131]) entraîne $a_3(E) = 0$ ou ± 2. D'après les congruences (15), on a donc

$$\pm 1 \equiv a_3(E) \pmod{p},$$

ce qui conduit de nouveau à une contradiction. Cela termine la démonstration du Théorème 1.1.

4.2. Démonstration du Théorème 1.2. On a $r' = 1$. On distingue deux cas suivant la valeur de $v_2(d)$.

1. Supposons $v_2(d) = 2$. D'après la proposition 3.4, on a $N(\rho_p^E) = 25$. Or l'espace $\mathcal{S}_2^+(25)$ est réduit à 0. D'où le théorème dans ce cas.
2. Supposons $v_2(d) = 3$ ou 4. Dans ce cas, on a $N(\rho_p^E) = 50$, ce qui entraîne, par le même argument que celui utilisé dans le Section 4.1, le résultat.

4.3. Démonstration du Théorème 1.3. Supposons que l'on soit dans le cas où les coefficients $a_n(f)$ sont dans $\mathbb{Z}$. Les congruences (16) sont réalisées. On utilise ici la méthode symplectique reposant sur le lemme suivant ([**8**, p. 180]). Notons $\Delta_m(A)$ le discriminant minimal de A.

Lemme 4.2. *Soient ℓ_1 et ℓ_2 deux nombres premiers distincts, autres que p. Supposons que E et A aient réduction de type multiplicatif en ℓ_i et que p ne divise pas $v_{\ell_i}(\Delta_m)$, auquel cas p ne divise pas non plus $v_{\ell_i}(\Delta_m(A))$ $(i = 1, 2)$. Alors, les classes modulo p de $v_{\ell_1}(\Delta_m)v_{\ell_2}(\Delta_m)$ et $v_{\ell_1}(\Delta_m(A))v_{\ell_2}(\Delta_m(A))$ diffèrent multiplicativement par un carré de $\mathbb{F}_p$.*

On suppose ici que d s'écrit

$$d = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}, \quad \text{avec } \alpha = 3 \text{ ou } 4 \quad \text{et} \quad 1 \leqslant \beta \leqslant 4,\ 0 \leqslant \gamma \leqslant 4.$$

D'après la proposition 3.4, on a alors:

$$N(\rho_p^E) = 150.$$

Une base de $\mathcal{S}_2^+(150)$ correspond aux trois classes d'isogénie de courbes elliptiques sur $\mathbb{Q}$ de conducteur 150. Ainsi ρ_p^E est isomorphe à la représentation de $G_{\mathbb{Q}}$ dans les points de p-torsion de l'une des courbes notées 150A1, 150B1 et 150C1 dans les tables de [3]. Par ailleurs, E a réduction multiplicative en 2 et 3 (Lemmes 2.7 et 2.10) et d'après le Lemme 3.5, on a donc:

$$v_2(\Delta_m) \equiv \begin{cases} 4 \pmod{p} & \text{si } \alpha = 3 \\ 8 \pmod{p} & \text{si } \alpha = 4. \end{cases} \tag{18}$$

D'après le Lemme 2.6, 3 divise $a+b$ et d'après le Lemme 2.7, on a donc:

$$v_3(\Delta_m) \equiv 4\beta \pmod{p}. \tag{19}$$

Les entiers $v_2(\Delta_m)$ et $v_3(\Delta_m)$ ne sont pas divisibles par p.

On distingue alors deux cas suivant la valeur de l'entier α.

4.3.1. Supposons $\alpha = 3$. On distingue deux cas selon que 5 divise on non $a+b$.

1. Supposons que 5 divise $a+b$. Démontrons que l'on a les assertions suivantes:

$$\begin{cases} 3 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4, \\ 6 \pmod{p} \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 2. \end{cases} \tag{20}$$

D'après le Lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est 2 ou $2p$. Or les courbes notées 150A1 et 150B1 dans [3] ont réduction additive en 5 et leurs invariants modulaires sont entiers en 5. Les valuations de leurs discriminants minimaux en 5 sont respectivement 3 et 9. L'indice de ramification en 5 des extensions de $\mathbb{Q}$ engendrées par leurs points de p-torsion vaut donc 4 ([18, p. 312]). Puisque l'on a $p \neq 2$, cela entraîne que ρ_p^E est isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [3]. On applique alors le résultat du Lemme 4.2 avec les courbes E et A, et les nombres premiers $\ell_1 = 2$, $\ell_2 = 3$. On a $v_2\big(\Delta_m(A)\big) = 4$ et $v_3\big(\Delta_m(A)\big) = 3$. D'après (18) et (19), on obtient ainsi:

$$3 \pmod{p} \equiv \beta \pmod{p} \pmod{(\mathbb{F}_p^*)^2},$$

d'où les assertions (20).

2. Supposons que 5 ne divise pas $a+b$. Dans ce cas, vérifions que l'on a:

$$\begin{cases} 2 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 6 \pmod p \in (\mathbf{F}_p^*)^2 & \text{si } \beta = 3. \end{cases} \tag{21}$$

L'invariant modulaire de E est entier en 5. D'après le Lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}(E[p])/\mathbb{Q}$ est 4. Or la courbe elliptique notée 150C1 a un invariant modulaire non entier en 5. Comme ci-dessus, on en déduit que ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [3]. On a $v_2\big(\Delta_m(A)\big) = 2$ et $v_3\big(\Delta_m(A)\big) = 1$. D'après le Lemme 4.2 et les congruences (18) et (19), on obtient:

$$2 \pmod p \equiv \beta \pmod p \pmod{(\mathbf{F}_p^*)^2},$$

d'où les assertions (21).

Démontrons le Théorème 1.3 si $\alpha = 3$. Supposons $\gamma \geqslant 1$. Dans ce cas, d'après le Lemme 2.6, 5 divise $a+b$. Par hypothèse, on a $\beta \in \{1, 2, 4\}$. Par ailleurs, on a les équivalences:

$$3 \pmod p \notin (\mathbf{F}_p^*)^2 \Longleftrightarrow p \equiv 5 \text{ ou } 7 \pmod{12}, \tag{22}$$

et

$$6 \pmod p \notin (\mathbf{F}_p^*)^2 \Longleftrightarrow p \equiv 7, 11, 13 \text{ ou } 17 \pmod{24}, \tag{23}$$

d'où le résultat dans ce cas.

Supposons $\gamma = 0$, c'est-à-dire, 5 ne divise pas d. On a alors $\beta = 1$ ou 4. Et, d'après ce qui précède, 2 (mod p) ou 3 (mod p) appartient à $(\mathbf{F}_p^*)^2$ suivant que 5 divise ou non $a+b$.

De l'équivalence

$$2 \pmod p \notin (\mathbf{F}_p^*)^2 \Longleftrightarrow p \equiv 3 \text{ ou } 5 \pmod 8, \tag{24}$$

on déduit:

$$3 \pmod p \notin (\mathbf{F}_p^*)^2 \text{ et } 2 \pmod p \notin (\mathbf{F}_p^*)^2 \Longleftrightarrow p \equiv 5 \text{ ou } 19 \pmod{24}. \tag{25}$$

Compte tenu des deux alinéas précédents, cela prouve le Théorème 1.3 si $\alpha = 3$.

4.3.2. SUPPOSONS $\alpha = 4$. La démarche est identique à celle du paragraphe précédent: seules les congruences obtenues diffèrent. On explicitera donc les calculs sans répéter exhaustivement les raisonnements.

1. Supposons que 5 divise $a+b$. La représentation ρ_p^E est alors isomorphe à ρ_p^A, où A est la courbe elliptique notée 150C1 dans [3]. On déduit du Lemme 4.2 les congruences:

$$3 \pmod p \equiv 2\beta \pmod p \pmod{(\mathbf{F}_p^*)^2}.$$

Autrement dit, on a:

$$\begin{cases} 6 \pmod p \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 1 \text{ ou } 4 \\ 3 \pmod p \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 2 \\ 2 \pmod p \in (\mathbb{F}_p^*)^2 & \text{si } \beta = 3. \end{cases}$$

2. Supposons que 5 ne divise pas $a+b$. On sait qu'alors ρ_p^E est isomorphe à ρ_p^A, où A est l'une des courbes elliptiques notées 150A1 et 150B1 dans [3]. On obtient dans ce cas:

$$\beta \pmod p \in (\mathbb{F}_p^*)^2.$$

Démontrons alors le Théorème 1.3 si $\alpha = 4$.

Supposons $\gamma = 0$, c'est-à-dire, 5 ne divise pas d. Alors par hypothèse $\beta = 2$ ou 3. D'après les alinéas ci-dessus, 2 (mod p) ou 3 (mod p) appartient à $(\mathbb{F}_p^*)^2$. D'où le résultat dans ce cas, d'après la congruence (25).

Supposons $\gamma \geqslant 1$. Alors 5 divise $a+b$ et $\beta \in \{1,2,3,4\}$. Si $\beta = 1$ ou 4, on a le résultat avec la congruence (23). Les cas où $\beta = 2$ et $\beta = 3$ se déduisent respectivement des congruences (22) et (24).

Ceci achève la démonstration du Théorème 1.3.

4.4. Démonstration du Théorème 1.4. On rappelle que p est un nombre premier $\geqslant 7$, (a,b,c) un élément de $S_p(3)$ et E la courbe d'équation (6) attachée à (a,b,c).

D'après la proposition 3.3, on a:

$$N(\rho_p^E) = \begin{cases} 150 & \text{si } a \text{ est impair;} \\ 600 & \text{si } v_2(a) \geqslant 2; \\ 1200 & \text{si } v_2(a) = 1. \end{cases}$$

Les newforms appartenant aux espaces $\mathcal{S}_2^+(150)$, $\mathcal{S}_2^+(600)$ et $\mathcal{S}_2^+(1200)$ sont toutes à coefficients entiers relatifs. Elles correspondent donc à des courbes elliptiques. Il y a en trois de conducteur 150, neuf de conducteur 600 et dix-neuf de conducteur 1200, soit trente-et-une courbes au total. Par commodité pour le lecteur, on donne en Appendice la liste des équations de ces courbes elliptiques ainsi que la valeur des invariants dont on aura besoin.

On considère les deux ensembles de courbes elliptiques suivants, avec les notations des tables de [3]:

$$\begin{aligned} \mathcal{F}_1 &= \{150\text{C1}, 600\text{A1}, 600\text{F1}, 1200\text{E1}, 1200\text{G1}, 1200\text{J1}, 1200\text{P1}\}; \\ \mathcal{F}_2 &= \{150\text{A1}, 150\text{B1}, 600\text{C1}, 600\text{H1}, 1200\text{B1}, 1200\text{I1}, 1200\text{M1} \\ &\qquad 1200\text{N1}, 1200\text{Q1}, 1200\text{S1}\}. \end{aligned}$$

Le lemme suivant décrit les isomorphismes possibles entre ρ_p^E et les représentations ρ_p^A où A est l'une des trente-et-une courbes elliptiques de conducteur 150, 600 et 1200.

LEMME 4.3.

1. *Si 5 divise $a+b$, alors il existe A dans $\mathcal{F}_1$ tel que ρ_p^E soit isomorphe à ρ_p^A;*
2. *Si 5 ne divise pas $a+b$, alors il existe A dans $\mathcal{F}_2$ tel que ρ_p^E soit isomorphe à ρ_p^A.*

DÉMONSTRATION: La représentation ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique A de conducteur 150, 600 ou 1200. Définissons l'ensemble suivant:

$$\begin{aligned}\mathcal{G} = \{&150A1, 150B1, 600B1, 600C1, 600D1, 600E1, 600G1, 600H1, 600I1,\\ &1200A1, 1200B1, 1200C1, 1200D1, 1200F1, 1200H1, 1200I1, 1200K1,\\ &1200L1, 1200M1, 1200N1, 1200O1, 1200Q1, 1200R1, 1200S1\}.\end{aligned}$$

D'après le tableau 2 de l'Appendice, l'ensemble $\mathcal{G}$ (respectivement $\mathcal{F}_1$) correspond précisément aux courbes de conducteur 150, 600 et 1200 ayant un invariant modulaire j entier en 5 (respectivement non entier en 5).

On rappelle que la courbe E a réduction additive en 5 (Lemme 2.8).

1. Supposons tout d'abord que 5 divise $a+b$. D'après le Lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}\big(E[p]\big)/\mathbb{Q}$ est $2p$ (car $v_5(d) \neq 3, 4$). Or les courbes de l'ensemble $\mathcal{G}$ ont toutes réduction additive en 5 et leur invariant modulaire est entier en 5. Leur défaut de semi-stabilité en 5 est alors d'ordre 2, 3, 4 ou 6 (voir le tableau 2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune des courbes de l'ensemble $\mathcal{G}$. Autrement dit, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_1$.

2. Supposons que 5 ne divise pas $a+b$. L'invariant modulaire de E est entier en 5 (Lemme 2.8). D'après le Lemme 4.1, l'indice de ramification en 5 de l'extension $\mathbb{Q}\big(E[p]\big)/\mathbb{Q}$ est 4. Or les courbes A de l'ensemble $\mathcal{F}_1$ ont toutes réduction additive en 5 et leur invariant modulaire n'est pas entier en 5. L'indice de ramification en 5 de l'extension $\mathbb{Q}(A[p])/\mathbb{Q}$ est alors $2p$ (voir tableau 2). En particulier, ρ_p^E n'est isomorphe à la représentation modulo p d'aucune de ces courbes.

Par ailleurs, parmi les courbes de l'ensemble $\mathcal{G}$, seules celles de l'ensemble $\mathcal{F}_2$ ont un défaut de semi-stabilité en 5 d'ordre 4. On en déduit que dans ce cas, ρ_p^E est isomorphe à ρ_p^A où A est une courbe de l'ensemble $\mathcal{F}_2$.

Ceci achève la démonstration du Lemme 4.3.

REMARQUE. Parmi les courbes des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$ du début du paragraphe, les courbes suivantes ont le même invariant modulaire j:

- 150C1 et 1200P1,
- 600A1 et 1200E1,
- 600F1 et 1200G1,
- 150A1, 150B1, 1200M1 et 1200Q1,
- 600C1, 600H1, 1200B1 et 1200I1,
- 600D1 et 1200A1,
- 1200N1 et 1200S1.

Leur invariant modulaire étant différent de 0 et de 1728, elles sont donc isomorphes sur une extension quadratique de $\mathbb{Q}$. L'ensemble $\mathcal{E}_1$ (respectivement $\mathcal{E}_2$) du Théorème 1.4 est un ensemble de représentants des classes d'isomorphisme des courbes de l'ensemble $\mathcal{F}_1$ (respectivement $\mathcal{F}_2$).

En particulier, pour toute courbe A de l'ensemble $\mathcal{F}_1$ (respectivement $\mathcal{F}_2$), il existe une unique courbe F de l'ensemble $\mathcal{E}_1$ (respectivement $\mathcal{E}_2$) de même invariant modulaire que A. On a alors pour tout nombre premier ℓ:

$$a_\ell(A)^2 = a_\ell(F)^2. \tag{26}$$

Montrons à présent le Théorème 1.4. D'après le Lemme 4.3, ρ_p^E est isomorphe à ρ_p^A où A est une courbe des ensembles $\mathcal{F}_1$ et $\mathcal{F}_2$. On note F l'unique courbe elliptique des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$ de même invariant modulaire que A. Soit alors n un entier $\geqslant 2$ tel que le couple (F, n) vérifie la condition 1 du Théorème 1.4 si A appartient à $\mathcal{F}_1$ et la condition 2 si A appartient à $\mathcal{F}_2$. On a le résultat suivant.

LEMME 4.4. *La courbe E a bonne réduction en q. Autrement dit, q ne divise pas c.*

DÉMONSTRATION: Supposons que ce ne soit pas le cas. Dans ce cas, q divise c et d'après le Lemme 2.7, la courbe E a réduction multiplicative en q. Comme A a bonne réduction en q, il vient d'après [**14**, Proposition 3(iii)]:

$$a_q(A) \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

Or, d'après (26), on a $a_q(A)^2 = a_q(F)^2$. C'est en contradiction avec les hypothèses du thèorème. D'où le lemme.

Désignons par $\overline{a}$ et $\overline{b}$ les réductions de a et b modulo q. On distingue à présent deux cas.

1. Supposons que 5 divise $a+b$, c'est-à-dire, $F \in \mathcal{E}_1$. D'après les Lemmes 2.5 et 2.6, il existe c_1 et c_2 deux entiers tels que:

$$5(a+b) = 3c_1^p, \quad \phi(a,b) = 5c_2^p \quad \text{et} \quad c = c_1c_2.$$

De plus d'après le Lemme 4.4, q ne divise pas c, ainsi

$$u = c_1^p \pmod{q} \in \mu_n(\mathbb{F}_q) \quad \text{et} \quad v = c_2^p \pmod{q} \in \mu_n(\mathbb{F}_q).$$

On a alors:

$$5(\overline{a}+\overline{b}) = 3u \quad \text{et} \quad \phi(\overline{a},\overline{b}) = 5v.$$

En posant

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^4},$$

on obtient:

$$5(\overline{a}' + \overline{b}') = 3 \quad \text{et} \quad \phi(\overline{a}', \overline{b}') = 5\zeta. \tag{27}$$

On en déduit que $\overline{b}'$ est racine du polynôme

$$P_{1,\zeta}(X) = X^4 - \frac{6}{5}X^3 + \frac{18}{25}X^2 - \frac{27}{125}X + \frac{81}{3125} - \zeta \in \mathbb{F}_q[X].$$

Avec les notations de la partie 1, l'égalité $P_{1,\zeta}(\overline{b}') = 0$ entraîne alors

$$\zeta \in \widetilde{A}(n, q).$$

Choisissons $\alpha_{1,\zeta}$ une racine carrée de $-225+10\delta_{1,\zeta}$ et $\beta_{1,\zeta}$ une racine carrée de $-225-10\delta_{1,\zeta}$ dans une clôture algébrique $\overline{\mathbb{F}_q}$ de $\mathbb{F}_q$. Les racines de $P_{1,\zeta}$ dans $\overline{\mathbb{F}_q}$ sont:

$$\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{1,\zeta}$ ou $\beta_{1,\zeta}$ est dans $\mathbb{F}_q$ et que $\zeta \in A(n, q)$. Par ailleurs, on a (formule (27))

$$\overline{a}' = \frac{3}{5} - \overline{b}'.$$

D'où:

$$\{\overline{a}', \overline{b}'\} = \left\{\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}\right\} \quad \text{ou} \quad \{\overline{a}', \overline{b}'\} = \left\{\frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}\right\}.$$

On a donc respectivement

$$\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{1,\zeta}}{125} \quad \text{ou} \quad \overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{1,\zeta}}{125}.$$

Explicitons à présent l'équation de la courbe sur $\mathbb{F}_q$ déduite de (6) par réduction modulo q. Compte tenu de ce qui précède, il s'agit de l'équation

$$y^2 = x^3 - 5u^2(\overline{a}'^2 + \overline{b}'^2)x^2 + 5u^4\phi(\overline{a}', \overline{b}')x$$

qui est isomorphe sur $\mathbb{F}_q$ à la courbe d'équation

$$y^2 = x^3 - 5(\overline{a}'^2 + \overline{b}'^2)x^2 + 5\phi(\overline{a}', \overline{b}')x. \tag{28}$$

Si $\overline{a}'^2 + \overline{b}'^2 = -(\delta_{1,\zeta})/125$, il s'agit de la courbe la courbe $F_{1,\zeta}$ d'équation

$$y^2 = x^3 + \frac{\delta_1, \zeta}{25}x^2 + 25\zeta x. \tag{29}$$

Si $\overline{a}'^2 + \overline{b}'^2 = (\delta_{1,\zeta})/125$, il s'agit de la tordue quadratique de $F_{1,\zeta}$ par $\sqrt{-1}$, notée $F'_{1,\zeta}$. Elle a pour équation

$$y^2 = x^3 - \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x. \tag{30}$$

Posons alors

$$a'_q(\zeta) = q + 1 - n'_{1,q}(\zeta) \tag{31}$$

où $n'_{1,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F'_{1,\zeta}$. On a

$$a'_q(\zeta) = \pm a_q(\zeta).$$

Il en résulte l'égalité

$$a_q(E)^2 = a_q(\zeta)^2. \tag{32}$$

D'après la congruence (16) et l'égalité (26), on en déduit que:

$$a_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p}.$$

C'est en contradiction avec la condition $1(c)$ du Théorème 1.4.

2. Supposons que 5 ne divise pas $a+b$. Comme ci-dessus, il existe alors c_1 et c_2 deux entiers tels que:

$$a + b = 3c_1^p, \quad \phi(a,b) = c_2^p \quad \text{et} \quad c = c_1 c_2.$$

D'après le Lemme 4.4, q ne divise pas c, ainsi:

$$u = c_1^p \pmod{q} \in \mu_n(\mathbb{F}_q) \quad \text{et} \quad v = c_2^p \pmod{q} \in \mu_n(\mathbb{F}_q).$$

On a alors:

$$\overline{a} + \overline{b} = 3u \quad \text{et} \quad \phi(\overline{a}, \overline{b}) = v.$$

En posant

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{et} \quad \zeta = \frac{v}{u^4},$$

on obtient:

$$\overline{a}' + \overline{b}' = 3 \quad \text{et} \quad \phi(\overline{a}', \overline{b}') = \zeta. \tag{33}$$

On en déduit que $\overline{b}'$ est racine du polynôme

$$P_{2,\zeta}(X) = X^4 - 6X^3 + 18X^2 - 27X + \frac{81 - \zeta}{5} \in \mathbb{F}_q[X].$$

Avec les notations de la partie 1, l'égalité $P_{2,\zeta}(\overline{b}') = 0$ entraîne alors

$$\zeta \in \widetilde{B}(n,q).$$

Choisissons $\alpha_{2,\zeta}$ une racine carrée de $-225+10\delta_{2,\zeta}$ et $\beta_{2,\zeta}$ une racine carrée de $-225-10\delta_{2,\zeta}$ dans $\overline{\mathbb{F}_q}$. Les racines de $P_{2,\zeta}$ dans $\overline{\mathbb{F}_q}$ sont alors:

$$\frac{3}{2} + \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} + \frac{\beta_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\beta_{2,\zeta}}{10}.$$

Il en résulte que $\overline{b}'$ est l'un de ces éléments. On en déduit que $\alpha_{2,\zeta}$ ou $\beta_{2,\zeta}$ est dans $\mathbb{F}_q$ et que $\zeta \in B(n,q)$. Par ailleurs, on a (formule (33))

$$\overline{a}' = 3 - \overline{b}'.$$

D'où:

$$\{\overline{a}', \overline{b}'\} = \left\{\frac{3}{2} + \frac{\alpha_{2,\zeta}}{10}, \frac{3}{2} - \frac{\alpha_{2,\zeta}}{10}\right\} \quad \text{ou} \quad \{\overline{a}', \overline{b}'\} = \left\{\frac{3}{2} + \frac{\beta_{2,\zeta}}{10}, \frac{3}{2} - \frac{\beta_{2,\zeta}}{10}\right\}.$$

On a donc respectivement

$$\overline{a}'^2 + \overline{b}'^2 = \frac{\delta_{2,\zeta}}{5} \quad \text{ou} \quad \overline{a}'^2 + \overline{b}'^2 = -\frac{\delta_{2,\zeta}}{5}.$$

Explicitons à présent l'équation de la courbe sur $\mathbb{F}_q$ déduite de (6) par réduction modulo q. Il s'agit de l'équation

$$y^2 = x^3 - 5u^2(\overline{a}'^2 + \overline{b}'^2)x^2 + 5u^4\phi(\overline{a}', \overline{b}')x$$

qui est isomorphe sur $\mathbb{F}_q$ à la courbe d'équation

$$y^2 = x^3 - 5(\overline{a}'^2 + \overline{b}'^2)x^2 + 5\phi(\overline{a}', \overline{b}')x.$$

Si $\overline{a}'^2 + \overline{b}'^2 = -(\delta_{2,\zeta})/5$, il s'agit de la courbe $F_{2,\zeta}$ d'équation

$$y^2 = x^3 + \delta_{2,\zeta}x^2 + 5\zeta x. \tag{34}$$

Si $\overline{a}'^2 + \overline{b}'^2 = (\delta_{2,\zeta})/5$, il s'agit de la tordue quadratique de $F_{2,\zeta}$ par $\sqrt{-1}$, notée $F'_{2,\zeta}$. Elle a pour équation

$$y^2 = x^3 - \delta_{2,\zeta}x^2 + 5\zeta x. \tag{35}$$

Posons alors comme ci-dessus

$$b'_q(\zeta) = q + 1 - n'_{2,q}(\zeta) \tag{36}$$

où $n'_{2,q}(\zeta)$ le nombre de points rationnels sur $\mathbb{F}_q$ de $F'_{2,\zeta}$. On a, à nouveau

$$b'_q(\zeta) = \pm b_q(\zeta),$$

puis

$$a_q(E)^2 = b_q(\zeta)^2. \tag{37}$$

D'après la congruence (16) et l'égalité (26), on en déduit que:

$$b_q(\zeta)^2 \equiv a_q(F)^2 \pmod{p},$$

ce qui contredit la condition 2(c) du Théorème 1.4.

On aboutit ainsi à une contradiction à l'existence de $(a,b,c) \in S_p(3)$. Par suite, $S_p(3)$ est vide. Cela termine la démonstration du Théorème 1.4.

4.5. DÉMONSTRATION DE LA PROPOSITION 1.1. Il s'agit de montrer que l'équation $x^5 + y^5 = 3z^p$ n'admet pas de solution propre et non triviale pour $5 \leqslant p \leqslant 10^6$. C'est connu pour $p = 5$ (voir [6]).

L'équation $x^5 + y^5 = 3z^7$. On suppose que l'on a $p = 7$. Pour toute courbe elliptique A de $\mathcal{F}_1$ et $\mathcal{F}_2$, il s'agit de montrer que ρ_7^E n'est pas isomorphe à ρ_7^A (Lemme 4.3). Pour certaines de ces courbes A, on utilise pour cela la remarque suivante qui est une conséquance directe de la démonstration du Théorème 1.4.

REMARQUE. Soit A l'une des courbes elliptiques de $\mathcal{F}_1$ (respectivement de $\mathcal{F}_2$). Soit F l'unique courbe de $\mathcal{E}_1$ (respectivement de $\mathcal{E}_2$) ayant le même invariant modulaire que A. Si l'on démontre l'existence d'un entier $n \geqslant 2$ pour lequel la condition 1 (respectivement la condition 2) du Théorème 1.4 est satisfaite, alors les représentations ρ_7^E et ρ_7^A ne sont pas isomorphes.

En utilisant cette remarque, on parvient à éliminer directement les courbes suivantes:

$$150A1, 150B1, 150C1, 600A1, 600F1, 1200E1,$$
$$1200G1, 1200P1, 1200M1, 1200N1, 1200Q1, 1200S1.$$

En effet, si $A \in \{150C1, 1200P1\}$, le couple $(F, n) = (150C1, 16)$ vérifie la condition 1 du Théorème 1.4. On en déduit, comme au paragraphe précédent, que ρ_7^E et ρ_7^A ne sont pas isomorphes. De même:

1. si $A \in \{600A1, 1200E1\}$, le couple $(F, n) = (600A1, 16)$ vérifie la condition 1 du théorème.
2. Si $A \in \{600F1, 1200G1\}$, le couple $(F, n) = (600F1, 16)$ vérifie la condition 1 du théorème.
3. Si $A \in \{150A1, 150B1, 1200M1, 1200Q1\}$, le couple $(F, n) = (150A1, 4)$ vérifie la condition 2 du théorème.
4. Si $A \in \{1200N1, 1200S1\}$, le couple $(F, n) = (1200N1, 6)$ vérifie la condition 2 du théorème.

Il reste à montrer que ρ_7^E n'est pas isomorphe à ρ_7^A où A est l'une des courbes

$$1200J1,\ 600C1,\ 600H1,\ 1200B1 \text{ et } 1200I1.$$

Supposons que ρ_7^E soit isomorphe à ρ_7^A où $A = 1200J1$. D'après le Lemme 4.4, E a bonne réduction en $q = 43$ car

$$a_q(1200J1) = 4 \not\equiv \pm 2 \pmod 7. \tag{38}$$

De plus, d'après le Lemme 4.3, 5 divise $a + b$. Déterminons les équations possibles de la courbe de Frey réduite modulo 43. On a

$$\mu_6(\mathbb{F}_{43}) = \{1 \pmod{43}, 6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43},$$
$$37 \pmod{43}, 42 \pmod{43}\},$$

puis

$$\widetilde{A}(6,43) = \{6 \pmod{43}, 7 \pmod{43}, 36 \pmod{43}, 37 \pmod{43}, 42 \pmod{43}\}$$

et

$$A(6,43) = \{6 \pmod{43}, 7 \pmod{43}\}.$$

Avec les notations du paragraphe précédent, on a donc $\zeta = 6 \pmod{43}$ ou $\zeta = 7 \pmod{43}$.

Supposons que $\zeta = 6 \pmod{43}$. Alors, toujours avec les notations du paragraphe précédent, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,6}(X) &= X^4 + 16X^3 - X^2 - 4X + 22 \\ &= (X+2)(X+6)(X^2+8X+9) \in \mathbb{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = -2 \pmod{43}$ ou $-6 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (37 \pmod{43}, -2 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (41 \pmod{43}, -6 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbb{F}_{43}$ à la courbe $F'_{1,6}$ d'équation (voir (28) et (30))

$$y^2 = x^3 - 28x^2 + 21x. \tag{39}$$

Supposons que $\zeta = 7 \pmod{43}$. Alors, on a que $\overline{b}'$ est racine du polynôme

$$\begin{aligned} P_{1,7}(X) &= X^4 + 16X^3 - X^2 - 4X + 21 \\ &= (X+23)(X+28)(X^2+8X+22) \in \mathbb{F}_{43}[X]. \end{aligned}$$

D'où $\overline{b}' = 20 \pmod{43}$ ou $15 \pmod{43}$ et

$$(\overline{a}', \overline{b}') = (15 \pmod{43}, 20 \pmod{43})$$

ou

$$(\overline{a}', \overline{b}') = (20 \pmod{43}, 15 \pmod{43}).$$

La courbe de Frey réduite modulo 43 est alors isomorphe sur $\mathbb{F}_{43}$ à la courbe $F_{1,7}$ d'équation (voir (28) et (29))

$$y^2 = x^3 + 14x^2 + 3x. \tag{40}$$

Il en résulte que (39) et (40) sont les deux seules équations possibles pour la réduite de la courbe de Frey modulo 43. En particulier, on a $a_q(E) = a'_q(6) = -8$ ou $a_q(E) = a_q(7) = 10$ (voir (3) et (31)). D'après l'égalité (38) ci-dessus et la congruence (16), on a donc:

$$4 \equiv -8 \pmod{7} \quad \text{ou} \quad 4 \equiv 10 \pmod{7}.$$

On en déduit une contradiction. Les représentations ρ_7^E et ρ_7^A où $A = 1200J1$ ne sont donc pas isomorphes.

On procède de même pour éliminer les isomorphismes entre ρ_7^E et ρ_7^A où $A = 600C1, 1200B1$ et $1200I1$. On explicite donc certains calculs sans répéter exhaustivement les raisonnements.

Supposons que ρ_7^E soit isomorphe à ρ_7^A où A est la courbe 1200B1 ou la courbe 1200I1. Posons $n = 10$ et $q = 71$. On a

$$a_{71}(1200B1) = a_{71}(1200I1) = 4.$$

Donc, d'après le Lemme 4.4, la courbe E a bonne réduction en q. On vérifie qu'il y a quatre équations possibles pour la réduite de E modulo 71. Il s'agit des courbes suivantes (voir (5) et (36) et les équations (34) et (35)):

$$\begin{aligned}
F'_{2,5} &: y^2 = x^3 - 24x^2 + 25x \quad \text{et } b'_{71}(5) = 0,\\
F_{2,5} &: y^2 = x^3 + 24x^2 + 25x \quad \text{et } b_{71}(5) = 0,\\
F'_{2,57} &: y^2 = x^3 - 14x^2 + x \quad \text{et } b'_{71}(57) = -8,\\
F'_{2,70} &: y^2 = x^3 - 32x^2 + 66x \quad \text{et } b'_{71}(70) = -4.
\end{aligned}$$

Par ailleurs, on a les congruences

$$a_{71}(E) \equiv b'_{71}(5),\ b_{71}(5),\ b'_{71}(57) \text{ ou } b'_{71}(70) \pmod 7.$$

D'où il résulte

$$4 \equiv 0,\ 3 \text{ ou } 6 \pmod 7.$$

On en déduit une contradiction: les représentations ρ_7^E et ρ_7^A où $A = 1200B1$ ou $1200I1$ ne sont pas isomorphes.

De même, les représentations ρ_7^E et ρ_7^A, où A est la courbe 600C1, ne sont pas isomorphes. D'après le Lemme 4.4, la courbe E a bonne réduction en $q = 197$ car $a_{197}(600C1) = 6$. Comme par ailleurs 5 ne divise pas $a+b$, on a onze équations possibles pour la courbe E réduite modulo 197 (voir équations (34) et (35)). De plus,

$$\begin{aligned}
&b_{197}(104) = 4, \quad b'_{197}(113) = 14, \quad b_{197}(113) = 14, \quad b'_{197}(120) = 10,\\
&b_{197}(120) = 10, \quad b'_{197}(178) = -12, \quad b_{197}(196) = 8, \quad b'_{197}(77) = -18,\\
&b_{197}(77) = -18, \quad b'_{197}(87) = 2, \quad b'_{197}(87) = 2.
\end{aligned}$$

On conclut comme ci-dessus que les représentations ρ_7^E et ρ_7^A, où $A = 600C1$ ne sont pas isomorphes.

En revanche, pour la courbe $A = 600H1$ il n'existe aucun entier n tel que $6 < n < 1000$ pour lequel la méthode ci-dessus s'applique. Elle s'applique cependant

avec $n = 6$, pourvu que l'on sache montrer que E a bonne réduction en $q = 43$, ce que le Lemme 4.3 ne nous permet pas d'affirmer car

$$a_{43}(600\text{H}1) = -12 \equiv 2 \pmod 7.$$

Pour montrer que E a bonne réduction en 43, on utilise alors le résultat suivant.

Lemme 4.5. *Soient q un nombre premier et A une courbe elliptique sur $\mathbb{Q}$ ayant bonne réduction en q. Supposons que ρ_7^E soit isomorphe à ρ_7^A et que q vérifie les deux conditions suivantes:*

1. *on a $q \equiv 1 \pmod 7$ et $q \not\equiv 1 \pmod 5$.*
2. *On a*
$$a_q(A) \not\equiv 2\left(\frac{5}{q}\right) \pmod 7,$$
où $(5/q)$ est le symbole de Legendre.

Alors, E a bonne réduction en q.

Démonstration: Supposons que E ait mauvaise réduction en q. Puisque l'on a $q \neq 2$, 5, la courbe E a réduction de type multiplicatif en q (Lemme 2.7). On a donc:

$$a_q(E) = \left(\frac{-c_6}{q}\right).$$

L'hypothèse $q \not\equiv 1 \pmod 5$ entraîne que q divise $a + b$ (Lemme 2.6). Par suite, on a:

$$-c_6 = 2^6 \cdot 5^3 a^6 \pmod q,$$

d'où l'on déduit que l'on a

$$\left(\frac{-c_6}{q}\right) = \left(\frac{5}{q}\right).$$

Les représentations ρ_7^E et ρ_7^A étant isomorphes et A ayant bonne réduction en q, on a ([**14**, Proposition 3(iii)]):

$$a_q(E)a_q(A) \equiv q + 1 \pmod 7,$$

et compte tenu de la congruence $q \equiv 1 \pmod 7$, on obtient

$$a_q(E)a_q(A) \equiv 2 \pmod 7.$$

On a donc

$$a_q(A) \equiv 2\left(\frac{5}{q}\right) \pmod 7,$$

ce qui contredit la condition 2. D'où le lemme.

Déduisons-en que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes. Supposons le contraire. La courbe E a bonne réduction en $q = 43$. En effet, on a

$$a_{43}(A) = -12 \equiv 2 \pmod 7. \tag{41}$$

Puisque $(5/43) = -1$, on a

$$2 \equiv a_{43}(A) \not\equiv 2\left(\frac{5}{43}\right) \pmod 7,$$

d'où l'assertion d'après le Lemme 4.5.

Par ailleurs, avec les notations de la partie 1, on a $B(6,43) = \{42 \pmod{43}\}$ et l'on vérifie que l'on a une seule courbe possible pour la réduction de E modulo 43. Elle a pour équation (voir (35)):

$$F'_{2,42} : y^2 = x^3 - 16x^2 + 38x.$$

On en déduit avec les formules (16), (36) et (41) que l'on a

$$2 \equiv a_{43}(A) \equiv b'_{43}(42) \equiv -1 \pmod 7.$$

On obtient ainsi une contradiction et le fait que ρ_7^E et ρ_7^A, pour $A = 600\text{H}1$, ne sont pas isomorphes.

REMARQUE. La même démonstration (appliquée à nouveau à $q = 43$) permettrait de redémontrer que les représentations ρ_7^E et ρ_7^A où $A = 1200\text{I}1$ ne sont pas isomorphes.

On a donc montré que $S_7(3)$ est vide.

L'équation $x^5+y^5 = 3z^p$, pour $p \geqslant 11$. Pour $p \geqslant 11$, on utilise le critère énoncé dans le Théorème 1.4 et le programme Fermat disponible à l'adresse www.math.jussieu.fr/ billerey.

Pour tout nombre premier p tel que $11 \leqslant p \leqslant 10^6$, et pour toute courbe elliptique F des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, on trouve un entier $n \geqslant 2$ tel que le couple (F, n) vérifie la condition 1 du Théorème 1.4 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

On obtient ainsi la proposition 1.1.

REMARQUE. On a indiqué dans le tableau 1 de l'Appendice A, les premières valeurs d'entiers n trouvés pour chaque courbe elliptique de $\mathcal{E}_1$ et $\mathcal{E}_2$.

APPENDICES

A—TABLEAU DE VALEURS. On a vu la Section 4.4 que si $q = np + 1$ est un nombre premier congru à 1 modulo p et si E a bonne réduction en q, on est dans l'un des cas suivants (voir (32) et (37)):

1. il existe un élément $\zeta \in A(n, q)$ tel que

$$a_q(E) \equiv \pm a_q(\zeta) \pmod p.$$

2. Il existe un élément $\zeta \in B(n, q)$ tel que

$$a_q(E) \equiv \pm b_q(\zeta) \pmod p.$$

Il en résulte qu'il existe au plus $4n$ valeurs possibles pour la classe de $a_q(E)$ modulo p car les ensembles $A(n,q)$ et $B(n,q)$ sont de cardinal $\leqslant n$. Plus p est grand et n petit et plus la *probabilité* (en un sens heuristique) qu'une congruence de la forme

$$a_q(E)^2 \equiv a_q(F)^2 \pmod{p},$$

où F est l'une des courbes elliptiques des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$, soit réalisée, est faible.

Cela porte à croire que, pour une courbe F des ensembles $\mathcal{E}_1$ ou $\mathcal{E}_2$ donnée, l'existence d'un entier n satisfaisant aux conditions du Théorème 1.4 est d'autant plus probable que p est grand. De plus, on constate que pour les petites valeurs de p, on est souvent obligé de choisir une valeur de n pour chaque courbe elliptique, ce qui est ≪rarement≫ nécessaire lorsque p est grand (disons $p > 10000$).

Dans le tableau 1, on a on a indiqué dans la première colonne la liste des nombres premiers p compris entre 11 et 150. Les courbes elliptiques inscrites sur la première ligne sont celles des ensembles $\mathcal{E}_1$ et $\mathcal{E}_2$. Pour un nombre premier p et une courbe elliptique F comme ci-dessus, on lit dans la case correspondante un entier n tel que le couple (F,n) vérifie la condition 1 du Théorème 1.4 si F appartient à $\mathcal{E}_1$ et la condition 2 si F appartient à $\mathcal{E}_2$.

Ces valeurs ont été obtenues à l'aide du programme Fermat disponible à l'adresse www.math.jusieu.fr/ billerey..

B—Courbes de conducteur 150, 600 et 1200

Les notations du tableau 2 sont celles des tables de [3]. Pour un représentant F de chaque classe d'isogénie de courbes de conducteur 150, 600 ou 1200, on donne successivement:

1. un quintuplet $[a_1,a_2,a_3,a_4,a_6]$ tel que

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

soit une équation minimale de Weierstrass de F,
2. l'invariant modulaire j_F de F,
3. la valuation en 5, $v_5(j_F)$, de l'invariant modulaire j_F de F,
4. la valuation en 5, $v_5\big(\Delta_m(F)\big)$, du discriminant minimal de F,
5. l'indice de ramification e en 5 de l'extension $\mathbb{Q}(F[p])/\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de la courbe F. Si $v_5(j_F) \geqslant 0$, c'est le dénominateur de $v_5\big(\Delta_m(F)\big)/12$ et si $v_5(j_F) < 0$, compte tenu du fait que p ne divise pas $v_5(j_F)$, on a $e = 2p$ (voir [2]).

	150C1	600A1	600F1	1200J1	150A1	600C1	1200N1
11	2	2	2	2	2	2	2
13	4	4	4	4	6	4	4
17	6	6	6	6	14	8	14
19	10	24	24	10	22	22	12
23	2	2	2	2	2	2	2
29	2	2	2	2	2	2	2
31	10	10	22	22	10	10	42
37	4	4	4	4	4	4	6
41	2	2	2	2	2	2	2
43	4	4	4	4	10	4	4
47	6	6	6	6	6	6	6
53	2	2	2	2	2	2	2
59	12	18	18	12	12	18	12
61	12	6	12	6	12	6	6
67	4	4	4	4	4	4	4
71	8	8	8	8	8	8	8
73	4	4	6	4	4	4	6
79	4	4	18	18	18	4	4
83	2	2	2	2	2	2	2
97	4	4	4	4	4	4	4
101	8	6	6	6	8	36	6
103	6	12	10	12	10	10	6
107	6	6	6	6	6	6	6
109	30	10	10	10	10	10	10
113	14	2	14	2	2	2	2
127	4	18	4	4	4	4	4
131	2	2	8	2	2	2	2
137	6	6	6	6	6	6	6
139	4	4	4	4	4	4	4
149	8	8	8	8	8	8	8

Table 1: Tableau des premières valeurs d'entiers n vérifiant les conditions du Théorème 1.4.

courbe	équation	j_F	$v_5(j_F)$	$v_5(\Delta_m(F))$	e
150A1	$[1,0,0,-3,-3]$	$-24389/12$	0	3	4
150B1	$[1,1,0,-75,-375]$	$-24389/12$	0	9	4
150C1	$[1,1,1,37,281]$	$357911/2160$	-1	7	$2p$
600A1	$[0,-1,0,-383,3012]$	$24918016/45$	-1	7	$2p$
600B1	$[0,-1,0,7,-3]$	$5120/3$	1	2	6
600C1	$[0,-1,0,32,-68]$	$27436/27$	0	3	4
600D1	$[0,1,0,17,38]$	$2048/3$	0	6	2
600E1	$[0,1,0,-233,1563]$	$-8780800/2187$	2	4	3
600F1	$[0,-1,0,92,-188]$	$21296/15$	-1	7	$2p$
600G1	$[0,-1,0,-5833,207037]$	$-8780800/2187$	2	10	6
600H1	$[0,1,0,792,-6912]$	$27436/27$	0	9	4
600I1	$[0,1,0,167,-37]$	$5120/3$	1	8	3
1200A1	$[0,-1,0,17,-38]$	$2048/3$	0	6	2
1200B1	$[0,-1,0,792,6912]$	$27436/27$	0	9	4
1200C1	$[0,-1,0,167,37]$	$5120/3$	1	8	3
1200D1	$[0,-1,0,-233,-1563]$	$-8780800/2187$	2	4	3
1200E1	$[0,1,0,-383,-3012]$	$24918016/45$	-1	7	$2p$
1200F1	$[0,1,0,7,3]$	$5120/3$	1	2	6
1200G1	$[0,1,0,92,188]$	$21296/15$	-1	7	$2p$
1200H1	$[0,1,0,-5833,-207037]$	$-8780800/2187$	2	10	6
1200I1	$[0,1,0,32,68]$	$27436/27$	0	3	4
1200J1	$[0,-1,0,-8,-1488]$	$-1/15$	-1	7	$2p$
1200K1	$[0,-1,0,27,-243]$	$20480/243$	1	2	6
1200L1	$[0,-1,0,-333,3537]$	$-40960/27$	1	8	3
1200M1	$[0,-1,0,-48,192]$	$-24389/12$	0	3	4
1200N1	$[0,-1,0,-333,-2088]$	$131072/9$	0	9	4
1200O1	$[0,1,0,-13,23]$	$-40960/27$	1	2	6
1200P1	$[0,1,0,592,-16812]$	$357911/2160$	-1	7	$2p$
1200Q1	$[0,1,0,-1208,21588]$	$-24389/12$	0	9	4
1200R1	$[0,1,0,-133,563]$	$-102400/3$	2	4	3
1200S1	$[0,1,0,-13,-22]$	$131072/9$	0	3	4

Table 2: Classes d'isogénie des courbes elliptiques de conducteur 150, 600 et 1200

References

[1] A.O.L. Atkin et J. Lehner, 'Hecke Operators on $\Gamma_0(m)$', *Math. Ann.* **185** (1970), 134–160.

[2] É. Cali et A. Kraus, 'Sur la p-différente du corps des points de ℓ-torsion des courbes elliptiques, $\ell \neq p$', *Acta Arith.* **104** (2002), 1–21.

[3] J. Cremona, *Algorithms for modular elliptic curves*, (second edition) (Cambridge University Press, Cambridge, 1997).

[4] H. Darmon, 'Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation', *C. R. Math. Rep. Acad. Sci. Canada* **19** (1997), 3–14.

[5] H. Darmon et A. Granville, 'On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$', *Bull. London Math. Soc.* **27** (1995), 513–544.

[6] L. Dirichlet, 'Mémoire sur l'impossibilité de quelques équations indéterminées du cinquième degré', *J. Reine Angew. Math.* **3** (1828), 354–375.

[7] G. Frey, 'Links between stable elliptic curves and certain diophantine equations', *Ann. Univ. Sarav. Ser. Math.* **1** (1986), 1–40.

[8] E. Halberstadt et A. Kraus, 'Courbes de Fermat: résultats et problèmes', *J. Reine Angew. Math.* **548** (2002), 167–234.

[9] M.A. Kenku, 'On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-Isogeny class', *J. Number Theory* **15** (1982), 199–202.

[10] A. Kraus, 'Quelques remarques à propos des invariants c_4, c_6 et Δ d'une courbe elliptique', *Acta Arith.* **54** (1989), 75–80.

[11] A. Kraus, *Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique*, Dissertationes Math., 1997, **pp.** 364.

[12] A. Kraus, 'Sur l'équation $a^3 + b^3 = c^p$', *Experiment Math.* **7** (1998), 1–13.

[13] A. Kraus, 'Une question sur les équations $x^m - y^m = Rz^n$', *Compositio Math.* **132** (2002), 1–26.

[14] A. Kraus et J. Oesterlé, 'Sur une question de B. Mazur', *Math. Ann.* **293** (1992), 259–275.

[15] G. Ligozat, *Courbes modulaires de genre* 1, Bull. Soc. Math. France, Mém. **43** (Société Mathématique de France, 1975).

[16] I. Papadopoulos, 'Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3', *J. Number Theory* **44** (1993), 119–152.

[17] K.A. Ribet, 'On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms', *Invent. Math.* **100** (1990), 431–476.

[18] J.-P. Serre, 'Propriétés galoisiennes des points d'ordre fini des courbes elliptiques', *Invent. Math.* **15** (1972), 259–331.

[19] J.-P. Serre, 'Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$', *Duke Math. J.* **54** (1987), 179–230.

[20] J.H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106** (Springer-Verlag, Berlin, Heidelberg, New York, 1992).

[21] J. Tate, 'Algorithm for determining the type of a singular fiber in an elliptic pencil', in *Modular functions of one variable*, Lect. Notes in Math. **273**, 1975, **pp.** 33–52.

[22] A. Wiles, 'Modular elliptic curves and Fermat's Last Theorem', *Ann. of Math.* **141** (1995), 443–551.

Institut de Mathématiques
UMR 7586, Case 247
Place Jussieu
75252 Paris
France
e-mail: billerey@math.jussieu.fr

Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 1272–1294
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

Formes homogènes de degré 3 et puissances p-ièmes

Nicolas Billerey

Université Paris 6, Projet théorie des nombres, UMR 7586, Case 247, 4, place Jussieu, Institut de Mathématiques, 75252 Paris, France

Reçu le 14 décembre 2006 ; révisé le 17 septembre 2007

Disponible sur Internet le 4 mars 2008

Communiqué par M. Bennett

Abstract

In this paper, we are interested in diophantine equations of type $F(x, y) = dz^p$ where F is a separable homogeneous form of degree $\geqslant 3$ with integer coefficients, d a fixed integer $\geqslant 1$ and p a prime number $\geqslant 7$. As a consequence of the *abc* conjecture, if p is sufficiently large and (a, b, c) is a nontrivial proper solution of the above equation, we have $c = \pm 1$. In the case where F has degree 3, we associate to (a, b, c) an elliptic curve defined over $\mathbb{Q}$ called the Frey curve or Hellegouarch–Frey curve. This allows us to deduce our conjecture from another one about elliptic curves attributed to G. Frey and B. Mazur (which is itself a consequence of the *abc* conjecture). We then applied our construction to the study of an explicit form. We give some results about the set of nontrivial proper solutions of the equation considered for several values of d.

Keywords: Forms of degree higher than two; Elliptic curves; Modular representations

1. Introduction

On se propose de faire quelques remarques sur la conjecture suivante.

Conjecture 1.1 *(A). Soient $F \in \mathbb{Z}[X, Y]$ une forme homogène séparable de degré $\geqslant 3$ et d un entier $\geqslant 1$. Il existe une constante $C_{d,F} > 0$ ne dépendant que de d et F telle que si p est un*

Adresse e-mail : billerey@math.jussieu.fr.
URL : http://www.institut.math.jussieu.fr/~billerey/.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.11.004

nombre premier $> C_{d,F}$ *et* (a, b, c) *un triplet d'entiers non nuls premiers entre eux vérifiant l'égalité*

$$F(a, b) = dc^p,$$

alors on a $c = \pm 1$.

Les seuls résultats déjà connus sur cette conjecture concernent certains cas particuliers d'équations de Fermat généralisées où d est un entier convenablement choisi et où $F(x, y)$ est l'une des formes suivantes (cf. [5,9,13,21,23]) :

$$x^3 + y^3, \quad x^4 + y^4, \quad x^4 - y^4, \quad x^5 + y^5 \quad \text{et} \quad x^6 + y^6.$$

Les équations $F(x, y) = \pm d$ d'inconnues x, y dans $\mathbb{Z}$ sont appelées équations de Thue. Elles ont été particulièrement étudiées. On sait par exemple qu'elles n'ont qu'un nombre fini de solutions (cf. par exemple [15, p. 363]). Par ailleurs, si $p \geqslant 5$ est fixé, un théorème de [11] affirme qu'il n'existe qu'un nombre fini de triplets d'entiers non nuls (a, b, c) premiers entre eux tels que $F(a, b) = dc^p$. La conjecture (A) entraîne donc que l'ensemble des triplets (a, b, c) d'entiers non nuls premiers entre eux pour lesquels il existe un nombre premier $p \geqslant 5$ tel que $F(a, b) = dc^p$, est fini.

On rappelle dans l'Appendice A que la conjecture (A) est une conséquence de la conjecture *abc*.

Dans cet article, on s'intéresse plus spécifiquement aux équations diophantiennes de la forme

$$F(x, y) = dz^p, \tag{1}$$

où F est une forme homogène séparable de degré 3 à coefficients entiers relatifs, p un nombre premier $\geqslant 7$ et d un entier $\geqslant 1$.

Le cas particulier de l'équation (1)

$$x^3 + y^3 = z^p, \tag{2}$$

a été étudié par H. Darmon et A. Granville [11] et A. Kraus [21]. Leur approche repose sur l'étude modulaire de la représentation galoisienne des points de p-torsion d'une certaine courbe elliptique, appelée parfois courbe de Frey ou courbe de Hellegouarch–Frey, associée à une hypothétique solution de l'équation (2).

Conformément à la terminologie utilisée dans [11], on dira qu'un triplet d'entiers $(a, b, c) \in \mathbb{Z}^3$ est solution de l'équation (1) si $F(a, b) = dc^p$, qu'elle est propre si a, b et c sont premiers entre eux et qu'elle est non triviale si abc est non nul.

Dans la partie 2, on généralise la construction de la courbe de Frey associée à l'équation (2) dans [11] à toutes les formes homogènes séparables de degré 3

$$F(x, y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3,$$

avec t_0, t_1, t_2 et t_3 entiers relatifs. Si (a, b, c) est une solution propre et non triviale de (1), la courbe E que l'on construit a pour équation

$$E\colon\ y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 = t_1 a - t_2 b, \\ a_4 = t_0 t_2 a^2 + (3t_0 t_3 - t_1 t_2)ab + t_1 t_3 b^2, \\ a_6 = t_0^2 t_3 a^3 - t_0\big(t_2^2 - 2t_1 t_3\big)a^2 b + t_3\big(t_1^2 - 2t_0 t_2\big)ab^2 - t_0 t_3^2 b^3. \end{cases}$$

On démontre au théorème 2.3 que si p est assez grand et $c \neq \pm 1$, alors E est une courbe de Frey au sens de la définition 2.2.

Cette construction offre l'avantage de relier le problème diophantien soulevé par l'équation (1) à des résultats ou conjectures classiques de théorie des nombres ou, plus spécifiquement, de la théorie des courbes elliptiques. Tel est le cas, par exemple, de la conjecture suivante, attribuée à G. Frey et B. Mazur (cf. [10] et [22]) :

Conjecture 1.2 *(Frey–Mazur). Soit A une courbe elliptique définie sur $\mathbb{Q}$. On désigne par $\mathcal{F}_A$ l'ensemble des nombres premiers ℓ pour lesquels il existe une courbe elliptique $A^{(\ell)}$ définie sur $\mathbb{Q}$, non isogène à A sur $\mathbb{Q}$, telle que les modules galoisiens des points de ℓ-torsion de A et A' soient isomorphes. Alors, l'ensemble $\mathcal{F}_A$ est fini.*

Cette conjecture n'a actuellement été démontrée pour aucune courbe elliptique. Si A est une courbe elliptique définie sur $\mathbb{Q}$, on sait que 2, 3 et 5 sont dans $\mathcal{F}_A$.

En utilisant la construction de E, on montre (proposition 2.9) que la conjecture ci-dessus implique la conjecture (A) pour les formes homogènes de degré 3.

On donne par ailleurs dans l'Appendice B une démonstration, due à Kraus, du fait que la conjecture *abc* implique (via une forme faible de la conjecture de Szpiro) la conjecture de Frey–Mazur. On a donc en résumé le diagramme d'implications suivant.

$$\begin{array}{ccc} \text{Conjecture de Frey–Mazur} & \Longleftarrow\!\!= & \text{Conjecture } abc \\ \Downarrow & & \Downarrow \\ \text{Conjecture (A) pour } \deg(F) = 3 & & \text{Conjecture (A)} \end{array}$$

Si F une forme homogène séparable de degré $\geqslant 3$ à coefficients entiers relatifs, on pose $f(x) = F(x, 1)$. Lorsque $d = 1$ et $y = 1$, l'équation (1) s'écrit

$$f(x) = z^p. \tag{3}$$

En 1920, Nagell a démontré que pour le polynôme

$$f(x) = x^3 + x^2 + x + 1, \tag{4}$$

l'équation (3) n'admettait pas de solution non triviale ($xz \neq 0$) pour $p \geqslant 3$ et seulement $(x, z) = (7, 20)$ lorsque $p = 2$ [27, p. 73]. Outre le cas particulier de l'équation de Catalan, $x^3 \pm z^p = 1$, on trouvera d'autres exemples de résolution de telles équations dans [3] et [6].

Suivant l'exemple de Nagell, nous illustrons dans la partie 3 la construction de la courbe de Frey précédente avec l'étude de l'équation (1) lorsque F est la forme homogène de degré 3 suivante

$$F(x, y) = x^3 + x^2 y + x y^2 + y^3. \tag{5}$$

Si (a, b, c) appartient à l'ensemble $S_p(d)$ des solutions propres et non triviales de l'équation (1) où F est la forme ci-dessus et d un entier $\geqslant 1$, on lui associe la courbe E d'équation

$$E\colon\ y^2 = x^3 + (a-b)x^2 + (a+b)^2x + a^3 + a^2b - ab^2 - b^3.$$

Pour certains entiers d libres de puissances troisièmes, on obtient plusieurs résultats sur $S_p(d)$. À titre d'exemple, on montre par des arguments de nature modulaire (théorème 3.2) que si $d = 2, 6, 10$ ou 22, alors $S_p(d)$ est vide pour $p \geqslant 7$. De même, si ℓ est un nombre premier vérifiant certaines conditions explicites, alors $S_p(2\ell)$ est vide lorsque p est suffisamment grand. Tel est le cas, par exemple, lorsque $\ell = 19, 43, 59, 61, 67, 83$ (théorème 3.3).

Bien que notre construction ne permette pas de retrouver le résultat de Nagell (correspondant au cas où $d = 1$ et $y = 1$), on explique dans la partie 4 comment la théorie modulaire permet d'aborder, voire de résoudre complètement, certaines équations diophantiennes, certes plus artificielles mais néanmoins non triviales, de la forme (1) ou (3) lorsque le polynôme considéré est de degré $\geqslant 3$.

2. La courbe elliptique E

On considère dans cette partie une forme homogène séparable de degré 3 à coefficients entiers relatifs

$$F(x, y) = t_0x^3 + t_1x^2y + t_2xy^2 + t_3y^3.$$

Posons $f(x) = F(x, 1)$. Le polynôme F étant séparable, il en va de même pour f.

On considère un nombre premier $p \geqslant 7$, un entier $d \geqslant 1$ et (a, b, c) une solution propre et non triviale de l'équation (1).

2.1. Équation de la courbe E

On commence par supposer $t_0 \neq 0$, i.e. $\deg(f) = 3$. Soit $K = \mathbb{Q}(\alpha, \beta, \gamma)$ l'extension de $\mathbb{Q}$ dans $\mathbb{C}$ engendrée par les racines α, β, γ du polynôme f. On a alors la factorisation suivante :

$$F(x, y) = t_0(x - \alpha y)(x - \beta y)(x - \gamma y).$$

On associe à (a, b, c) une courbe elliptique $E/\mathbb{Q}$ comme suit. Posons :

$$\begin{cases} A = t_0(\beta - \gamma)(a - \alpha b), \\ B = t_0(\gamma - \alpha)(a - \beta b), \\ C = t_0(\alpha - \beta)(a - \gamma b). \end{cases}$$

Par construction, on a

$$A + B + C = 0.$$

Soit $\mathcal{E}$ la cubique d'équation :

$$\mathcal{E}\colon\ Y^2 = X(X - A)(X + B). \tag{6}$$

Son discriminant est

$$\Delta(\mathcal{E}) = 16(AB)^2(A+B)^2 = 16\mathfrak{D}(f)F(a,b)^2,$$

où $\mathfrak{D}(f)$ est le discriminant du polynôme f. L'entier c étant non nul et le polynôme f séparable, on a $\Delta(\mathcal{E}) \neq 0$. L'équation (6) définit donc une courbe elliptique sur K.

Considérons les trois éléments u_1, u_2 et u_3 de K définis par

$$\begin{cases} u_1 = t_0(\alpha a + \gamma\beta b), \\ u_2 = t_0(\beta a + \gamma\alpha b), \\ u_3 = t_0(\gamma a + \beta\alpha b). \end{cases}$$

Ils vérifient les égalités : $A = u_2 - u_3$, $B = u_3 - u_1$ et $C = u_1 - u_2$. Le changement de variables

$$x = X + u_3, \qquad y = Y, \tag{7}$$

transforme alors l'équation (6) en l'équation :

$$E\colon\ y^2 = (x-u_1)(x-u_2)(x-u_3).$$

Cette courbe E a pour équation :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6, \tag{8}$$

avec

$$\begin{cases} a_2 = t_1a - t_2b, \\ a_4 = t_0t_2a^2 + (3t_0t_3 - t_1t_2)ab + t_1t_3b^2, \\ a_6 = t_0^2t_3a^3 - t_0\big(t_2^2 - 2t_1t_3\big)a^2b + t_3\big(t_1^2 - 2t_0t_2\big)ab^2 - t_0t_3^2b^3. \end{cases}$$

La courbe elliptique E est donc définie sur $\mathbb{Q}$ et le changement de variables (7) fournit un isomorphisme défini sur K de $\mathcal{E}$ sur E. De plus, les invariants standard $c_4(E)$ et $\Delta(E)$ de (8) sont inchangés par rapport à ceux de $\mathcal{E}$ (cf. [38]). On les note respectivement c_4 et Δ. On a :

$$\begin{cases} c_4 = 16\big(\big(t_1^2 - 3t_0t_2\big)a^2 + (t_1t_2 - 9t_0t_3)ab + \big(t_2^2 - 3t_1t_3\big)b^2\big), \\ \Delta = 16\mathfrak{D}(f)F(a,b)^2 \\ \quad \text{où } \mathfrak{D}(f) = -27t_0^2t_3^2 + \big(18t_1t_2t_3 - 4t_2^3\big)t_0 - 4t_3t_1^3 + t_1^2t_2^2. \end{cases} \tag{9}$$

Supposons $t_0 = 0$. Dans ce cas, on associe à (a,b,c) la courbe elliptique $E/\mathbb{Q}$ d'équation

$$E\colon\ y^2 = x^3 + (t_1a - t_2b)x^2 + t_1(t_3b - t_2a)bx + t_1^2t_3ab^2.$$

Il s'agit de la courbe d'équation (8) avec $t_0 = 0$.

Remarque 2.1. Supposons qu'il existe $x_0 \in \mathbb{Q}$ racine du polynôme f. Alors, E a un point d'ordre 2 rationnel sur $\mathbb{Q}$. Si $x_0 = 0$, tel est le cas du point $(t_2b, 0)$, sinon tel est le cas de $(t_0x_0a - \frac{t_3}{x_0}b, 0)$.

2.2. La courbe de Frey E

On rappelle que p est un nombre premier $\geqslant 7$ et que (a, b, c) est une solution propre et non triviale de l'équation (1). Notons $\overline{\mathbb{Q}}$ la clôture algébrique de $\mathbb{Q}$ dans $\mathbb{C}$ et $\mathrm{G}_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ le groupe de Galois absolu de $\mathbb{Q}$. Soit A une courbe elliptique définie sur $\mathbb{Q}$ et $A[p]$ le sous-groupe de $A(\overline{\mathbb{Q}})$ constitué des points de p-torsion de A. C'est un $\mathbb{F}_p$-espace vectoriel de dimension 2 sur lequel le groupe $\mathrm{G}_{\mathbb{Q}}$ opère continûment. Par le choix d'une base de $A[p]$ sur $\mathbb{F}_p$, on en déduit un homomorphisme de groupes

$$\rho_p^A : \mathrm{G}_{\mathbb{Q}} \longrightarrow \mathbf{GL}_2(\mathbb{F}_p).$$

On associe à cette représentation un poids k qui est un entier $\geqslant 2$ et un conducteur $N(\rho_p^A)$ qui est un entier $\geqslant 1$, premier à p, qui divise le conducteur N_A de A (cf. [32, §1]). Désignons par Δ_A le discriminant minimal de A. Si ℓ est un nombre premier, notons v_ℓ la valuation ℓ-adique de $\mathbb{Q}$.

Définition 2.2. Soit $A/\mathbb{Q}$ une courbe elliptique définie sur $\mathbb{Q}$. On désigne par S_A l'ensemble des nombres premiers de mauvaise réduction de A. Soient S un sous-ensemble de S_A et p un nombre premier. On dira que A est une courbe de Frey associée au couple (p, S) si les trois conditions suivantes sont satisfaites.

(1) La représentation ρ_p^A est irréductible.
(2) L'ensemble S est strictement inclus dans S_A.
(3) Pour tout nombre premier $\ell \in S_A \setminus S$, la courbe A a réduction multiplicative en ℓ et $v_\ell(\Delta_A) \equiv 0 \pmod{p}$.

Avec la définition ci-dessus, on a le résultat suivant.

Théorème 2.3. *Il existe une constante $\alpha(d, F) \geqslant 0$ ne dépendant que de d et F telle que si $c \neq \pm 1$ et $p > \alpha(d, F)$, alors la courbe E est une courbe de Frey associée au couple (p, S) où S est l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ de mauvaise réduction.*

Démontrons à présent cet énoncé.

2.2.1. Résultats préliminaires

On a la relation suivante :

$$U(a, b)F(a, b) + V(a, b)c_4 = -16\mathfrak{D}(f)b^4, \tag{10}$$

où

$$\begin{cases} U(a, b) = 16\big(3t_0\big(3t_0t_2 - t_1^2\big)a + \big(t_1^3 - 6t_0t_1t_2 + 27t_0^2t_3\big)b\big), \\ V(a, b) = 3t_0^2a^2 + 2t_0t_1ab + \big(4t_0t_2 - t_1^2\big)b^2. \end{cases}$$

On en déduit le lemme suivant.

Lemme 2.4. *Soit ℓ un nombre premier divisant Δ et ne divisant pas $2d\mathfrak{D}(f)$. L'équation* (8) *est minimale en ℓ et la courbe E a réduction multiplicative en ℓ. De plus, $v_\ell(\Delta_E)$ est multiple de p.*

Démonstration. Soit ℓ un nombre premier impair ne divisant pas $d\mathfrak{D}(f)$ et divisant $\Delta = 2^4\mathfrak{D}(f)d^2c^{2p}$. Nécessairement, ℓ divise l'entier c. Supposons par l'absurde que ℓ divise le coefficient c_4. D'après la relation (10), l'entier ℓ divise alors également $16\mathfrak{D}(f)b^4$. Or ℓ ne divise pas $2\mathfrak{D}(f)$, donc ℓ divise b. De l'expression de $F(a,b)$, on en déduit que ℓ divise t_0a^3. Si ℓ ne divise pas a, alors ℓ divise t_0 et d'après l'expression du coefficient c_4 de la courbe E ci-dessus, il vient que ℓ divise également t_1. Mais alors ℓ divise $\mathfrak{D}(f)$ d'après l'expression (9) ci-dessus. C'est une contradiction. Donc ℓ divise a. Comme ℓ divise aussi b et c, c'est contraire au fait que (a,b,c) soit une solution propre de (1). On en déduit que ℓ ne divise pas c_4.

La congruence $v_\ell(\Delta_E) \equiv 0 \pmod{p}$ résulte de l'égalité $v_\ell(\Delta) = v_\ell(\Delta_E)$ et de l'expression (9) du coefficient Δ. □

Lemme 2.5. *Pour p assez grand, la représentation ρ_p^E est irréductible. Si E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, c'est le cas pour $p \geqslant 11$. Si l'invariant modulaire j de E est différent de -15^3 et 255^3, la représentation ρ_7^E est irréductible.*

Démonstration. La représentation ρ_p^E est irréductible dès que $p > 163$ d'après [26].

Supposons que E a un point d'ordre 2 rationnel sur $\mathbb{Q}$ (c'est par exemple le cas si f est réductible sur $\mathbb{Q}$ d'après la remarque 2.1). Si ρ_p^E était réductible, le groupe $E(\overline{\mathbb{Q}})$ possèdrait un sous-groupe d'ordre $2p$ stable par $G_{\mathbb{Q}}$, de sorte que la courbe modulaire $Y_0(2p)$ aurait un point rationnel sur $\mathbb{Q}$. Or, si $p \geqslant 11$, B. Mazur et M. Kenku ont démontré que l'ensemble $Y_0(2p)(\mathbb{Q})$ est vide (cf. [17]). D'où le résultat dans ce cas.

Le cas $p = 7$ se traite en remarquant que la courbe modulaire $Y_0(14)$ est la courbe elliptique notée 14A1 dans les tables de [8] et qu'elle possède exactement deux points rationnels sur $\mathbb{Q}$ qui correspondent aux deux classes de $\overline{\mathbb{Q}}$-isomorphisme des courbes elliptiques d'invariants $j = -15^3$ et 255^3 [25, p. 45]. D'où le lemme. □

Lemme 2.6. *Si p ne divise pas $d\mathfrak{D}(f)$, alors on a $k = 2$.*

Démonstration. On suppose que p ne divise pas $d\mathfrak{D}(f)$. Alors, d'après le lemme 2.4, l'équation (8) est minimale en p, la courbe E a réduction semi-stable en p et l'exposant de p dans le discriminant minimal de E est multiple de p. D'où $k = 2$ [32, prop. 5]. □

Le lemme suivant servira à plusieurs reprises (pour un résultat plus précis, voir [36, V §4]).

Lemme 2.7. *Soit S' un ensemble fini de nombres premiers. Il n'existe qu'un nombre fini de triplets d'entiers (u,v,m) vérifiant les trois conditions suivantes* :

(1) *on a $F(u,v) = m$,*
(2) *les entiers u et v sont premiers entre eux,*
(3) *l'entier m a tous ses diviseurs premiers dans S'.*

Démonstration. Posons $S' = \{p_1, \ldots, p_r\}$. Soit $n \in \mathbb{Z} \setminus \{0\}$. L'ensemble

$$\left\{(x,y) \in \mathbb{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x,y) = n\right\}$$

est fini [15, p. 363].

On en déduit que si $\mathcal{N} = \{\pm p_1^{\alpha_1} \cdots p_r^{\alpha_r},\ \text{avec } 0 \leqslant \alpha_i \leqslant 2\}$, alors l'ensemble

$$\mathcal{F} = \left\{ (x, y) \in \mathbb{Z}\left[\frac{1}{S'}\right]^2 \;\middle|\; F(x, y) = n,\ \text{avec } n \in \mathcal{N} \right\}$$

est encore fini.

Soit (u, v, m) un triplet d'entiers vérifiant les trois conditions du lemme. Il existe un unique entier $Z > 0$ ayant tous ses diviseurs premiers dans S' tel que $m = Z^3 n$ avec $n \in \mathcal{N}$. On a alors

$$F\left(\frac{u}{Z}, \frac{v}{Z}\right) = n.$$

En particulier, il existe r et s tels que

$$\left(\frac{u}{Z}, \frac{v}{Z}\right) = (r, s) \in \mathcal{F}.$$

Les entiers u et v étant premiers entre eux, l'entier Z est le plus petit dénominateur commun > 0 de r et s. On en déduit qu'il n'existe qu'un nombre fini de valeurs possibles pour u et v et, par conséquent, pour m. Cela démontre le lemme. □

Notations. Soit S' un ensemble fini non vide de nombres premiers. On désigne par $\mathcal{F}_{F,S'}$ l'ensemble (fini) des triplets (u, v, m) satisfaisant aux trois conditions du lemme 2.7. On pose alors

$$N_{F,S'} = \begin{cases} \max\{|m|, (u, v, m) \in \mathcal{F}_{F,S'}\} & \text{si } \mathcal{F}_{F,S'} \neq \emptyset, \\ 1 & \text{sinon.} \end{cases} \tag{11}$$

L'entier $N_{F,S'}$ ne dépend que de F et S'.

Lemme 2.8. *Il existe une constante $\beta(d, F) \geqslant 0$ ne dépendant que de d et F telle que si $p > \beta(d, F)$, alors l'une des deux conditions suivantes est réalisée* :

(1) *on a $c = \pm 1$,*
(2) *il existe un nombre premier ne divisant pas $2d\mathfrak{D}(f)$ en lequel E a mauvaise réduction.*

Démonstration. Supposons la seconde condition non réalisée. Alors, d'après le lemme 2.4, l'entier c a tous ses diviseurs premiers dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)$. Par ailleurs, si $\operatorname{pgcd}(a, b)$ désigne le pgcd de a et b, alors $(\operatorname{pgcd}(a, b))^3$ divise d. Posons

$$a' = \frac{a}{\operatorname{pgcd}(a, b)}, \quad b' = \frac{b}{\operatorname{pgcd}(a, b)} \quad \text{et} \quad d' = \frac{d}{(\operatorname{pgcd}(a, b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.7, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations précédentes)

$$\beta(d, F) = \frac{\log N_{F,S'}}{\log 2} \geqslant 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $\beta(d, F)$. Si l'on a $p > \beta(d, F)$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. Cela démontre le lemme 2.8. □

2.2.2. Fin de la démonstration du théorème 2.3

Notons S l'ensemble des diviseurs premiers de $2d\mathfrak{D}(f)$ en lesquels la courbe E a mauvaise réduction. D'après le lemme 2.5, il existe une constante $\gamma(d, F) \geqslant 5$ telle que si $p > \gamma(d, F)$, alors ρ_p^E est irréductible. Posons, avec les notations du lemme 2.8, $\alpha(d, F) = \max(\beta(d, F), \gamma(d, F))$. Si $c \neq \pm 1$ et $p > \alpha(d, F)$, alors $p > \beta(d, F)$ et, d'après le lemme 2.8, il existe un nombre premier de mauvaise réduction qui ne soit pas dans S, i.e. $S_E \setminus S \neq \emptyset$. Par ailleurs, d'après le lemme 2.4, pour tout nombre premier $\ell \in S_E \setminus S$, E a réduction multiplicative en ℓ et $v_\ell(\Delta_E) \equiv 0 \pmod{p}$. D'où le théorème.

2.3. Lien avec la conjecture de Frey–Mazur

Notation. Soit A une courbe elliptique définie sur $\mathbb{Q}$. On pose, avec les notations de la conjecture de Frey–Mazur,

$$\nu_A = \max\{\ell \mid \ell \in \mathcal{F}_A\}.$$

D'après cette conjecture, $\nu_A \in \mathbb{N}$.

Proposition 2.9. *La conjecture de Frey–Mazur implique la conjecture* (A) *pour les formes de degré* 3.

Démonstration. D'après les lemmes 2.5 et 2.6, on peut sans restriction supposer la représentation ρ_p^E irréductible et de poids 2. Le conducteur $N(\rho_p^E)$ est majoré par une constante M indépendante du quadruplet (a, b, c, p). En effet, si ℓ est un diviseur premier de $N(\rho_p^E)$, alors, d'après le lemme 2.4 et [19, p. 28], ℓ divise $2d\mathfrak{D}(f)$. De plus, on a $v_2(N(\rho_p^E)) \leqslant 8$, $v_3(N(\rho_p^E)) \leqslant 5$ et si $\ell \geqslant 5$, $v_\ell(N(\rho_p^E)) \leqslant 2$ (cf. [29]). On peut donc, par exemple, choisir $M = (2d\mathfrak{D}(f))^8$.

Par ailleurs, d'après le théorème 3 de [20], il existe une constante $\eta_{d,F}$ ne dépendant que de d et F telle que si $p > \eta_{d,F}$, alors il existe une courbe elliptique A définie sur $\mathbb{Q}$ de conducteur $N_A = N(\rho_p^E)$ telle que les représentations ρ_p^E et ρ_p^A soient isomorphes.

Supposons l'inégalité suivante vérifiée

$$p > \nu_{d,F} = \max\{\eta_{d,F}, \nu_{A'} \mid A' \text{ courbe elliptique sur } \mathbb{Q} \text{ telle que } N_{A'} \leqslant M\}.$$

L'entier M ne dépendant que de d et F, il en va de même pour $\nu_{d,F}$. Considérons alors ℓ un nombre premier divisant c et ne divisant pas $2d\mathfrak{D}(f)N_A$. En particulier, ℓ divise Δ sans diviser $2d\mathfrak{D}(f)$, donc, d'après le lemme 2.4, la courbe E a mauvaise réduction multiplicative en ℓ. De plus, comme $p > \nu_{d,F} \geqslant \nu_A$, les courbes E et A sont $\mathbb{Q}$-isogènes d'après la conjecture de Frey–Mazur et on a

$$1 = v_\ell(N_E) = v_\ell(N_A) = 0, \quad \text{car } \ell \text{ ne divise pas } N_A.$$

C'est une contradiction. On en déduit que c a tous ses diviseurs premiers inclus dans l'ensemble S' des diviseurs premiers de $2d\mathfrak{D}(f)\prod N_{A'}$ où le produit porte sur l'ensemble fini

(cf. [35, IX §6]) des classes de $\mathbb{Q}$-isomorphisme de courbes elliptiques A' définies sur $\mathbb{Q}$ de conducteur $\leqslant M$.

Si $\mathrm{pgcd}(a,b)$ désigne le pgcd de a et b, alors $(\mathrm{pgcd}(a,b))^3$ divise d. Posons

$$a' = \frac{a}{\mathrm{pgcd}(a,b)}, \quad b' = \frac{b}{\mathrm{pgcd}(a,b)} \quad \text{et} \quad d' = \frac{d}{(\mathrm{pgcd}(a,b))^3}.$$

Le triplet $(a', b', d'c^p)$ vérifie les trois conditions du lemme 2.7, i.e. appartient à l'ensemble fini $\mathcal{F}_{F,S'}$. Posons (avec les notations (11))

$$C_{d,F} = \frac{\log N_{F,S'}}{\log 2} \geqslant 0.$$

L'ensemble S' ne dépendant que de F et d, il en va de même pour $C_{d,F}$. Et, si $p > C_{d,F}$, alors $d'2^p > N_{F,S'}$. On a donc $c = \pm 1$. C'est l'énoncé de la conjecture (A). □

3. Étude d'un exemple

À titre d'exemple, on applique, dans cette partie, la construction précédente au cas particulier de la forme homogène

$$F(x,y) = x^3 + x^2y + xy^2 + y^3.$$

Soient p un nombre premier $\geqslant 7$ et d un entier $\geqslant 1$. Rappelons que $S_p(d)$ désigne l'ensemble des solutions propres et non triviales de l'équation

$$F(x,y) = x^3 + x^2y + xy^2 + y^3 = dz^p. \tag{12}$$

Dans toute cette partie, on fait l'hypothèse suivante :

l'entier d est libre de puissance troisième.

Sous cette hypothèse, si (a,b,c) appartient à $S_p(d)$, alors les entiers a, b et c sont premiers entre eux deux-à-deux.

En utilisant la courbe E d'équation (8) associée un élément de $S_p(d)$, et la méthode modulaire (dont le principe est résumé au début du paragraphe 3.3), on démontre plusieurs résulats sur l'équation (12).

Le premier concerne le cas $d = 1$.

Théorème 3.1. *Soit (a,b,c) un élément de $S_p(1)$. Alors, l'entier c est impair.*

Pour certaines valeurs de l'entier d, on a un résultat complet.

Théorème 3.2. *Les ensembles $S_p(2)$, $S_p(6)$, $S_p(10)$ et $S_p(22)$ sont vides.*

Soit ℓ est un nombre premier $\geqslant 13$. On souhaite montrer, comme au théorème précédent pour $\ell = 3, 5$ et 11, la vacuité de l'ensemble $S_p(2\ell)$ (au-moins lorsque p est grand). Cela sera le cas si ℓ vérifie certaines conditions. Plus précisément, on désigne par g la fonction définie sur $\mathbb{N}^*$ par

$$g(n) = \begin{cases} \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n < 2^9, \\ 18 + 2\frac{\log n}{\log 2} & \text{si } 2^9 \leqslant n < 2^{362}, \\ \frac{50}{13} \cdot \frac{\log(n)}{\log(2)} & \text{si } n \geqslant 2^{362}. \end{cases}$$

On dira que ℓ satisfait à la propriété (P) si pour tout entier k vérifiant l'inégalité

$$2 \leqslant k < g(\ell),$$

aucun des entiers $\ell - 1$, $\ell - 2^k$, $\ell + 2^k$ et $2^k - \ell$ n'est un carré.

On a alors le résultat suivant.

Théorème 3.3. *On suppose que ℓ vérifie la propriété* (P)*. Il existe une constante $\kappa(\ell)$ ne dépendant que de ℓ telle que si $p > \kappa(\ell)$, alors l'ensemble $S_p(2\ell)$ est vide.*

Remarque 3.4. On peut par exemple prendre $\kappa(\ell) = (4\sqrt{\ell+1} + 1)^{4(\ell-1)}$. L'amélioration de cette borne est, dans la pratique, limitée par la connaissance des newform (au sens de [1]) de poids 2 et de niveau 64ℓ. Par exemple, pour $\ell = 11$, on a $\kappa(11) \approx 7 \cdot 10^{46}$, alors que $S_p(22)$ est vide pour $p \geqslant 7$ d'après le théorème 3.2. Les nombres premiers $13 \leqslant \ell \leqslant 200$ satisfaisant à la condition (P) sont

$$\ell = 19, 43, 59, 61, 67, 83, 107, 109, 131, 139, 149, 157, 163, 167, 179, 181 \text{ et } 191.$$

La suite de la partie 3 est consacrée à la démonstration des théorèmes 3.1, 3.2 et 3.3.

3.1. La courbe elliptique E

Soit (a, b, c) un élément de $S_p(d)$. À un tel triplet on associe la courbe elliptique $E/\mathbb{Q}$ définie par l'équation (8) avec $t_0 = t_1 = t_2 = t_3 = 1$:

$$y^2 = x^3 + (a-b)x^2 + (a+b)^2 x + a^3 + a^2 b - ab^2 - b^3. \tag{13}$$

La courbe E possède un unique point d'ordre 2 rationnel sur $\mathbb{Q}$, à savoir $(b-a, 0)$.

On a $\mathfrak{D}(f) = -16$ et les invariants standard (c_4, c_6, Δ) associés à E sont les suivants (cf. (9) et [38]) :

$$\begin{cases} c_4 = -32\big(a^2 + 4ab + b^2\big), \\ c_6 = -128\big(5a^3 + 3a^2 b - 3ab^2 - 5b^3\big), \\ \Delta = -2^8 F(a,b)^2 = -2^8 c^{2p} d^2. \end{cases} \tag{14}$$

Rappelons que N_E désigne le conducteur de E et Δ_E son discrimant minimal. Posons

$$r = \prod_{\ell \mid cd,\, \ell \neq 2} \ell.$$

Lemme 3.5. *La courbe E est semi-stable en dehors de* 2. *Elle a réduction additive en* 2. *L'équation* (13) *est globalement minimale.*

(1) *Supposons d impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a*

$$N_E = \begin{cases} 2^6 r & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 r & \text{si } ab \text{ est pair.} \end{cases}$$

L'invariant modulaire j de E est entier en 2 *si et seulement si ab est pair.*

(2) *Supposons $v_2(d) = 1$. Alors on a*

$$ab \equiv -1 \pmod 4 \quad \text{et} \quad N_E = 2^6 r.$$

L'invariant modulaire j de E n'est pas entier en 2.

(3) *Supposons $v_2(d) = 2$. Alors ab est impair et on a*

$$N_E = \begin{cases} 2^5 r & \text{si } ab \equiv 1 \pmod 4, \\ 2^6 r & \text{si } ab \equiv -1 \pmod 4. \end{cases}$$

L'invariant modulaire j de E est entier en 2 *si et seulement si $ab \equiv 1 \pmod 4$.*

De plus, si ℓ est un nombre premier impair, alors p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

Démonstration. Soit ℓ un nombre premier impair. Supposons tout d'abord que l'entier ℓ divise Δ. D'après l'expression (14) ci-dessus, l'entier ℓ divise alors

$$F(a,b) = (a+b)\left(a^2+b^2\right) = dc^p. \tag{15}$$

Remarquons que ℓ ne divise pas ab. Dans le cas contraire, l'entier a, par exemple, serait divisible par ℓ. Cela entrainerait que ℓ divise b (car ℓ divise $F(a,b)$) ce qui est contraire au fait que les entiers a et b sont premiers entre eux.

On en déduit que ℓ ne divise pas c_4. En effet, on a

$$c_4 \equiv \begin{cases} -2^6 ab \pmod \ell & \text{si } \ell \text{ divise } a+b, \\ -2^7 ab \pmod \ell & \text{si } \ell \text{ divise } a^2+b^2. \end{cases}$$

L'équation (13) est donc minimale en ℓ et la courbe E a mauvaise réduction de type multiplicatif en ℓ. On a $v_\ell(\Delta) = v_\ell(\Delta_E)$.

D'autre part, si ℓ ne divise pas Δ, la courbe E a bonne réduction en ℓ et l'équation (13) est minimale en ℓ.

Par ailleurs, on a dans les deux cas,

$$v_\ell(\Delta_E) = v_\ell(\Delta) \equiv 2v_\ell(d) \pmod p.$$

En particulier, p divise $v_\ell(\Delta_E)$ si et seulement si ℓ ne divise pas d.

Étudions à présent la minimalité de (13) et le type de réduction de E en 2.

(1) Supposons ab impair. Alors,

$$F(a,b) \equiv 2(a+b) \pmod 8 \quad \text{et} \quad v_2(c_4) = 6.$$

(a) Si $ab \equiv 1 \pmod 4$, alors $v_2(F(a,b)) = 2$ donc nécessairement $v_2(d) = 2$ et c est impair. On vérifie que l'on a

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (6, \geqslant 9, 12). \tag{16}$$

D'après le tableau II de [29], l'équation (13) est minimale en 2 et on est dans le cas I_ν^* avec $\nu = 2$ ou $\nu = 3$. Avec l'algorithme de Tate [38, p. 50] on trouve $\nu = 3$ et on a $v_2(N_E) = 5$. De plus, l'invariant j est entier en 2 dans ce cas.

(b) Si $ab \equiv -1 \pmod 4$, alors $v_2(F(a,b)) \geqslant 3$, donc c est pair. De plus,

$$v_2(\Delta) = 8 + 2v_2(d) + 2pv_2(c) \geqslant 22.$$

Par ailleurs, on a

$$-\frac{c_6}{128} \equiv 5a + 3b - 3a - 5b \equiv 4a \pmod 8.$$

On en déduit

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (6, 9, \geqslant 22).$$

D'après [29], l'équation (13) est minimale en 2 et on a $v_2(N_E) = 6$. L'invariant j n'est pas entier en 2.

(2) Supposons ab pair. La solution (a,b,c) étant propre, a est pair et b impair (ou a est impair et b pair). On en déduit que c et d sont nécessairement impairs. D'où

$$\big(v_2(c_4), v_2(c_6), v_2(\Delta)\big) = (5, 7, 8). \tag{17}$$

D'après [29], l'équation (13) est minimale en 2 et on a $v_2(N_E) = 7$. L'invariant j de E est entier en 2.

D'où le résultat. □

3.2. La représentation ρ_p^E

Lemme 3.6. *La représentation ρ_p^E est (absolument) irréductible.*

Démonstration. La courbe E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, donc d'après le lemme 2.5, la représentation ρ_p^E est irréductible pour $p \geqslant 11$. Posons $t = a/b$. Alors, l'égalité $j = -15^3$ ou 255^3 (où j est l'invariant modulaire de E) conduit à

$$2^7 \frac{(t^2+4t+1)^3}{t^3+t^2+t+1} = -15^3 \text{ ou } 255^3.$$

Or ces équations n'ont pas de solution rationnelle comme on le vérifie facilement. Cela démontre l'irréductibilité de ρ_7^E et le lemme. □

Lemme 3.7. *On a $k = 2$ si p ne divise pas d et $k = p + 1$ sinon.*

Démonstration. Supposons que p ne divise pas d. Alors d'après les lemmes 2.6 et 3.5, on a $k = 2$.

Supposons que p divise d. D'après le lemme 3.5, la courbe E a alors réduction de type multiplicatif en p et p ne divise pas $v_p(\Delta_E)$. Cela conduit à $k = p + 1$, d'où le résultat. □

Posons

$$r' = \prod_{\ell \mid d,\, \ell \neq 2, p} \ell.$$

Lemme 3.8.

(1) *On suppose que d est impair. Alors, $ab \not\equiv 1 \pmod 4$ et on a*

$$N\big(\rho_p^E\big) = \begin{cases} 2^6 r' & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 r' & \text{si } ab \text{ est pair.} \end{cases}$$

(2) *On suppose que $v_2(d) = 1$. Alors on a*

$$ab \equiv -1 \pmod 4 \quad \text{et} \quad N\big(\rho_p^E\big) = 2^6 r'.$$

(3) *On suppose que $v_2(d) = 2$. Alors ab est impair et on a*

$$N\big(\rho_p^E\big) = \begin{cases} 2^5 r' & \text{si } ab \equiv 1 \pmod 4, \\ 2^6 r' & \text{si } ab \equiv -1 \pmod 4. \end{cases}$$

Démonstration. Soit $\ell \neq p$ un nombre premier impair de mauvaise réduction. D'après le lemme 3.5, ℓ divise cd, l'équation (13) est minimale en ℓ et E a mauvaise réduction de type multiplicatif en ℓ.

Supposons que ℓ ne divise pas d. Alors, $v_\ell(\Delta_E)$ est multiple de p (lemme 3.5). On en déduit que $v_\ell(N(\rho_p^E)) = 0$ [19, p. 28].

Supposons que ℓ divise d. Alors, $v_\ell(\Delta_E)$ n'est pas multiple de p (lemme 3.5) et on a $v_\ell(N(\rho_p^E)) = 1$ [19, p. 28].

D'après le lemme 3.5, la courbe E a donc réduction additive en 2 et on a $v_2(N(\rho_p^E)) = v_2(N_E)$ [19, p. 28]. D'où le lemme. □

3.3. Démonstrations des théorèmes 3.1, 3.2 et 3.3

On suppose dans tout ce paragraphe qu'il existe $(a, b, c) \in S_p(d)$ où p est un nombre premier $\geqslant 7$ et d l'un des entiers considérés dans les énoncés des théorèmes 3.1, 3.2 et 3.3.

Notations et rappels. Soit $n \in \mathbb{N}^*$. On désigne par $\mathcal{S}_2^+(n)$ l'espace des newform (au sens de [1]) de poids 2 pour le sous-groupe $\Gamma_0(n)$ de $\mathrm{SL}_2(\mathbb{Z})$. On dit que $f \in \mathcal{S}_2^+(n)$ est normalisée si son développement de Fourier à l'infini s'écrit

$$f = q + \sum_{m \geqslant 2} a_m(f) q^m, \quad \text{avec } q = e^{2i\pi\tau}.$$

Il y a exactement $\dim_{\mathbb{C}}(\mathcal{S}_2^+(n))$ formes normalisées dans $\mathcal{S}_2^+(n)$. Pour une telle forme, notons K_f le corps de rationalité des coefficients $a_m(f)$, $m \geqslant 2$, et $\mathrm{N}_{K_f/\mathbb{Q}}$ la norme de l'extension $K_f/\mathbb{Q}$.

Si $A/\mathbb{Q}$ est une courbe elliptique, on note

$$L_A(s) = \sum_{m \geqslant 0} a_m(A) m^{-s}$$

sa fonction L de Hasse–Weil.

Rappelons le résultat bien connu suivant (cf. par exemple [33]).

Proposition 3.9. *Il existe $f \in \mathcal{S}_k^+(N(\rho_p^E))$ normalisée telle que pour tout nombre premier ℓ, les conditions suivantes soient réalisées.*

(1) *Si ℓ divise N_E et ne divise pas $pN(\rho_p^E)$, alors*

$$p \text{ divise } \mathrm{N}_{K_f/\mathbb{Q}}\big(a_\ell(f) \pm (\ell+1)\big).$$

(2) *Si ℓ ne divise pas pN_E, alors il existe un entier $r \leqslant \sqrt{l}$ tel que*

$$p \text{ divise } \mathrm{N}_{K_f/\mathbb{Q}}\big(a_\ell(f) \pm 2r\big).$$

Pour l'assertion (3.9), on utilise le fait que, comme E a un point d'ordre 2 rationnel sur $\mathbb{Q}$, le coefficient $a_\ell(E)$ est pair. On a de plus $|a_\ell(E)| \leqslant 2\sqrt{\ell}$ d'après les bornes de Weil.

Si f, vérifiant les conditions de la proposition 3.9, a ses coefficients $a_m(f)$ dans $\mathbb{Z}$, alors elle correspond à une courbe elliptique E_f de conducteur $N(\rho_p^E)$ définie sur $\mathbb{Q}$ et les représentations ρ_p^E et $\rho_p^{E_f}$ sont isomorphes.

Soit $\mathbb{Q}(E[p])/\mathbb{Q}$ l'extension de $\mathbb{Q}$ engendrée par les coordonnées des points de p-torsion de E. C'est une extension galoisienne de $\mathbb{Q}$. Soit e son indice de ramification en 2.

Lemme 3.10. *Supposons $ab \equiv -1 \pmod 4$. On a $e = 2p$.*

Démonstration. Supposons $ab \equiv -1 \pmod 4$. D'après lemme 3.5, l'invariant modulaire j de E n'est pas entier en 2. De plus, on a

$$v_2(j) = 18 - \big(8 + 2v_2(d) + 2pv_2(c)\big) \equiv 10 - 2v_2(d) \not\equiv 0 \pmod p$$

car $v_2(d) = 0$ ou 1 par hypothèse. On en déduit $e = 2p$ [7, cor. 1]. □

3.3.1. Démonstration du théorème 3.1

Supposons $d = 1$. D'après le lemme 3.8, on a

$$N(\rho_p^E) = \begin{cases} 2^6 & \text{si } ab \equiv -1 \pmod 4, \\ 2^7 & \text{si } ab \text{ est pair.} \end{cases}$$

Supposons $ab \equiv -1 \pmod 4$. L'espace $\mathcal{S}_2^+(64)$ n'est constitué que d'une seule classe de $\mathbb{Q}$-isogénie de courbe elliptique de conducteur 64. Par ailleurs, la courbe E a potentiellement réduction multiplicative en 2 et son défaut de semi-stabilité en 2 est d'ordre $2p$ (lemme 3.10). Or, les courbes de conducteur 64 ont réduction additive en 2 et leur invariant modulaire est entier. Si A est une telle courbe, l'indice de ramification en 2 de l'extension $\mathbb{Q}(A[p])/\mathbb{Q}$ est 8 (cf. [8] et [18]). Les représentations ρ_p^E et ρ_p^A ne sont donc pas isomorphes. On en déduit que ab est pair. D'où le théorème 3.1.

3.3.2. Démonstration du théorème 3.2

Supposons que $d \in \{2, 6, 10, 22\}$. D'après le lemme 3.8, on a $ab \equiv -1 \pmod 4$ et

$$N(\rho_p^E) = \begin{cases} 2^6 & \text{si } d = 2, \\ 2^6 \cdot 3 & \text{si } d = 6, \\ 2^6 \cdot 5 & \text{si } d = 10, \\ 2^6 \cdot 11 & \text{si } d = 22 \text{ et } p \neq 11, \\ 2^6 & \text{si } d = 22 \text{ et } p = 11. \end{cases}$$

De plus, d'après le lemme 3.10, on a $e = 2p$.

3.3.2.1. Supposons $d = 2$. On a alors $N(\rho_p^E) = 64$. On montre, avec le même argument qu'au paragraphe 3.3.1, que l'ensemble $S_p(2)$ est vide.

3.3.2.2. Supposons $d = 6$. L'espace $\mathcal{S}_2^+(192)$ est de dimension 4 et engendré par quatre classes de $\mathbb{Q}$-isogénie de courbes elliptiques définies sur $\mathbb{Q}$ (cf. [37]). Toutes ont réduction additive en 2 et un invariant modulaire entier en 2. Leur défaut de semi-stabilité en 2 est d'ordre 8 ou 24 (cf. [8] et [18]). En particulier, il est différent de $2p$. On en déduit que l'ensemble $S_p(6)$ est vide.

3.3.2.3. Supposons $d = 10$. L'espace $\mathcal{S}_2^+(320)$ est engendré par six classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 320 et deux formes modulaires f_1 et f_2 dont les coefficients de Fourier sont conjugués sur $\mathbb{Q}(\sqrt{2})$ (cf. [37]). La forme $f = f_1$ ou f_2 est à coefficients dans l'anneau d'entiers du corps K_f engendré sur $\mathbb{Q}$ par une racine α du polynôme $X^2 - 8$ [37]. Avec les notations de la proposition 3.9, on a pour $\ell = 3$, le tableau suivant.

$a_3(f)$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) \pm 4)$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f))$	$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) \pm 2)$
α	8	-8	-4

La forme f ne vérifie donc pas les conditions de la proposition 3.9. On en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbb{Q}$ de conducteur 320. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2 (leur défaut de semi-stabilité en 2 divise 24 d'après [31, p. 386], en particulier il est différent de $2p$). L'ensemble $S_p(10)$ est donc vide.

3.3.2.4. Supposons $d = 22$ et $p \neq 11$. L'espace $\mathcal{S}_2^+(704)$ est constitué de douze classes de $\mathbb{Q}$-isogénie de courbes elliptiques de conducteur 704 et de huit formes modulaires. Chacune de ces huit formes est conjuguée par l'action de $G_{\mathbb{Q}}$ à l'une des quatre formes notées 704M1, 704N1, 704O1 et 704P1 dans [37]. Avec les notations de la proposition 3.9, on a le tableau suivant pour $\ell = 3$.

Newform f	704M1	704N1	704O1	704P1
Polynôme P_f tel que				
$K_f = \mathbb{Q}(\alpha)$ et $P_f(\alpha) = 0$	$X^2 + X - 4$	$X^2 - X - 4$	$X^2 + X - 4$	$X^2 - X - 4$
$a_3(f)$	α	α	α	α
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) + 4)$	8	16	8	16
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) - 4)$	16	8	16	8
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f))$	-4	-4	-4	-4
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) + 2)$	-2	2	-2	2
$\mathrm{N}_{K_f/\mathbb{Q}}(a_3(f) - 2)$	2	-2	2	-2

Aucune de ces formes ne vérifiant les conditions de la proposition 3.9, on en déduit que ρ_p^E est isomorphe à la représentation ρ_p^A d'une courbe elliptique $A/\mathbb{Q}$ de conducteur 704. C'est absurde car elles ont toutes réduction additive en 2 et un invariant modulaire entier en 2. L'ensemble $S_p(22)$ est donc vide dans ce cas.

3.3.2.5. Supposons $d = 22$ et $p = 11$. La représentation ρ_{11}^E est irréductible, de poids 12 (lemme 3.7) et de conducteur 64. Je remercie le referee de m'avoir signalé que ρ_{11}^E « provient » alors d'une newform de poids 2 et de niveau $12 \cdot 64 = 704$ (voir [30, (2.2)] et [12, lem. 2.1]). Autrement dit, de façon analogue à la proposition 3.9, il existe $f \in \mathcal{S}_2^+(12 \cdot 64)$ normalisée telle pour tout nombre premier $\ell \neq 2, 11$, les conditions suivantes soient réalisées :

(1) si ℓ divise N_E, alors 11 divise $\mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm (\ell + 1))$.
(2) Il existe un entier $r \leqslant \sqrt{l}$ tel que 11 divise $\mathrm{N}_{K_f/\mathbb{Q}}(a_\ell(f) \pm 2r)$.

On contredit alors l'existence d'une telle forme par les mêmes arguments qu'à l'alinéa précédent. On en déduit que l'ensemble $S_{11}(22)$ est vide.

Cela démontre le théorème 3.2.

3.3.3. Démonstration du théorème 3.3

Supposons $d = 2\ell$, où ℓ est un nombre premier $\geqslant 13$ satisfaisant à la propriété (P). La représentation ρ_p^E est alors irréductible pour $p \geqslant 7$ et de poids 2 dès que $p \neq \ell$ (lemmes 3.6 et 3.7). On a alors $ab \equiv -1 \pmod 4$ et $N(\rho_p^E) = 2^6\ell$.

D'après [20, th. 3], il existe une constante $\kappa(\ell) > \ell$ ne dépendant que de ℓ vérifiant la condition suivante : si $p > \kappa(\ell)$, alors il existe une courbe elliptique E' définie sur $\mathbb{Q}$, de conducteur $N(\rho_p^E) = 2^6\ell$, telle que les représentations ρ_p^E et $\rho_p^{E'}$ soient isomorphes.

Quitte à augmenter $\kappa(\ell)$, on peut de plus supposer que E' a un point d'ordre 2 rationnel sur $\mathbb{Q}$ (cf. démonstration du th. 4 de [20] et [34, IV-6]).

Lorsqu'il n'existe pas de courbe elliptique sur $\mathbb{Q}$ de conducteur 64ℓ ayant au-moins un point d'ordre 2 rationnel sur $\mathbb{Q}$, on a une contradiction. Or c'est précisément le cas lorsque ℓ vérifie la

propriété (P) d'après un théorème de W. Ivorra (cf. [16]). D'après [20], on peut prendre $\kappa(\ell) = (4\sqrt{\ell+1}+1)^{4(\ell-1)}$. On en déduit le théorème 3.3.

Remarque 3.11. Pour caractériser l'existence de courbe elliptique sur $\mathbb{Q}$ ayant un point d'ordre deux rationnel sur $\mathbb{Q}$ et un conducteur 64ℓ, Ivorra [16] utilise les bornes données par Beukers (corollaires 1 et 2 de [4]) sur les solutions de l'équation de Ramanujan–Nagell. Ces bornes ont depuis été améliorées par Bauer et Bennett [2]. Notre définition de la fonction g prend en compte ces améliorations (lorsque $2^9 \leqslant n < 2^{362}$ on a adapté la démonstration du corollaire 2 de [4] aux nouvelles bornes).

4. Remarques en degré $\geqslant 3$

4.1. Courbe de Frey en degré 6

Soit F un polynôme homogène de degré 6 séparable à coefficients entiers. Sous certaines conditions portant sur F, on peut, comme à la partie 2, construire une courbe elliptique ayant de bonnes propriétés de réduction, associée à l'équation (1).

Par exemple, pour $F(x,y) = \Phi_9(x,y) = x^6 + x^3y^3 + y^6$, on obtient la courbe elliptique suivante :

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{cases} a_2 = 3ab, \\ a_4 = -3\big(a^4 - a^3b + 2a^2b^2 - ab^3 + b^4\big), \\ a_6 = a^6 - 9a^5b + 9a^4b^2 - 19a^3b^3 + 9a^2b^4 - 9ab^5 + b^6. \end{cases} \tag{18}$$

Son discriminant est $\Delta = 2^4 \cdot 3^4 \cdot \Phi_9(a,b)^2$. Elle est semi-stable en dehors de 2 et 3. Une telle courbe devrait permettre d'obtenir des résultats analogues à ceux de la partie 3 pour la forme $F = \Phi_9$.

4.2. Détermination des solutions entières de certaines équations superelliptiques

Dans les parties 2 et 3, on a associé une courbe de Frey à une équation diophantienne donnée. On illustre ici sur un exemple la possibilité de montrer la vacuité de l'ensemble des solutions d'une équation en partant de la donnée d'une courbe elliptique bien choisie.

Soit t une indéterminée. On considère la courbe $E/\mathbb{Q}[t]$ d'équation :

$$E\colon\ y^2 + txy = x^3 + (1+t)x.$$

Ses coefficients $\Delta(t)$ et $c_4(t)$ sont les éléments suivants de $\mathbb{Q}[t]$:

$$\Delta(t) = t^6 + 2t^5 + t^4 - 64t^3 - 192t^2 - 192t - 64,$$
$$c_4(t) = t^4 - 48t - 48.$$

De plus, si R désigne leur résultant, on a :

$$R = 2^{16}.$$

Autrement dit, la courbe E est semi-stable en dehors de 2. On spécialise en t entier. Si t est divisible par 4, la valuation en 2 de $\Delta(t)$ est 6. De même, si $v_2(t) = 1$, alors $v_2(\Delta(t)) = 4$. Enfin, si t est impair, $\Delta(t)$ est pair et $c_4(t)$ impair.

Par ailleurs, $(0, 0)$ est un point d'ordre 2 de E rationnel sur $\mathbb{Q}$. La représentation ρ_p^E est donc irréductible pour $p \geqslant 11$ (lemme 2.5). De plus, l'invariant modulaire j de E est différent de -15^3 et 255^3. On en déduit que ρ_7^E est également irréductible (lemme 2.5).

On suppose à présent qu'il existe un entier c tel que t vérifie l'équation superelliptique :

$$\Delta(t) = c^p,$$

où p est un nombre premier $\geqslant 7$. D'après les remarques ci-dessus, t est impair. Dans ce cas, la courbe E est semi-stable et la représentation ρ_p^E est de poids 2 et de conducteur 1. C'est absurde. Cela contredit l'existence de c.

Remerciements

Je remercie M. Hindry et A. Kraus pour les conversations que j'ai eues avec eux pendant la préparation de ce travail.

Appendice A. La conjecture *abc* implique la conjecture (A)

Dans [24], M. Langevin montre que la conjecture *abc* est équivalente à la conjecture suivante.

Conjecture A.1. *Soient $F \in \mathbb{Z}[X, Y]$ une forme homogène séparable de degré $\geqslant 3$ et ε un réel > 0. Il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que pour tout couple (a, b) d'entiers non nuls premiers entre eux, on a* :

$$\operatorname{rad}\big(F(a,b)\big) \geqslant C_{\varepsilon,F} \max\big(|a|, |b|\big)^{\deg(F)-2-\varepsilon},$$

où $\operatorname{rad}(n)$*, $n \in \mathbb{N}^*$, désigne le produit de tous les nombres premiers divisant n.*

Déduisons la conjecture (A) de cet énoncé.

Proposition A.2. *La conjecture abc implique la conjecture* (A).

Démonstration. Soient F une forme homogène séparable de degré $\geqslant 3$ à coefficients entiers relatifs et d un entier $\geqslant 1$. On considère (a, b, c) une solution propre et non triviale de (1). Posons

$$a' = \frac{a}{\operatorname{pgcd}(a,b)} \quad \text{et} \quad b' = \frac{b}{\operatorname{pgcd}(a,b)},$$

où $\operatorname{pgcd}(a, b)$ désigne le pgcd de a et b. Les entiers a, b et c étant premiers entre eux, on en déduit que $(\operatorname{pgcd}(a, b))^{\deg(F)}$ divise d. On a alors

$$F(a',b') = d'c^p, \quad \text{où } d' = \frac{d}{(\operatorname{pgcd}(a,b))^{\deg(F)}}. \tag{A.1}$$

Les entiers a' et b' étant premiers entre eux, on déduit de la conjecture ci-dessus que pour tout $\varepsilon > 0$, il existe une constante $C_{\varepsilon,F} > 0$ ne dépendant que de ε et F telle que

$$\operatorname{rad}\big(F(a',b')\big) \geqslant C_{\varepsilon,F} \max\big(|a'|,|b'|\big)^{\deg(F)-2-\varepsilon}. \tag{A.2}$$

Or, d'après (A.1), on a $\operatorname{rad}(F(a',b')) \leqslant |d'c|$. Par ailleurs, il existe une constante M_F ne dépendant que de F telle que

$$\max\big(|a'|,|b'|\big)^{\deg(F)} \geqslant M_F\big|d'c^p\big|.$$

On déduit alors de (A.2) l'inégalité suivante

$$|d'c| \geqslant C_{\varepsilon,F}\big(M_F\big|d'c^p\big|\big)^{\alpha}, \quad \text{où } \alpha = 1 - \frac{2+\varepsilon}{\deg(F)}.$$

Supposons $\varepsilon < 1$. On a alors $0 < \alpha < 1$ et

$$|c|^{\alpha p-1} \leqslant \frac{|d'|^{1-\alpha}}{C_{\varepsilon,F} M_F^{\alpha}}.$$

Pour p suffisamment grand, cela implique $c = \pm 1$. C'est le résultat voulu. □

Appendice B. La conjecture *abc* implique la conjecture de Frey–Mazur

La conjecture de Szpiro (forme faible) affirme l'existence de constantes absolues α et β telles que pour toute courbe elliptique A définie sur $\mathbb{Q}$, on ait

$$|\Delta_A| < \alpha N_A^{\beta}, \tag{B.1}$$

où Δ_A désigne le discriminant minimal de A et N_A son conducteur. Cet énoncé est une conséquence de la conjecture *abc* (cf. [28]). Nous allons montrer qu'il implique la conjecture de Frey–Mazur.

Proposition B.1. *La conjecture abc implique la conjecture de Frey–Mazur.*

Ce résultat m'a été communiqué par A. Kraus. Il figure, sous forme de notes non publiées, dans les Comptes-Rendus du Séminaire de Théorie des Nombres de Caen (exposé XVIII, année 1989–1990).

Démonstration. Rappelons le résultat suivant. □

Lemme B.2. *Soient A et A' deux courbes elliptiques définies sur $\mathbb{Q}$ telles que pour une infinité de nombres premiers p, les modules galoisiens des points de p-torsion de A et A' soient isomorphes. Alors, les courbes A et A' sont isogènes.*

Démonstration (lemme B.2). Notons S la réunion des places de mauvaise réduction de A et A'. Si en un nombre premier p les modules galoisiens des points de p-torsion de A et A' sont isomorphes, on a

$$a_\ell(A) \equiv a_\ell(A') \pmod{p} \quad \text{pour } \ell \notin S \cup \{p\} \quad \text{(cf. [31, 5.2])}.$$

Par hypothèse, ces congruences sont satisfaites pour une infinité de nombres premiers p. On en déduit les égalités

$$a_\ell(A) = a_\ell(A') \quad \text{pour } \ell \notin S.$$

D'après un théorème de G. Faltings, cela implique que les courbes A et A' sont isogènes [14, §5, cor. 2]. D'où le lemme. □

Soit A une courbe elliptique définie sur $\mathbb{Q}$. Si ℓ est un nombre premier, on rappelle que v_ℓ désigne la valuation ℓ-adique de $\mathbb{Q}$. Considérons un nombre premier $p \in \mathcal{F}_A$, c'est-à-dire pour lequel il existe une courbe elliptique $A^{(p)}$ définie sur $\mathbb{Q}$ telle que les représentations ρ_p^A et $\rho_p^{A^{(p)}}$ soient isomorphes. D'après [19, p. 28], il existe une constante $c(A) > 7$ ne dépendant que de A telle que si $p > c(A)$ alors

$$N\big(\rho_p^A\big) = N_A. \tag{B.2}$$

Les représentations ρ_p^A et $\rho_p^{A^{(p)}}$ étant isomorphes, on a, en particulier,

$$N\big(\rho_p^A\big) = N\big(\rho_p^{A^{(p)}}\big). \tag{B.3}$$

On en déduit que N_A divise $N_{A^{(p)}}$. On écrit

$$N_{A^{(p)}} = N_A \cdot u_p. \tag{B.4}$$

Montrons alors que u_p^p divise le discriminant minimal $\Delta_{A^{(p)}}$ de $A^{(p)}$.

On considère pour cela un nombre premier $\ell \neq p$. Alors

$$v_\ell\big(N\big(\rho_p^{A^{(p)}}\big)\big) = v_\ell(N_{A^{(p)}})$$

sauf si $A^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{A^{(p)}})$ [19, p. 28]. Autrement dit, si ℓ divise u_p, alors, d'après les égalités (B.2) et (B.3) et la remarque ci-dessus, $A^{(p)}$ a en ℓ réduction multiplicative et p divise $v_\ell(\Delta_{A^{(p)}})$. En particulier, $v_\ell(u_p) = 1$.

L'entier $N(\rho_p^A)$ est, par définition, premier à p. D'après l'égalité (B.2), la courbe A a donc bonne réduction en p et le poids de ρ_p^A est 2 (cf. [32]). On en déduit que la représentation $\rho_p^{A^{(p)}}$ est également de poids 2 et que l'on est dans l'un des cas suivants :

(1) la courbe $A^{(p)}$ a bonne réduction en p ;
(2) la courbe $A^{(p)}$ a mauvaise réduction multiplicative en p et l'exposant de p dans $\Delta_{A^{(p)}}$ est multiple de p ;
(3) la courbe $A^{(p)}$ a mauvaise réduction additive en p.

Or d'après [19, p. 6], si $A^{(p)}$ a mauvaise réduction additive en p et si $\rho_p^{A^{(p)}}$ est de poids 2, alors, $p \leqslant 7$. C'est absurde car on a supposé $p > c(A) > 7$. Le cas (3) ne peut donc pas se produire.

On en déduit donc, comme annoncé, que u_p^p divise $\Delta_{A^{(p)}}$. On applique à présent l'inégalité (B.1) à la courbe $A^{(p)}$. On a :

$$|\Delta_{A^{(p)}}| < \alpha N_{A^{(p)}}^{\beta}.$$

Or d'après l'égalité (B.4) et le fait que u_p^p divise $\Delta_{A^{(p)}}$, on a

$$|u_p|^{p-\beta} < \alpha N_A^{\beta}.$$

Il existe donc une constante $p(A)$ ne dépendant que de A telle que si $p > p(A)$, alors $u_p = 1$. On en déduit

$$N_{A^{(p)}} = N_A.$$

Or, à $\mathbb{Q}$-isomorphisme près, il n'y a qu'un nombre fini de courbes elliptiques de conducteur donné. Le lemme B.2 entraîne alors le résultat.

Références

[1] A.O.L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, Math. Ann. 185 (1970) 134–160.
[2] M. Bauer, M.A. Bennett, Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation, Ramanujan J. 6 (2) (2002) 209–270.
[3] M.A. Bennett, V. Vatsal, S. Yazdani, Ternary Diophantine equations of signature $(p, p, 3)$, Compos. Math. 140 (6) (2004) 1399–1416.
[4] F. Beukers, On the generalized Ramanujan–Nagell equation, I, Acta Arith. 38 (4) (1980/81) 389–410.
[5] N. Billerey, Équations de Fermat de type $(5, 5, p)$, Bull. Austral. Math. Soc. 76 (2) (2007) 161–194.
[6] Y. Bugeaud, G. Hanrot, M. Mignotte, Sur l'équation diophantienne $(x^n - 1)/(x - 1) = y^q$, III, Proc. London Math. Soc. (3) 84 (1) (2002) 59–78.
[7] É Cali, A. Kraus, Sur la p-différente du corps des points de l-torsion des courbes elliptiques, $l \neq p$, Acta Arith. 104 (1) (2002) 1–21.
[8] J.E. Cremona, Algorithms for Modular Elliptic Curves, second ed., Cambridge Univ. Press, Cambridge, 1997.
[9] H. Darmon, The equation $x^4 - y^4 = z^p$, C. R. Math. Rep. Acad. Sci. Canada 15 (6) (1993) 286–290.
[10] H. Darmon, Serre's conjectures, in: Seminar on Fermat's Last Theorem, Toronto, ON, 1993–1994, in: CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 135–153.
[11] H. Darmon, A. Granville, On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27 (6) (1995) 513–543.
[12] F. Diamond, The refined conjecture of Serre, in: Elliptic Curves, Modular Forms, & Fermat's Last Theorem, Hong Kong, 1993, in: Ser. Number Theory, vol. I, Int. Press, Cambridge, MA, 1995, pp. 22–37.
[13] J.S. Ellenberg, Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$, Amer. J. Math. 126 (4) (2004) 763–787.
[14] G. Faltings, Finiteness theorems for abelian varieties over number fields, in: Arithmetic Geometry, Storrs, CT, 1984, Springer, New York, 1986, pp. 9–27.
[15] M. Hindry, J.H. Silverman, Diophantine geometry, Grad. Texts in Math., vol. 201, Springer-Verlag, New York, 2000, an introduction.
[16] W. Ivorra, Courbes elliptiques sur $\mathbf{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbf{Q}$, de conducteur $2^N p$, Dissertationes Math. (Rozprawy Mat.) 429 (2004) 55.
[17] M.A. Kenku, On the number of $\mathbf{Q}$-isomorphism classes of elliptic curves in each $\mathbf{Q}$-isogeny class, J. Number Theory 15 (2) (1982) 199–202.
[18] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, Manuscripta Math. 69 (4) (1990) 353–385.

[19] A. Kraus, Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique, Dissertationes Math. (Rozprawy Mat.) 364 (1997) 39.
[20] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, Canad. J. Math. 49 (6) (1997) 1139–1161.
[21] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, Experiment. Math. 7 (1) (1998) 1–13.
[22] A. Kraus, On the equation $x^p + y^q = z^r$: A survey, Ramanujan J. 3 (3) (1999) 315–333.
[23] A. Kraus, Une question sur les équations $x^m - y^m = Rz^n$, Compos. Math. 132 (1) (2002) 1–26.
[24] M. Langevin, Imbrications entre le théorème de Mason, la descente de Belyi et les différentes formes de la conjecture (abc), J. Théor. Nombres Bordeaux 11 (1) (1999) 91–109, les XXèmes Journées Arithmétiques (Limoges, 1997).
[25] G. Ligozat, Courbes modulaires de genre 1, Mém. Bull. Soc. Math. France 43 (1975), supplément au Bull. Soc. Math. France, Tome 103, no. 3.
[26] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. 44 (2) (1978) 129–162.
[27] T. Nagell, Collected Papers of Trygve Nagell, vol. 1, Queen's Papers in Pure and Appl. Math., vol. 121, Queen's University, Kingston, ON, 2002, edited by Paulo Ribenboim and with a short biography of Nagell by J.W.S. Cassels [reprinted from Acta Arith. 55 (1990), no. 2, 109–112].
[28] J. Oesterlé, Nouvelles approches du "théorème" de Fermat, Astérisque 161–162 (1988) 165–186, séminaire Bourbaki, vol. 1987/88, exp. No. 694, 4.
[29] I. Papadopoulos, Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3, J. Number Theory 44 (2) (1993) 119–152.
[30] K.A. Ribet, Report on mod l representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, in: Motives, Seattle, WA, 1991, in: Proc. Sympos. Pure Math., vol. 55, Amer. Math. Soc., Providence, RI, 1994, pp. 639–676.
[31] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (4) (1972) 259–331.
[32] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. 54 (1) (1987) 179–230.
[33] J.-P. Serre, Travaux de Wiles (et Taylor, ...). I, Astérisque 237 (1996) 319–332, séminaire Bourbaki, vol. 1994/95, exp. No. 803, 5.
[34] J.-P. Serre, Abelian l-Adic Representations and Elliptic Curves, Res. Notes Math., vol. 7, A K Peters Ltd., Wellesley, MA, 1998, with the collaboration of Willem Kuyk and John Labute, revised reprint of the 1968 original.
[35] J.H. Silverman, The Arithmetic of Elliptic Curves, Grad. Texts in Math., vol. 106, Springer-Verlag, New York, 1992, corrected reprint of the 1986 original.
[36] V.G. Sprindžuk, Classical Diophantine Equations, Lecture Notes in Math., vol. 1559, Springer-Verlag, Berlin, 1993.
[37] W. Stein, The modular forms database, http://modular.math.washington.edu/Tables.
[38] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in: Modular Functions of One Variable, IV, Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972, in: Lecture Notes in Math., vol. 476, Springer, Berlin, 1975, pp. 33–52.

Semi-stabilité des courbes elliptiques

Nicolas Billerey

Dissertationes Mathematicae 468 (2009), 1-57

Table des matières

Abstract

Let K be a finite extension of $\mathbb{Q}_2$ complete with a discrete valuation v, $\overline{K}$ an algebraic closure of K, and K_{nr} its maximal unramified subextension. Let E be an elliptic curve defined over K with additive reduction over K and having an integral modular invariant j. There exists a smallest extension L of K_{nr} over which E has good reduction. For some congruences modulo 12 of the valuation $v(j)$ of j, we give the degree of the extension L/K_{nr}. When K is a quadratic ramified extension of $\mathbb{Q}_2$, we determine explicitly this degree in terms of the coefficients of a Weierstrass equation of E.

Remerciements. Je remercie vivement Alain Kraus pour les nombreuses discussions que j'ai eues avec lui durant la préparation de ce travail ainsi que pour sa relecture minutieuse du document.

2010 *Mathematics Subject Classification*: Primary 11G07.
Key words and phrases: elliptic curves over local fields.
Received 17.7.2008.

Introduction

Étant donnés un nombre premier p, une clôture algébrique $\overline{\mathbb{Q}_p}$ de $\mathbb{Q}_p$ et une extension finie K de $\mathbb{Q}_p$ contenue dans $\overline{\mathbb{Q}_p}$, on considère une courbe elliptique E définie sur K ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire j est entier. Il existe alors une plus petite extension L de la clôture non ramifiée K_{nr} de K dans $\overline{\mathbb{Q}_p}$ où E acquiert bonne réduction. Si E_n désigne le groupe des points de n-torsion de E, on a $L = K_{nr}(E_n)$ pour tout entier $n \geq 3$ non divisible par p ([4, §2, cor. 3]). Le groupe $\Phi = \mathrm{Gal}(L/K_{nr})$ est connu dans le cas où $p \geq 3$ ([2]). Lorsque $p = 2$, il est soit cyclique d'ordre 2, 3, 4 ou 6, soit d'ordre 8 et isomorphe à un groupe quaternionien, soit d'ordre 24 et isomorphe à $\mathrm{SL}_2(\mathbb{F}_3)$. La détermination précise du groupe Φ lorsque $p = 2$ n'a été menée que dans deux cas : par A. Kraus pour $K = \mathbb{Q}_2$ ([2]) et par É. Cali pour toutes les extensions finies $K/\mathbb{Q}_2$ non ramifiées ([1]).

Le présent travail a deux objectifs : d'une part, établir en fonction de la valuation de j modulo 12 plusieurs résultats généraux sur le groupe Φ, valables pour toute extension finie $K/\mathbb{Q}_2$ et, d'autre part, le déterminer explicitement en fonction des coefficients d'une équation de Weierstrass de E dans le cas des extensions quadratiques ramifiées de $\mathbb{Q}_2$. Combiné avec les travaux de Cali et Kraus, ce dernier résultat achève le calcul du groupe Φ pour toutes les extensions de $\mathbb{Q}_2$ de degré ≤ 2.

1. Énoncés des résultats

Soient K une extension finie de $\mathbb{Q}_2$ d'indice de ramification e, π une uniformisante de K et v la valuation de K normalisée par $v(\pi) = 1$. Soit E une courbe elliptique définie sur K d'invariant modulaire j ayant mauvaise réduction de type additif sur K et dont l'invariant modulaire est de valuation ≥ 0.

L'article se compose de deux parties. Dans la première on établit l'ordre du groupe Φ pour certaines valeurs de la congruence de $v(j)$ modulo 12. Les seuls résultats généraux connus sont les suivants ([2, th. 2]) :

1. Si $v(j) = 0$, alors on a $|\Phi| = 2$.
2. Supposons $v(j) \geq 12e$.
   (i) Si $v(j)$ est divisible par 3, on a $|\Phi| = 2$.
   (ii) Si $v(j)$ n'est pas divisible par 3, on a $|\Phi| = 3$ si le type de Néron de E est IV ou IV* et $|\Phi| = 6$ sinon.

En particulier, aucun résultat n'a été démontré si $0 < v(j) < 12e$. Dans ce cas, on obtient l'énoncé suivant.

THÉORÈME 1. *Supposons* $0 < v(j) < 12e$.

1. *Si* $v(j) \equiv \pm 3 \pmod{12}$, *alors* $|\Phi| = 8$.
2. *Si* $v(j) \equiv \pm 1 \pmod{12}$ *ou* $v(j) \equiv \pm 5 \pmod{12}$, *alors* $|\Phi| = 24$.
3. *Si* $v(j) \equiv \pm 2 \pmod{12}$ *et* $|6e - v(j)| > 2e$, *alors* $|\Phi| = 24$.

Dans tous les autres cas, la valuation de j ne suffit pas à déterminer l'ordre du groupe Φ (cf. [1] et le théorème 2 ci-dessous).

Dans la seconde partie de ce travail, on détermine le groupe Φ lorsque K est une extension quadratique ramifiée de $\mathbb{Q}_2$. Il y a exactement six telles extensions que l'on regroupe en deux ensembles de la façon suivante :

$$\Omega_1 = \{\mathbb{Q}_2(\sqrt{-1}), \mathbb{Q}_2(\sqrt{3})\}, \qquad \Omega_2 = \{\mathbb{Q}_2(\sqrt{2}), \mathbb{Q}_2(\sqrt{-2}), \mathbb{Q}_2(\sqrt{6}), \mathbb{Q}_2(\sqrt{-6})\}.$$

On suppose E donnée par une équation de Weierstrass entière, non nécessairement minimale, et dont (c_4, c_6, Δ) sont les invariants standard ([5]) qui lui sont associés. On a $j = c_4^3/\Delta$. Dans le cas où jc_6 est non nul, on pose

$$c_4 = \pi^{v(c_4)} c_4', \qquad c_6 = \pi^{v(c_6)} c_6', \qquad \Delta = \pi^{v(\Delta)} \Delta', \qquad j' = c_4'^3/\Delta'.$$

On introduit les conditions suivantes :

$$\Delta' \equiv 1 + \pi \pmod 2, \tag{C1}$$
$$c_4' \equiv 1 + \pi \pmod 2, \tag{C1$'$}$$
$$j' \equiv 1 + \pi^2 \pmod{\pi^3}, \tag{C2}$$
$$c_4' \equiv 1 + \pi^2 \pmod 4 \quad \text{ou} \quad c_4' \equiv 1 + \pi^3 \pmod 4. \tag{C3}$$

REMARQUES.

1. Les conditions ci-dessus sont indépendantes du modèle choisi pour représenter la courbe E. En particulier, il n'est pas nécessaire qu'il soit minimal.
2. Elles ne dépendent pas non plus du choix de l'uniformisante de K.

Notations. On note ε l'unité de l'anneau des entiers de K définie par

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2.$$

On définit alors les ensembles suivants de couples d'unités de l'anneau des entiers de K :

$$\begin{aligned}\mathcal{L}_1 = \{&(-\varepsilon^2 + 6 + \pi^6 + \pi^7, -\varepsilon), (-\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7, -\varepsilon + \pi^4),\\ &(-\varepsilon^2 + 6 + \pi^6, -\varepsilon + \pi^5), (-\varepsilon^2 + 2\pi^4 + 6 + \pi^6, -\varepsilon + \pi^4 + \pi^5),\\ &(-\varepsilon^2 + 2\varepsilon\pi^2 + 6 - \pi^4 + \pi^6, -\varepsilon + \pi^2), (-\varepsilon^2 + 2\varepsilon\pi^2 + 6 + \pi^4 + \pi^6, -\varepsilon + \pi^2 + \pi^4),\\ &(-\varepsilon^2 + 2\varepsilon\pi^2 + 6 - \pi^4 + \pi^6 + \pi^7, -\varepsilon + \pi^2 + \pi^5),\\ &(-\varepsilon^2 + 2\varepsilon\pi^2 + 6 + \pi^4 + \pi^6 + \pi^7, -\varepsilon + \pi^2 + \pi^4 + \pi^5), (-\varepsilon^2 + 2\varepsilon\pi^3 + 6, -\varepsilon + \pi^3),\\ &(-\varepsilon^2 + 2\varepsilon\pi^3 + 6 + 2\pi^4, -\varepsilon + \pi^3 + \pi^4), (-\varepsilon^2 + 2\varepsilon\pi^3 + 6 + \pi^7, -\varepsilon + \pi^3 + \pi^5),\\ &(-\varepsilon^2 + 2\varepsilon\pi^3 + 6 + 2\pi^4 + \pi^7, -\varepsilon + \pi^3 + \pi^4 + \pi^5),\end{aligned}$$

$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6,-\varepsilon+\pi^2+\pi^3),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6,-\varepsilon+\pi^2+\pi^3+\pi^4),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3-\pi^4+6+\pi^7,-\varepsilon+\pi^2+\pi^3+\pi^5),$$
$$(-\varepsilon^2+2\varepsilon\pi^2+2\varepsilon\pi^3+\pi^4+6+\pi^7,-\varepsilon+\pi^2+\pi^3+\pi^4+\pi^5)\},$$

$$\mathcal{L}_2=\left\{\left(-1,\frac{2}{\pi^2}\right),\left(-1+\pi^2+\pi^3,\frac{2}{\pi^2}\right),\left(1,\frac{2}{\pi^2}+\pi^2\right),\right.$$
$$\left(1+\pi^2+\pi^3,\frac{2}{\pi^2}+\pi^2\right),\left(-1+\pi^3,\frac{2}{\pi^2}+\pi^3\right),\left(-1+\pi^2,\frac{2}{\pi^2}+\pi^3\right),$$
$$\left.\left(1+\pi^3,\frac{2}{\pi^2}+\pi^2+\pi^3\right),\left(1+\pi^2,\frac{2}{\pi^2}+\pi^2+\pi^3\right)\right\}.$$

THÉORÈME 2. *On suppose que l'extension $K/\mathbb{Q}_2$ est quadratique ramifiée. On est dans l'un des cas suivants.*

1. *Si $v(j)=0$, on a $|\Phi|=2$.*
2. *Si $v(j)\in\{1,2,5,7,10,11,13,14,17,19,22,23\}$, on a $|\Phi|=24$.*
3. *Si $v(j)\in\{3,9,15,21\}$, on a $|\Phi|=8$.*
4. *Supposons $v(j)=4$.*
   (a) *Supposons que la condition (C1) soit satisfaite.*
   On a $|\Phi|=3$ si les conditions suivantes sont satisfaites :
      (i) $v(\Delta)\equiv 8 \pmod{12}$.
      (ii) *Si $K\in\Omega_1$, on a $c_6'\equiv 1+\pi^2 \pmod 4$ ou $c_6'\equiv 1+\pi^3 \pmod 4$.*
      (iii) *Si $K\in\Omega_2$, on a $c_6'\equiv 1 \pmod 4$ ou $c_6'\equiv 1+\pi^2+\pi^3 \pmod 4$.*
   On a $|\Phi|=6$ sinon.
   (b) *Si la condition (C1) n'est pas satisfaite, on a $|\Phi|=24$.*
5. *Supposons $v(j)=6$. On a*
$$|\Phi|=\begin{cases}4 & \text{si la condition (C1) est satisfaite,}\\ 8 & \text{sinon.}\end{cases}$$
6. *Supposons $v(j)=8$.*
   (a) *Supposons que la condition (C2) soit satisfaite.*
   On a $|\Phi|=3$ si les deux conditions suivantes sont satisfaites :
      (i) $v(\Delta)\equiv 4 \pmod{12}$.
      (ii) *Il existe $(a,b)\in\mathcal{L}_1$ tel que $c_4'\equiv a \pmod{\pi^8}$ et $c_6'\equiv b \pmod{\pi^6}$.*
   On a $|\Phi|=6$ sinon.
   (b) *Si la condition (C2) n'est pas satisfaite, on a $|\Phi|=24$.*
7. *Supposons $v(j)=12$.*
   (a) *Si $2v(c_6)=3v(c_4)+1$, on a $|\Phi|=8$.*
   (b) *Supposons $2v(c_6)=3v(c_4)+2$.*

(i) *Si* $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1}') \text{ est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

(ii) *Si* $K \in \Omega_2$, *on a*

$$|\Phi| = \begin{cases} 8 & \text{si la condition (C1}') \text{ est satisfaite,} \\ 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

(c) *Si* $2v(c_6) = 3v(c_4) + 3$, *on a*

$$|\Phi| = \begin{cases} 8 & \text{si } K \in \Omega_1, \\ 4 & \text{si } K \in \Omega_2. \end{cases}$$

(d) *Supposons* $2v(c_6) - 3v(c_4) \geq 4$.

(i) *Si* $K \in \Omega_1$, *on a*

$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite et } v(c_4) \text{ est pair,} \\ 4 & \text{sinon.} \end{cases}$$

(ii) *Si* $K \in \Omega_2$, *on a* $|\Phi| = 8$.

8. *Supposons* $v(j) = 16$.

(a) *Supposons que la condition (C2) soit satisfaite.*
On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*

(i) $v(\Delta) \equiv 8 \pmod{12}$.

(ii) *Il existe* $(a, b) \in \mathcal{L}_2$ *tel que* $c_4' \equiv a \pmod 4$ *et* $c_6' \equiv b \pmod 4$.

On a $|\Phi| = 6$ *sinon.*

(b) *Si la condition (C2) n'est pas satisfaite, on a* $|\Phi| = 24$.

9. *Supposons* $v(j) = 18$. *On a*

$$|\Phi| = \begin{cases} 4 & \text{si la condition (C1}') \text{ est satisfaite,} \\ 8 & \text{sinon.} \end{cases}$$

10. *Supposons* $v(j) = 20$.

(a) *Supposons que la condition (C1}') soit satisfaite.*
On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*

(i) $v(\Delta) \equiv 4 \pmod{12}$.

(ii) $c_6' \equiv \pi^2/2 + 2 \pmod 4$ *ou* $c_6' \equiv \pi^2/2 + \pi^3 \pmod 4$.

On a $|\Phi| = 6$ *sinon.*

(b) *Si la condition (C1}') n'est pas satisfaite, on a* $|\Phi| = 24$.

11. *Supposons* $v(j) \geq 24$.

(a) *Si* 3 *divise* $v(\Delta)$, *on a* $|\Phi| = 2$.

(b) *Supposons que* 3 *ne divise pas* $v(\Delta)$.

On a $|\Phi| = 3$ *si les deux conditions suivantes sont satisfaites :*

(i) $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$.

(ii) $c_6' \equiv \pi^2/2 \pmod 4$ *ou* $c_6' \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$.

On a $|\Phi| = 6$ *sinon.*

Dans l'Appendice A, on montre que chacun des cas ci-dessus se réalise.

2. Le cas des extensions quelconques

2.1. Lemmes sur les carrés. On reprend les notations de la section 1. Il existe une unique extension quadratique non ramifiée de K dans $\overline{K}$. On la note N. Lorsque l'extension $K/\mathbb{Q}_2$ est totalement ramifiée, le corps résiduel de N est de cardinal 4 et un système de représentants est $\mu_3 \cup \{0\}$, où μ_3 est l'ensemble des racines cubiques de l'unité. On note $\mathcal{O}_K$ (resp. $\mathcal{O}_N$) l'anneau des entiers de K (resp. de N) et $\mathcal{U}_K$ (resp. $\mathcal{U}_N$) ses unités.

Par commodité, on rappelle le résultat suivant ([2, lem. 7]).

LEMME 1. *Soit x un élément de $\mathcal{U}_K$ congru à 1 modulo $4\mathcal{O}_K$. Alors, x est un carré dans K_{nr}.*

On en déduit le résultat suivant.

LEMME 2. *Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si il existe un élément y de $\mathcal{U}_N$ tel que*

$$x \equiv y^2 \pmod{4\mathcal{O}_N}.$$

Démonstration. La condition est nécessaire car si x est un carré dans K_{nr}, c'est un carré dans une extension quadratique non ramifiée de K, donc dans N. Réciproquement, s'il existe un élément y de N tel que $x \equiv y^2 \pmod{4\mathcal{O}_N}$, alors, d'après le lemme 1, x est un carré dans la clôture non ramifiée de N dans $\overline{K}$. Or $N_{nr} = K_{nr}$ car N/K est non ramifiée. D'où le lemme.

Lorsque l'extension $K/\mathbb{Q}_2$ est totalement ramifiée, on a le résultat plus précis suivant.

LEMME 3. *Supposons l'extension $K/\mathbb{Q}_2$ totalement ramifiée. Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si il existe un élément $y \in \mathcal{U}_K$ tel que $x \equiv y^2 \pmod{4\mathcal{O}_K}$. Autrement dit, x est un carré dans K_{nr} si et seulement si il existe des éléments $a_0, a_1, \ldots, a_{e-1}$ tels que les deux conditions suivantes soient satisfaites :*

1. $a_0 = 1$ *et* $a_j = 0$ *ou* 1 *pour* $1 \leq j \leq e-1$.
2. *On a*

$$x \equiv (a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2 \pmod{4\mathcal{O}_K}. \tag{2.1}$$

Démonstration. La condition est suffisante d'après le lemme précédent.

Réciproquement, supposons que x soit un carré dans K_{nr}. Il existe alors y dans $\mathcal{O}_N$ tel que $x = y^2$. On choisit comme système de représentants du corps résiduel de N l'ensemble μ_3 des racines cubiques de l'unité. On écrit le développement de Hensel de y modulo 2 :

$$y \equiv a_0 + a_1\pi + \cdots + a_{e-1}\pi^{e-1} \pmod{2\mathcal{O}_N}, \quad \text{où } a_j \in \mu_3 \cup \{0\}.$$

Soit i un entier ≥ 0 et $P(i)$ la proposition de récurrence suivante

$$\ll a_0, \ldots, a_i = 0 \text{ ou } 1 \gg.$$

Montrons $P(0)$. L'extension $K/\mathbb{Q}_2$ étant totalement ramifiée, x est congru à 1 modulo $\pi\mathcal{O}_K$, d'où $y^2 \equiv 1 \pmod{\pi\mathcal{O}_K}$. Or π est une uniformisante de N, donc $\pi\mathcal{O}_N$ est un idéal premier de $\mathcal{O}_N$. On en déduit $y \equiv \pm 1 \pmod{\pi\mathcal{O}_N}$. Puis, comme $-1 \equiv 1 \pmod{\pi}$, il vient $y \equiv 1 \pmod{\pi\mathcal{O}_N}$. Cela démontre $P(0)$ et on a $a_0 = 1$. Si $e = 1$, cela démontre le résultat.

Supposons $e > 1$. Soit $i \geq 0$ tel que $i < e-1$ et $P(i)$ vraie. Montrons $P(i+1)$. Posons

$$z = \frac{1}{\pi^{i+1}}(y - (1 + a_1\pi + \cdots + a_i\pi^i)).$$

L'élément z est dans $\mathcal{O}_N$. Calculons $z^2 \pmod{\pi\mathcal{O}_N}$ de deux façons différentes.

D'une part, on a

$$z^2 = \frac{1}{\pi^{2(i+1)}}(y^2 - 2y(1 + a_1\pi + \cdots + a_i\pi^i) + (1 + a_1\pi + \cdots + a_i\pi^i)^2).$$

Or

$$2y(1 + a_1\pi + \cdots + a_i\pi^i) \equiv 2(1 + a_1\pi + \cdots + a_i\pi^i)^2 \pmod{\pi^{e+i+1}\mathcal{O}_N}.$$

Comme $x = y^2$, on en déduit donc

$$z^2 \equiv \frac{1}{\pi^{2(i+1)}}(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2) \pmod{\pi^{e-1-i}\mathcal{O}_N}.$$

Posons

$$\alpha = \frac{1}{\pi^{2(i+1)}}\,(x - (1 + a_1\pi + \cdots + a_i\pi^i)^2).$$

Alors, par hypothèse de récurrence, $\alpha \in \mathcal{O}_N \cap K = \mathcal{O}_K$ et, en particulier,

$$\alpha \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

On en déduit alors

$$z^2 \equiv 0 \text{ ou } 1 \pmod{\pi\mathcal{O}_N}.$$

D'autre part, on a

$$z \equiv a_{i+1} \pmod{\pi\mathcal{O}_N}, \quad \text{puis} \quad z^2 \equiv a_{i+1}^2 \pmod{\pi\mathcal{O}_N}.$$

On en déduit $a_{i+1} = 0$ ou 1. D'où le résultat par récurrence. On a donc $x \equiv (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2 \pmod{4\mathcal{O}_N}$ avec $a_1, \ldots, a_{e-1} = 0$ ou 1. D'où

$$\frac{1}{4}(x - (1 + a_1\pi + \cdots + a_{e-1}\pi^{e-1})^2) \in \mathcal{O}_N \cap K = \mathcal{O}_K.$$

D'où la congruence annoncée.

Lemme 4. *Soit x un élément de K_{nr} de valuation 0. Alors, toutes les racines cubiques de x dans $\overline{K}$ sont dans K_{nr}.*

Démonstration. L'élément x est une unité des entiers de $K(x)$. Elle s'écrit en particulier $x = \xi \cdot b$, où ξ est une racine de l'unité d'ordre impair et b une unité principale des entiers de $K(x)$, i.e. $b \equiv 1 \pmod{\pi\mathcal{O}_{K(x)}}$. Or, ξ est un cube dans K_{nr} et le lemme de Hensel appliqué au polynôme $X^3 - b$ de $\mathcal{O}_{K(x)}[X]$ montre qu'il en va de même pour b. D'où le résultat.

On rappelle que e désigne l'indice de ramification de l'extension $K/\mathbb{Q}_2$.

LEMME 5. *Soient K'/K_{nr} une extension finie de degré n impair, x et y deux éléments de K' de valuation ≥ 0 et ρ un rationnel positif. On suppose que les conditions suivantes sont satisfaites :*

1. $v(x-y)=\rho$.
2. $\rho = r/s$, *avec r et s entiers premiers entre eux et r impair.*
3. $\rho \leq 2e$.

Alors, l'un au-moins des éléments x et y n'est pas un carré dans K'.

Démonstration. Supposons que $x=a^2$ et $y=b^2$ soient des carrés dans K'. On a $v(2b) = e+v(b) = e+v(y)/2 \geq \rho/2$ par hypothèse.

Supposons $v(a-b) < \rho/2$. Alors, d'après l'égalité $a+b = a-b+2b$, on en déduit $v(a+b) = v(a-b) < \rho/2$. Or, c'est absurde car $v(a-b)+v(a+b) = v(a^2-b^2) = \rho$. On a donc $v(a-b) \geq \rho/2$ et de même $v(a+b) \geq \rho/2$. D'où $v(a-b) = v(a+b) = \rho/2$. Mais, r et n étant impairs, $\rho/2 \notin v(K') \subset (1/n)\mathbb{Z}$. D'où une contradiction et le lemme.

2.2. La courbe $\widetilde{E}$. On reprend les notations de la section 1. En particulier, e désigne l'indice de ramification de $K/\mathbb{Q}_2$ et on note encore v le prolongement de la valuation normalisée v de K à une clôture algébrique $\overline{K}$ de K . On choisit une racine cubique $\Delta^{1/3}$ de Δ dans $\overline{K}$. On note M l'extension de K_{nr} engendrée par $\Delta^{1/3}$. D'après le lemme 4, si $v(\Delta)$ est divisible par 3, alors $\Delta^{1/3}$ est dans K_{nr}, i.e. l'extension M/K_{nr} est triviale. Réciproquement, si $\Delta^{1/3}$ est dans K_{nr}, alors $v(\Delta)$ est divisible par 3 car $v(K_{nr}) \subset \mathbb{Z}$.

On pose, pour t dans l'ensemble μ_3 des racines cubiques de l'unité

$$A_t = c_4 - 12t\Delta^{1/3} \quad \text{et} \quad B_t = c_4^2 + 12tc_4\Delta^{1/3} + (12t\Delta^{1/3})^2.$$

Lorsque $t=1$, on retrouve les éléments $A_1 = A$ et $B_1 = B$ de [2, th. 3]. On a également $A_tB_t = c_6^2$. De plus, d'après le lemme 4, A_t et B_t sont dans K_{nr} si et seulement si 3 divise $v(\Delta)$, i.e. si et seulement si 3 divise $v(j)$. On désigne par $j^{1/3}$ la racine cubique de j dans $\overline{K}$ définie par l'égalité

$$j^{1/3} = c_4/\Delta^{1/3}.$$

On fait l'hypothèse $v(j) > 6e$. L'équation suivante définit alors un modèle entier d'une courbe elliptique, notée $\widetilde{E}$, sur K :

$$y^2 + 2xy = x^3 + \frac{j}{3(j-1728)}x + \frac{j}{3^3(j-1728)}. \tag{2.2}$$

Les coefficients standard $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ de $\widetilde{E}$ sont donnés par les égalités suivantes :

$$\widetilde{c_4} = -2^4\frac{1728}{j-1728} = -2^{10}\cdot 3^3\frac{\Delta}{c_6^2}, \qquad \widetilde{c_6} = 2^6\frac{1728}{j-1728} = 2^{12}\cdot 3^3\frac{\Delta}{c_6^2}, \tag{2.3}$$

$$\widetilde{\Delta} = -2^{12}\frac{1728j}{(j-1728)^3} = -2^{18}\cdot 3^3\frac{c_4^3\Delta^2}{c_6^6}. \tag{2.4}$$

On vérifie que $v(\widetilde{\Delta}) = v(j)$. De plus, $\widetilde{j} = \widetilde{c_4}^3/\widetilde{\Delta} = 1728^2/j$, d'où en particulier $v(\widetilde{j}) = 12e - v(j)$.

On choisit de noter $\widetilde{\Delta}^{1/3}$ la racine cubique de $\widetilde{\Delta}$ définie par l'égalité

$$\widetilde{\Delta}^{1/3} = -2^6 \cdot 3\frac{j^{1/3}}{j-1728} = -2^6 \cdot 3\frac{c_4\Delta^{2/3}}{c_6^2}.$$

Pour $t \in \mu_3$, on définit, comme pour E ci-dessus, le coefficient

$$\widetilde{B}_t = \widetilde{c_4}^2 + 12t\widetilde{c_4}\widetilde{\Delta}^{1/3} + (12t\widetilde{\Delta}^{1/3})^2.$$

À nouveau, $\widetilde{B}_t$ est dans K_{nr} si et seulement si 3 divise $v(j)$. Posons à présent

$$w_t = 2^4 \cdot 3 \cdot t^2\frac{\Delta^{1/3}}{c_6}.$$

Proposition 1. *On est dans l'un des cas suivants :*

1. *Si $v(j)$ est divisible par 3, alors w_t appartient à K_{nr}.*
2. *Si $v(j)$ n'est pas divisible par 3, alors w_t n'appartient pas à K_{nr} et w_t appartient à M qui est l'unique extension de degré 3 de K_{nr}.*

De plus, pour $t \in \mu_3$,

$$\widetilde{B}_t = w_t^4 B_{t^2}.$$

Démonstration. Les deux premières assertions résultent du lemme 4. On a

$$12 \cdot \frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} = \frac{1}{12} \cdot \frac{c_4}{\Delta^{1/3}}.$$

D'où

$$\frac{\widetilde{B}_t}{\widetilde{c_4}^2} = 1 + 12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}} + \left(12t\frac{\widetilde{\Delta}^{1/3}}{\widetilde{c_4}}\right)^2 = 1 + \frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}} + \left(\frac{t}{12} \cdot \frac{c_4}{\Delta^{1/3}}\right)^2$$
$$= \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2\left(1 + 12t^2\frac{\Delta^{1/3}}{c_4} + \left(12t^2\frac{\Delta^{1/3}}{c_4}\right)^2\right) = \left(t\frac{c_4}{12\Delta^{1/3}}\right)^2 \cdot \frac{B_{t^2}}{c_4^2}.$$

D'où, comme $\widetilde{c_4} = -2^{10} \cdot 3^3\Delta/c_6^2$, on a

$$\widetilde{B}_t = 2^{16} \cdot 3^4 \cdot t^2\frac{\Delta^{4/3}}{c_6^4}B_{t^2} = w_t^4 B_{t^2}$$

et la proposition.

On note, comme $\widetilde{j} \neq 0$, $\widetilde{c_4} = \pi^{v(\widetilde{c_4})}\widetilde{c_4}'$, $\widetilde{\Delta} = \pi^{v(\widetilde{\Delta})}\widetilde{\Delta}'$ et $\widetilde{j} = \pi^{v(\widetilde{j})}\widetilde{j}'$. On vérifie alors d'après les formules (2.3) et (2.4) que l'on a le résultat suivant.

Lemme 6. *On a*

$$\widetilde{\Delta}' = -3^3 \cdot \left(\frac{2}{\pi^e}\right)^{18}\frac{c_4'^3\Delta'^2}{c_6'^6} \quad \textit{et} \quad j'\widetilde{j}' = 3^6 \cdot \left(\frac{2}{\pi^e}\right)^{12}.$$

2.3. Démonstration du théorème 1. On suppose que $0 < v(j) < 12e$. On reprend les notations introduites à la section 2.2 et on choisit une racine carrée $B^{1/2}$ de B dans $\overline{K}$. On pose alors

$$C = 2(c_4 + 6\Delta^{1/3} + B^{1/2}).$$

La proposition suivante est à peu de choses près [1, prop. 1].

PROPOSITION 2. *Supposons $c_6 \neq 0$ et $v(j) \equiv 0 \pmod 3$. Alors, si pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}, on a $|\Phi| = 8$.*

Démonstration. D'après [2, th. 3], il s'agit de montrer que C n'est pas un carré dans $K_{nr}(B^{1/2})$. On a $A_t B_t = c_6^2$, qui est non nul par hypothèse. Donc A_t est un carré dans K_{nr} si et seulement si B_t l'est. De plus, $c_4 \neq 0$ (car B_t n'est pas un carré dans K_{nr}). Posons

$$\nu = 1 + \frac{B^{1/2}}{c_4}.$$

Alors, $(1, \nu)$ est une base de $K_{nr}(B^{1/2})$ sur K_{nr}. Supposons que C soit un carré dans $K_{nr}(B^{1/2})$. Il existe deux éléments a et b de K_{nr} tels que

$$C = c_4(12j^{-1/3} + 2\nu) = (a + b\nu)^2. \tag{2.5}$$

Or, on vérifie que $\nu^2 = 2\nu + 12j^{-1/3} + 144j^{-2/3}$. Mais $j^{1/3} \in K_{nr}$ car $v(j) \equiv 0 \pmod 3$, donc d'après (2.5), il vient

$$\begin{cases} c_4 = b(a+b), \\ 12c_4 j^{-1/3} = a^2 + b^2(12j^{-1/3} + 144j^{-2/3}), \end{cases}$$

puis, $a^2 - 12abj^{-1/3} + 144b^2j^{-2/3} = 0$. Autrement dit, il existe $t \neq 1$ dans μ_3 tel que $a = -12tbj^{-1/3}$. D'où $c_4 = b^2(1 - 12tj^{-1/3})$. Or, $A_t = c_4(1 - 12tj^{-1/3})$, donc $A_t = b^2(1 - 12tj^{-1/3})^2$ est un carré dans K_{nr} et B_t l'est aussi, et ceci contredit l'hypothèse. D'où le résultat.

2.3.1. Démonstration de l'assertion 1. On fait l'hypothèse $v(j) \equiv \pm 3 \pmod{12}$. En particulier, $v(j) \equiv 0 \pmod 3$, donc $j^{1/3} \in K_{nr}$.

Supposons, dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est impair et vérifie l'inégalité $0 < v(12j^{-1/3}) \leq 2e$. Alors, pour $t \in \mu_3$,

$$\frac{B_t}{c_4^2} = 1 + 12tj^{-1/3} + (12tj^{-1/3})^2$$

est une unité de K_{nr} et

$$v\left(\frac{B_t}{c_4^2} - 1\right) = v(12tj^{-1/3}) = 2e - \frac{v(j)}{3}.$$

D'après le lemme 5 appliqué à $K' = K_{nr}$, $x = B_t/c_4^2$, $y = 1$ et $\rho = 2e - v(j)/3$, B_t n'est pas un carré dans K_{nr}. D'après la proposition 2, on a donc $|\Phi| = 8$.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, pour tout $t \in \mu_3$, $\widetilde{B}_t$ n'est pas un carré dans K_{nr}. Or, d'après la proposition 1, cela vaut aussi pour B_{t^2}. Ainsi, pour tout t dans μ_3, B_{t^2} n'est pas un carré dans K_{nr}. D'après la proposition 2, cela implique $|\Phi| = 8$.

Cela démontre l'assertion 1 du théorème 1.

2.3.2. Démonstration de l'assertion 2. On fait l'hypothèse $v(j) \equiv \pm 1$ ou $\pm 5 \pmod{12}$. En particulier, $v(j)$ est impair et n'est pas divisible par 3.

Supposons, dans un premier temps, $v(j) < 6e$ de sorte que $v(12j^{-1/3}) = 2e - v(j)/3$ est > 0. On a alors

$$v\left(\frac{B}{c_4^2} - 1\right) = v(12j^{-1/3}) = 2e - \frac{v(j)}{3} = \frac{6e - v(j)}{3} \leq 2e.$$

Or, par hypothèse, $6e - v(j)$ est impair et n'est pas divisible par 3. D'après le lemme 5 appliqué à $K' = K_{nr}(\Delta^{1/3}) = M$, $x = B/c_4^2$, $y = 1$ et $\rho = (6e - v(j))/3$, B n'est pas un carré dans M.

Par ailleurs, si $v(j) > 6e$, alors la courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $12e - v(j)$. Autrement dit, $\widetilde{E}$ satisfait aux hypothèses précédentes. Donc, $\widetilde{B}$ n'est pas un carré dans M. Or, d'après la proposition 1, cela vaut aussi pour B.

D'après [2, th. 3], cela implique $|\Phi| = 24$ et l'assertion 2 du théorème 1.

2.3.3. Démonstration de l'assertion 3. On a $v(j) \equiv \pm 2 \pmod{12}$ de sorte que $v(j)$ n'est pas divisible par 3. Supposons tout d'abord $v(j) < 6e$. Alors,

$$\frac{B}{c_4^2} = 1 + 12j^{-1/3} + 144j^{-2/3}$$

est une unité de M. Notons π_0 une racine cubique de π dans $\overline{K}$ et supposons que B soit un carré dans M. Il existe alors a, b et c dans K_{nr} tels que

$$\frac{B}{c_4^2} = (a + b\pi_0 + c\pi_0^2)^2 = (a^2 + 2bc\pi) + (c^2\pi + 2ab)\pi_0 + (b^2 + 2ac)\pi_0^2. \tag{2.6}$$

Or, $v(\pi_0) = 1/3$, donc $v(a)$, $v(b\pi_0)$ et $v(c\pi_0^2)$ sont distincts ; puis, d'après l'égalité

$$0 = v\left(\frac{B}{c_4^2}\right) = 2v(a + b\pi_0 + c\pi_0^2),$$

il vient $v(a) = 0$, $v(b) \geq 0$ et $v(c) \geq 0$. Posons par ailleurs

$$u = \frac{j^{1/3}}{\pi_0^{v(j)}}.$$

On a $u^3 = j'$ et $v(j') = 0$, donc $u \in K_{nr}$ en vertu du lemme 4.

On distingue à présent deux cas selon la congruence de $v(j)$ modulo 12.

Supposons $v(j) \equiv 2 \pmod{12}$. Écrivons $v(j) = 12k + 2$, $k \geq 0$. Alors,

$$j^{-1/3} = u^{-1}\pi_0^{-12k-2} = \frac{u^{-1}}{\pi^{4k+1}}\pi_0 \quad \text{et} \quad j^{-2/3} = \frac{u^{-2}}{\pi^{8k+2}}\pi_0^2,$$

puis

$$\frac{B}{c_4^2} = 1 + 12\frac{u^{-1}}{\pi^{4k+1}}\pi_0 + 144\frac{u^{-2}}{\pi^{8k+2}}\pi_0^2$$

et l'on peut identifier dans (2.6) les coefficients de la décomposition dans la base $(1, \pi_0, \pi_0^2)$. Il vient en particulier (comme $u \in K_{nr}$)

$$\begin{cases} c^2\pi + 2ab = 12 \cdot u^{-1}/\pi^{4k+1}, \\ b^2 + 2ac = 144 \cdot u^{-2}/\pi^{8k+2}. \end{cases} \tag{2.7}$$

Supposons $2v(b) \geq 4e - 8k - 2 = v(144u^{-2}/\pi^{8k+2})$. Alors, d'après (2.7), on a $v(2ac) = e + v(c) \geq 4e - 8k - 2$. Puis, comme $e + v(b) > 2e - 4k - 1$, on a $v(c^2\pi) = 2v(c) + 1 =$

$2e-4k-1$, i.e. $v(c)=e-2k-1$. Or,

$$e-2k-1\geq 3e-8k-2,\quad \text{d'où}\quad v(j)\geq 4e.$$

Si $v(j)<4e$, on a une contradiction et l'hypothèse $2v(b)\geq v(144u^{-2}/\pi^{8k+2})$ est absurde.

Supposons que tel soit le cas, i.e. $v(j)<4e$. Alors, $2v(b)<4e-8k-2$, puis d'après (2.7), $e+v(c)=2v(b)$, d'où $2v(c)+1=4v(b)-2e+1$. On distingue à présent trois cas.

1. Supposons $2v(c)+1=e+v(b)$. Alors, $3(v(b)-e)+1=0$, d'où une contradiction en réduisant cette égalité modulo 3.
2. Supposons $2v(c)+1>e+v(b)$, i.e. $4v(b)-2e+1>e+v(b)$. Alors, d'après (2.7), $e+v(b)=2e-4k-1$, i.e. $v(b)=e-4k-1$. Or, $4v(b)-2e+1>e+v(b)$ par hypothèse. Donc $v(j)<0$. C'est une contradiction.
3. Supposons $2v(c)+1<e+v(b)$. Alors, d'après (2.7), $2v(c)+1=2e-4k-1$, puis $v(c)=e-2k-1$. Or, $2v(b)=v(c)+e$, donc $2v(b)=2e-2k-1$. On en déduit une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse que B est un carré dans M est absurde si $v(j)\equiv 2 \pmod{12}$ et $v(j)<4e$.

Supposons $v(j)\equiv -2 \pmod{12}$. Écrivons $v(j)=12k+10$, $k\geq 0$. Alors,

$$j^{-1/3}=u^{-1}\pi_0^{-12k-10}=\frac{u^{-1}}{\pi^{4k+4}}\pi_0^2\quad\text{et}\quad j^{-2/3}=\frac{u^{-2}}{\pi^{8k+7}}\pi_0,$$

puis

$$\frac{B}{c_4^2}=1+144\frac{u^{-2}}{\pi^{8k+7}}\pi_0+12\frac{u^{-1}}{\pi^{4k+1}}\pi_0^2$$

et l'on peut identifier dans (2.6) les coefficients de la décomposition dans la base $(1,\pi_0,\pi_0^2)$. Il vient en particulier (comme $u\in K_{nr}$)

$$\begin{cases} c^2\pi+2ab=144\cdot u^{-2}/\pi^{8k+7},\\ b^2+2ac=12\cdot u^{-1}/\pi^{4k+4}.\end{cases}\tag{2.8}$$

On distingue trois cas.

1. Supposons $2v(b)>2e-4k-4$, i.e. $v(b)>e-2k-2$. Alors, d'après (2.8), on a $e+v(c)=2e-4k-4$, i.e. $v(c)=e-4k-4$. Donc $2v(c)+1=2e-8k-7$, puis $2v(c)+1<4e-8k-7=v(144u^{-2}/\pi^{8k+7})$. Alors, d'après (2.8), $v(2ab)=e+v(b)=2v(c)+1=2e-8k-7$. Autrement dit, $v(b)=e-8k-7$, d'où $e-8k-7>e-2k-2$. Or cela équivaut à $v(j)<0$. D'où une contradiction.
2. Supposons $2v(b)<2e-4k-4$, i.e. $v(b)<e-2k-2$. Alors, d'après (2.8), on a $e+v(c)=2v(b)$, puis $2v(c)+1=4v(b)-2e+1$. En réduisant modulo 3, on constate que l'égalité $e+v(b)=4v(b)-2e+1$ est impossible. De plus,

   $$2v(c)+1=4v(b)-2e+1>e+v(b)\iff v(b)>e-1/3\iff v(b)\geq e,$$

   car e et $v(b)$ sont entiers. Or, l'hypothèse faite entraîne $v(b)<e$. On a alors $2v(c)+1=4v(b)-2e+1=4e-8k-7$, puis $2v(b)=3e-4k-4$. Comme $2v(b)<2e-4k-4$, on en déduit $e<0$. C'est donc une contradiction et l'hypothèse $2v(b)<2e-4k-4$ était absurde.

3. On a donc finalement $2v(b) = 2e - 4k - 4$, i.e. $v(b) = e - 2k - 2$. Donc

$$e + v(b) = 2e - 2k - 2 < 4e - 8k - 7 \iff v(j) < 4e.$$

Autrement dit, si $v(j) < 4e$, il vient, d'après (2.8), $2v(c) + 1 = e + v(b) = 2e - 2k - 2$. D'où une contradiction en réduisant cette égalité modulo 2.

Après examen de tous les cas possibles, on a finalement montré que l'hypothèse que B est un carré dans M est absurde si $v(j) \equiv -2 \pmod{12}$ et $v(j) < 4e$.

Il reste donc à voir que si $v(j) \equiv \pm 2 \pmod{12}$ et $v(j) > 8e$, alors B n'est pas un carré dans M. On considère, pour ce faire, la courbe $\widetilde{E}$ d'équation (2.2). On a

$$v(\widetilde{j}) = 12e - v(j) \equiv -v(j) \equiv \pm 2 \pmod{12} \quad \text{et} \quad v(\widetilde{j}) < 4e.$$

Autrement dit, la courbe $\widetilde{E}$ satisfait aux hypothèses précédentes, donc $\widetilde{B}$ n'est pas un carré dans M et B non plus, d'après la proposition 1.

D'après [2, th. 3], on a donc $|\Phi| = 24$. Cela démontre bien l'assertion 3 du théorème 1 et achève sa démonstration.

3. Le cas des extensions quadratiques

On reprend les notations des sections 1 et 2.1 et l'on suppose l'extension $K/\mathbb{Q}_2$ quadratique ramifiée. Désignons par π_0 une racine cubique de π dans $\overline{K}$. C'est une uniformisante de l'extension $K_{nr}(\pi_0)/K_{nr}$.

3.1. Lemmes généraux

LEMME 7. *Soit x un élément de $\mathcal{U}_K$. Alors,*

$$x^2 \equiv \begin{cases} 1 \pmod{4\pi} & \text{si } x \equiv 1 \pmod 2, \\ 1 + \pi^2 + \pi^3 \pmod 4 & \text{si } x \equiv 1 + \pi \pmod 2. \end{cases}$$

En particulier, $x^2 \equiv 1 \pmod 2$.

Démonstration. Si $x \equiv 1 \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1 + 2a$. Puis $x^2 = 1 + 4a(a+1)$. Or, $a(a+1) \equiv 0 \pmod \pi$, donc $x^2 \equiv 1 \pmod 4$. De même, si $x \equiv 1+\pi \pmod 2$, alors il existe a dans $\mathcal{O}_K$ tel que $x = 1+\pi+2a$. Puis $x^2 \equiv 1+\pi^2+2\pi \pmod 4$. Or, 2 est associé à π^2, d'où $2\pi \equiv \pi^3 \pmod 4$ et la congruence annoncée. Dans les deux cas, on a $x^2 \equiv 1 \pmod 2$. D'où le résultat.

LEMME 8. *Soit x un élément de $\mathcal{U}_K$. Alors, x est un carré dans K_{nr} si et seulement si $x \equiv 1$ ou $1 + \pi^2 + \pi^3 \pmod 4$.*

Démonstration. D'après le lemme 3, x est un carré dans K_{nr} si et seulement si x est un carré modulo $4\mathcal{O}_K$. On conclut alors avec le lemme précédent.

LEMME 9. *Soient x un élément de $\mathcal{U}_K$ congru à 1 modulo 4 et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$. Alors, $\sqrt{x} \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$.*

Démonstration. D'après le lemme 8, $\sqrt{x} \in K_{nr}$. Supposons $v(\sqrt{x}-1) < 2$. Alors, d'après l'égalité $\sqrt{x}+1 = \sqrt{x}-1+2$, il vient $v(\sqrt{x}+1) = v(\sqrt{x}-1) < 2$. Donc $v(x-1) < 4$, ce qui est contraire aux hypothèses. D'où le lemme.

Pour chacune des six extensions quadratiques ramifiées de $\mathbb{Q}_2$, on indique dans le tableau ci-dessous un choix d'uniformisante.

K	$\mathbb{Q}_2(\sqrt{-1})$	$\mathbb{Q}_2(\sqrt{3})$	$\mathbb{Q}_2(\sqrt{2})$	$\mathbb{Q}_2(\sqrt{-2})$	$\mathbb{Q}_2(\sqrt{6})$	$\mathbb{Q}_2(\sqrt{-6})$
π	$1+\sqrt{-1}$	$1+\sqrt{3}$	$\sqrt{2}$	$\sqrt{-2}$	$\sqrt{6}$	$\sqrt{-6}$

Avec ces choix, si K est dans Ω_1, on vérifie que

$$2 \equiv \pi^2 + \pi^3 \pmod 4 \quad \text{et} \quad -1 \equiv 1 + \pi^2 + \pi^3 \pmod 4. \tag{3.1}$$

De même, si K est dans Ω_2, on a

$$2 \equiv \pi^2 \pmod 4 \quad \text{et} \quad -1 \equiv 1 + \pi^2 \pmod 4. \tag{3.2}$$

Remarque. On vérifie que le développement de Hensel de 2 modulo 4 est indépendant du choix de l'uniformisante de K.

On rappelle que l'on a posé

$$\varepsilon = 3 \cdot \left(\frac{2}{\pi^2}\right)^2. \tag{3.3}$$

Lemme 10. *On a*

$$\varepsilon \equiv \begin{cases} 1 \pmod 4 & \text{si } K \in \Omega_1, \\ -1 \equiv 1 + \pi^2 \pmod 4 & \text{si } K \in \Omega_2. \end{cases}$$

En particulier, $\varepsilon \equiv 1 \pmod 2$.

Démonstration. D'après les congruences (3.1) et (3.2), on a

$$\frac{2}{\pi^2} \equiv \begin{cases} 1 + \pi \pmod 2 & \text{si } K \in \Omega_1, \\ 1 \pmod 2 & \text{si } K \in \Omega_2. \end{cases}$$

D'où le résultat en élévant au carré.

3.2. Carrés dans l'extension quadratique non ramifiée de K. Par unicité d'une extension quadratique non ramifiée de K dans $\overline{K}$, on a $N = K(\zeta)$ où ζ est une racine primitive cubique de l'unité dans $\overline{K}$.

Lemme 11. *Soit x une unité de l'anneau d'entiers de $K(\zeta)$ congrue modulo 4 à l'un des éléments suivants :*

$$1 + \zeta\pi^2, \quad 1 + \zeta^2\pi^2, \quad 1 + \zeta\pi^2 + \zeta\pi^3, \quad 1 + \zeta^2\pi^2 + \zeta^2\pi^3.$$

Alors, x n'est pas un carré dans K_{nr}.

Démonstration. On raisonne par l'absurde. D'après le lemme 2, il existe un élément y dans l'unique extension quadratique non ramifiée N' de $K(\zeta)$ tel que

$$x \equiv y^2 \pmod{4\mathcal{O}_{N'}}.$$

Notons $\mathcal{R}$ un système de représentants du corps résiduel de N' contenant l'ensemble $\{0, 1, \zeta, \zeta^2\}$. Le développement de Hensel de y modulo 2 s'écrit

$$y \equiv a_0 + a_1\pi \pmod{2\mathcal{O}_{N'}},$$

avec $a_0 \in \mathcal{R} \setminus \{0\}$ et $a_1 \in \mathcal{R}$. Les éléments 2 et π^2 de K étant associés, on en déduit

$$x \equiv y^2 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{N'}}. \tag{3.4}$$

Par unicité du développement de Hensel, on a

$$a_0^2 = 1 \quad \text{et} \quad a_1^2 = \zeta \text{ ou } \zeta^2.$$

Or, les polynômes X^2-1, $X^2-\zeta$ et $X^2-\zeta^2$ de $\mathcal{O}_{K(\zeta)}[X]$ ont toutes leurs racines dans $\mathcal{O}_{K(\zeta)}$. On en déduit donc

$$a_0 = 1 \quad \text{et} \quad a_1 = \zeta \text{ ou } \zeta^2.$$

En substituant ces valeurs dans l'équation (3.4), on obtient $x \equiv 1+\zeta\pi^2+\zeta^2\pi^3 \pmod 4$ ou $x \equiv 1+\zeta^2\pi^2+\zeta\pi^3 \pmod 4$. D'où une contradiction et le lemme.

3.3. Carrés dans l'extension cubique $K(\pi_0)$

Lemme 12. *Soit x une unité des entiers de $K(\pi_0)$ congrue modulo 4 à l'un des éléments suivants :*

$$1+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8, \quad 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10}, \quad 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k,$$

où h et k sont soit nuls, soit des sommes de puissances >0 de π_0^3. Alors, x n'est pas un carré dans $K_{nr}(\pi_0)$.

Démonstration. On raisonne par l'absurde. L'extension $K(\pi_0)/\mathbb{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3, un élément y de $\mathcal{U}_{K(\pi_0)}$ tel que $x \equiv y^2 \pmod 4$. Notons $1+a_1\pi_0+a_2\pi_0^2+a_3\pi_0^3+a_4\pi_0^4+a_5\pi_0^5$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. On a

$$\begin{aligned} x \equiv y^2 \equiv 1 &+ a_1^2\pi_0^2 + a_2^2\pi_0^4 + a_3^2\pi_0^6 + a_4^2\pi_0^8 + a_5^2\pi_0^{10} + 2a_1\pi_0 + 2a_2\pi_0^2 + 2a_3\pi_0^3 \\ &+ 2a_4\pi_0^4 + 2a_5\pi_0^5 + 2a_1a_2\pi_0^3 + 2a_1a_3\pi_0^4 + 2a_1a_4\pi_0^5 + 2a_2a_3\pi_0^5 \pmod{4\mathcal{O}_{K(\pi_0)}}. \end{aligned}$$

Si $x \equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \pmod 4$, alors, par unicité du développement de Hensel, on a $a_1 = a_2 = 1$. Si $a_3 = 1$, le coefficient devant π_0^6 dans le membre de droite de la congruence ci-dessus est non nul, ce qui est absurde. On a donc $a_3 = 0$. Or, $2 \equiv \pi_0^6 \pmod{\pi_0^9}$ car $2 \equiv \pi^2 \pmod{\pi^3}$. D'où

$$x \equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \equiv 1+\pi_0^2+\pi_0^4+\pi_0^7+(a_4+1)\pi_0^8+\pi_0^9+a_5\pi_0^{10} \pmod 4,$$

ce qui est à nouveau absurde car le coefficient devant π_0^9 est nul dans le membre de gauche et non nul dans celui de droite.

Donc nécessairement $x \not\equiv 1+\pi_0^2+\pi_0^4+\pi_0^2h+\pi_0^4k \pmod 4$ et $a_1 = 0$. Autrement dit, le coefficient de π_0^7 dans le développement de x est nul. On en déduit $x \equiv 1+\pi_0^8 \pmod 4$, i.e. $a_1 = a_2 = a_3 = 0$. Comme 2 est associé à π_0^6, il vient alors

$$x \equiv 1 + a_4\pi_0^8 + a_5^2\pi_0^{10} + 2a_4\pi_0^4 + 2a_5\pi_0^5 \pmod 4 \quad \text{et} \quad a_4 = a_5 = 1.$$

Puis, comme $2 \equiv \pi_0^6 \pmod{\pi_0^9}$, on a $x \equiv 1+\pi_0^8+\pi_0^{11} \pmod 4$. D'où la contradiction et le lemme.

LEMME 13. *L'unité* $1+\pi_0^8+\pi_0^{11}$ *est un carré dans* $K_{nr}(\pi_0)$. *On a les équivalences suivantes :*

$$1+\pi_0^4+\pi_0^8+\pi_0^{10} \text{ est un carré dans } K_{nr}(\pi_0) \iff K\in\Omega_1,$$
$$1+\pi_0^4+\pi_0^8 \text{ est un carré dans } K_{nr}(\pi_0) \iff K\in\Omega_2.$$

Démonstration. D'après la relation $2\equiv\pi^2 \pmod{\pi^3}$, on a $2\equiv\pi_0^6 \pmod{\pi_0^9}$, d'où

$$1+\pi_0^8+\pi_0^{11}\equiv(1+\pi_0^4+\pi_0^5)^2 \pmod 4$$

et le fait que $1+\pi_0^8+\pi_0^{11}$ est un carré dans $K_{nr}(\pi_0)$ (lemme 2). Par ailleurs, on a

$$(1+\pi_0^4+\pi_0^8+\pi_0^{10})(1+\pi_0^4+\pi_0^8)\equiv 1+\pi_0^8 \pmod 4$$

et $1+\pi_0^8$ n'est pas un carré dans $K_{nr}(\pi_0)$ d'après le lemme précédent. Autrement dit, si l'un des éléments $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ et $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$, alors l'autre ne l'est pas.

Si $K\in\Omega_1$, d'après la relation (3.1), on a

$$1+\pi_0^4+\pi_0^8+\pi_0^{10}\equiv(1+\pi_0^2+\pi_0^5)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8$ ne l'est pas.

Si $K\in\Omega_2$, d'après la relation (3.2), on a

$$1+\pi_0^4+\pi_0^8\equiv(1+\pi_0^2)^2 \pmod 4.$$

Donc $1+\pi_0^4+\pi_0^8$ est un carré dans $K_{nr}(\pi_0)$ et $1+\pi_0^4+\pi_0^8+\pi_0^{10}$ ne l'est pas.

D'où les équivalences annoncées.

3.4. Carrés dans une extension quadratique ramifiée de K. D'après le lemme 8, l'unité $1+\pi^3$ de K n'est pas un carré dans K_{nr}. Notons γ une solution dans $\overline{K}$ de l'équation à coefficients dans $\mathcal{O}_K$

$$X^2-\frac{2}{\pi}X-\pi=0. \tag{3.5}$$

LEMME 14. *L'élément* γ *est une uniformisante de l'extension* $K(\sqrt{1+\pi^3})/K$ *et on a*

$$\pi\equiv\gamma^2+\gamma^3 \pmod 2.$$

Démonstration. D'après l'équation (3.5), on a $v(\gamma)=1/2$ et $\gamma\in K(\sqrt{1+\pi^3})$. Donc γ est bien une uniformisante de l'extension $K(\sqrt{1+\pi^3})/K$. Par ailleurs, on a $\gamma^2=(2/\pi)\gamma+\pi$, donc $\gamma^3=(4/\pi^2)\gamma+2+\pi\gamma$. D'où

$$\gamma^2+\gamma^3\equiv\frac{2}{\pi}\gamma+\pi+\pi\gamma\equiv\pi \pmod 2,$$

car $4/\pi^2\equiv 2/\pi+\pi\equiv 0 \pmod 2$. D'où le lemme.

LEMME 15. *Soient* x *un élément de* $\mathcal{U}_K$ *et* $\sqrt{x}$ *une racine carrée de* x *dans* $\overline{K}$. *On suppose* $x\equiv 1+\pi^3 \pmod 4$. *Alors,* $K_{nr}(\sqrt{x})=K_{nr}(\sqrt{1+\pi^3})$ *et* $\sqrt{x}\equiv 1+\gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{x})}}$.

Démonstration. La première assertion résulte du lemme 1. D'après le lemme 14, γ est une uniformisante de $K(\sqrt{1+\pi^3})/K$. Notons $a_0+a_1\gamma+a_2\gamma^2+a_3\gamma^3$, avec $a_i=0$ ou 1, le développement de Hensel de $\sqrt{x}$ modulo 2 (il est indépendant du choix de la racine

carrée). Alors, d'après le lemme 14, on a $\pi^2 \equiv \gamma^4 + \gamma^6 \pmod 4$, $\pi^3 \equiv \gamma^6 + \gamma^7 \pmod 4$, puis, comme 2 est associé à π^2, $2 \equiv \gamma^4 \pmod{\gamma^6}$. Donc

$$\begin{aligned} 1 + \gamma^6 \equiv x &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_0a_1\gamma + 2a_0a_2\gamma^2 \pmod{\gamma^7} \\ &\equiv a_0^2 + a_1^2\gamma^2 + a_2^2\gamma^4 + a_0a_1\gamma^5 + (a_3^2 + a_0a_2)\gamma^6 \pmod{\gamma^7}. \end{aligned}$$

Par unicité du développement de Hensel, on en déduit $a_0 = 1$, $a_1 = a_2 = 0$ et $a_3 = 1$. D'où le lemme.

LEMME 16. *Soit x une unité des entiers de $K(\sqrt{1+\pi^3})$. On suppose que x vérifie l'une des deux conditions suivantes :*

1. *x est congrue modulo 4 à l'un des quatre éléments*

$$1 + \gamma^4 + \gamma^6 + \gamma^7, \quad 1 + \gamma^4, \quad 1 + \gamma^6, \quad 1 + \gamma^7.$$

2. $x \equiv 1 + \gamma^2 + \gamma^3 \pmod 2$.

Alors, x n'est pas un carré dans $K_{nr}(\sqrt{1+\pi^3})$.

Démonstration. On raisonne par l'absurde. L'extension $K(\sqrt{1+\pi^3})/\mathbb{Q}_2$ étant totalement ramifiée, il existe, d'après le lemme 3, une unité y des entiers de $K(\sqrt{1+\pi^3})$ telle que $x \equiv y^2 \pmod 4$. Notons $1 + a_1\gamma + a_2\gamma^2 + a_3\gamma^3$, avec $a_i = 0$ ou 1, le développement de Hensel de y modulo 2. On a alors

$$x \equiv y^2 \equiv 1 + a_1^2\gamma^2 + a_2^2\gamma^4 + 2a_1\gamma + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Par unicité du développement de Hensel, x ne vérifie pas la seconde condition (le coefficient de γ^3 est nul). Il vient alors $a_1 = 0$, puis

$$x \equiv 1 + a_2^2\gamma^4 + a_3^2\gamma^6 + 2a_2\gamma^2 + 2a_3\gamma^3 \pmod 4.$$

Or, on a $2 \equiv \gamma^4 \pmod{\gamma^6}$ car $2 \equiv \pi^2 \pmod{\pi^3}$. Donc

$$x \equiv \begin{cases} 1 \pmod 4 & \text{si } (a_2, a_3) = (0,0), \\ 1 + \gamma^4 + \gamma^6 \pmod 4 & \text{si } (a_2, a_3) = (1,0), \\ 1 + \gamma^6 + \gamma^7 \pmod 4 & \text{si } (a_2, a_3) = (0,1), \\ 1 + \gamma^4 + \gamma^7 \pmod 4 & \text{si } (a_2, a_3) = (1,1). \end{cases}$$

D'où la contradiction et le résultat.

3.5. Carrés dans $K_{nr}(\sqrt{3})$. D'après le lemme 8 et les relations (3.1) et (3.2), 3 est un carré dans K_{nr} si et seulement si K est dans Ω_1. Notons $\sqrt{3}$ une racine carrée de 3 dans $\overline{K}$. Soient x un élément de $\mathcal{U}_K$ et $\sqrt{x}$ une racine carrée de x dans $\overline{K}$.

LEMME 17. *Supposons $K \in \Omega_1$ et $x \equiv 3 \pmod 4$. Alors,*

$$\sqrt{3} \equiv \sqrt{x} \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}}.$$

Démonstration. Supposons $v(\sqrt{3} - \sqrt{x}) < 2$. Alors, d'après l'égalité $\sqrt{3} + \sqrt{x} = \sqrt{3} - \sqrt{x} + 2\sqrt{x}$, on a $v(\sqrt{3}-\sqrt{x}) = v(\sqrt{3}+\sqrt{x}) < 2$, puis $v(3-x) < 4$, ce qui est absurde. D'où $v(\sqrt{3}-\sqrt{x}) \geq 2$ ou, autrement dit, $\sqrt{3} \equiv \sqrt{x} \pmod{2\mathcal{O}_{K_{nr}}}$. L'extension $K(\sqrt{x})/K$ est non ramifiée (elle est même éventuellement triviale). En particulier, on peut choisir un système de représentants $\mathcal{R}$ du corps résiduel de $K(\sqrt{x})$ contenu dans $\{0, 1, \zeta, \zeta^2\}$. Notons alors

$a_0+a_1\pi$ le développement de Hensel modulo $2\mathcal{O}_{K_{nr}}$ de $\sqrt{x}$. On a $a_0, a_1 \in \mathcal{R} \subset \{0, 1, \zeta, \zeta^2\}$. Puis, d'après la relation (3.1),

$$3 \equiv 1 + \pi^2 + \pi^3 \equiv a_0^2 + a_1^2\pi^2 + a_0a_1\pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Par unicité du développement de Hensel, on en déduit $a_0 = a_1 = 1$. D'où le lemme.

On suppose désormais $K \in \Omega_2$ de sorte que 3 n'est pas un carré dans K_{nr}.

LEMME 18. *Supposons $K \in \Omega_2$. L'unité x est un carré dans $K_{nr}(\sqrt{3})$ si et seulement si $x \equiv 1 \pmod 2$.*

Démonstration. Supposons que x soit un carré dans $K_{nr}(\sqrt{3})$. Il existe alors a et b deux éléments de K_{nr} tels que $x = (a+b\sqrt{3})^2$. Puis, comme $(1, \sqrt{3})$ est une base de l'extension $K_{nr}(\sqrt{3})/K_{nr}$, on a $x = a^2 + 3b^2$ et $ab = 0$. Si $b = 0$, on en déduit que x est un carré dans K_{nr}, et si $a = 0$ que $x/3$ est un carré dans K_{nr}. Réciproquement, si x ou $x/3$ est un carré dans K_{nr}, alors x est un carré dans $K_{nr}(\sqrt{3})$. Par ailleurs, d'après le lemme 8, x est un carré dans K_{nr} si et seulement si $x \equiv 1 \pmod 4$ ou $x \equiv 1 + \pi^2 + \pi^3 \pmod 4$. De plus, d'après la relation (3.2), on a $3 \equiv 1 + \pi^2 \pmod 4$. Donc, d'après le lemme 8, $x/3$ est un carré dans K_{nr} si et seulement si $x \equiv 1 + \pi^2$ ou $1 + \pi^3 \pmod 4$. On en déduit le résultat avec l'équivalence précédente.

Notons η une uniformisante de $K(\sqrt{3})$. C'est une extension quadratique de K.

LEMME 19. *Supposons $K \in \Omega_2$ et $x \equiv 3 \pmod 4$. Alors, $K_{nr}(\sqrt{x}) = K_{nr}(\sqrt{3})$ et*

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \text{et} \quad \sqrt{x} \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Démonstration. L'égalité résulte du lemme 1. L'extension $K(\sqrt{3})/K$ étant totalement ramifiée, π est associé à η^2 et on a

$$\pi \equiv \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}} \quad \text{ou} \quad \pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

Dans les deux cas, d'après (3.2), on a $2 \equiv \eta^4 \pmod{\eta^6}$. Notons $a_0 + a_1\eta + a_2\eta^2 + a_3\eta^3$, avec $a_i = 0$ ou 1, le développement de Hensel de $\sqrt{3}$ modulo 2. D'après la (3.2), on a alors

$$\begin{aligned} 3 \equiv 1 + \pi^2 \equiv a_0^2 + a_1^2\eta^2 + a_2^2\eta^4 + a_3^2\eta^6 \\ + 2a_0a_1\eta + 2a_0a_2\eta^2 + 2a_0a_3\eta^3 + 2a_1a_2\eta^3 \pmod 4. \end{aligned}$$

Par unicité du développement de Hensel, comme π^2 est associé à η^4, il vient $a_0 = 1$, $a_1 = 0$ et $a_2 = 1$. D'où, comme $2 \equiv \eta^4 \pmod{\eta^6}$,

$$\begin{aligned} 3 &\equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4 \\ &\equiv \begin{cases} 1 + \eta^4 + \eta^6 \pmod 4 & \text{si } a_3 = 0, \\ 1 + \eta^4 + \eta^7 \pmod 4 & \text{si } a_3 = 1. \end{cases} \end{aligned} \tag{3.6}$$

Supposons $\pi \equiv \eta^2 \pmod 2$. Alors, d'après (3.2), on a $2 \equiv \pi^2 \equiv \eta^4 \pmod 4$, et donc $3 \equiv 1 + \eta^4 \pmod 4$. D'après (3.6), c'est une contradiction. On a donc nécessairement

$$\pi \equiv \eta^2 + \eta^3 \pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où $2 \equiv \eta^4 + \eta^6 \pmod{4\mathcal{O}_{K(\sqrt{3})}}$ et, en remplaçant dans (3.6),

$$1 + \eta^4 + \eta^6 \equiv 1 + \eta^4 + (a_3^2 + 1)\eta^6 + a_3\eta^7 \pmod 4.$$

On en déduit $a_3 = 0$. D'où $\sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K(\sqrt{3})}}$.

Supposons $v(\sqrt{3}-\sqrt{x})<2$. Alors, d'après l'égalité $\sqrt{3}+\sqrt{x}=\sqrt{3}-\sqrt{x}+2\sqrt{x}$, on a $v(\sqrt{3}-\sqrt{x})=v(\sqrt{3}+\sqrt{x})<2$, puis $v(3-x)<4=v(4)$, ce qui est absurde. D'où $v(\sqrt{3}-\sqrt{x})\geq 2$ ou, autrement dit, $\sqrt{3}\equiv\sqrt{x}\pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}$. D'où le lemme.

LEMME 20. *Supposons $K\in\Omega_2$. L'unité $3+2\sqrt{3}$ de l'anneau d'entiers de $K(\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$.*

Démonstration. L'extension $K(\sqrt{3})/\mathbb{Q}_2$ est totalement ramifiée. Supposons que $3+2\sqrt{3}$ soit un carré dans $K_{nr}(\sqrt{3})$. Alors, d'après le lemme 3, il existe une unité y des entiers de $K(\sqrt{3})$ telle que $3+2\sqrt{3}\equiv y^2\pmod{4\mathcal{O}_{K(\sqrt{3})}}$. Or, d'après le lemme 19, on a $3+2\sqrt{3}\equiv 1+2\eta^2\equiv 1+\eta^6\pmod 4$. Notons $a_0+a_1\eta+a_2\eta^2+a_3\eta^3$, avec $a_i=0$ ou 1, le développement de Hensel de y modulo 2. En utilisant la relation $2\equiv 1+\eta^4+\eta^6\pmod 4$ déduite du lemme 19 et de la relation (3.2), on a

$$\begin{aligned}3+2\sqrt{3}\equiv 1+\eta^6\equiv a_0^2+a_1^2\eta^2+a_2^2\eta^4+a_0a_1\eta^5+(a_3^2+a_0a_2)\eta^6\\ +(a_0a_1+a_0a_3+a_1a_2)\eta^7\pmod{4\mathcal{O}_{K(\sqrt{3})}}.\end{aligned}$$

Par unicité du développement de Hensel, il vient $a_0=1$, $a_1=0$ et $a_2=0$. On a donc

$$1+\eta^6\equiv 1+a_3^2\eta^6+a_3\eta^7\pmod{4\mathcal{O}_{K(\sqrt{3})}}.$$

D'où une contradiction car $a_3=0$ ou 1. D'où le lemme.

LEMME 21. *Soit y une unité des entiers de $K(\sqrt{3})$. On suppose que y est un carré dans $K_{nr}(\sqrt{3})$. Alors,*

$$y\equiv 1\pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}\quad ou\quad y\equiv 1+\eta^2\pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Démonstration. L'extension $K(\sqrt{3})/\mathbb{Q}_2$ est totalement ramifiée. Comme y est un carré dans $K_{nr}(\sqrt{3})$, il existe, d'après le lemme 3, une unité z des entiers de $K(\sqrt{3})$ telle que $y\equiv z^2\pmod 4$. Notons $1+a_1\eta$, avec $a_1=0$ ou 1, le développement de Hensel de z modulo η^2. Alors,

$$y\equiv z^2\equiv 1+a_1^2\eta^2\pmod{2\mathcal{O}_{K(\sqrt{3})}}.$$

D'où le lemme car $a_1=0$ ou 1.

3.6. Notations et préliminaires aux démonstrations. On reprend les notations introduites aux sections précédentes en explicitant le choix de la racine cubique $\Delta^{1/3}$ de Δ. D'après le lemme de Hensel appliqué au polynôme $X^3-\Delta'$ de $\mathcal{O}_K[X]$, Δ' possède une unique racine cubique dans K. On la note δ. On choisit alors de prendre

$$\Delta^{1/3}=\pi_0^{v(\Delta)}\delta$$

de sorte que si $v(\Delta)\equiv 0\pmod 3$, on a $\Delta^{1/3}\in K$. Notons θ l'unité de K définie par

$$\theta=\varepsilon\frac{\delta}{c_4'}. \tag{3.7}$$

On choisit une racine $B^{1/2}$ de B dans $\overline{K}$ et on pose

$$C=2(c_4+6\Delta^{1/3}+B^{1/2}).$$

Alors,

$$\frac{C}{\pi^{v(c_4)}} = c'_4\left[2\left(1+\frac{B^{1/2}}{c_4}\right)+\theta\pi_0^{12-v(j)}\right] \tag{3.8}$$

est une unité de $K(B^{1/2})$.

3.6.1. Cas où $v(j)<12$. On a, pour t dans μ_3,

$$\frac{B_t}{c_4^2} = 1+12tj^{-1/3}+144t^2j^{-2/3} = 1+t\theta\pi_0^{12-v(j)}+(t\theta\pi_0^{12-v(j)})^2, \tag{3.9}$$

car $12j^{-1/3} = 3(2/\pi^2)^2\pi_0^{12-v(j)}\delta/c'_4 = \theta\pi_0^{12-v(j)}$.

Par ailleurs, l'égalité $c_4^3-c_6^2 = 1728\Delta$ s'écrit

$$\pi^{3v(c_4)}c_4'^3-\pi^{2v(c_6)}c_6'^2 = 3^3\cdot 2^6\pi^{v(\Delta)}\Delta',$$

puis

$$c_4'^3-c_6'^2 = \varepsilon^3\pi^{12-v(j)}\Delta', \tag{3.10}$$

car $2v(c_6)=3v(c_4)$. D'où

$$1-\frac{c_6'^2}{c_4'^3} = (\theta\pi_0^{12-v(j)})^3. \tag{3.11}$$

Lemme 22. *Supposons $v(j)\le 8$. Alors,*

$$c'_4 \equiv c_4'^3 \equiv c_6'^2 \pmod 4.$$

Démonstration. En réduisant l'égalité (3.11) modulo 2, on en déduit, avec le lemme 7, $c'_4\equiv 1 \pmod 2$, puis $c'_4\equiv c_4'^3 \pmod 4$. Les congruences annoncées résultent alors de la même égalité réduite modulo 4, car $v(j)\le 8$.

3.6.2. Cas où $v(j)=12$. Pour t dans μ_3, on a

$$\frac{B_t}{c_4^2} = 1+12tj^{-1/3}+144t^2j^{-2/3} = 1+t\theta+(t\theta)^2. \tag{3.12}$$

Le corps K étant totalement ramifié, pour $t=1$, B/c_4^2 est une unité de $\mathcal{O}_K$.

Par ailleurs, l'égalité $c_4^3-c_6^2=1728\Delta$ s'écrit comme à la relation (3.11),

$$1-\pi^{2v(c_6)-3v(c_4)}\frac{c_6'^2}{c_4'^3} = \theta^3. \tag{3.13}$$

La somme de deux unités n'en étant pas une, on a $2v(c_6)-3v(c_4)>0$.

3.6.3. Cas où $v(j)>12$. On considère alors la courbe $\widetilde{E}$ d'équation (2.2). Son invariant modulaire $\widetilde{j}$ est de valuation $v(\widetilde{j}) = 24-v(j)<12$.

Lemme 23. *On a*

$$\widetilde{\Delta}' \equiv c'_4 \pmod 2 \quad \textit{et} \quad j'\cdot\widetilde{j}' \equiv 1 \pmod 4.$$

Démonstration. Cela résulte des lemmes 6 et 7.

3.7. Démonstration du théorème 2. L'assertion 1 du théorème 2 résulte de l'assertion (i) de [2, th. 2]. L'assertion 11 résulte de [2, th. 2(iv)] et de la proposition 13. On suppose donc désormais que $1\le v(j)\le 23$. D'où en particulier $j\neq 0$.

L'assertion 2 lorsque $v(j)\neq 10$ et $v(j)\neq 14$ ainsi que l'assertion 3 résultent directement du théorème 1.

Démontrons à présent les autres assertions du théorème 2 (la détermination des types de Néron est reportée à la section 3.8).

3.7.1. Démonstration de l'assertion 2 lorsque $v(j) = 10$ ou 14. Supposons $v(j) = 10$. On vérifie, avec la relation (3.9), que

$$\frac{B}{c_4^2} = 1 + \theta\pi_0^2 + (\theta\pi_0^2)^2.$$

Or, $\varepsilon \equiv \pm 1 \pmod 4$ (lemme 10), donc, d'après (3.7), $\theta \equiv \pm\delta/c_4' \pmod 4$. D'après (3.1) et (3.2), on a alors

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^2 + \pi_0^4 + \pi_0^2 h + \pi_0^4 k \pmod 4,$$

où h et k sont soit nuls, soit des sommes de puissances > 0 de π_0^3. D'après le lemme 12, B n'est pas un carré dans M. D'où $|\Phi| = 24$ dans ce cas d'après [2, th. 3(ii)].

Supposons $v(j) = 14$. Alors, la courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 10$. Autrement dit, $\widetilde{B}$ n'est pas un carré dans M. D'après la proposition 1, il en va de même pour B et donc $|\Phi| = 24$ d'après [2, th. 3(ii)].

3.7.2. Démonstration de l'assertion 4. On suppose $v(j) = 4$.

Lemme 24. *On a*

$$\frac{B}{c_4^2} \equiv 1 + \pi_0^8\Delta' \pmod 4.$$

De plus, B est un carré dans M si et seulement si $\Delta' \equiv 1 + \pi \pmod 2$.

Démonstration. D'après les lemmes 7 et 10, on a

$$\varepsilon \equiv 1 \pmod 2 \quad \text{et} \quad \delta \equiv \Delta' \pmod 2.$$

De plus, d'après les lemmes 7 et 22, on a $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. D'où $\theta \equiv \Delta' \pmod 2$, puis $\theta\pi_0^8 \equiv \pi_0^8\Delta' \pmod 4$. La congruence annoncée résulte alors de l'égalité (3.9) appliquée à $t = 1$. On en déduit que B est un carré dans M si et seulement si l'unité $1 + \pi_0^8\Delta'$ de l'anneau des entiers de $K(\pi_0)$ l'est (lemme 1). Or,

$$1 + \pi_0^8\Delta' \equiv \begin{cases} 1 + \pi_0^8 \pmod 4 & \text{si } \Delta' \equiv 1 \pmod 2, \\ 1 + \pi_0^8 + \pi_0^{11} \pmod 4 & \text{si } \Delta' \equiv 1 + \pi \pmod 2. \end{cases}$$

On conclut à l'équivalence annoncée avec les lemmes 12 et 13.

Lorsque la condition (C1) n'est pas satisfaite, l'assertion 4 résulte du lemme précédent et de [2, th. 3(ii)]. Lorsque la condition (C1) est satisfaite, l'assertion 4 se déduit du lemme précédent, de [2, th. 3(ii)] et des propositions 4 et 5.

3.7.3. Démonstration de l'assertion 10. On suppose $v(j) = 20$. La courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 4$. D'après la proposition 1, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après le lemme 24, c'est le cas si et seulement si $\widetilde{\Delta}' \equiv 1 + \pi \pmod 2$. D'après le lemme 23, cela équivaut à $c_4' \equiv 1 + \pi \pmod 2$.

Lorsque la condition (C1′) n'est pas satisfaite, l'assertion 10 résulte de l'équivalence ci-dessus et de [2, th. 3(ii)]. Lorsque (C1′) est satisfaite, l'assertion 10 se déduit de l'équivalence ci-dessus, de [2, th. 3(ii)] et de la proposition 11.

3.7.4. Démonstration de l'assertion 5. On suppose $v(j) = 6$.

LEMME 25. *Pour tout $t \in \mu_3$,*

$$\frac{B_t}{c_4^2} \equiv 1 + t\Delta'\pi^2 \pmod 4.$$

De plus, B_t est un carré dans K_{nr} si seulement si

$$t = 1 \quad et \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration. D'après le lemme 10, on a $\varepsilon \equiv 1 \pmod 2$, et d'après le lemme 7, $\delta \equiv \Delta' \pmod 2$. Puis d'après le lemme 22, $c_4' \equiv c_6'^2 \equiv 1 \pmod 2$. On en déduit $\theta \equiv \Delta' \pmod 2$. D'où la congruence annoncée avec la relation (3.9). De plus, B_t est un carré dans K_{nr} si et seulement si l'unité $1 + t\Delta'\pi^2$ de N l'est. Supposons que tel soit le cas. Alors, comme $\Delta' \equiv 1$ ou $1 + \pi \pmod 2$, on a, d'après le lemme 11, $t = 1$, puis $\Delta' \equiv 1 + \pi \pmod 2$. Réciproquement, si $t = 1$ et $\Delta' \equiv 1 + \pi \pmod 2$, alors $1 + t\Delta'\pi^2 \equiv (1 + \pi)^2 \pmod 4$ et $B = B_1$ est un carré dans K_{nr}. D'où le lemme.

Supposons $\Delta' \equiv 1 + \pi \pmod 2$. Alors, d'une part, d'après le lemme précédent, $B = B_1$ est un carré dans K_{nr}, donc $|\Phi| = 2$ ou 4, d'après [2, th. 3(i)]. D'autre part, B_t pour $t \neq 1$ n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). On en déduit que nécessairement $|\Phi| = 4$.

Supposons $\Delta' \not\equiv 1 + \pi \pmod 2$. Alors, d'après le lemme précédent, pour tout $t \in \mu_3$, B_t n'est pas un carré dans K_{nr}. Donc d'après la proposition 2, on a $|\Phi| = 8$ (on a $c_6 \neq 0$ car $v(j) \neq 12$).

3.7.5. Démonstration de l'assertion 9. Supposons $v(j) = 18$. La courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 6$. D'après la proposition 1, si $t \in \mu_3$, B_t est un carré dans K_{nr} si seulement si $\widetilde{B}_{t^2}$ l'est. Or, d'après le lemme 25, on a

$$\widetilde{B}_{t^2} \in (K_{nr})^2 \iff t = 1 \text{ et } \widetilde{\Delta}' \equiv 1 + \pi \pmod 2.$$

D'après le lemme 23, on en déduit l'équivalence

$$B_t \in (K_{nr})^2 \iff t = 1 \text{ et } c_4' \equiv 1 + \pi \pmod 2.$$

L'assertion 9 résulte alors, comme au paragraphe précédent, de l'équivalence ci-dessus et de [2, th. 3(i)].

3.7.6. Démonstration de l'assertion 6. Supposons $v(j) = 8$.

LEMME 26. *On a*

$$\frac{B}{c_4^2} \equiv 1 + \varepsilon j'\pi_0^4 + \pi_0^8 \pmod 4.$$

De plus, B est un carré dans M si et seulement si $j' \equiv 1 + \pi^2 \pmod{\pi^3}$.

Démonstration. L'élément c_4'/δ est une unité de K, donc d'après le lemme 7, on a

$$\left(\frac{c_4'}{\delta}\right)^4 \equiv 1 \pmod 4, \quad \text{d'où} \quad j' = \frac{c_4'^3}{\delta^3} \equiv \frac{\delta}{c_4'} \pmod 4.$$

D'après les lemmes 10 et 7,

$$\varepsilon^2 j'^2 \pi_0^8 \equiv \pi_0^8 \pmod 4.$$

D'où la congruence annoncée d'après (3.9).

Supposons $K \in \Omega_1$. Alors, d'après le lemme 10, $\varepsilon \equiv 1 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1+\pi_0^4+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi^2 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi+\pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 12 et 13 que B est un carré dans M si et seulement si $j' \equiv 1+\pi^2 \pmod{\pi^3}$.

Supposons $K \in \Omega_2$. Alors, d'après le lemme 10, $\varepsilon \equiv -1 \equiv 1+\pi^2 \pmod 4$. Donc

$$\frac{B}{c_4^2} \equiv \begin{cases} 1+\pi_0^4+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8+\pi_0^{10} \pmod 4 & \text{si } j' \equiv 1+\pi \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi^2 \pmod{\pi^3}, \\ 1+\pi_0^4+\pi_0^7+\pi_0^8 \pmod 4 & \text{si } j' \equiv 1+\pi+\pi^2 \pmod{\pi^3}. \end{cases}$$

On vérifie alors avec les lemmes 12 et 13 que B est un carré dans M si et seulement si $j' \equiv 1+\pi^2 \pmod{\pi^3}$. D'où le lemme.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 6 résulte du lemme ci-dessus et de [2, th. 3(ii)]. Lorsque la condition (C2) est satisfaite, l'assertion 6 résulte du lemme ci-dessus, de [2, th. 3(ii)] et de la proposition 7.

3.7.7. Démonstration de l'assertion 8. Supposons $v(j) = 16$. La courbe $\widetilde{E}$ d'équation (2.2) a un invariant modulaire $\widetilde{j}$ de valuation $v(\widetilde{j}) = 8$. D'après la proposition 1, B est un carré dans M si seulement si $\widetilde{B}$ l'est. Or, d'après l'assertion 6 du théorème 2, c'est le cas si et seulement si $\widetilde{j}' \equiv 1+\pi^2 \pmod{\pi^3}$. D'après le lemme 23, cela équivaut à $j' \equiv 1+\pi^2 \pmod{\pi^3}$ car $j' \equiv 1/\widetilde{j}' \pmod{\pi^3}$.

Lorsque la condition (C2) n'est pas satisfaite, l'assertion 8 résulte de l'équivalence ci-dessus et de [2, th. 3(ii)]. Lorsque (C2) est satisfaite, l'assertion 8 résulte de l'équivalence ci-dessus, de [2, th. 3(ii)] et de la proposition 9.

3.7.8. Démonstration de l'assertion 7a. On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 1$.

LEMME 27. *Pour t dans μ_3,*

$$\theta \equiv 1+\pi \pmod 2 \quad \text{et} \quad \frac{B_t}{c_4^2} \equiv 1+t+t^2+t\pi \pmod 2.$$

Démonstration. D'après la relation (3.13), on a $\theta^3 \equiv 1+\pi \pmod 2$. Puis, d'après le lemme 7, on a $\theta^2 \equiv 1 \pmod 2$, d'où $\theta \equiv \theta^3 \equiv 1+\pi \pmod 2$. La seconde congruence résulte alors de la première et de la relation (3.12). D'où le lemme.

Supposons $t = 1$. Alors, $B/c_4^2 \equiv 1+\pi \pmod 2$. Donc, d'après le lemme 8, B n'est pas un carré dans K_{nr}.

Supposons $t \neq 1$. Alors, $v(B_t) = 1$ est impair. Donc, B_t n'est pas un carré dans K_{nr}.

Autrement dit, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}. D'après la proposition 2, on a $|\Phi| = 8$.

Cela démontre l'assertion 7a du théorème 2.

3.7.9. Démonstration de l'assertion 7b. On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 2$. En particulier, $v(c_4)$ est pair.

LEMME 28. *On a*

$$\theta \equiv 1 + \pi^2 c'_4 \pmod 4 \quad \textit{et} \quad B/c_4^2 \equiv 3 + \pi^2 c'_4 \pmod 4.$$

Démonstration. D'après la relation (3.13), on a $\theta^3 \equiv 1 \pmod 2$. Donc, d'après le lemme 7, $\theta \equiv \theta^3 \equiv 1 + \pi^2 c'_4 \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (3.12) appliquée à $t = 1$. D'où le lemme.

LEMME 29. *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. $K \in \Omega_1$ *et* $c'_4 \equiv 1 + \pi \pmod 2$.
2. $K \in \Omega_2$ *et* $c'_4 \equiv 1 \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}$, *puis*

$$B^{1/2}/c_4 \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}} \quad \textit{et} \quad C/\pi^{v(c_4)} \equiv c'_4 + \pi^2 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Démonstration. Sous ces hypothèses, d'après (3.1) et (3.2) et le lemme 28,

$$B/c_4^2 \equiv 1 \pmod 4.$$

D'après le lemme 9, il vient $B^{1/2}/c_4 \equiv 1 \pmod{2\mathcal{O}_{K_{nr}}}$. En particulier,

$$B^{1/2}/c_4 + 1 \equiv 0 \pmod{2\mathcal{O}_{K_{nr}}}.$$

Donc, d'après (3.8), on a

$$C/\pi^{v(c_4)} \equiv c'_4\theta \pmod{4\mathcal{O}_{K_{nr}}}.$$

Puis, d'après le lemme 28, $c'_4\theta \equiv c'_4 + \pi^2 \pmod 4$. D'où le résultat annoncé.

On reprend les notations du §3.4. En particulier, γ est une uniformisante de l'extension $K(\sqrt{1+\pi^3})$.

LEMME 30. *Supposons que l'une des deux conditions suivantes soit satisfaite :*

1. $K \in \Omega_1$ *et* $c'_4 \equiv 1 \pmod 2$.
2. $K \in \Omega_2$ *et* $c'_4 \equiv 1 + \pi \pmod 2$.

Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3})$ *est une extension quadratique de* K_{nr}, *puis*

$$B^{1/2}/c_4 \equiv 1 + \gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}},$$

$$C/\pi^{v(c_4)} \equiv c'_4 + \gamma^4 + \gamma^6 + \gamma^7 \pmod{4\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}}.$$

Démonstration. Sous ces hypothèses, d'après (3.1) et (3.2) et le lemme 28,

$$B/c_4^2 \equiv 1 + \pi^3 \pmod 4.$$

D'après le lemme 15, on a donc

$$K_{nr}(B^{1/2}) = K_{nr}(\sqrt{1+\pi^3}) \quad \text{et} \quad B^{1/2}/c_4 \equiv 1 + \gamma^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{1+\pi^3})}},$$

d'où la première congruence. Puis, d'après (3.8),

$$C/\pi^{v(c_4)} \equiv c'_4(2\gamma^3 + \theta) \pmod{4\mathcal{O}_{K_{nr}}}.$$

Or, 2 est associé à γ^4, donc $2c_4'\gamma^3 \equiv \gamma^7 \pmod 4$. Et, d'après le lemme 14, $\pi^2 \equiv \gamma^4 + \gamma^6 \pmod 4$. Donc, d'après le lemme 28, $c_4' + \gamma^4 + \gamma^6 \pmod 4$. D'où le lemme.

On procède comme suit pour finir la démonstration de l'assertion 7b.

1. Supposons $K \in \Omega_1$. Si la condition (C1′) est satisfaite, on est dans un cas d'application du lemme 29. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^2$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 8, ce n'est jamais le cas car $c_4' + \pi^2 \equiv 1 + \pi \pmod 2$ (condition (C1′)). On en déduit que $|\Phi| = 4$ dans ce cas ([2, th. 3(i)]).

   Si la condition (C1′) n'est pas satisfaite, on est dans un cas d'application du lemme 30. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c_4' + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$ l'est. Or, d'après le lemme 14, on a

$$c_4' + \gamma^4 + \gamma^6 + \gamma^7 \equiv \begin{cases} 1 + \gamma^4 + \gamma^6 + \gamma^7 \pmod 4 & \text{si } c_4' \equiv 1 \pmod 4, \\ 1 + \gamma^7 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^2 \pmod 4, \\ 1 + \gamma^4 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^3 \pmod 4, \\ 1 + \gamma^6 \pmod 4 & \text{si } c_4' \equiv 1 + \pi^2 + \pi^3 \pmod 4. \end{cases}$$

   D'après le lemme 16, C n'est donc pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([2, th. 3(i)]).

2. Supposons $K \in \Omega_2$. Si la condition (C1′) est satisfaite, on est dans un cas d'application du lemme 30. En particulier, B n'est pas un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans $K_{nr}(B^{1/2})$ si et seulement si l'unité $c_4' + \gamma^4 + \gamma^6 + \gamma^7$ des entiers de $K(\sqrt{1+\pi^3})$ l'est. Or, $c_4' + \gamma^4 + \gamma^6 + \gamma^7 \equiv c_4' \equiv 1 + \gamma^2 + \gamma^3 \pmod 2$. Donc, d'après le lemme 16, C n'est pas un carré dans $K_{nr}(B^{1/2})$ et $|\Phi| = 8$ dans ce cas ([2, th. 3(i)]).

   Si la condition (C1′) n'est pas satisfaite, on est dans un cas d'application du lemme 29. En particulier, B est un carré dans K_{nr}. De plus, comme $v(c_4)$ est pair, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^2$ de $\mathcal{O}_K$ l'est. Autrement dit, d'après le lemme 8, C est un carré dans K_{nr} si et seulement si $c_4' \equiv 1 + \pi^2$ ou $1 + \pi^3 \pmod 4$. D'après [2, th. 3(i)], on a donc

$$|\Phi| = \begin{cases} 2 & \text{si la condition (C3) est satisfaite,} \\ 4 & \text{sinon.} \end{cases}$$

Cela achève la démonstration de l'assertion 7b du théorème 2.

3.7.10. Démonstration de l'assertion 7c. On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) = 3$.

Lemme 31. *Pour tout t dans μ_3,*

$$\theta \equiv 1 + \pi^3 \pmod 4 \quad \textit{et} \quad B_t/c_4^2 \equiv 1 + t + t^2 + t\pi^3 \pmod 4.$$

Démonstration. D'après la relation (3.13), on a $\theta^3 \equiv 1 \pmod 2$, et d'après le lemme 7, $\theta^2 \equiv 1 \pmod 2$, d'où $\theta \equiv 1 \pmod 2$. D'après [2, th. 3(i)] et (3.13) on a alors $\theta \equiv \theta^3 \equiv 1 + \pi^3 \pmod 4$. La seconde congruence résulte alors de la première et de l'égalité (3.12). D'où le lemme.

On déduit du lemme 31 que pour $t \neq 1$ dans μ_3, $v(B_t) = 1$ est impair. En particulier, B_t n'est pas un carré dans K_{nr}.

On procède comme suit pour finir la démonstration de l'assertion 7c.

1. Supposons $K \in \Omega_1$. Alors, d'après le lemme 31 et (3.1), on a
$$B/c_4^2 \equiv 3 + \pi^3 \equiv 1 + \pi^2 \pmod 4.$$
Autrement dit, d'après le lemme 8, B n'est pas un carré dans K_{nr}. Par suite, pour tout t dans μ_3, B_t n'est pas un carré dans K_{nr}. D'après la proposition 2, cela implique $|\Phi| = 8$.
2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 31 et (3.2), on a
$$B/c_4^2 \equiv 3 + \pi^3 \equiv 1 + \pi^2 + \pi^3 \pmod 4.$$
Autrement dit, d'après le lemme 8, B est un carré dans K_{nr}. D'après [2, th. 3(i)], on a donc $|\Phi| = 2$ ou 4. Or, pour $t \neq 1$ dans μ_3, B_t n'est pas un carré dans K_{nr}, donc $|\Phi| = 4$ ou 8 (*loc. cit.*). Cela implique que nécessairement $|\Phi| = 4$ dans ce cas.

Cela achève la démonstration de l'assertion 7c du théorème 2.

3.7.11. Démonstration de l'assertion 7d. On a $v(j) = 12$ et $2v(c_6) - 3v(c_4) \geq 4$.

Lemme 32. *On a*
$$\theta \equiv 1 \pmod 4 \quad \textit{et} \quad B/c_4^2 \equiv 3 \pmod 4.$$

Démonstration. D'après (3.13), on a $\theta^3 \equiv 1 \pmod 2$, et d'après le lemme 7, $\theta^2 \equiv 1 \pmod 2$, d'où $\theta \equiv 1 \pmod 2$. D'après [2, th. 3(i)] et (3.13) on a alors $\theta \equiv \theta^3 \equiv 1 \pmod 4$. La seconde congruence résulte alors de (3.12).

Lemme 33. *Supposons $K \in \Omega_1$. Alors, $K_{nr}(B^{1/2}) = K_{nr}$ et*
$$B^{1/2}/c_4 \equiv 1 + \pi \pmod{2\mathcal{O}_{K_{nr}}} \quad \textit{et} \quad C/\pi^{v(c_4)} \equiv c_4' + \pi^3 \pmod{4\mathcal{O}_{K_{nr}}}.$$

Démonstration. D'après le lemme 32, on a $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$. Or, 3 est un carré dans K_{nr} car K est dans Ω_1. D'où l'égalité annoncée. La première congruence résulte du lemme 17 et de la congruence $B/c_4^2 \equiv 3 \pmod 4$ du lemme 32. D'après l'égalité (3.8), le lemme 32 et la première congruence ci-dessus, on a
$$C/\pi^{v(c_4)} \equiv c_4'(2\pi + 1) \pmod{4\mathcal{O}_{K_{nr}}}.$$
D'où le résultat car $2c_4'\pi \equiv \pi^3 \pmod 4$.

On reprend les notations du §3.5. En particulier, η désigne, lorsque $K \in \Omega_2$, une uniformisante de $K(\sqrt{3})$.

Lemme 34. *Supposons $K \in \Omega_2$. Alors, $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ et*
$$B^{1/2}/c_4 \equiv \sqrt{3} \equiv 1 + \eta^2 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}},$$
$$C/\pi^{v(c_4)} \equiv c_4'(3 + 2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$

Démonstration. L'égalité et la première congruence résultent des lemmes 32 et 19. La seconde congruence résulte de la première, du lemme 32 et de (3.8).

On procède comme suit pour finir la démonstration de l'assertion 7d.

1. Supposons $K \in \Omega_1$. Si $v(c_4) = v(C)$ est impair, alors C n'est pas un carré dans $K_{nr}(B^{1/2}) = K_{nr}$. Donc $|\Phi| = 4$ d'après [2, th. 3(i)]. Si $v(c_4)$ est pair, alors, d'après le lemme 33, B est un carré dans K_{nr}. De plus, C est un carré dans K_{nr} si et seulement si l'unité $c_4' + \pi^3$ de $\mathcal{O}_K$ l'est. Or, d'après le lemme 8, c'est le cas si et seulement si la condition (C3) est satisfaite. D'où le résultat d'après [2, th. 3(i)].
2. Supposons $K \in \Omega_2$. Alors, d'après le lemme 34, B n'est pas un carré dans K_{nr}. Si $v(c_4)$ est impair, on a
$$\frac{C}{\pi^{v(c_4)-1}\eta^2} \equiv c_4'\beta(3+2\sqrt{3}) \pmod{4\mathcal{O}_{K_{nr}(\sqrt{3})}},$$
où β est une unité des entiers de $K(\sqrt{3})$ telle que $\pi = \eta^2\beta$. On en déduit que C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'\beta(3+2\sqrt{3})$ de $K(\sqrt{3})$ est un carré dans $K_{nr}(\sqrt{3})$. Or, d'après le lemme 19, on a $\beta \equiv 1+\eta \pmod{\eta^2}$. D'où $c_4'\beta(3+2\sqrt{3}) \equiv 1+\eta \pmod{\eta^2}$. On en déduit avec le lemme 21 que C n'est pas un carré dans $K_{nr}(\sqrt{3})$. D'où $|\Phi| = 8$ dans ce cas d'après [2, th. 3(i)].
Supposons $v(c_4)$ pair. Alors, C est un carré dans $K_{nr}(B^{1/2}) = K_{nr}(\sqrt{3})$ si et seulement si l'unité $c_4'(3+2\sqrt{3})$ de $K(\sqrt{3})$ l'est. Si c_4' est un carré dans $K_{nr}(\sqrt{3})$, alors C n'est pas un carré dans $K_{nr}(\sqrt{3})$, car d'après le lemme 20, $3+2\sqrt{3}$ ne l'est pas. Si c_4' n'est pas un carré dans $K_{nr}(\sqrt{3})$, alors d'après le lemme 18, on a $c_4' \equiv 1+\pi \pmod 2$. D'après le lemme 19, on a alors
$$c_4'(3+2\sqrt{3}) \equiv 1+\pi \equiv 1+\eta^2+\eta^3 \pmod{2\mathcal{O}_{K_{nr}(\sqrt{3})}}.$$
Donc, d'après le lemme 21, $c_4'(3+2\sqrt{3})$ n'est pas un carré dans $K_{nr}(\sqrt{3})$ et il en va de même pour C d'après l'équivalence ci-dessus. D'où $|\Phi| = 8$ dans ce cas d'après [2, th. 3(i)].

Cela achève la démonstration de l'assertion 7d du théorème 2.

3.8. Calculs des types de Néron. D'après [5], la courbe E admet un modèle de Weierstrass de la forme
$$Y^2 = X^3 - \frac{c_4}{48}X - \frac{c_6}{864}. \tag{W_0}$$
Ce modèle est entier si et seulement si $v(c_4) \geq 8$ et $v(c_6) \geq 10$. Dans toute cette section, on note Δ_m le discriminant minimal de E.

3.8.1. Cas où $v(j) = 4$. On suppose que le modèle de Weierstrass de E vérifie $v(j) = 4$ et la condition (C1), i.e. $\Delta' \equiv 1+\pi \pmod 2$. D'après la formule (3.10), on a
$$c_4'^3 - c_6'^2 = \varepsilon^3\pi^8\Delta', \tag{3.14}$$
où l'on a posé $\varepsilon = 3(2/\pi^2)^2$.

LEMME 35. *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV*. Alors, $v(\Delta_m) = 8$.*

Démonstration. D'après [2, th. 2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. C'est en contradiction avec la condition $v(j) = 4$. Par ailleurs, si E est de type IV*, on a $v(\Delta_m) = 8$. D'où le lemme.

LEMME 36. *Supposons* $v(\Delta) \equiv 8 \pmod{12}$. *Alors,* $v(\Delta_m) = 8$ *si et seulement si* $c'_6 \equiv 1 \pmod 2$.

Démonstration. Supposons $v(\Delta) \equiv 8 \pmod{12}$. D'après l'appendice B, quitte à faire un changement de variables, on peut supposer

$$(v(c_4), v(c_6), v(\Delta)) = (8, 12, 20).$$

La courbe E correspond alors à un cas 7 de Tate ou à un cas non minimal. Le modèle (W_0) de E est entier et, avec les notations de [5], on a

$$b_2 = 0, \quad b_4 = -2\frac{c_4}{48} = -6\frac{c'_4}{\varepsilon^2}, \quad b_6 = -4\frac{c_6}{864} = -2^3\frac{c'_6}{\varepsilon^3}, b_8 = -\left(\frac{c_4}{48}\right)^2 = -3^2\frac{c'^2_4}{\varepsilon^4}.$$

Examinons à présent à quelle condition le système suivant de congruences admet une solution (r, s) dans $\mathcal{O}_K$:

$$\begin{cases} b_8 + 3r^2 b_4 + 3r^4 \equiv 0 \pmod{4\pi}, \\ r \equiv s^2 \pmod 2. \end{cases}$$

Comme $v(b_8) = 0$, si (r, s) est une solution, on a nécessairement $r \in \mathcal{U}_K$, donc s est également une unité et, d'après la seconde congruence, $r \equiv 1 \pmod 2$ (et on peut choisir $s = 1$). On a alors $r^2 \equiv r^4 \equiv 1 \pmod{4\pi}$, et de même $\varepsilon^2 \equiv \varepsilon^4 \equiv 1 \pmod{4\pi}$. Donc

$$-9c'^2_4 - 18c'_4 + 3 \equiv 0 \pmod{4\pi}.$$

Autrement dit, le système précédent admet une solution si et seulement si $c'^2_4 + 2c'_4 \equiv 3 \pmod{4\pi}$. Or, d'après la relation (3.14) et le lemme 7, on a $c'_4 \equiv 1 \pmod 2$, puis $c'^2_4 \equiv 1 \pmod{4\pi}$ et $c'_4 \equiv c'^2_6 \pmod{4\pi}$. Donc $3 \equiv c'^2_4 + 2c'_4 \equiv 1 + 2c'^2_6 \pmod{4\pi}$. Mais, par ailleurs,

$$1 + 2c'^2_6 \equiv \begin{cases} 3 \pmod{4\pi} & \text{si } c'_6 \equiv 1 \pmod 2, \\ 3 + \pi^4 \pmod{4\pi} & \text{si } c'_6 \equiv 1 + \pi \pmod 2. \end{cases}$$

On en déduit qu'il existe une solution (r, s) au système de congruences ci-dessus si et seulement si $c'_6 \equiv 1 \pmod 2$. On conclut alors au lemme avec [3, prop. 4].

LEMME 37. *Supposons* $c'_6 \equiv 1 \pmod 2$. *Alors,*

$$c'_4 \equiv (1 + \pi^4)(1 - c'^2_6) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Démonstration. On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 10). En réduisant l'égalité (3.14) modulo 2, on obtient $c'_4 \equiv 1 \pmod 2$. Puis, d'après le lemme 7, on a $c'_4 \equiv c'^3_4 \pmod{4\pi}$ et, comme $c'_6 \equiv 1 \pmod 2$, $c'^2_6 \equiv 1 \pmod{4\pi}$. Comme d'après (3.14), on a $c'^3_4 \equiv c'^2_6 \pmod{4\pi}$, il vient $c'_4 \equiv 1 \pmod{4\pi}$. On en déduit $c'^2_4 \equiv 1 \pmod{\pi^7}$, puis $c'^3_4 \equiv c'_4 \pmod{\pi^7}$. D'où $c'_4 \equiv c'^2_6 \pmod{\pi^7}$ avec la relation (3.14) réduite modulo π^7. Posons donc $c'_4 = c'^2_6 + \pi^7 a$, avec $a \in \mathcal{O}_K$. On a

$$c'^3_4 \equiv c'^6_6 + 3\pi^7 c'^4_6 a \pmod{\pi^{10}}.$$

Or, $c_6'^4 \equiv 1 \pmod{\pi^3}$ et $3 \equiv 1+\pi^2 \pmod{\pi^3}$, donc $c_4'^3 \equiv c_6'^6 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}$, puis

$$c_4'^3 - c_6'^2 \equiv c_6'^6 - c_6'^2 + \pi^7 a + \pi^9 a \pmod{\pi^{10}}.$$

Mais, comme $c_6'^2 \equiv 1 \pmod{\pi^5}$ car $c_6' \equiv 1 \pmod 2$, on a $c_6'^2 + 1 \equiv 2 \pmod{\pi^5}$ et

$$c_6'^6 - c_6'^2 = c_6'^2(c_6'^2+1)(c_6'^2-1) \equiv 2(c_6'^2-1) \equiv 2(c_4' - \pi^7 a - 1) \pmod{\pi^{10}}.$$

Autrement dit, $c_4'^3 - c_6'^2 \equiv 2c_4' - 2 - \pi^7 a + \pi^9 a \pmod{\pi^{10}}$ et $c_4'^3 - c_6'^2 \equiv c_4' + c_6'^2 - 2 + \pi^9 a \pmod{\pi^{10}}$. Par ailleurs, d'après l'hypothèse (C1), on a $c_4'^3 - c_6'^2 \equiv \pi^8 + \pi^9 \pmod{\pi^{10}}$. On en déduit donc

$$c_4' \equiv -c_6'^2 + 2 + \pi^8 + \pi^9(a+1) \pmod{\pi^{10}}.$$

Or, $\pi^9(a+1) = \pi^2(c_4' - c_6'^2 + \pi^7)$. Donc $(1-\pi^2)c_4' \equiv -(1+\pi^2)c_6'^2 + 2 + \pi^8 + \pi^9 \pmod{\pi^{10}}$. D'où

$$c_4' \equiv \frac{1+\pi^2}{1-\pi^2}(1-c_6'^2) + 1 + \pi^8 + \pi^9 \pmod{\pi^{10}}.$$

Enfin, $(1+\pi^2)/(1-\pi^2) \equiv 1 + \pi^4 \pmod{\pi^5}$ et donc le résultat car $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$. Cela démontre le lemme.

Posons

$$a_2 = \frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6' - 1\right), \quad a_4 = \frac{1}{\pi^4}\left(\frac{3}{\varepsilon^2}(c_6'^2 - c_4') - 4\right), \quad a_6 = \frac{1}{\pi^6}\left(\frac{c_6'}{\varepsilon^3}(c_6'^2 - 3c_4' - 2) - 4\right).$$

PROPOSITION 3. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. *Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E *pour lequel*

$$a_4 \equiv \frac{1}{\pi^2}(c_6'^2 - 1) + \varepsilon \pmod 4, \quad a_6 \equiv \frac{\varepsilon}{\pi^2}\left(\frac{c_6'}{\varepsilon} + 1\right) + \pi^2 + \pi^3 \pmod 4,$$

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4, \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Démonstration. Le changement de variables

$$X = x + \frac{1}{\pi^2}\frac{c_6'}{\varepsilon}, \qquad Y = y + \frac{x}{\pi} + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Les éléments $2/\pi$ et $4/\pi^3$ sont entiers. D'après le lemme 36, on a $c_6' \equiv 1 \pmod 2$. Donc, d'après le lemme 10, le coefficient a_2 est entier. Vérifions que a_4 et a_6 le sont aussi et qu'ils satisfont aux congruences annoncées. D'après le lemme 37, on a

$$\begin{aligned}\pi^4 a_4 &\equiv \frac{3}{\varepsilon^2}(c_6'^2 - (1+\pi^4)(1-c_6'^2) - 1) - 4 \pmod{\pi^8}\\ &\equiv \frac{3}{\varepsilon^2}(2+\pi^4)(c_6'^2 - 1) - 4 \pmod{\pi^8}.\end{aligned}$$

Or, $c_6'^2 - 1 \equiv 0 \pmod{\pi^5}$, donc $v(a_4) = 0$ et a_4 est une unité de $\mathcal{O}_K$. Puis, on a $\pi^4 a_4 \equiv 2(c_6'^2 - 1) - 4 \pmod{\pi^8}$ et

$$a_4 \equiv \left(\frac{2}{\pi^2}\right)\frac{1}{\pi^2}(c_6'^2 - 1) - \left(\frac{2}{\pi^2}\right)^2 \pmod 4.$$

On en déduit la congruence annoncée pour a_4 car $v(c_6'^2-1)\geq 5$ et $2/\pi^2$ est une unité. Examinons à présent le coefficient a_6. On a, d'après le lemme 37,

$$\begin{aligned}\pi^6 a_6 &= \frac{c_6'}{\varepsilon^3}(c_6'^2-3c_4'-2)-4\\ &\equiv \frac{c_6'}{\varepsilon^3}(c_6'^2-3(1+\pi^4)(1-c_6'^2)-5)+\pi^8+\pi^9-4 \pmod{\pi^{10}}\\ &\equiv \frac{c_6'}{\varepsilon^3}((4+3\pi^4)(c_6'^2-1)-4)+\pi^8+\pi^9-4 \pmod{\pi^{10}}.\end{aligned}$$

Or, $4+3\pi^4\equiv 0 \pmod{\pi^5}$ et $c_6'^2-1\equiv 0 \pmod{\pi^5}$, donc $\pi^6 a_6\equiv -4c_6'/\varepsilon^3-4+\pi^8+\pi^9 \pmod{\pi^{10}}$. Puis, comme $\varepsilon^2\equiv 1 \pmod{\pi^6}$, on a

$$\pi^6 a_6\equiv -4\left(\frac{c_6'}{\varepsilon}+1\right)+\pi^8+\pi^9 \pmod{\pi^{10}}.$$

D'où $v(a_6)\geq 0$ car $c_6'/\varepsilon+1\equiv 0 \pmod 2$ et

$$a_6\equiv -\left(\frac{2}{\pi^2}\right)^2\frac{1}{\pi^2}\left(\frac{c_6'}{\varepsilon}+1\right)+\pi^2+\pi^3 \pmod 4.$$

D'où la congruence annoncée pour a_6 par définition de ε.

On en déduit

$$3a_6\equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6'+3\right)+\pi^2+\pi^3 \pmod 4.$$

Or, $3\equiv -5\equiv -1-4 \pmod{\pi^6}$, donc

$$3a_6\equiv \frac{\varepsilon}{\pi^2}\left(\frac{3}{\varepsilon}c_6'-1\right)-\frac{4}{\pi^2}\varepsilon+\pi^2+\pi^3 \pmod 4.$$

Or, $4\equiv \pi^4 \pmod{\pi^6}$, donc, par définition du coefficient a_2, on a $3a_6\equiv \varepsilon a_2+\pi^3 \pmod 4$. C'est la congruence voulue.

Enfin, par définition du coefficient a_2,

$$\begin{aligned}\pi^2 a_2\left(a_2+\frac{2}{\pi^2}\right)&=\frac{1}{\pi^2}\left(\frac{3}{\varepsilon}c_6'-1\right)\left(\frac{3}{\varepsilon}c_6'+1\right)\equiv\frac{1}{\pi^2}\left(\frac{9}{\varepsilon^2}c_6'^2-1\right)\pmod 4\\ &\equiv\frac{1}{\pi^2}(c_6'^2-1)\pmod 4 \quad \text{car } 9/\varepsilon^2\equiv 1 \pmod{\pi^6}\\ &\equiv a_4-\varepsilon \pmod 4\end{aligned}$$

d'après la première congruence. Cela achève la démonstration de la proposition 3.

Posons

$$r=\frac{2}{\pi^2}+\pi \quad \text{et} \quad t=\pi.$$

Notons b_2, b_4, b_6 et b_8 les invariants standard associés au modèle (W) de E.

Lemme 38. *Supposons* $(v(c_4),v(c_6),v(\Delta))=(4,6,8)$. *Alors,*

$$b_8+3rb_6+3r^2b_4+r^3b_2+3r^4\equiv 0 \pmod{\pi^5}.$$

De plus, la courbe E correspond à un cas ≥ 7 de Tate si et seulement si $(a_2+1)(\pi^3+2a_2)+2\equiv \pi^2+\pi^3 \pmod 4$.

Démonstration. On considère le modèle (W) de E de la proposition 3. On a

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2, \quad b_4 = \frac{2^3}{\pi^4} + 2a_4, \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6 b,$$
$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2.$$

On en déduit les congruences suivantes :

$$b_2 \equiv -\varepsilon\pi^2 + 4a_2 \pmod{4\pi}, \quad b_4 \equiv 2(a_4 - \varepsilon) \equiv 0 \pmod{4\pi},$$
$$b_6 \equiv \pi^2 + 4a_2 \pmod{4\pi}, \quad b_8 \equiv \pi^2(a_2 - \varepsilon a_6) + 1 + 4a_2 \equiv 1 \pmod{4\pi}$$

car $a_2 - \varepsilon a_6 \equiv 2a_2 \pmod{\pi^3}$.

L'entier r de $\mathcal{O}_K$ est une unité de $\mathcal{O}_K$ et on a

$$\begin{aligned} b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 &\equiv 1 + 3r\pi^2 + 4a_2 - \varepsilon r^3\pi^2 + 4a_2 + 3 \pmod{4\pi} \\ &\equiv 4 + \pi^2(3 - \varepsilon r^2) \pmod{4\pi} \\ &\equiv 4 + \pi^2((2/\pi^2)^2 - r^2) \pmod{4\pi}. \end{aligned}$$

Or, $r^2 \equiv (2/\pi^2)^2 + \pi^2 \pmod{\pi^3}$. Donc $4 + \pi^2((2/\pi^2)^2 - r^2) \equiv 0 \pmod{4\pi}$. Autrement dit, $r = 2/\pi^2 + \pi$ vérifie la condition (a) de [3, prop. 3]. On a alors, d'après les congruences de la proposition 3,

$$\begin{aligned} a_6 + ra_4 + r^2a_2 + r^3 &= a_6 + \left(\frac{2}{\pi^2} + \pi\right)a_4 + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \\ &\equiv \pi^3 - \varepsilon a_2 + \left(\frac{2}{\pi^2} + \pi\right)\left(\varepsilon + \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right)\right) \\ &\quad + \left(\frac{2}{\pi^2} + \pi\right)^2 a_2 + \left(\frac{2}{\pi^2} + \pi\right)^3 \pmod 4 \\ &\equiv \pi^3 - \varepsilon a_2 + \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2a_2\left(a_2 + \frac{2}{\pi^2}\right) - \varepsilon a_2 + \frac{4}{\pi}a_2 + \pi^2 a_2 \\ &\quad - \varepsilon\left(\frac{2}{\pi^2}\right) + \pi\varepsilon + 2 + \pi^3 \pmod 4 \\ &\equiv \pi^3(a_2 + 1) + 2a_2(a_2 + 1) + 2 \equiv (a_2 + 1)(\pi^3 + 2a_2) + 2 \pmod 4. \end{aligned} \tag{3.15}$$

Par ailleurs, $v((a_2 + 1)(\pi^3 + 2a_2)) \geq 3$, donc en particulier,

$$a_6 + ra_4 + r^2a_2 + r^3 \equiv 2 \equiv \pi^2 \pmod{\pi^3}.$$

On a alors, avec $t = \pi$,

$$\begin{aligned} t\left(\frac{4}{\pi^3}\right) + t^2 + rt\left(\frac{2}{\pi}\right) &\equiv \pi^2\left(\frac{2}{\pi^2}\right)^2 + \pi^2 + 2\left(\frac{2}{\pi^2} + \pi\right) \pmod 4 \\ &\equiv \pi^2 + \pi^2 + \pi^2 + \pi^3 \pmod 4 \\ &\equiv \pi^2 + \pi^3 \pmod 4. \end{aligned} \tag{3.16}$$

Donc, en particulier, $t(4/\pi^3) + t^2 + rt(2/\pi) \equiv \pi^2 \pmod{\pi^3}$. On déduit alors de [3, prop. 3] appliqué à r et t et des congruences (3.15) et (3.16) que l'on est dans un cas ≥ 7 de Tate si et seulement si $(a_2 + 1)(\pi^3 + 2a_2) + 2 \equiv \pi^2 + \pi^3 \pmod 4$. D'où le lemme.

LEMME 39. *Supposons* $c_6' \equiv 1 \pmod 2$. *Alors,* $v((a_2+1)(\pi^3+2a_2)) \geq 3$. *De plus, on a* $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ *si et seulement si* $a_2 \equiv 0$ *ou* $1+\pi \pmod 2$.

Démonstration. D'après l'hypothèse faite, a_2 est entier. On a $v((a_2+1)(\pi^3+2a_2)) \geq 3$. De plus, $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$ si et seulement si $v((a_2+1)(\pi^3+2a_2)) = 3$. Or, $v((a_2+1)(\pi^3+2a_2)) = 3$ si et seulement si $v(a_2) \geq 2$ ou $v(a_2+1) = 1$. D'où le résultat.

PROPOSITION 4. *Supposons* $K \in \Omega_1$. *On a* $|\Phi| = 3$ *si et seulement si les conditions suivantes sont satisfaites*

1. $v(\Delta) \equiv 8 \pmod{12}$.
2. $c_6' \equiv 1+\pi^2 \pmod 4$ *ou* $c_6' \equiv 1+\pi^3 \pmod 4$.

Démonstration. Supposons $|\Phi| = 3$. D'après [2, th. 2(i)], E est de type IV ou IV*. Donc, d'après le lemme 35, E est de type IV* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut de plus supposer $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. Puis, d'après le lemme 36, on a $c_6' \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 38, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_1, il vient $(a_2+1)(\pi^3+2a_2) \equiv 0 \pmod 4$. Autrement dit, d'après le lemme 39, on a $a_2 \equiv 1$ ou $\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_1, on a, d'après le lemme 10,

$$\pi^2 a_2 \equiv -c_6' - 1 \pmod 4, \quad \text{d'où} \quad c_6' \equiv \pi^2 a_2 - 1 \equiv \pi^2 a_2 + 1 + \pi^2 + \pi^3 \pmod 4.$$

On en déduit $c_6' \equiv 1+\pi^2$ ou $1+\pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 36, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (4,6,8)$. D'après l'appendice B, E correspond alors à un cas 6, 7 ou 8 (type IV*) de Tate. Par ailleurs, comme K est dans Ω_1, on a $a_2 \equiv (3c_6'-1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 1$ ou $\pi \pmod 2$. Donc, d'après le lemme 39, $(a_2+1)(\pi^3+2a_2) \equiv 0 \pmod 4$, puis, comme K est dans Ω_1, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Autrement dit, d'après le lemme 38, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est dans un cas 8. Toujours d'après le lemme 38, comme la condition (a) de [3, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 1$ ou $\pi \pmod 2$ et $r \equiv 1 \pmod 2$. En effet, ou bien $a_2 + 1 \equiv 0 \pmod 2$ et on choisit $s = 0$, ou bien $a_2 + 1 \equiv 1+\pi \pmod 2$ et on choisit $s = 1$. La condition (b) de [3, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [2, th. 2(i)]. Cela démontre la proposition.

PROPOSITION 5. *Supposons* $K \in \Omega_2$. *On a* $|\Phi| = 3$ *si et seulement si les conditions suivantes sont satisfaites :*

1. $v(\Delta) \equiv 8 \pmod{12}$.
2. $c_6' \equiv 1 \pmod 4$ *ou* $c_6' \equiv 1+\pi^2+\pi^3 \pmod 4$.

Démonstration. Supposons $|\Phi| = 3$. D'après [2, th. 2(i)], E est de type IV ou IV*. Donc, d'après le lemme 35, E est de type IV* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un

changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. Puis, d'après le lemme 36, on a $c'_6 \equiv 1 \pmod 2$. Comme on est dans un cas ≥ 7 de Tate, on a, d'après le lemme 38, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Donc, comme K est dans Ω_2, il vient $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$. Autrement dit, d'après le lemme 39, on a $a_2 \equiv 0$ ou $1+\pi \pmod 2$. Or, par définition du coefficient a_2, lorsque K est dans Ω_2, on a, d'après le lemme 10,

$$\pi^2 a_2 \equiv c'_6 - 1 \pmod 4, \quad \text{d'où} \quad c'_6 \equiv \pi^2 a_2 + 1 \pmod 4.$$

On en déduit $c'_6 \equiv 1$ ou $1+\pi^2+\pi^3 \pmod 4$.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c'_6 \equiv 1 \pmod 2$ et, d'après le lemme 36, on a $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$. D'après l'appendice B, E correspond à un cas 6, 7 ou 8 (type IV*) de Tate. Par ailleurs, comme K est dans Ω_2, on a $a_2 \equiv (c'_6 - 1)/\pi^2 \pmod 2$, d'où $a_2 \equiv 0$ ou $1+\pi \pmod 2$. Donc, d'après le lemme 39, $(a_2+1)(\pi^3+2a_2) \equiv \pi^3 \pmod 4$, puis, comme K est dans Ω_2, $(a_2+1)(\pi^3+2a_2)+2 \equiv \pi^2+\pi^3 \pmod 4$. Autrement dit, d'après le lemme 38, on est dans un cas ≥ 7 de Tate. Vérifions que l'on est dans un cas 8. Toujours d'après le lemme 38, comme la condition (a) de [3, prop. 4] est vérifiée, on doit s'assurer qu'il existe un entier s de $\mathcal{O}_K$ tel que

$$a_2 + r \equiv s^2 + s\pi \pmod 2.$$

Or, c'est bien le cas car $a_2 \equiv 0$ ou $1+\pi \pmod 2$ et $r \equiv 1+\pi \pmod 2$. En effet, ou bien $a_2+1+\pi \equiv 1+\pi \pmod 2$ et on choisit $s=1$, ou bien $a_2+1+\pi \equiv 0 \pmod 2$ et on choisit $s=0$. La condition (b) de [3, prop. 4] est donc vérifiée et on est bien dans un cas 8 de Tate. On conclut alors que $|\Phi| = 3$ avec [2, th. 2(i)]. Cela démontre la proposition.

3.8.2. Cas où $v(j) = 8$. On suppose que le modèle de Weierstrass de E vérifie $v(j) = 8$ et la condition (C2), i.e. $j' \equiv 1+\pi^2 \pmod{2\pi}$. D'après la formule (3.10), on a

$$c'^3_4 - c'^2_6 = \varepsilon^3 \pi^4 \Delta'. \tag{3.17}$$

Lemme 40. *La courbe E n'est pas de type IV*. Supposons qu'elle soit de type IV. Alors, $v(\Delta_m) = 4$.*

Démonstration. D'après [2, th. 2(i)], si E est de type IV*, on a $v(\Delta_m) = 8$. C'est en contradiction avec la condition $v(j) = 8$. Par ailleurs, si E est de type IV, on a $v(\Delta_m) = 4$. D'où le lemme.

Lemme 41. *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, $v(\Delta_m) = 4$ si et seulement si $c'_6 \equiv 1 \pmod 2$.*

Démonstration. Supposons $v(\Delta) \equiv 4 \pmod{12}$. D'après l'appendice B, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8, 12, 16)$. Le modèle (W_0) de E est alors entier et la courbe E correspond à un cas 7 de Tate ou à un cas non minimal. Exactement comme dans la démonstration du lemme 35, on montre qu'il n'est pas minimal si et seulement si $c'_6 \equiv 1 \pmod 2$. D'où le lemme.

Lemme 42. *Supposons $c'_6 \equiv 1 \pmod 2$. Alors, $c'_4 \equiv c'^2_6 + \varepsilon\pi^4 \pmod{\pi^7}$.*

Démonstration. On a $\varepsilon \equiv \pm 1 \pmod 4$, d'où $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, puis $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ (lemme 10). En réduisant l'égalité (3.17) modulo 2, on obtient $c'_4 \equiv 1 \pmod 2$. Puis, d'après le lemme 7, on a $c'_4 \equiv c'^3_4 \pmod{4\pi}$ et $c'^2_6 \equiv 1 \pmod{4\pi}$ car $c'_6 \equiv 1 \pmod 2$. Comme d'après (3.17), on a $c'^3_4 \equiv c'^2_6 + \pi^4 \pmod{4\pi}$, il vient

$$c'_4 \equiv 1 + \pi^4 \pmod{4\pi}. \tag{3.18}$$

On en déduit $c'^2_4 \equiv 1 + 2\pi^4 \equiv 1 + \pi^6 \pmod{4\pi^3}$, puis

$$c'^3_4 \equiv c'_4 + \pi^6 \pmod{4\pi^3}. \tag{3.19}$$

Par ailleurs, d'après la relation (3.18), on a, en particulier, $c'_4 \equiv 1 \pmod{2\pi}$, donc l'hypothèse $j' \equiv 1 + \pi^2 \pmod{2\pi}$ implique

$$\Delta' \equiv 1 + \pi^2 \pmod{2\pi}. \tag{3.20}$$

Autrement dit, d'après l'égalité (3.17) et la congruence (3.19),

$$c'_4 \equiv c'^2_6 + \varepsilon\pi^4 \pmod{\pi^7},$$

car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$, donc, en particulier, $\varepsilon^2 \equiv 1 \pmod{2\pi}$. D'où le résultat.

Posons

$$a_2 = \frac{1}{\pi^2}(3\varepsilon c'_6 - 1), \qquad a_4 = \frac{1}{\pi^4}\frac{3}{\varepsilon^2}(\varepsilon^4 c'^2_6 - c'_4), \qquad a_6 = \frac{1}{\pi^6}\frac{c'_6}{\varepsilon^3}(\varepsilon^6 c'^2_6 - 3c'_4\varepsilon^2 - 2).$$

Proposition 6. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors, l'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel $a_4 \equiv 1 \pmod 2$ *et* $a_6 \equiv 1 \pmod \pi$.

Démonstration. Le changement de variables

$$X = x + \frac{\varepsilon c'_6}{\pi^2}, \qquad Y = y + \frac{x}{\pi}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $2/\pi$ est entier. D'après le lemme 41, on a $c'_6 \equiv 1 \pmod 2$. De plus, d'après le lemme 10, le coefficient a_2 est entier. Vérifions que les coefficients a_4 et a_6 sont entiers et satisfont aux congruences annoncées.

On a

$$\pi^4 a_4 = \frac{3}{\varepsilon^2}(\varepsilon^4 c'^2_6 - c'_4) \equiv \frac{3}{\varepsilon^2}(c'^2_6 - c'_4) \equiv 3\frac{\pi^4}{\varepsilon^2} \equiv \pi^4 \pmod{\pi^6},$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^6}$ et, d'après le lemme 42, $c'_4 \equiv c'^2_6 + \pi^4 \pmod{\pi^6}$. D'où $a_4 \equiv 1 \pmod 2$.

Examinons à présent le coefficient a_6. D'après le lemme 42,

$$\begin{aligned}\frac{\varepsilon^3}{c'_6}\pi^6 a_6 &\equiv \varepsilon^2 c'^2_6 - 3c'_4\varepsilon^2 - 2\varepsilon^2 \pmod{4\pi^3} \\ &\equiv \varepsilon^2(c'^2_6 - 3c'_4 - 2) \equiv \varepsilon^2(-2c'_4 - 2 - \varepsilon\pi^4) \pmod{4\pi^3},\end{aligned}$$

car $\varepsilon^4 \equiv 1 \pmod{\pi^7}$. Or, $-\varepsilon\pi^4 = -12$ et, d'après le lemme 42 et la congruence $c_6' \equiv 1 \pmod 2$, on a $c_4' + 1 \equiv 2 + \pi^4 \pmod{4\pi}$. Donc

$$\frac{\varepsilon^3}{c_6'}\pi^6 a_6 \equiv -2\pi^4 \equiv \pi^6 \pmod{4\pi^3}.$$

Comme ε^3/c_6' est une unité de $\mathcal{O}_K$, il en résulte $a_6 \equiv 1 \pmod\pi$ et la proposition.

LEMME 43. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors, E ne correspond pas à un cas* 4 *de Tate.*

Démonstration. D'après l'appendice B, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 6. Supposons qu'il corresponde à un cas ≥ 4. D'après la congruence $a_4 \equiv 1 \pmod 2$, $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 2]. Par ailleurs, avec les notations de [5],

$$b_2 \equiv \pi^2 \pmod{2\pi}, \quad b_4 \equiv \pi^2 \pmod{2\pi}, \quad b_6 \equiv 0 \pmod{2\pi}, \quad b_8 \equiv \pi^2 a_6 - 1 \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv \pi^2 a_6 + 2 \equiv \pi^2(a_6 + 1) \pmod{2\pi}$. D'où le résultat d'après [3, prop. 2] et la congruence $a_6 \equiv 1 \pmod\pi$.

LEMME 44. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. *Alors, a_2 et a_6 sont entiers et*

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c_6' + 1) \pmod 2, \qquad c_6' \equiv \pi^2 a_2 - \varepsilon \pmod 4,$$

$$a_6 \equiv \frac{1}{\pi^6}(c_6'^2 - 3c_4' - 2) \pmod 2, \qquad c_4' \equiv -c_6'^2 + 6 + \pi^6 a_6 \pmod{\pi^8}.$$

Démonstration. Les éléments a_2 et a_6 sont entiers d'après la proposition 6. On a $3\varepsilon \equiv -\varepsilon \pmod 4$, d'où les deux premières congruences. De plus, $\varepsilon^4 \equiv 1 \pmod{\pi^8}$ et $2 \equiv 2\varepsilon^2 \pmod{\pi^8}$. Donc

$$a_6 \equiv \frac{1}{\pi^6}\frac{c_6'}{\varepsilon}\left(c_6'^2 - 3c_4' - 2\right) \pmod 2.$$

D'où la troisième congruence car $c_6'/\varepsilon \equiv 1 \pmod 2$. On en déduit

$$c_4' \equiv \pi^6 a_6 + \frac{1}{3}(c_6'^2 - 2) \pmod{\pi^8}.$$

Or, $1/3 \equiv -1 \pmod{2\pi}$ et $c_6'^2 - 1 \equiv 0 \pmod{4\pi}$ car $c_6' \equiv 1 \pmod 2$. Donc, $(c_6'^2 - 1)/3 \equiv 1 - c_6'^2 \pmod{\pi^8}$. Comme par ailleurs $-1/3 \equiv 5 \pmod{\pi^8}$, on en déduit la dernière congruence et le lemme.

PROPOSITION 7. *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites :*

1. $v(\Delta) \equiv 4 \pmod{12}$.
2. *Il existe $(a, b) \in \mathcal{L}_1$ tel que $c_4' \equiv a \pmod{\pi^8}$ et $c_6' \equiv b \pmod{\pi^6}$.*

Démonstration. Supposons $|\Phi| = 3$. D'après [2, th. 2(i)], E est de type IV ou IV*. Donc, d'après le lemme 40, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. La première condition est donc satisfaite et d'après le lemme 41, on a $c_6' \equiv 1 \pmod 2$. De plus, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. D'après la proposition 6, le modèle (W) de E est entier. Exprimons à présent le fait que l'on n'est pas dans un cas 3 de Tate. On a $a_4 \equiv 1 \pmod 2$, donc $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 1].

Supposons $a_2 \equiv 1 \pmod{\pi}$. Alors, $t = 0$ satisfait à la seconde relation. Puis,

$$a_2 + a_6 \equiv a_6 + a_4 + a_2 + 1 \equiv 0 \pmod{2},$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]).

Supposons $a_2 \equiv 0 \pmod{\pi}$. Alors, $t = 1$ satisfait à la seconde relation. Puis,

$$a_6 + a_4 + a_2 - \frac{2}{\pi} \equiv a_2 + a_6 + 1 + \pi \equiv 0 \pmod{2},$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). D'où $a_2 + a_6 \equiv 1 + \pi \pmod{2}$. Autrement dit, $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod{2}$. De plus, d'après le lemme 44,

$$c_6' \equiv \pi^2 a_2 - \varepsilon \pmod{4} \quad \text{et} \quad c_4' \equiv -c_6'^2 + 6 + \pi^6 a_6 \pmod{\pi^8}. \tag{3.21}$$

Par ailleurs, d'après la proposition 6 et les congruences $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod{2}$,

$$(a_2 \pmod{2},\ a_6 \pmod{2}) \in \{(0, 1+\pi), (1,1), (\pi,1), (1+\pi, 1+\pi)\}.$$

On déduit alors des congruences de la formule (3.21) les quatre couples $(c_4' + c_6'^2 \pmod{\pi^8},\ c_6' \pmod{4})$ possibles. À chaque classe $c_6' \pmod 4$ correspond quatre valeurs possibles pour $c_6' \pmod{\pi^6}$. En remplaçant $c_6'^2 \pmod{\pi^8}$ par sa valeur dans la seconde congruence de (3.21), on obtient ainsi les seize couples $(c_4' \pmod{\pi^8}, c_6' \pmod{\pi^6})$ de l'ensemble $\mathcal{L}_1$.

Réciproquement, supposons les conditions de l'énoncé satisfaites. Alors, $c_6' \equiv 1 \pmod 2$ et, d'après le lemme 41, $v(\Delta_m) = 4$. Quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$. Alors, d'après l'appendice B, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 1]. De plus, d'après le lemme 44,

$$a_2 \equiv \frac{1}{\pi^2}(\varepsilon c_6' + 1) \pmod 2 \quad \text{et} \quad a_6 \equiv \frac{1}{\pi^6}(c_6'^2 - 3c_4' - 2) \pmod 2.$$

On vérifie alors que pour chacun des seize couples de l'ensemble $\mathcal{L}_1$, on a $a_2 + a_6 \equiv 0$ ou $1 + \pi \pmod 2$.

Supposons $a_2 + a_6 \equiv 0 \pmod 2$. Alors, $t = 0$ satisfait à la seconde relation de divisibilité de [3, prop. 1] et $a_6 + a_4 + a_2 + 1 \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_2 + a_6 \equiv 1 + \pi \pmod 2$, alors, $t = 1$ convient et $a_6 + a_4 + a_2 - 2/\pi \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4. Par ailleurs, d'après le lemme 43, on n'est pas dans un cas 4. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [2, th. 2(i)].

3.8.3. Cas où $v(j) = 16$. On suppose que le modèle de Weierstrass de E vérifie $v(j) = 16$ et la condition (C2), i.e. $j' \equiv 1 + \pi^2 \pmod{2\pi}$.

LEMME 45. *La courbe E n'est pas de type IV. Supposons qu'elle soit de type IV*. Alors, $v(\Delta_m) = 8$.*

Démonstration. D'après [2, th. 2(i)], si E est de type IV, on a $v(\Delta_m) = 4$. Cela contredit la condition $v(j) = 16$. Par ailleurs, si E est de type IV*, alors $v(\Delta_m) = 8$. D'où le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2} \quad \text{et} \quad a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3}.$$

PROPOSITION 8. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. *Alors, l'équation*

$$y^2 = x^3 + a_4x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E. *De plus, les coefficients* a_4 *et* a_6 *sont deux unités de* $\mathcal{O}_K$ *satisfaisant aux congruences suivantes :*

$$a_4 \equiv c_4' \pmod 4, \qquad a_6 \equiv \left(\frac{\pi^2}{2}\right) c_6' \pmod 4,$$
$$a_4 \equiv 1 \pmod 2, \qquad a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}.$$

Démonstration. Sous l'hypothèse $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, le modèle proposé n'est rien d'autre que le modèle (W_0) de E. En effet, on a

$$-\frac{c_4}{48} = -3\frac{c_4'}{\varepsilon^2} = a_4 \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} = a_6.$$

Les coefficients a_4 et a_6 sont deux unités de $\mathcal{O}_K$. De plus,

$$a_4 = -\frac{3}{\varepsilon^2}c_4' \equiv c_4' \pmod 4 \quad \text{et} \quad a_6 = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3} \equiv \left(\frac{\pi^2}{2}\right)c_6' \pmod 4$$

car $\varepsilon^2 \equiv 1 \pmod 4$. On a enfin

$$j' = \left(\frac{2}{\pi^2}\right)^8 \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

D'où $a_4^3 \equiv a_6^2 + \pi^2 \pmod{2\pi}$, d'après la condition (C2). Or, a_6 étant une unité de $\mathcal{O}_K$, on a $a_6^2 \equiv 1 \pmod 2$. D'où $a_4 \equiv 1 \pmod 2$ et $a_4^2 \equiv 1 \pmod 4$. D'où le résultat.

LEMME 46. *Supposons que* E *soit de type IV*. Alors,* $c_6' \equiv 2/\pi^2 \pmod 2$.

Démonstration. D'après le lemme 45, on a $v(\Delta_m) = 8$. Donc, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On considère alors le modèle (W) de E de la proposition 8. On a $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv (\pi^2/2)c_6' \pmod 2$. D'après [3, prop. 1] appliquée à $r = t = 1$, on a alors, comme E correspond à un cas 8 de Tate,

$$0 \equiv a_6 + a_4 \equiv 1 + (\pi^2/2)c_6' \pmod 2.$$

D'où le résultat.

LEMME 47. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$ *et* $c_6' \equiv 2/\pi^2 \pmod 2$. *Alors, la courbe* E *est de type IV* si et seulement si* $a_4 + a_6 \equiv 0$ *ou* $\pi^2 + \pi^3 \pmod 4$.

Démonstration. D'après l'appendice B, la courbe E correspond à un cas 3, 4, 6, 7 ou 8 (type IV*) de Tate. Pour le modèle (W) de E de la proposition 8, on a, avec les notations de [5],

$$b_2 = 0, \quad b_4 = 2a_4 = -\frac{6}{\varepsilon^2}c_4', \quad b_6 = 4a_6 = -4\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3}, \quad b_8 = -a_4^2 = -9\frac{c_4'^2}{\varepsilon^4}.$$

D'après les hypothèses faites et la proposition 8, on a $a_6 \equiv (\pi^2/2)c_6' \equiv 1 \pmod 2$ et $a_4 \equiv 1 + \pi^2 \pmod{2\pi}$. Donc, d'après [3, prop. 1] appliqué à $r = t = 1$, on est dans un cas ≥ 4 de Tate. De plus, comme $\varepsilon \equiv \pm 1 \pmod 4$, on a

$$b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -9 - 4 - 18(1 + \pi^2) + 3 \equiv 0 \pmod{4\pi}.$$

Donc d'après [3, prop. 2] appliqué à $r = 1$, on est dans un cas ≥ 5 de Tate. Vérifions que l'on n'est jamais dans un cas 7. En effet, d'après ce qui précède, $r = 1$ satisfait à la condition (a) de [3, prop. 3] et $s = 1$ satisfait à la condition (b), donc on n'est pas dans un cas 7. Autrement dit, on est dans un cas 8 si et seulement si on n'est pas dans un cas 6, c'est-à-dire, d'après [3, prop. 3(b)], si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 + a_4 + 1 \equiv t^2 \pmod 4$. Or, $a_6 + a_4 + 1$ étant une unité de $\mathcal{O}_K$, on en déduit que $t \in \mathcal{U}_K$ et on conclut avec le lemme 7.

PROPOSITION 9. *On a $|\Phi| = 3$ si et seulement si les conditions suivantes sont satisfaites :*

1. $v(\Delta) \equiv 8 \pmod{12}$.
2. *Il existe $(a, b) \in \mathcal{L}_2$ tel que $c_4' \equiv a \pmod 4$ et $c_6' \equiv b \pmod 4$.*

Démonstration. Supposons $|\Phi| = 3$. D'après [2, th. 2(i)], E est de type IV ou IV*. Donc, d'après le lemme 45, E est de type IV* (cas 8 de Tate) et $v(\Delta_m) = 8$. Quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. D'après le lemme 46, on a de plus $c_6' \equiv 2/\pi^2 \pmod 2$. Donc d'après le lemme 47 on a $a_4 + a_6 \equiv 0$ ou $\pi^2 + \pi^3 \pmod 4$. Or, d'après la proposition 8,

$$a_4 + a_6 \equiv c_4' + \left(\frac{\pi^2}{2}\right) c_6' \pmod 4.$$

On en déduit que l'on a ou bien $c_4' \equiv -(\pi^2/2)c_6' \pmod 4$, ou bien $c_4' \equiv -(\pi^2/2)c_6' + \pi^2 + \pi^3 \pmod 4$. En distinguant chaque fois selon les quatre valeurs possibles pour $c_6' \pmod 4$, on obtient les huit couples ($c_4' \pmod 4$, $c_6' \pmod 4$) possibles. On vérifie alors qu'il existe $(a, b) \in \mathcal{L}_2$ tel que a (resp. b) soit un représentant de c_4' (resp. c_6') modulo 4.

Réciproquement, si les deux conditions de l'énoncé sont satisfaites, alors d'après l'appendice B, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. On vérifie de plus que nécessairement $c_6' \equiv 2/\pi^2 \pmod 2$. D'après la proposition 8 et la seconde hypothèse, il vient alors

$$a_4 + a_6 \equiv c_4' + \left(\frac{\pi^2}{2}\right) c_6' \equiv 0 \text{ ou } \pi^2 + \pi^3 \pmod 4.$$

Donc d'après le lemme 47, E est de type IV*. D'où $|\Phi| = 3$ d'après [2, th. 2(i)].

3.8.4. Cas où $v(j) = 20$. On suppose que le modèle de Weierstrass de E vérifie $v(j) = 20$ et la condition (C1′), i.e. $c_4' \equiv 1 + \pi \pmod 2$.

LEMME 48. *La courbe E n'est pas de type IV*. Supposons qu'elle soit de type IV. Alors, $v(\Delta_m) = 4$.*

Démonstration. D'après [2, th. 2(i)], si E est de type IV*, on a $v(\Delta_m) = 8$, ce qui contredit $v(j) = 20$. Par ailleurs, si E est de type IV, alors $v(\Delta_m) = 4$. D'où le lemme.

LEMME 49. *Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, $v(\Delta_m) = 4$ si et seulement si $c_6' \equiv \pi^2/2 \pmod 2$.*

Démonstration. Supposons $v(\Delta) \equiv 4 \pmod{12}$. Alors, d'après l'appendice B, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (12, 14, 16)$. Le modèle ($W_0$) de E est alors entier. D'après l'appendice B, il correspond à un cas 10 de

Tate ou à un cas non minimal. Examinons donc à quelle condition il est minimal. Avec les notations de [5], on a, pour le modèle (W_0) de E,

$$b_6 = -4\frac{c_6}{864} = -2^3\pi^2\frac{c_6'}{\varepsilon^3}, \qquad b_8 = -\left(\frac{c_4}{48}\right)^2.$$

En particulier, $v(b_8) = 8$, donc $r = 0$ satisfait à la condition de [3, prop. 6]. S'il existe un entier x de K tel que

$$b_6 \equiv x^2 \pmod{\pi^{10}},$$

alors nécessairement $v(x) = 4$, car $v(b_6) = 8$. Puis, il vient

$$c_6' \equiv \left(\frac{\pi^2}{2}\right)\left(\frac{x}{2\pi^2}\right)^2 \pmod 2.$$

D'où $c_6' \equiv \pi^2/2 \pmod 2$ car $x/2\pi^2 \in \mathcal{U}_K$.

Réciproquement, si $c_6' \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ convient. Avec [3, prop. 6], cela démontre le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2}, \qquad a_6 = -\frac{1}{\pi^2}\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c_6' + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right).$$

PROPOSITION 10. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. *Alors, l'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + a_4x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E pour lequel $a_4 \equiv 1 + \pi \pmod 2$.

Démonstration. Le changement de variables

$$X = x, \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition.

Le coefficient $4/\pi^3$ est entier. Vérifions que les coefficients a_4 et a_6 sont également entiers et que $a_4 \equiv 1 + \pi \pmod 2$.

On a

$$a_4 = -3\frac{c_4'}{\varepsilon^2} \equiv -3(1+\pi) \equiv 1 + \pi \pmod 2,$$

car $c_4' \equiv 1 + \pi \pmod 2$ d'après la condition (C1′).

D'après le lemme 49, on a $c_6' \equiv \pi^2/2 \pmod 2$. D'où

$$\pi^2 a_6 = -\frac{1}{\varepsilon^3}\left(\left(\frac{2}{\pi^2}\right)c_6' + \varepsilon^3\left(\frac{2}{\pi^2}\right)^2\right) \equiv 0 \pmod 2,$$

car $\varepsilon \equiv 1 \pmod 2$ (lemme 10). D'où la proposition.

LEMME 50. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. *Alors, E ne correspond pas à un cas 4 de Tate.*

Démonstration. D'après l'appendice B, la courbe E correspond à un cas 3 (II), 4 (III) ou 5 (IV) de Tate. Soit (W) le modèle de E de la proposition 10. Supposons qu'il corresponde

à un cas ≥ 4 de Tate. D'après la congruence $a_4 \equiv 1+\pi \pmod 2$, $r=1$ satisfait à la première relation de divisibilité de [3, prop. 2]. Par ailleurs, avec les notations de [5],

$$b_2 = 0, \quad b_4 = -6\frac{c_4'}{\varepsilon^2} \equiv \pi^2 \pmod{2\pi}, \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6 \equiv \pi^2 \pmod{2\pi},$$

$$b_8 = -9\frac{c_4'^2}{\varepsilon^4} \equiv -(1+\pi)^2 \equiv -(1+\pi^2) \pmod{2\pi}.$$

Donc, $b_8 + 3b_6 + 3b_4 + b_2 + 3 \equiv -(1+\pi^2) + 3\pi^2 + 3\pi^2 + 3 \equiv 0 \pmod{2\pi}$. D'où le résultat d'après [3, prop. 2].

LEMME 51. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (8,8,4)$. *Alors,* a_6 *est entier et*

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right)c_6'\right) \pmod 2 \quad \textit{et} \quad c_6' \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

Démonstration. Sous l'hypothèse faite, $c_6' \equiv \pi^2/2 \pmod 2$ et l'élément a_6 est entier. Comme $\varepsilon \equiv \pm 1 \pmod 4$, on a de plus,

$$-\pi^2 a_6 \equiv \left(\frac{2}{\pi^2}\right)\varepsilon c_6' + \left(\frac{2}{\pi^2}\right)^2 \equiv \left(\frac{2}{\pi^2}\right)^2\left(1 + 3\left(\frac{2}{\pi^2}\right)c_6'\right) \pmod 4.$$

Or, $(2/\pi^2)^2 \equiv 1 \pmod 2$ et $v(1 + 3(2/\pi^2)c_6') \geq 2$, d'où

$$\pi^2 a_6 \equiv 1 - \left(\frac{2}{\pi^2}\right)c_6' \pmod 4$$

et la première congruence. On en déduit alors la seconde car $\pi^4 \equiv 4 \pmod{\pi^6}$.

PROPOSITION 11. *On a* $|\Phi| = 3$ *si et seulement si les conditions suivantes sont satisfaites :*

1. $v(\Delta) \equiv 4 \pmod{12}$.
2. $c_6' \equiv \pi^2/2 + 2 \pmod 4$ *ou* $c_6' \equiv \pi^2/2 + \pi^3 \pmod 4$.

Démonstration. Supposons $|\Phi| = 3$. D'après [2, th. 2(i)], E est de type IV ou IV*. Donc, d'après le lemme 48, E est de type IV (cas 5 de Tate) et $v(\Delta_m) = 4$. Donc, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8,8,4)$. De plus, d'après le lemme 49, on a $c_6' \equiv \pi^2/2 \pmod 2$. Les coefficients a_4 et a_6 sont alors entiers d'après la proposition 10. Exprimons le fait que l'on n'est pas dans le cas 3 de Tate. On a $a_4 \equiv 1 \pmod \pi$, donc $r=1$ satisfait à la première relation de divisibilité de [3, prop. 1].

Supposons $a_6 \equiv 1 \pmod \pi$. Alors, $t=1$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 - \pi \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). Donc $a_6 \equiv 1 \pmod 2$ car $a_4 \equiv 1+\pi \pmod 2$ d'après la proposition 10.

Supposons $a_6 \equiv 0 \pmod \pi$. Alors, $t=0$ vérifie $t^2 - a_6 \equiv 0 \pmod \pi$. Puis,

$$a_4 + a_6 + 1 \equiv 0 \pmod 2,$$

car on est dans un cas ≥ 4 de Tate ([3, prop. 1]). D'où $a_6 \equiv \pi \pmod 2$ car $a_4 \equiv 1 + \pi \pmod 2$ d'après la proposition 10. La troisième condition est donc satisfaite. Autrement

dit, $a_6 \equiv 1$ ou $\pi \pmod 2$. Or, d'après le lemme 51,

$$c_6' \equiv \frac{\pi^2}{2} + 2a_6 \pmod 4.$$

D'où la seconde condition.

Réciproquement, supposons les deux conditions de l'énoncé satisfaites. Alors, $c_6' \equiv \pi^2/2 \pmod 2$. D'après le lemme 49, on a donc $v(\Delta_m) = 4$ et on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$. D'après l'appendice B, E correspond à un cas 3, 4 ou 5 de Tate. Montrons que E ne correspond pas à un cas 3. On considère le modèle de E de la proposition 10. Comme a_4 est une unité, $r = 1$ satisfait à la première relation de divisibilité de [3, prop. 1].

Par ailleurs, d'après le lemme 51, on a

$$a_6 \equiv \frac{1}{\pi^2}\left(1 - \left(\frac{2}{\pi^2}\right)c_6'\right) \pmod 2.$$

D'où $a_6 \equiv 1$ ou $\pi \pmod 2$.

Supposons $a_6 \equiv 1 \pmod 2$. Alors, $t = 1$ satisfait à la seconde relation de divisibilité de [3, prop. 1] et $a_4 + a_6 - \pi \equiv 0 \pmod 2$, donc on est dans un cas ≥ 4 de Tate. De même, si $a_6 \equiv \pi \pmod 2$, alors, $t = 0$ convient et $a_4 + a_6 + 1 \equiv 0 \pmod 2$ et on est encore dans un cas ≥ 4. Par ailleurs, d'après le lemme 50, on n'est pas dans un cas 4. On est donc dans un cas 5 (type IV) et $|\Phi| = 3$, d'après [2, th. 2(i)].

3.8.5. Cas où $v(j) \geq 24$. On suppose que le modèle de Weierstrass de E vérifie $v(j) \geq 24$ et que 3 ne divise pas $v(\Delta)$.

LEMME 52. *On suppose $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. Alors, E est de type IV* si et seulement si $c_6' \equiv \pi^2/2 \pmod 4$ ou $c_6' \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$.*

Démonstration. On considère le modèle (W_0) de E. Sous l'hypothèse faite, ce modèle est entier et il correspond à un cas 3, 6 ou 8 (type IV*) de Tate (d'après l'appendice B). De plus, on a

$$-\frac{c_4}{48} = -\frac{3}{\varepsilon^2}\pi^{v(c_4)-8}c_4' \quad \text{et} \quad -\frac{c_6}{864} = -\left(\frac{2}{\pi^2}\right)\frac{c_6'}{\varepsilon^3}. \tag{3.22}$$

Les deux premières relations de congruence de [3, prop. 1] sont satisfaites par $r = 0$ et $t = 1$, puis

$$-\frac{c_6}{864} - 1 \equiv \left(\frac{2}{\pi^2}\right)c_6' - 1 \pmod 2.$$

Autrement dit, on est dans un cas ≥ 4 si et seulement si $c_6' \equiv \pi^2/2 \pmod 2$. Avec les notations de [5], on a $b_8 = -(c_4/48)^2$, donc $v(b_8) \geq 6$ et $r = 0$ satisfait la condition (a) de [3, prop. 3]. On conclut alors que E est de type IV* si et seulement si il existe t dans $\mathcal{O}_K$ tel que $-c_6/864 \equiv t^2 \pmod 4$. D'après le lemme 7 et la seconde égalité (3.22), c'est le cas si et seulement si $c_6' \equiv \pi^2/2$ ou $\pi^2/2 + 2 + \pi^3 \pmod 4$. D'où le lemme.

LEMME 53. *On suppose $v(\Delta) \equiv 4 \pmod{12}$. Alors, $v(\Delta_m) = 4$ si et seulement si $c_6' \equiv \pi^2/2 \pmod 2$.*

Démonstration. D'après l'appendice B, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (\geq 14, 14, 16)$. Le modèle ($W_0$) de E est alors entier.

De plus, $v(\Delta_m) = 4$ si et seulement si ce modèle est non minimal, c'est-à-dire, toujours d'après l'appendice B, si et seulement si il ne correspond pas à un cas 10 de Tate. Avec les notations de [5], on a $b_8 = -(c_4/48)^2$ et $v(c_4/48) \geq 6$, donc $v(b_8) \geq 12$. On en déduit que $r = 0$ satisfait la première relation de congruence de [3, prop. 6]. Par ailleurs, pour ce modèle, on a $b_6 = -4c_6/864 = -8\pi^2 c_6'/\varepsilon^3$. Puis, le modèle ($W_0$) est non minimal si et seulement si il existe x dans $\mathcal{O}_K$ tel que

$$-8\pi^2 \frac{c_6'}{\varepsilon^3} \equiv x^2 \pmod{\pi^{10}},$$

autrement dit, si et seulement si il existe x dans $\mathcal{O}_K$ tel que $8\pi^2 c_6' \equiv x^2 \pmod{\pi^{10}}$. Comme c_6' est une unité de $\mathcal{O}_K$, si un tel x existe, on a nécessairement $v(x) = 4$ et la congruence ci-dessus équivaut à $c_6' \equiv (\pi^2/2)(x/2\pi^2)^2 \pmod 2$, puis $c_6' \equiv \pi^2/2 \pmod 2$ d'après le lemme 7. Réciproquement, si $c_6' \equiv \pi^2/2 \pmod 2$, alors $x = 2\pi^2$ satisfait à la congruence ci-dessus. Cela démontre le lemme.

Posons

$$a_4 = -3\frac{c_4'}{\varepsilon^2}\pi^{v(c_4)-8}, \qquad a_6 = -\frac{1}{\pi^6}\left(4 + 2\pi^2 \frac{c_6'}{\varepsilon^3}\right).$$

PROPOSITION 12. *Supposons* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, l'équation*

$$y^2 + \frac{4}{\pi^3} y = x^3 + a_4 x + a_6 \tag{W}$$

définit un modèle de Weierstrass entier de E.

Démonstration. Le changement de variables

$$X = x, \qquad Y = y + \frac{2}{\pi^3}$$

transforme le modèle (W_0) de E en le modèle de la proposition. Les coefficients $4/\pi^3$ et a_4 sont entiers. Vérifions que c'est également le cas pour a_6. D'après le lemme 53, on a $c_6' \equiv \pi^2/2 \pmod 2$. Puis,

$$-\pi^6 a_6 = 4 + 2\pi^2 \frac{c_6'}{\varepsilon^3} \equiv 4 + 2\pi^2 c_6' \pmod{\pi^6}.$$

Comme $4 \equiv \pi^4 \pmod{\pi^6}$, on a donc $-\pi^6 a_6 \equiv 0 \pmod{\pi^6}$ et a_6 est entier. D'où la proposition.

LEMME 54. *On suppose* $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. *Alors, E est de type IV si et seulement si* $c_6' \equiv \pi^2/2 \pmod 4$ *ou* $c_6' \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$.

Démonstration. On considère le modèle (W) de E de la proposition 12. Il correspond, d'après l'appendice B, à un cas 3 ou 5 (type IV) de Tate. Comme $v(a_4) \geq 2$ (car $v(c_4) \geq 10$), $r = 0$ satisfait à la première relation de congruence de [3, prop. 1]. On est donc dans un cas 5 de Tate si et seulement si il existe t dans $\mathcal{O}_K$ tel que $a_6 \equiv t^2 + t\pi \pmod 2$, autrement dit, si et seulement si $a_6 \equiv 0$ ou $1 + \pi \pmod 2$. Or, comme $-\pi^6 a_6 \equiv 4 + 2\pi^2 \varepsilon c_6' \pmod{\pi^8}$, la congruence $a_6 \equiv 0 \pmod 2$ équivaut à $c_6' \equiv -4/(2\pi^2\varepsilon) \equiv \pi^2/2 \pmod 4$. De même, $a_6 \equiv 1 + \pi \pmod 2$ équivaut à

$$c_6' \equiv -\frac{4}{2\pi^2\varepsilon} + \frac{\pi^6}{2\pi^2\varepsilon} + \frac{\pi^7}{2\pi^2\varepsilon} \equiv \frac{\pi^2}{2} + 2 + \pi^3 \pmod 4.$$

D'où le lemme.

PROPOSITION 13. *On a* $|\Phi| = 3$ *si et seulement si les deux conditions suivantes sont satisfaites :*

1. $v(\Delta) \equiv 4 \pmod{12}$ *ou* $v(\Delta) \equiv 8 \pmod{12}$.
2. $c_6' \equiv \pi^2/2 \pmod 4$ *ou* $c_6' \equiv \pi^2/2 + 2 + \pi^3 \pmod 4$.

Démonstration. On suppose que $|\Phi| = 3$. Alors, d'après [2], E est de type IV ou IV*. Supposons qu'elle soit de type IV. Dans ce cas, $v(\Delta_m) = 4$ et quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. Puis d'après le lemme 54, on a $c_6' \equiv \pi^2/2$ ou $\pi^2/2 + 2 + \pi^3 \pmod 4$. D'où la première condition de l'énoncé. De même, si la courbe E est de type IV*, alors, d'après [2], on a $v(\Delta_m) = 8$ et quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$. D'après le lemme 52, on a donc $c_6' \equiv \pi^2/2$ ou $\pi^2/2 + 2 + \pi^3 \pmod 4$.

Réciproquement, supposons que les deux conditions de l'énoncé soient satisfaites. Si $v(\Delta) \equiv 4 \pmod{12}$, comme $c_6' \equiv \pi^2/2 \pmod 2$, on a $v(\Delta_m) = 4$ d'après le lemme 53. Quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (\geq 10, 8, 4)$. On conclut avec le lemme 54 que la courbe E est de type IV. De même, si $v(\Delta) \equiv 8 \pmod{12}$, alors d'après l'appendice B, quitte à faire un changement de variables, on peut supposer $(v(c_4), v(c_6), v(\Delta)) = (\geq 11, 10, 8)$ et on conclut que la courbe E est de type IV* avec le lemme 52. Autrement dit, E est de type IV ou IV* et $|\Phi| = 3$ d'après [2, th. 2]. D'où la proposition.

A. Exemples

On montre dans cet appendice que tous les cas du théorème 2 se réalisent. C'est immédiat pour les assertions 1, 2 et 3 en raison de l'existence d'une courbe elliptique sur K d'invariant j donné. On adopte dans toute cette section les notations de [5].

A.1. Cas où $v(j) \geq 24$**.** La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{13}}{48}x - \frac{\pi^{12}}{864}$$

vérifie $v(j) = 27$ et $v(\Delta) = 12$. D'après le théorème 2, $|\Phi| = 2$ et le cas 11(a) se réalise.

Vérifions qu'il en va de même du cas 11(b). La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{11}}{48}x - \frac{\pi^{10}a}{864}, \quad \text{avec } a \in \mathcal{U}_K,$$

vérifie $v(j) = 25$ et $v(\Delta) = 8$. D'après le théorème 2, on a donc

$$|\Phi| = \begin{cases} 3 & \text{si } a \equiv 2/\pi^2 \pmod 4 \text{ ou } a \equiv 2/\pi^2 + 2 + \pi^3 \pmod 4, \\ 6 & \text{sinon,} \end{cases}$$

et le cas 11(b) se réalise également.

A.2. Cas où $v(j) = 16$**, 18 et 20.** Pour $i = 16$, 18 ou 20, l'équation

$$y^2 + \pi^2 xy = x^3 - \frac{36\pi^8}{\pi^i - 1728}x - \frac{\pi^{12}}{\pi^i - 1728} \tag{A.1}$$

définit un modèle entier d'une courbe elliptique sur K d'invariant modulaire $j = \pi^i$. En particulier, $j' = 1$. De plus,

$$c_4 = \pi^8 + \frac{1728\pi^8}{\pi^i - 1728} = \pi^8\left(1 - \frac{1}{1 - \frac{\pi^i}{1728}}\right) = \frac{\pi^{8+i}}{1728}\left(1 + \sum_{k\geq 1}\left(\frac{\pi^i}{1728}\right)^k\right).$$

Donc, en particulier, $v(c_4) = 8 + i - 12$ et $c_4' \equiv \pi^{12}/(3^3 \cdot 2^6) \equiv 1/\varepsilon^3 \equiv 1 \pmod 2$. Autrement dit, la courbe ci-dessus ne vérifie ni (C1′), ni (C2). Cela démontre que les cas 8(b) et 10(b) du théorème 2 se réalisent.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{12}(1+\pi)}{48}x - \frac{\pi^{15}}{864} \tag{A.2}$$

vérifie $v(j) = 18$ et $c_4' = 1 + \pi$. La condition (C1′) est donc vérifiée. Avec l'exemple précédent pour $i = 18$, cela montre que le cas 9 se réalise également.

A.2.1. Cas où $v(j) = 16$ et la condition (C2) est vérifiée. On commence par démontrer le résultat suivant.

Proposition 14. *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 = x^3 + a_4x + a_6,$$

avec a_4 et a_6 deux unités vérifiant $a_4 \equiv a_6^2 + \pi^2 \pmod{2\pi}$. Alors,

$$(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8) \quad \text{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

Démonstration. On a $b_2 = 0$, $b_4 = 2a_4$, $b_6 = 4a_6$ et $b_8 = -a_4^2$. Donc,

$$c_4 = -48a_4, \qquad c_6 = -864a_6 \quad \text{et} \quad \Delta = -16(4a_4^3 + 27a_6^2).$$

Comme a_4 et a_6 sont deux unités de $\mathcal{O}_K$, en particulier $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$. De plus,

$$j' = \frac{a_4^3}{a_6^2 + 4(a_4/3)^3} \equiv \frac{a_4^3}{a_6^2} \pmod{2\pi}.$$

Or, $a_4^2 \equiv 1 \pmod{2\pi}$, car $a_4 \equiv a_6^2 \pmod 2$. D'où $j' \equiv a_4/a_6^2 \equiv 1 + \pi^2 \pmod{2\pi}$. Cela démontre la proposition.

Exemple 1. *La courbe E d'équation*

$$y^2 = x^3 - x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, la condition (C2) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 14. De plus,

$$c_4' = \frac{48}{\pi^8} = \frac{1}{3}\varepsilon^2 \equiv -1 \pmod 4 \quad \text{et} \quad c_6' = -\frac{864}{\pi^{10}} = -\frac{2^5 \cdot 3^3}{\pi^{10}} \equiv \frac{2}{\pi^2} \pmod 4.$$

Le couple $(-1, 2/\pi^2) \in \mathcal{L}_2$ est alors un représentant modulo 4 du couple (c_4' (mod 4), c_6'' (mod 4)). On conclut que $|\Phi| = 3$ avec l'assertion 8 du théorème 2.

Exemple 2. *La courbe E d'équation*

$$y^2 = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 10, 8)$, *la condition* (C2) *et* $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 14. De plus,

$$c_6' = -\frac{864}{\pi^{10}}(1+\pi) \equiv \frac{2}{\pi^2} + \pi \pmod 2.$$

En particulier, il n'existe aucun couple (a, b) de $\mathcal{L}_2$ tel que $c_6' \equiv b \pmod 4$. On conclut que $|\Phi| = 6$ avec l'assertion 8 du théorème 2.

Cela démontre que tous les cas de l'assertion 8 se réalisent.

A.2.2. Cas où $v(j) = 20$ et la condition (C1′) est vérifiée. On commence par démontrer le résultat suivant.

Proposition 15. *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{4}{\pi^3}y = x^3 + a_4 x + a_6,$$

avec $a_4 \equiv 1 + \pi \pmod 2$. *Alors,*

$$(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4) \quad \textit{et} \quad c_4' \equiv 1 + \pi \pmod 2.$$

Démonstration. On a $b_4 = 2a_4$ et donc $v(b_4) = 2$. On en déduit que $c_4 = -24b_4$ vérifie $v(c_4) = 8$, puis $c_4' = -(2^4 \cdot 3/\pi^8)a_4 = -3(2/\pi^2)^4 a_4 \equiv 1 + \pi \pmod 2$. De même, $b_6 = (4/\pi^3)^2 + 4a_6$ et donc $v(b_6) = 2$. D'où $c_6 = -216b_6$ vérifie $v(c_6) = 8$. Enfin, $\Delta = -8b_4^3 - 27b_6^2$ vérifie $v(\Delta) = 4$. D'où la proposition.

Exemple 3. *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + (1+\pi)x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$, *la condition* (C1′) *et* $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 15. De plus,

$$c_6' = -\frac{432}{\pi^8}\left(2 + \frac{8}{\pi^6}\right) \equiv 2 + \frac{8}{\pi^6} \equiv \frac{\pi^2}{2} + 2 \pmod 4.$$

On conclut que $|\Phi| = 3$ avec l'assertion 10 du théorème 2.

Exemple 4. *La courbe E d'équation*

$$y^2 + \frac{4}{\pi^3}y = x^3 + (1+\pi)x$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (8, 8, 4)$, *la condition* (C1′) *et* $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 15. De plus,

$$c_6' = -\frac{3456}{\pi^6} \equiv -\frac{1}{3}\left(\frac{\pi^2}{2}\right)\varepsilon^4 \equiv \frac{\pi^2}{2} \pmod 4.$$

On conclut que $|\Phi| = 6$ avec l'assertion 10 du théorème 2.

Cela démontre que tous les cas de l'assertion 10 se réalisent.

A.3. Cas où $v(j) = 12$. La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{14}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4) + 1$. Cela montre que le cas 7a du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{16}}{864}, \quad \text{où } a \in \mathcal{U}_K,$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4) + 2$. Elle vérifie la condition (C1′) si et seulement si $a \equiv 1 + \pi \pmod 2$. Elle vérifie la condition (C3) si et seulement si $a \equiv 1 + \pi^2$ ou $1 + \pi^3 \pmod 4$. Cela montre que le cas 7b du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^9}{48}x - \frac{\pi^{15}}{864}$$

vérifie $v(j) = 12$ et $2v(c_6) = 3v(c_4) + 3$, donc le cas 7c du théorème 2 se réalise.

La courbe d'équation

$$y^2 = x^3 - \frac{\pi^{10}a}{48}x - \frac{\pi^{17}}{864}, \quad \text{où } a \in \mathcal{U}_K,$$

vérifie $v(j) = 12$, $v(c_4) = 10$ et $2v(c_6) - 3v(c_4) = 4$. Elle vérifie (C3) si et seulement si $a \equiv 1 + \pi^2$ ou $1 + \pi^3 \pmod 4$. Cela montre que le cas 7d du théorème 2 se réalise.

Cela démontre que tous les cas de l'assertion 7 se réalisent.

A.4. Cas où $v(j) = 4$, 6 ou 8. On considère la courbe $\widetilde{E}$ d'équation (2.2) déduite de la courbe d'équation (A.1). Elle vérifie $v(j) = 24 - i$, où $i = 16$, 18 ou 20, c'est-à-dire $v(j) = 4$, 6 ou 8. Ses invariants standard sont notés $(\widetilde{c_4}, \widetilde{c_6}, \widetilde{\Delta})$ et satisfont d'après le lemme 23 aux congruences suivantes :

$$\widetilde{\Delta} \equiv c_4' \pmod 2 \quad \text{et} \quad \widetilde{j'} \equiv 1 \pmod 4.$$

En particulier, $\widetilde{E}$ ne vérifie ni la condition (C1), ni (C2). Cela démontre que les cas 4(b) et 6(b) du théorème 2 se réalisent.

De même, la courbe $\widetilde{E}$ d'équation (2.2) déduite de la courbe d'équation (A.2) vérifie $v(j) = 6$ et la condition (C1). Avec l'exemple précédent, cela montre que le cas 5 se réalise également.

A.4.1. Cas où $v(j) = 4$ et la condition (C1) est vérifiée. On commence par démontrer le résultat suivant qui est une réciproque partielle à la proposition 3.

Proposition 16. *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$a_6 + \varepsilon a_2 \equiv \pi^3 \pmod 4 \quad \textit{et} \quad \pi^2 a_2\left(a_2 + \frac{2}{\pi^2}\right) \equiv a_4 - \varepsilon \pmod 4.$$

Alors,

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8), \quad c_6' \equiv 1 \pmod 2 \quad et \quad \Delta' \equiv 1 + \pi \pmod 2.$$

Démonstration. On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2, \quad b_4 = \frac{2^3}{\pi^4} + 2a_4, \quad b_6 = \left(\frac{4}{\pi^3}\right)^2 + 4a_6,$$
$$b_8 = \left(\frac{2}{\pi}\right)^2 a_6 - \frac{2^3}{\pi^4}a_4 + 4a_2a_6 + \frac{2^4}{\pi^6}a_2 - a_4^2.$$

On en déduit, avec la définition de ε, que

$$b_2 = \frac{\pi^2}{3}\varepsilon + 4a_2, \quad b_4 = \frac{2}{3}\varepsilon + 2a_4, \quad b_6 = \frac{\pi^2}{9}\varepsilon^2 + 4a_6,$$
$$b_8 = \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2.$$

En utilisant les congruences $a_2 \equiv a_6 \pmod 2$ et $a_4 \equiv \varepsilon \pmod{2\pi}$, il vient alors

$$v(b_2) = 2, \quad v(b_4) \geq 5, \quad v(b_6) = 2 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c_6' \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c_6' \equiv 1 \pmod 2$.

Il reste donc à montrer que, d'une part, $v(\Delta) = 8$, et d'autre part, $\Delta' \equiv 1+\pi \pmod 2$. C'est équivalent à montrer $\Delta \equiv \pi^8 + \pi^9 \pmod{\pi^{10}}$. On utilise pour ce faire les congruences suivantes que l'on démontre ci-dessous :

$$b_2^2 \equiv \pi^4 + 2\pi^6 a_2 + \pi^8 a_2^2 \pmod{\pi^{10}}, \tag{A.3}$$
$$-27b_6^2 \equiv \pi^4 + \pi^8 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}}, \tag{A.4}$$
$$b_8 \equiv 1 + \pi^5 + 4a_2^2 + 2\pi^2 a_2 \pmod{\pi^6}, \tag{A.5}$$
$$9b_2b_4b_6 \equiv 2\pi^4(a_4 - \varepsilon) \pmod{\pi^{10}}. \tag{A.6}$$

D'après les égalités précédentes, on a

$$b_2^2 = \frac{\pi^4}{9}\varepsilon^2 + 16a_2^2 + 8\frac{\pi^2}{3}\varepsilon a_2.$$

Or, $\varepsilon^2/9 \equiv 1 \pmod{\pi^6}$, $4 \equiv \pi^4 \pmod{\pi^6}$ et $16 \equiv \pi^8 \pmod{\pi^{10}}$. Cela démontre la congruence (A.3). Pour les mêmes raisons,

$$b_6^2 = \frac{\pi^4}{3^4}\varepsilon^4 + 16a_6^2 + 8\frac{\pi^2}{9}\varepsilon a_6 \equiv \pi^4 + 2\pi^6 a_6 + \pi^8 a_6^2 \pmod{\pi^{10}}.$$

Puis, $-27 \equiv -3 \equiv 1 + \pi^4 \pmod{\pi^6}$. D'où la congruence (A.4).

Montrons à présent la congruence (A.5). On a

$$b_8 = \frac{\pi^2}{3}\varepsilon a_6 - \frac{2}{3}\varepsilon a_4 + 4a_2a_6 + \frac{\pi^2}{9}\varepsilon^2 a_2 - a_4^2$$
$$\equiv -\pi^2\varepsilon a_6 + 2\varepsilon a_4 + 4a_2a_6 + \pi^2 a_2 - a_4^2 \pmod{\pi^6}.$$

Or, $a_2+\varepsilon a_6 \equiv \pi^3 \pmod 4$ et $a_4 \equiv \varepsilon \pmod{2\pi}$. En particulier, $-a_4^2 \equiv 1-2\varepsilon a_4 \pmod{\pi^6}$ car $\varepsilon^2 \equiv 1 \pmod{\pi^6}$. On en déduit donc

$$b_8 \equiv \pi^2(2a_2+\pi^3)+1+4a_2^2 \equiv 1+\pi^5+4a_2^2+2\pi^2 a_2 \pmod{\pi^6}.$$

Enfin, $b_2 \equiv b_6 \equiv \pi^2 \pmod{\pi^6}$ et $b_4 \equiv 2(a_4-\varepsilon) \pmod{\pi^6}$. On en déduit la congruence (A.6).

Déduisons alors des congruences (A.3)–(A.6) celle annoncée pour Δ. On a

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6.$$

D'après (A.3) et (A.4) et l'hypothèse $a_2 \equiv a_6 \pmod 2$, on a $-27b_6^2 \equiv b_2^2+\pi^8 \pmod{\pi^{10}}$. Comme $v(8b_4^3) \geq 10$, on a, d'après la congruence (A.6) et l'égalité ci-dessus,

$$\Delta \equiv b_2^2(1-b_8)+\pi^8+2\pi^4(a_4-\varepsilon) \pmod{\pi^{10}}.$$

D'après (A.3) et (A.5), il vient alors

$$\Delta \equiv \pi^8+\pi^9+4\pi^4 a_2^2+2\pi^6 a_2+2\pi^4(a_4-\varepsilon) \pmod{\pi^{10}}.$$

Or, d'après la congruence de l'énoncé, $a_4-\varepsilon \equiv \pi^2 a_2^2+2a_2 \pmod 4$, on a $+2\pi^4(a_4-\varepsilon) \equiv 4\pi^4 a_2^2+2\pi^6 a_2 \pmod{\pi^{10}}$. En remplaçant dans la congruence ci-dessus, on obtient alors

$$\Delta \equiv \pi^8+\pi^9 \pmod{\pi^{10}},$$

ce qui est le résultat cherché. Cela achève la démonstration de la proposition 16.

EXEMPLE 5. *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2+\frac{2}{\pi}xy+\frac{4}{\pi^3}y = x^3-x^2+(1+\pi^3)x+1+\pi^3$$

vérifie $(v(c_4),v(c_6),v(\Delta))=(4,6,8)$, la condition (C1) et $|\Phi|=3$.

Démonstration. Les deux premières propriétés résultent de la proposition 16. De plus,

$$c_6' = -37\frac{2^6}{\pi^{12}} - 3\cdot 5\frac{2^6}{\pi^{10}} + 3\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c_6' \equiv \varepsilon+2+\pi^2 \pmod 4$. Or, comme K est dans Ω_1, on a $c_6' \equiv 1+\pi^3 \pmod 4$. On conclut que $|\Phi|=3$ avec l'assertion 4 du théorème 2.

EXEMPLE 6. *Supposons K dans Ω_1. La courbe E d'équation*

$$y^2+\frac{2}{\pi}xy+\frac{4}{\pi^3}y = x^3+x+\pi^3$$

vérifie $(v(c_4),v(c_6),v(\Delta))=(4,6,8)$, la condition (C1) et $|\Phi|=6$.

Démonstration. Les deux premières propriétés résultent de la proposition 16. De plus,

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon+2 \pmod 4.$$

Or, comme K est dans Ω_1, on a $c_6' \equiv 1+\pi^2+\pi^3 \pmod 4$. On conclut que $|\Phi|=6$ avec l'assertion 4 du théorème 2.

EXEMPLE 7. *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2+\frac{2}{\pi}xy+\frac{4}{\pi^3}y = x^3-x+\pi^3$$

vérifie $(v(c_4),v(c_6),v(\Delta))=(4,6,8)$, la condition (C1) et $|\Phi|=3$.

Démonstration. Les deux premières propriétés résultent de la proposition 16. De plus,

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} \equiv \varepsilon + 2 \pmod 4.$$

Or, comme K est dans Ω_2, on a $c_6' \equiv 1 \pmod 4$. On conclut que $|\Phi| = 3$ avec l'assertion 4 du théorème 2.

Exemple 8. *Supposons K dans Ω_2. La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy + \frac{4}{\pi^3}y = x^3 + x^2 - x + 1 + \pi^3$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 8)$, la condition (C1) et $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 16. De plus,

$$c_6' = -37\frac{2^6}{\pi^{12}} + 3\cdot 5\frac{2^6}{\pi^{10}} - 3\cdot 5\frac{2^5}{\pi^8} \pmod 4.$$

D'où $c_6' \equiv \varepsilon + 2 + \pi^2 \pmod 4$. Or, comme K est dans Ω_2, on a $c_6' \equiv 1 + \pi^2 \pmod 4$. On conclut que $|\Phi| = 6$ avec l'assertion 4 du théorème 2.

Cela démontre que tous les cas de l'assertion 4 se réalisent.

A.4.2. Cas où $v(j) = 8$ et la condition (C2) est vérifiée. On commence par démontrer le résultat suivant.

Proposition 17. *Supposons que E soit donnée par une équation de Weierstrass entière de la forme*

$$y^2 + \frac{2}{\pi}xy = x^3 + a_2x^2 + a_4x + a_6,$$

avec $a_4 \equiv 1 \pmod 2$ et $a_6 \equiv 1 \pmod \pi$. Alors,

$$(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4), \quad c_6' \equiv 1 \pmod 2 \quad \text{et} \quad j' \equiv 1 + \pi^2 \pmod{2\pi}.$$

Démonstration. On a tout d'abord,

$$b_2 = \left(\frac{2}{\pi}\right)^2 + 4a_2, \quad b_4 = 2a_4, \quad b_6 = 4a_6, \quad b_8 = \left(\frac{2}{\pi}\right)^2 a_6 + 4a_2a_6 - a_4^2.$$

En particulier, il vient

$$v(b_2) = 2, \quad v(b_4) = 2, \quad v(b_6) = 4 \quad \text{et} \quad v(b_8) = 0.$$

On en déduit que $c_4 = b_2^2 - 24b_4$ vérifie $v(c_4) = 4$ et $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$ vérifie $v(c_6) = 6$. De plus, on a $c_6' \equiv -b_2^3/\pi^6 \pmod 2$, puis, comme $b_2/\pi^2 \equiv 1 \pmod 2$, il vient $c_6' \equiv 1 \pmod 2$.

Enfin, $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$. Donc, en particulier, $v(\Delta) = 4$ et

$$j' = \frac{c_4'^3}{\Delta'} \equiv -\frac{1}{b_8} \equiv -\frac{1}{\pi^2 - a_4^2} \pmod{2\pi}.$$

Or, $a_4 \equiv 1 \pmod 2$, donc $a_4^2 \equiv 1 \pmod{2\pi}$ et $j' \equiv 1 + \pi^2 \pmod{2\pi}$. D'où la proposition 17.

Exemple 9. *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1 + \pi$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$, la condition (C2) et $|\Phi| = 3$.

Démonstration. Les deux premières propriétés résultent de la proposition 17. De plus,

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même,

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6} - 3^3\frac{2^5}{\pi^5}.$$

D'où $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 + \pi^5 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors,

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8},$$
$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^4 \pmod{\pi^6}.$$

Autrement dit, le couple $(a, b) = (-\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7, -\varepsilon + \pi^4)$ de l'ensemble $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que $|\Phi| = 3$ avec l'assertion 6 du théorème 2.

Supposons alors $K \in \Omega_2$. Alors,

$$c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \equiv -\varepsilon^2 + 6 + 2\pi^4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8},$$
$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 + \pi^5 \equiv -\varepsilon + \pi^5 \pmod{\pi^6}.$$

Autrement dit, le couple $(a, b) = (-\varepsilon^2 + 6 + \pi^6, -\varepsilon + \pi^5)$ de $\mathcal{L}_1$ vérifie $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que $|\Phi| = 3$ avec l'assertion 6 du théorème 2 dans ce cas également. D'où le résultat en général.

Exemple 10. *La courbe E d'équation*

$$y^2 + \frac{2}{\pi}xy = x^3 + x + 1$$

vérifie $(v(c_4), v(c_6), v(\Delta)) = (4, 6, 4)$, la condition (C2) et $|\Phi| = 6$.

Démonstration. Les deux premières propriétés résultent de la proposition 17. De plus,

$$c'_4 = \left(\frac{2}{\pi^2}\right)^4 - 3\left(\frac{2}{\pi}\right)^4 = \frac{1}{9}\varepsilon^2 - \frac{1}{3}\varepsilon^2\pi^4.$$

Donc, en particulier, $c'_4 \equiv -\varepsilon^2 - 6 + \pi^4 \pmod{\pi^8}$. De même,

$$c'_6 = -\frac{2^6}{\pi^{12}} + 3^2\frac{2^5}{\pi^8} - 3^3\frac{2^5}{\pi^6}.$$

D'où $c'_6 \equiv -\varepsilon/3 + 2 + 2\pi^2 \equiv 5\varepsilon + 2 + 2\pi^2 \pmod{\pi^6}$.

Supposons à présent $K \in \Omega_1$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 2\pi^4 + 6 + \pi^6 + \pi^7 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon + \pi^4 + \pi^5 \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a, b) de $\mathcal{L}_1$ vérifiant $c'_4 \equiv a \pmod{\pi^8}$ et $c'_6 \equiv b \pmod{\pi^6}$. On conclut que $|\Phi| = 6$ avec l'assertion 6 du théorème 2.

Supposons alors $K \in \Omega_2$. Alors, comme dans l'exemple précédent, on a $c'_4 \equiv -\varepsilon^2 + 6 + \pi^6 \pmod{\pi^8}$ et

$$c'_6 \equiv 5\varepsilon + 2 + 2\pi^2 \equiv -\varepsilon \pmod{\pi^6}.$$

Il n'existe alors aucun couple (a,b) de $\mathcal{L}_1$ vérifiant $c_4' \equiv a \pmod{\pi^8}$ et $c_6' \equiv b \pmod{\pi^6}$. On conclut que $|\Phi| = 6$ avec l'assertion 6 du théorème 2 dans ce cas également. D'où le résultat en général.

Cela démontre que tous les cas de l'assertion 6 se réalisent.

B. Tableaux de Papadopoulos

On explicite dans cet appendice le Tableau V de [3] dans le cas où, avec ses notations, $\lambda = 2$ (i.e. $e = 2$).

Type de Néron	II								
Cas de Tate	3								
$v(c_4)$	4	≥ 8	≥ 8	4	8	8	4	8	≥ 9
$v(c_6)$	6	8	10	6	11	≥ 12	6	12	11
$v(\Delta)$	4	4	8	6	10	12	7	13	10
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	4	4	8	6	10	12	7	13	10

Type de Néron	III									
Cas de Tate	4									
$v(c_4)$	4	8	8	4	8	9	9	9	9	9
$v(c_6)$	6	8	10	6	11	8	10	12	13	≥ 14
$v(\Delta)$	4	4	8	6	10	4	8	12	14	15
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	3	7	5	9	3	7	11	13	14

Type de Néron	IV		
Cas de Tate	5		
$v(c_4)$	4	8	≥ 10
$v(c_6)$	6	8	8
$v(\Delta)$	4	4	4
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	I_0^*								
Cas de Tate	6								
$v(c_4)$	8	4	8	8	4	8	≥ 10	≥ 10	≥ 10
$v(c_6)$	10	6	≥ 12	12	6	12	10	12	13
$v(\Delta)$	8	8	12	14	9	15	8	12	14
Conditions sup.	$*$	$*$	$*$	$*$			$*$	$*$	
$v(N)$	4	4	8	10	5	11	4	8	10

Type de Néron	I_1^*			I_3^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	10	10	6	≥ 12	12
$v(\Delta)$	8	8	8	11	12	12
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	3	3	3	4	5	5

Type de Néron	I_5^*			I_7^*		
Cas de Tate	7			7		
$v(c_4)$	4	8	10	4	8	10
$v(c_6)$	6	12	14	6	12	15
$v(\Delta)$	13	16	16	15	19	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	4	7	7	4	8	9

Type de Néron	I_2^*							
Cas de Tate	7							
$v(c_4)$	8	8	8	4	10	10	10	10
$v(c_6)$	≥ 12	12	12	6	12	14	≥ 15	15
$v(\Delta)$	12	14	16	10	12	16	18	19
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	6	8	10	4	6	10	12	13

Type de Néron	I_4^*					
Cas de Tate	7					
$v(c_4)$	8	8	4	10	10	10
$v(c_6)$	12	12	6	14	≥ 15	15
$v(\Delta)$	16	17	12	16	18	20
Conditions sup.	$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	8	9	4	8	10	12

Type de Néron	I_6^*			
Cas de Tate	7			
$v(c_4)$	4	8	10	10
$v(c_6)$	6	12	15	15
$v(\Delta)$	14	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$
$v(N)$	4	8	10	11

Type de Néron	I_ν^*, $\nu \geq 8$		
Cas de Tate	7		
$v(c_4)$	4	8	10
$v(c_6)$	6	12	15
$v(\Delta)$	$8+\nu$	$12+\nu$	$14+\nu$
Conditions sup.	$*$	$*$	$*$
$v(N)$	4	8	10

On notera à cet endroit que si $(v(c_4), v(c_6), v(\Delta))$ est le triplet $\big(10, 15, 14+\nu\big)$ et si ν est impair ≥ 9, Papadopoulos ne donne pas de condition supplémentaire $*$, mais il en existe une pour ce triplet si ν est pair ≥ 8.

Type de Néron	IV^*		
Cas de Tate	8		
$v(c_4)$	4	8	≥ 11
$v(c_6)$	6	10	10
$v(\Delta)$	8	8	8
Conditions sup.	$*$	$*$	$*$
$v(N)$	2	2	2

Type de Néron	III^*							
Cas de Tate	9							
$v(c_4)$	4	8	8	11	11	11	11	11
$v(c_6)$	6	12	≥ 12	12	14	15	16	≥ 17
$v(\Delta)$	10	14	12	12	16	18	20	21
Conditions sup.	$*$	$*$	$*$	$*$	$*$			
$v(N)$	3	7	5	5	9	11	13	14

Type de Néron	II^*						
Cas de Tate	10						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	15	12	14	≥ 12	6	12	12
$v(\Delta)$	18	12	16	12	11	17	16
Conditions sup.		$*$	$*$	$*$	$*$	$*$	$*$
$v(N)$	10	4	8	4	3	9	8

Type de Néron	Équation non minimale						
$v(c_4)$	≥ 12	≥ 12	≥ 12	8	4	8	8
$v(c_6)$	≥ 16	12	14	≥ 12	6	12	12
$v(\Delta)$	≥ 20	12	16	12	≥ 12	16	≥ 18
Conditions sup.		$*$	$*$	$*$	$*$	$*$	$*$

Références

[1] É. Cali, *Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié*, Canad. J. Math. 56 (2004), 673–698.

[2] A. Kraus, *Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive*, Manuscripta Math. 69 (1990), 353–385.

[3] I. Papadopoulos, *Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle* 2 *et* 3, J. Number Theory 44 (1993), 119–152.

[4] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Ann. of Math. 88 (1968), 492–517.

[5] J. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, in: Modular Functions of One Variable, Lecture Notes in Math. 273, Springer, 1975, 33–52.

MATHEMATICS OF COMPUTATION
Volume 79, Number 269, January 2010, Pages 535–544
S 0025-5718(09)02294-7
Article electronically published on July 22, 2009

SOLVING FERMAT-TYPE EQUATIONS $x^5 + y^5 = dz^p$

NICOLAS BILLEREY AND LUIS V. DIEULEFAIT

Abstract. In this paper, we are interested in solving the Fermat-type equations $x^5 + y^5 = dz^p$, where d is a positive integer and p a prime number ≥ 7. We describe a new method based on modularity theorems which allows us to improve all earlier results for this equation. We finally discuss the present limits of the method by looking at the case $d = 3$.

1. Introduction

Let p be a prime number ≥ 7 and d be a positive integer. We say that a solution (a, b, c) of the equation $x^5 + y^5 = dz^p$ is *primitive* if $(a, b) = 1$ and *non-trivial* if $c \neq 0$ (note that this is not the same definition as in [1]). Let us recall briefly the generalization of the so-called modular method of Frey for solving this equation.

Assume that (a, b, c) is a non-trivial primitive solution of $x^5 + y^5 = dz^p$. Then the equation

$$(\star) \qquad y^2 = x^3 - 5(a^2 + b^2)x^2 + 5\left(\frac{a^5 + b^5}{a + b}\right)x$$

defines an elliptic curve $E(a, b)$ over $\mathbf{Q}$ of conductor N (say) which is semistable at each prime different from 2 and 5. By results of Wiles, Taylor-Wiles, Diamond and Skinner-Wiles, $E(a, b)$ is modular. Furthermore, $E(a, b)$ is a Frey-Hellegouarch curve in the following sense: the Galois representation ρ_p on p-torsion points of $E(a, b)$ is irreducible and unramified outside 2, 5, p and the set of primes dividing d. The conductor $N(\rho_p)$ (prime to p) and the weight k of ρ_p are computed in [1, §3]. Thus, it follows from a theorem of Ribet that there exists a modular form f of weight k, level $N(\rho_p)$ and trivial character such that the associated p-adic representation $\sigma_{f,p}$ satisfies $\sigma_{f,p} \equiv \rho_p \pmod{p}$. More precisely, let us denote by a_q and a'_q the coefficients of the L-functions of E and f, respectively, by K_f the number field generated by all the a'_q's and by $N_{K_f/\mathbf{Q}}$ the corresponding norm map. We then have the following proposition.

Proposition 1.1. *There exists a primitive newform f of weight k and level $N(\rho_p)$ such that, for each prime q, the following conditions hold.*

(1) *If q divides N but q does not divide $pN(\rho_p)$, then*

$$p \text{ divides } N_{K_f/\mathbf{Q}}\left(a'_q \pm (q + 1)\right).$$

(2) *If q does not divide pN, then p divides $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$.*

Received by the editor July 10, 2008 and, in revised form, January 28, 2009.
2000 *Mathematics Subject Classification.* Primary 11F11, 11D41, 14H52; Secondary 11D59.
Key words and phrases. Modular forms, Fermat's equation, elliptic curves, Thue-Mahler equations.

The aim of the modular method is to contradict the existence of such a form f. We describe, in the following section, a method which allows us sometimes to reach this goal.

2. Description of the method

Fix a prime number $p \geq 7$ and a positive integer d. Consider in turn each newform f of weight k and level $N(\rho_p)$. Suppose there exists a prime number q (depending on p, d and f) such that the following conditions hold:

(1) The prime q does not divide $pN(\rho_p)$.
(2) The prime p does not divide $N_{K_f/\mathbf{Q}}\left(a'_q \pm (q+1)\right)$.
(3) Let $(a,b) \in \mathbf{F}_q^2$. Consider the cubic over $\mathbf{F}_q$ given by the equation (⋆). If it is non-singular, compute the number of its $\mathbf{F}_q$-points. When (a,b) describes $\mathbf{F}_q \times \mathbf{F}_q$, this gives rise to a finite list of coefficients. The prime p does not divide $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$, for any a_q in this list.

Then the equation $x^5 + y^5 = dz^p$ does not have a non-trivial primitive solution.

3. Applications to the Fermat equation

We apply, in this section, the method described above to some values of d.

3.1. Case where $d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$.

In this paragraph, we are interested in the case where

$$d = 2^\alpha \cdot 3^\beta \cdot 5^\gamma, \quad \text{with } \alpha \geq 2 \text{ and } \beta, \gamma \text{ arbitrary.}$$

The following theorem generalizes Theorems 1.2 and 1.3 of [1].

Theorem 3.1. *Assume d is as above. Then the equation $x^5 + y^5 = dz^p$ does not have any non-trivial primitive solutions for $p \geq 13$.*

Remark 3.2. Note that although our method fails to solve these Fermat equations for small values of p, it is expected that they do not have a non-trivial solution for any $p \geq 7$.

Proof of Theorem 3.1. Assume that (a,b,c) is a non-trivial primitive solution. It follows from [1, §3] that the representation ρ_p is irreducible of weight $k = 2$.

If $\beta = 0$, then we have $N(\rho_p) = 25$ or 50. Since there is no newform of weight 2 and level 25, we necessarily have $N(\rho_p) = 50$. There are exactly two such forms and both of them have rational coefficients. The curve $E(a,b)$ is semistable at $q = 3$. Assume that $E(a,b)$ has multiplicative reduction at 3. By Prop. 1.1, we have $a'_3 \pm 4 \equiv 0 \pmod{p}$. Besides, by [4], we have $a'_3 = \pm 1$, which is a contradiction, since $p \geq 13$. So, $E(a,b)$ has good reduction at $q = 3$ and by the proposition above, $\pm 1 = a'_3 \equiv a_3 \pmod{p}$. This is also a contradiction because a_3 is even ($E(a,b)$ has a non-trivial 2-torsion subgroup) and $|a_3| \leq 2\sqrt{3}$, i.e. $a_3 = 0$ or ± 2.

If $\beta > 0$, then we have $N(\rho_p) = 75$ or 150. Assume that we have $N(\rho_p) = 75$. By [4], there are exactly 3 primitive newforms of weight 2 and level 75. They all have coefficients in $\mathbf{Q}$ and the form f of Prop. 1.1 is one of them. Moreover, by [4], we have $a'_7 = 0$ or ± 3. Since $p \geq 13$, the first condition of Prop. 1.1 does not hold for $q = 7$ and $E(a,b)$ has good reduction at 7. Following the method described in the previous section, we find that a_7 belongs to the set $\{-4, -2, 2\}$. We then deduce that the second condition of Prop. 1.1 does not hold either. In other words, we have $N(\rho_p) = 150$.

There are exactly 3 primitive newforms of weight 2 and level 150, denoted by 150A1, 150B1 and 150C1 and f is one of them. If $f = 150B1$, then $a'_7 = 4$ and a contradiction follows as above. So, $f = 150A1$ or 150C1 and by [4], we have $a'_{11} = 2$. Since $p \geq 13$, the first condition of Prop. 1.1 does not hold for $q = 11$ and $E(a, b)$ has good reduction at 11. Besides, we have $a_{11} = 0$ or ± 4. So, the second condition of Prop. 1.1 does not hold either and we obtain a contradiction. This ends the proof of the theorem. □

3.2. **Case where $d = 7$.** In this paragraph, we prove the following theorem.

Theorem 3.3. *The equation $x^5 + y^5 = 7z^p$ does not have any non-trivial primitive solutions for $p \geq 13$.*

Proof. Assume that (a, b, c) is a non-trivial primitive solution. It follows from [1, §3], that the representation ρ_p is irreducible, of weight $k = 2$ (since $p \neq 7$) and level $N(\rho_p) = 350$, 1400 or 2800.

Let us first assume that the form f of Prop. 1.1 has eigenvalues which are not rational integers. There are exactly 19 such forms of level 350, 1400 or 2800 and for all of them we have $a'_3 = \alpha$, where α is the generator of the field K_f given in [4]. If $E(a, b)$ has good reduction at $q = 3$, we have $a_3 = \pm 2$. Furthermore, $N_{K_f/\mathbf{Q}}(a'_3 \pm 2)$ belong to the set $\{\pm 2, \pm 4, -6, \pm 10\}$. Since f satisfies the second condition of Prop. 1.1, we deduce that $E(a, b)$ has multiplicative reduction at 3.

If f is not one the forms denoted by 1400S1, 1400T1, 2800QQ1 or 2800RR1 in [4], then $N_{K_f/\mathbf{Q}}(a'_3 \pm 4)$ belong to $\{4, 8, 10, 12, 16, 20\}$ and p divides one of them. This is a contradiction. So, f is necessarily one of the four forms above and we have $N_{K_f/\mathbf{Q}}(a'_3 \pm 4) = \pm 2 \cdot 29$ or $\pm 2 \cdot 11$. It then follows that $p = 29$. Besides, if $E(a, b)$ has good reduction at $q = 17$, then $a_{17} \in \{0, 2, 4, \pm 6, -8\}$, but by [4], 29 does not divide $N_{K_f/\mathbf{Q}}(a'_{17})$, $N_{K_f/\mathbf{Q}}(a'_{17} - 2)$, $N_{K_f/\mathbf{Q}}(a'_{17} - 4)$, $N_{K_f/\mathbf{Q}}(a'_{17} \pm 6)$ and $N_{K_f/\mathbf{Q}}(a'_{17} + 8)$. So, $E(a, b)$ has multiplicative reduction at $q = 17$, and 29 divides $N_{K_f/\mathbf{Q}}(a'_{17} \pm 18) = \pm 2^6 \cdot 79$ or $\pm 2^4 \cdot 359$. This leads us again to a contradiction, and we conclude that the eigenvalues of f are all rational integers.

In other words, f corresponds to an elliptic curve defined over $\mathbf{Q}$. There are exactly 6 isogeny classes of elliptic curves of level 350, 14 of level 1400 and 33 of level 2800. For all of them, we will contradict the conditions of Prop. 1.1 with $q = 3$, 11, 19, 23 or 37. As we have seen in §2, if $E(a, b)$ has good reduction at q, we can list the possible values of a_q. For the above prime numbers q, we find

$$a_3 = \pm 2, \qquad a_{11} \in \{0, \pm 4\}, \qquad a_{19} \in \{0, \pm 4\},$$
$$a_{23} \in \{0, \pm 2, \pm 4, \pm 6, \pm 8\} \quad \text{and} \quad a_{37} \in \{0, -2, \pm 4, -6, \pm 8, \pm 10, 12\}.$$

By the Hasse-Weil bound, $E(a, b)$ has good reduction at $q = 3$. We then deduce that f satisfies $a'_3 = \pm 2$. Among these curves, let us begin to deal with those without 2-torsion rational over $\mathbf{Q}$. If f is one of the curves denoted by 2800W1 and 2800AA1 in [4], we have $a'_{11} = \pm 3$ and this contradicts the congruences of Prop. 1.1 with $q = 11$. If f is one of the curves denoted by 1400D1, 1400K1, 2800D1 and 2800N1, we have $a'_{11} = \pm 1$. We then have a contradiction except maybe for $p = 13$. Besides, for these four curves, we have $a'_{23} = \pm 3$ and the same argument implies another contradiction except for $p = 19$. Bringing these two results together implies that f is not one of these 4 forms. If now f is one of the curves denoted by 1400C1, 1400N1, 2800E1 and 2800M1, we have $a'_{11} = \pm 5$. We then have a contradiction

except maybe for $p = 17$. Besides, for these curves, we have $a'_{19} = \pm 2$. By the same argument as before, a contradiction follows once more.

The two remaining curves of level 350, 1400 or 2800 such that $a'_3 = \pm 2$, denoted by 1400H1 and 2800G1, are the only two curves with non-trivial 2-torsion group. They satisfy $a'_{19} = \pm 2$ and $a'_{37} = 6$. Since these values do not belong to the set of possible values for a_{19} and a_{37} described above, we finally have a contradiction to the existence of a non-trivial primitive solution of $x^5 + y^5 = 7z^p$. □

3.3. **Case where $d = 13$.** In this paragraph, we prove the following theorem.

Theorem 3.4. *The equation $x^5+y^5 = 13z^p$ does not have any non-trivial primitive solutions for $p \geq 19$.*

Proof. Assume that (a, b, c) is a non-trivial primitive solution. It follows from [1, §3], that the representation ρ_p is irreducible, of weight $k = 2$ (since $p \neq 13$) and level $N(\rho_p) = 650$, 2600 or 5200.

Let q be a prime number different from 2, 5, 13 and p. By Prop. 1.1, p divides either $N_{K_f/\mathbf{Q}}\left(a'_q \pm (q+1)\right)$ or $N_{K_f/\mathbf{Q}}\left(a'_q - a_q\right)$. In other words, p is a prime factor of the resultant R_q of the minimal polynomial of a'_q and $P_q(X) = (X^2 - (q+1)^2)\prod(X - a_q)$, where the product runs over all possible values of a_q. For instance, if $q = 3$, then $P_3(X) = (X^2 - 16)(X^2 - 4)$.

Let us first assume that f has rational Fourier coefficients. If $a'_3 \neq \pm 2$, then R_3 has only 2, 3, 5 and 7 as prime factors. So we deduce that $a'_3 = \pm 2$. There are exactly 6 such newforms of level 650, 5 of level 2600 and 37 of level 5200 (for the curves of level 5200, the notation will exceptionally refer to [2]) . For all of them, a'_7 does not belong to the list $\{\pm 2, -4\}$ of possible values for a_7 when $E(a, b)$ has good reduction at 7. The same observation holds for the 13 elliptic curves of level 5200 with $a'_3 = \pm 2$ except for those denoted by 5200S1, 5200BB1, 5200AA1 and 5200Z1 (in [2]). If f is one of the first three of them, then we have $a'_{11} = 6$ or ± 2. Besides, if $E(a, b)$ has good reduction at 11, then a_{11} belongs to $\{0, \pm 4\}$. So, this is a contradiction and $f = 5200Z1$. Nevertheless, in this case, $a'_{17} = -2$ does not belong to the set $\{0, 2, 4, \pm 6, -8\}$ of possible values for a_{17} when $E(a, b)$ has good reduction at 17. We then deduce that the Fourier coefficients of f are not all rational.

Let us now assume that $N(\rho_p) = 650$ or 2800. For each f in these levels, $a'_3 = \alpha$ is a root of the polynomial defining K_f given in [4]. We then verify that R_3 is supported only by 2 and 5 except for the curves denoted 2800QQ1 and 2800RR1. But they both satisfy $a'_7 = \pm 1$, which leads us to a contradiction.

So we necessarily have $N(\rho_p) = 5200$. There are exactly 29 newforms of this level with non-rational eigenvalues numbered from 38 to 66. Four of them (those numbered 39, 42, 46 and 47) satisfy $a'_3 = 0$ or ± 1. So, f is not one of them. If f is curve number 63, then the field of coefficients is generated by a root α of the polynomial $x^4 + 6x^3 - 18x^2 - 30x + 25$ and

$$a'_3 = \frac{1}{10}\left(\alpha^3 + 6\alpha^2 - 13\alpha - 20\right).$$

Its characteristic polynomial is then $x^4+2x^3-7x^2-8x+16$ and we get $R_3 = 2^{18}$ in this case. This is of course a contradiction. The same conclusion will follow if f is curve number 64, since, in this case, the generating polynomial is $x^4+6x^3-87x^2-492x+604$ and the characteristic polynomial of a'_3 is $x^4 - 2x^3 - 7x^2 + 8x + 16$.

For all the other curves, $a'_3 = \alpha$ is a root of the generating polynomial of K_f given in the tables and we have a contradiction in the same way as before, by looking at R_3 except for the following eight pairs (f, p) :

$$(f = 54, p = 43), \quad (f = 55, p = 43), \quad (f = 58, p = 23), \quad (f = 59, p = 67),$$
$$(f = 61, p = 23), \quad (f = 62, p = 67), \quad (f = 65, p = 23), \quad (f = 66, p = 43).$$

For all of these, we have a contradiction as before by looking at the coefficient a'_7, except for the last two curves where we have to consider a'_{19}.

We finally deduce a contradiction to the existence of a non-trivial primitive solution of the equation $x^5 + y^5 = 13z^p$. □

4. The case $d = 3$ and limitations of the method

As is clearly apparent, the method will not work if there exists an elliptic curve over $\mathbf{Q}$ of the form (⋆) and level $N(\rho_p)$ (for large p). For convenience, we adopt the following definition, which makes this observation precise (where Supp denotes the support of an integer and v_2 the 2-adic valuation of $\mathbf{Q}$).

Definition 4.1. We say that there is a modular obstruction for the equation $x^5 + y^5 = dz^p$ (or just for d) if there exist two coprime integers (a, b) such that the following two conditions hold.

(1) The integer $m = a^5 + b^5$ is non-zero and we have

$$\mathrm{Supp}(m) \setminus \{2, 5\} = \mathrm{Supp}(d) \setminus \{2, 5\}.$$

(2) We have :
- if $\mathrm{Supp}(d)$ is not included in $\{2, 5\}$, then $ab \neq 0$,
- if $\mathrm{Supp}(d)$ is included in $\{2, 5\}$ and d is even, then $ab \neq 0$,
- if d is odd, then $v_2(m) \neq 2$,
- if $v_2(d) = 1$, then we have either $v_2(m) \geq 3$, or $v_2(m) = 1$, or $\max(v_2(a), v_2(b)) = 1$,
- if $v_2(d) = 2$, then $v_2(m) = 2$,
- if $v_2(d) \geq 3$, then $v_2(m) \geq 3$.

The following lemma gives a sufficient condition to insure that there is no modular obstruction, for several given d.

Lemma 4.2. *Let d be a positive integer such that for any prime ℓ dividing d, we have $\ell \not\equiv 1 \pmod 5$. Then, there is a modular obstruction for d if and only if $d = 5^\gamma$ or $d = 2 \cdot 5^\gamma$ with $\gamma \geq 0$.*

Proof. Assume that there is a modular obstruction for d given by two coprime integers (a, b). Then $m = a^5 + b^5$ is non-zero and $\mathrm{Supp}(m) \setminus \{2, 5\} = \mathrm{Supp}(d) \setminus \{2, 5\}$. Following [1], let us denote by ϕ the irreducible polynomial

$$\phi(x, y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4.$$

By Lemmas 2.5 and 2.6 of [1] and the hypothesis, we have:

(1) either 5 divides m and then $\phi(a, b) = \pm 5$;
(2) or 5 does not divide m and then $\phi(a, b) = \pm 1$.

In other words, (a,b) is a solution of a Thue equation of the form $\phi(x,y) = A$, where $A = \pm 1$ or ± 5 and we can assume that $a \neq 0$ (ϕ is symmetric). Since ϕ is totally complex, this leads to

$$|A| = |a|^4 \prod_{k=1}^{4} |b/a - \alpha_k| \geq |a|^4 \sin^2\left(\frac{2\pi}{5}\right) \cdot \sin^2\left(\frac{4\pi}{5}\right) \geq 0.312 \cdot |a|^4,$$

where $\alpha_k = -\exp(2ik\pi/5)$, $k = 1, \ldots, 4$, are the roots of $\phi(1,x)$. This gives an upper bound for $|a|$.

In the first case, this implies that we have $(a,b) = (1,-1)$ or $(-1,1)$ and then $m = 0$, which is a contradiction. In the second case, we deduce

$$(a,b) \in \{(1,1), (-1,-1), (\pm 1, 0), (0, \pm 1)\}.$$

In other words, $m = \pm 1$ or $m = \pm 2$. By the first condition of Def. 4.1, there exist $\alpha, \gamma \geq 0$ such that $d = 2^\alpha \cdot 5^\gamma$. Since $v_2(m) = 0$ or 1, we have, by the second condition, $\alpha = 0$ or 1.

Conversely, if $d = 5^\gamma$ or $d = 2 \cdot 5^\gamma$ with $\gamma \geq 0$, there is a modular obstruction for d given, for example, by $(a,b) = (1,1)$. □

Remark 4.3. For $d = 11$, there is a modular obstruction given by the elliptic curves $E(2,3)$ or $E(3,-1)$. Note that, in general, finding a modular obstruction for d involves solving some Thue-Mahler equation. Such an equation can be explicitly solved ([5]), although its solution might turn out to be very complicated.

Let us now look at the case where $d = 3$. By the previous lemma, there is no modular obstruction. Nevertheless, as we will see, we were not able to solve this equation for all p.

Fix for now a prime p and let (a,b,c) be a non-trivial primitive solution of the equation $x^5 + y^5 = 3z^p$. The following lemma makes more precise Lemma 4.3 of [1]. We warn the reader that in this paragraph we are using only Stein's notation [4] for modular forms (including elliptic curves). This is not the case in [1], where the author was referring to Cremona's Tables of elliptic curves [2].

Lemma 4.4. *If $p \geq 17$, then we have*

(1) *either 5 divides $a+b$ and $f = 1200\text{K}1$, or*
(2) *5 does not divide $a+b$ and $f = 1200\text{A}1$.*

Proof. Assume that 5 divides $a+b$. By Lemma 4.3 of [1], f is one of the following newforms (in Stein's notation) :

$$150\text{B}1, 600\text{C}1, 600\text{A}1, 1200\text{O}1, 1200\text{R}1, 1200\text{E}1, 1200\text{K}1.$$

If $f = 150\text{B}1$, $600\text{C}1$, $1200\text{O}1$, $1200\text{R}1$ or $1200\text{E}1$, we have $a'_7 = 0$ or 4. Besides, if $E(a,b)$ has good reduction at 7, we have $a_7 = \pm 2$ or -4. We then obtain a contradiction by looking at the conditions of Prop. 1.1 for $q = 7$. If $f = 600\text{A}1$, then $a'_{13} = 6$. Besides, if $E(a,b)$ has good reduction at 13, then a_{13} belongs to the set $\{0, \pm 2, \pm 4\}$. So, there is again a contradiction. So, $f = 1200\text{K}1$ in this case.

Assume now that 5 does not divide $a+b$. By Lemma 4.3 of [1], f is one of the following newforms (in Stein's notation) :

$$150\text{A}1, 150\text{C}1, 600\text{D}1, 600\text{G}1, 1200\text{H}1, 1200\text{L}1, 1200\text{G}1, 1200\text{A}1, 1200\text{M}1, 1200\text{S}1.$$

For $f = 1200\text{S}1$ we have $a'_7 = 4$ and using this coefficient we derive again a contradiction. For all the other curves except $1200\text{A}1$, we have $a'_{11} = \pm 2$. Besides, if

$E(a,b)$ has good reduction at 11, we have $a_{11} = 0$ or ± 4. So, f is not one of them and we conclude that $f = 1200\text{A}1$ in this case. □

If $f = 1200\text{K}1$ or $1200\text{A}1$, then for any prime $q > 5$ smaller than 5000, the Fourier coefficient a'_q of f actually lies in the list of possible values for a_q. This is why we have not been able to prove the emptiness of the set of non-trivial primitive solutions for $d = 3$.

Nevertheless, we will give a criterion which is an improvement of the one given in [1] (cf. Th. 4.5). This allows us to conclude the argument for a fixed p; we have verified that it holds for any $17 \leq p \leq 10^7$. Let us consider q a prime number congruent to 1 modulo p, and write $q = np + 1$. The group $\mu_n(\mathbf{F}_q)$ of nth roots of unity in $\mathbf{F}_q$ has order n. We now define four subsets $A^{\pm}(n,q)$ and $B^{\pm}(n,q)$ of $\mu_n(\mathbf{F}_q)$ in the following way.

(1) Let $\widetilde{A}(n,q)$ be the subset of $\mu_n(\mathbf{F}_q)$ consisting of all ζ such that

$$405 + 62500\zeta \text{ is a square in } \mathbf{F}_q.$$

For such a ζ, let us consider the smallest integer $\delta_{1,\zeta} \geq 0$ such that

$$\delta_{1,\zeta}^2 \pmod q = 405 + 62500\zeta.$$

We define $A^+(n,q)$ (resp. $A^-(n,q)$) as the subset of $\widetilde{A}(n,q)$ consisting of ζ such that

$$-225 + 10\delta_{1,\zeta} \quad (\text{resp. } -225 - 10\delta_{1,\zeta})$$

is a square modulo q. For any $\zeta \in A^+(n,q)$, let us consider the cubic curve over $\mathbf{F}_q$ defined by the equation

$$F^+_{1,\zeta} : y^2 = x^3 - \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x.$$

Its discriminant $6480\zeta^2 = 2^4 \cdot 3^4 \cdot 5\zeta^2$ is non-zero and $F^+_{1,\zeta}$ is an elliptic curve over $\mathbf{F}_q$. Let us denote by $n^+_{1,q}(\zeta)$ the number of $\mathbf{F}_q$-rational points of $F^+_{1,\zeta}$ and write

$$a^+_q(\zeta) = q + 1 - n^+_{1,q}(\zeta).$$

If $\zeta \in A^-(n,q)$, let us define, in the same way, the cubic curve

$$F^-_{1,\zeta} : y^2 = x^3 + \frac{\delta_{1,\zeta}}{25}x^2 + 25\zeta x.$$

As a twist of $F^+_{1,\zeta}$, it is also an elliptic curve over $\mathbf{F}_q$ and we write

$$a^-_q(\zeta) = q + 1 - n^-_{1,q}(\zeta),$$

where $n^-_{1,q}(\zeta)$ denotes the number of $\mathbf{F}_q$-rational points of $F^-_{1,\zeta}$.

(2) Let $\widetilde{B}(n,q)$ be the subset of $\mu_n(\mathbf{F}_q)$ consisting of all ζ such that

$$405 + 20\zeta \text{ is a square in } \mathbf{F}_q.$$

For such a ζ, let us consider the smallest integer $\delta_{2,\zeta} \geq 0$ such that

$$\delta_{2,\zeta}^2 \pmod q = 405 + 20\zeta.$$

We define $B^+(n,q)$ (resp. $B^-(n,q)$) as the subset of $\widetilde{B}(n,q)$ consisting of ζ such that

$$-225 + 10\delta_{2,\zeta} \quad (\text{resp. } -225 - 10\delta_{2,\zeta})$$

is a square modulo q. For any $\zeta \in B^+(n,q)$, let us consider the cubic curve over $\mathbf{F}_q$ defined by the equation

$$F^+_{2,\zeta} : y^2 = x^3 - \delta_{2,\zeta} x^2 + 5\zeta x.$$

Its discriminant $2^4 \cdot 3^4 \cdot 5^3 \zeta^2$ is non-zero and $F^+_{2,\zeta}$ is an elliptic curve over $\mathbf{F}_q$. Let us denote by $n^+_{2,q}(\zeta)$ the number of $\mathbf{F}_q$-rational points of $F^+_{2,\zeta}$ and write

$$b^+_q(\zeta) = q + 1 - n^+_{2,q}(\zeta).$$

If $\zeta \in B^-(n,q)$, let us define, in the same way, the cubic curve

$$F^-_{2,\zeta} : y^2 = x^3 + \delta_{2,\zeta} x^2 + 5\zeta x.$$

As a twist of $F^+_{2,\zeta}$, it is also an elliptic curve over $\mathbf{F}_q$ and we write

$$b^-_q(\zeta) = q + 1 - n^-_{2,q}(\zeta),$$

where $n^-_{2,q}(\zeta)$ denotes the number of $\mathbf{F}_q$-rational points of $F^-_{2,\zeta}$.

Our criterion is stated in the following theorem. It is a refinement of [1, Th. 1.4], since only two curves have to be removed, instead of seven in loc. cit.

Theorem 4.5. *Let p be a prime number ≥ 17. Assume that the following two conditions hold.*

(1) *For the curve $f = 1200\text{K}1$, there exists an integer $n \geq 2$ such that*
   (a) *the integer $q = np + 1$ is a prime number;*
   (b) *we have $a'^2_q \not\equiv 4 \pmod{p}$;*
   (c) *for all ζ in $A^+(n,q)$, we have $a'_q \not\equiv a^+_q(\zeta) \pmod{p}$;*
   (d) *for all ζ in $A^-(n,q)$, we have $a'_q \not\equiv a^-_q(\zeta) \pmod{p}$.*

(2) *For the curve $f = 1200\text{A}1$, there exists an integer $n \geq 2$ such that*
   (a) *the integer $q = np + 1$ is a prime number;*
   (b) *we have $a'^2_q \not\equiv 4 \pmod{p}$;*
   (c) *for all ζ in $B^+(n,q)$, we have $a'_q \not\equiv b^+_q(\zeta) \pmod{p}$;*
   (d) *for all ζ in $B^-(n,q)$, we have $a'_q \not\equiv b^-_q(\zeta) \pmod{p}$.*

Then, there is no non-trivial primitive solution of $x^5 + y^5 = 3z^p$.

Proof. Let n be as in the theorem. By Lemma 4.4, ρ_p is isomorphic to the mod p representation $\overline{\sigma_{f,p}}$ of $f = 1200\text{A}1$ or $1200\text{K}1$. If $E(a,b)$ does not have good reduction at q, then $E(a,b)$ has multiplicative reduction ([1, Lem. 2.7]) and by [3, Prop. 3(*iii*)], we have

$$a'_q \equiv \pm(q+1) \equiv \pm 2 \pmod{p}.$$

This contradicts the conditions (4.5) and (4.5) of the theorem. So, we deduce that $E(a,b)$ has good reduction at q; in other words, q does not divide c.

We now follow step by step the discussion of [1, §4.4], without giving all the details. Let us denote by ϕ the polynomial $\phi(x,y) = x^4 - x^3y + x^2y^2 - xy^3 + y^4$ and by $\overline{a}$ (resp. $\overline{b}$) the reduction of a (resp. b) modulo q.

(1) Assume that 5 divides $a + b$. Then, there exist two integers c_1 and c_2 such that

$$5(a+b) = 3c_1^p, \quad \phi(a,b) = 5c_2^p \quad \text{and} \quad c = c_1 c_2.$$

Furthermore, if $u = c_1^p \pmod{q}$ and $v = c_2^p \pmod{q}$, then

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{and} \quad \zeta = \frac{v}{u^4}$$

satisfy

$$5(\overline{a}' + \overline{b}') = 3 \quad \text{and} \quad \phi(\overline{a}', \overline{b}') = 5\zeta.$$

We then deduce that $\overline{b}'$ is a root of the polynomial

$$P_{1,\zeta}(X) = X^4 - \frac{6}{5}X^3 + \frac{18}{25}X^2 - \frac{27}{125}X + \frac{81}{3125} - \zeta \in \mathbf{F}_q[X].$$

So, $\overline{b}'$ is one of the following elements:

$$\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}, \quad \frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \quad \frac{3}{10} - \frac{\beta_{1,\zeta}}{50},$$

where $\alpha_{1,\zeta}$ (resp. $\beta_{1,\zeta}$) is a square root of $-225 + 10\delta_{1,\zeta}$ (resp. $-225 - 10\delta_{1,\zeta}$) modulo q.

(a) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{10} + \frac{\alpha_{1,\zeta}}{50}, \frac{3}{10} - \frac{\alpha_{1,\zeta}}{50}\right\}.$$

Then ζ belongs to the set $A^+(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^+_{1,\zeta}$. So we deduce that

$$a_q \equiv a^+_q(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200K1. This contradicts our hypothesis (4.5).

(b) Assume that we have

$$\left\{\overline{a}', \overline{b}'\right\} = \left\{\frac{3}{10} + \frac{\beta_{1,\zeta}}{50}, \frac{3}{10} - \frac{\beta_{1,\zeta}}{50}\right\}.$$

Then ζ belongs to the set $A^-(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^-_{1,\zeta}$. So we deduce that

$$a_q \equiv a^-_q(\zeta) \pmod{p}.$$

But, by Lemma 4.4, we have $a_q \equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200K1. This contradicts our hypothesis (4.5).

We finally deduce that 5 does not divide $a + b$.

(2) If 5 does not divide $a + b$, then there exist two integers c_1 and c_2 such that

$$a + b = 3c_1^p, \quad \phi(a,b) = c_2^p \quad \text{and} \quad c = c_1c_2.$$

Furthermore, if $u = c_1^p \pmod{q}$ and $v = c_2^p \pmod{q}$, then

$$\overline{a}' = \frac{\overline{a}}{u}, \quad \overline{b}' = \frac{\overline{b}}{u} \quad \text{and} \quad \zeta = \frac{v}{u^4}$$

satisfy

$$\overline{a}' + \overline{b}' = 3 \quad \text{and} \quad \phi(\overline{a}', \overline{b}') = \zeta.$$

We then deduce that $\overline{b}'$ is a root of the polynomial

$$P_{2,\zeta}(X) = X^4 - 6X^3 + 18X^2 - 27X + \frac{81 - \zeta}{5} \in \mathbf{F}_q[X].$$

So, $\overline{b}'$ is one of the elements

$$\frac{3}{2} + \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\alpha_{2,\zeta}}{10}, \quad \frac{3}{2} + \frac{\beta_{2,\zeta}}{10}, \quad \frac{3}{2} - \frac{\beta_{2,\zeta}}{10},$$

where $\alpha_{2,\zeta}$ (resp. $\beta_{2,\zeta}$) is a square root of $-225+10\delta_{2,\zeta}$ (resp. $-225-10\delta_{2,\zeta}$) modulo q.

(a) Assume that we have

$$\left\{\overline{a}',\overline{b}'\right\}=\left\{\frac{3}{2}+\frac{\alpha_{2,\zeta}}{10},\frac{3}{2}-\frac{\alpha_{2,\zeta}}{10}\right\}.$$

Then ζ belongs to the set $B^+(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^+_{2,\zeta}$. So we deduce that

$$a_q\equiv b_q^+(\zeta)\pmod{p}.$$

But, by Lemma 4.4, we have $a_q\equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200A1. This contradicts our hypothesis (4.5).

(b) Assume that we have

$$\left\{\overline{a}',\overline{b}'\right\}=\left\{\frac{3}{2}+\frac{\beta_{2,\zeta}}{10},\frac{3}{2}-\frac{\beta_{2,\zeta}}{10}\right\}.$$

Then ζ belongs to the set $B^-(n,q)$ and the reduction modulo q of the curve $E(a,b)$ is isomorphic to $F^-_{2,\zeta}$. So we deduce that

$$a_q\equiv b_q^-(\zeta)\pmod{p}.$$

But, by Lemma 4.4, we have $a_q\equiv a'_q \pmod{p}$, where a'_q is the qth Fourier coefficient of 1200A1. This contradicts our hypothesis (4.5).

We finally deduce that there is no non-trivial primitive solution of the equation $x^5+y^5=3z^p$. □

Remark 4.6. For a given p, a `pari/gp` program giving an integer n as in the theorem is available at: `http://www.institut.math.jussieu.fr/billerey/Fermatnew`. Using this and [1, Prop. 1.1], we were able to prove that the equation $x^5+y^5=3z^p$ does not have a non-trivial primitive solution for $5\leq p\leq 10^7$.

References

1. Nicolas Billerey. Équations de Fermat de type $(5,5,p)$. *Bull. Austral. Math. Soc.*, 76(2):161–194, 2007. MR2353205 (2008i:11049)
2. J. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997. MR1628193 (99e:11068)
3. A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293:259–275, 1992. MR1166121 (93e:11074)
4. W. Stein. The Modular Forms Database. `http://modular.fas.harvard.edu/Tables`, 2004.
5. N. Tzanakis and B. M. M. de Weger. How to explicitly solve a Thue-Mahler equation. *Compositio Math.*, 84(3):223–288, 1992. MR1189890 (93k:11025)

Université Pierre et Marie Curie – Paris 6, UMR 7586, Case 247, 4, place Jussieu, Institut de Mathématiques, 75252 Paris, France

E-mail address: `billerey@math.jussieu.fr`

Departament d'Algebra i Geometria, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, (08007) Barcelona, Spain

E-mail address: `ldieulefait@ub.edu`

International Journal of Number Theory
Vol. 7, No. 4 (2011) 1001–1032

DOI: 10.1142/S1793042111004538

World Scientific
www.worldscientific.com

CRITÈRES D'IRRÉDUCTIBILITÉ POUR LES REPRÉSENTATIONS DES COURBES ELLIPTIQUES

NICOLAS BILLEREY
Institut für Experimentelle Mathematik
Universität Duisburg-Essen
Ellernstrs. 29, D-45326 Essen, Germany
billerey@gmail.com

Received 21 May 2010
Accepted 15 August 2010

Soit E une courbe elliptique définie sur un corps de nombres K. On dit qu'un nombre premier p est réductible pour le couple (E, K) si E admet une p-isogénie définie sur K. L'ensemble de tous ces nombres premiers est fini si et seulement si E n'a pas de multiplication complexe définie sur K. Dans cet article, on montre que l'ensemble des nombres premiers réductibles pour le couple (E, K) est contenu dans l'ensemble des diviseurs premiers d'une liste explicite d'entiers (dépendant de E et de K) dont une infinité d'entre eux est non nulle. Cela fournit un algorithme efficace de calcul dans le cas fini. D'autres critères moins généraux, mais néanmoins utiles sont donnés ainsi que de nombreux exemples numériques.

Mots clés: Courbes elliptiques; représentations galoisiennes; théorie du corps de classes.

Let E be an elliptic curve defined over a number field K. We say that a prime number p is reducible for (E, K) if E admits a p-isogeny defined over K. The so-called reducible set of all such prime numbers is finite if and only if E does not have complex multiplication over K. In this paper, we prove that the reducible set is included in the set of prime divisors of an explicit list of integers (depending on E and K), infinitely many of them being non-zero. It provides an efficient algorithm for computing it in the finite case. Other less general but rather useful criteria are given, as well as many numerical examples.

Keywords: Elliptic curves; Galois representations; class field theory.

Mathematics Subject Classification 2010: 11G05, 11F80, 11R37

0. Introduction

Soient $\overline{\mathbf{Q}}$ la clôture algébrique de $\mathbf{Q}$ dans $\mathbf{C}$ et K un corps de nombres contenu dans $\overline{\mathbf{Q}}$. Étant donnés une courbe elliptique E définie sur K et un nombre premier p, on note $E[p]$ le groupe des points de p-torsion de la courbe E. C'est un espace vectoriel de dimension 2 sur le corps $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ muni d'une action du groupe de Galois $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Cela fournit un homomorphisme

$$\rho_p : \mathrm{G}_K \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbf{F}_p).$$

Serre a démontré ([21]) que si E est sans multiplication complexe sur $\overline{\mathbf{Q}}$, il existe une constante $c(E,K)$ telle que pour tout nombre premier $p > c(E,K)$, la représentation ρ_p est surjective.

Dans ce travail, on s'intéresse à l'ensemble, noté $\mathrm{Red}(E/K)$, des nombres premiers p pour lesquels la représentation ρ_p ci-dessus est réductible. On dit alors pour simplifier que p est *réductible* pour le couple (E,K). L'ensemble $\mathrm{Red}(E/K)$ est généralement fini. Plus précisément, $\mathrm{Red}(E/K)$ est fini si et seulement E n'a pas de multiplication complexe sur K, i.e. $\mathrm{End}_K(E) = \mathbf{Z}$ (Proposition 1.2).

Lorsque E est sans multiplication complexe, Pellarin ([19]), à la suite de Masser et Wüstholz, a obtenu, comme corollaire de ses travaux, une majoration explicite des nombres premiers réductibles. Cependant, en raison des constantes qui y apparaîssent, ce résultat ne se prête malheureusement pas à une détermination *explicite* de l'ensemble $\mathrm{Red}(E/K)$. En utilisant des arguments de théorie du corps de classes, on obtient, dans ce travail, deux énoncés permettant d'y parvenir.

Notons d le degré de K sur $\mathbf{Q}$, D_K son discriminant, $\mathcal{O}_K$ son anneau d'entiers, h son nombre de classes et $N_{K/\mathbf{Q}}$ la norme de l'extension $K/\mathbf{Q}$ et supposons E donnée par une équation de Weierstrass à coefficients dans l'anneau $\mathcal{O}_K$ de discriminant Δ. Soit ℓ un nombre premier. Si E a mauvaise réduction en un idéal premier au-dessus de ℓ, on pose $B_\ell = 0$. Dans le cas contraire (c'est-à-dire pour presque tout ℓ), on dit, par abus de langage, que E a bonne réduction en ℓ et on associe alors à ℓ un polynôme P_ℓ^* à coefficients entiers dont certaines valeurs spéciales vont permettre de déterminer essentiellement l'ensemble $\mathrm{Red}(E/K)$. Ce polynôme est *explicitement* calculé uniquement à partir de la décomposition de $\ell\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$ et de la réduction de E en ces idéaux premiers (cf. Sec. 2.3 pour la construction précise). On pose alors:

$$B_\ell = \prod_{k=0}^{[\frac{d}{2}]} P_\ell^*(\ell^{12k})$$

où $[d/2]$ désigne la partie entière de $d/2$. Sous une forme légèrement affaiblie, le premier résultat que l'on obtient en vue de la détermination explicite de l'ensemble $\mathrm{Red}(E/K)$ s'énonce de la manière suivante:

Théorème 0.1 ([Théorème 2.4]). *Soit p un nombre premier réductible pour (E,K). Alors, on est dans l'une des situations suivantes*:

(1) *p divise $6D_K N_{K/\mathbf{Q}}(\Delta)$;*
(2) *pour tout nombre premier ℓ, le nombre premier p divise l'entier B_ℓ (si $d = 1$, on suppose $\ell \neq p$).*

De plus, en étudiant les propriétés des polynômes P_ℓ^* et des entiers B_ℓ, on obtient, dans le cas où d est impair, le corollaire particulièrement agréable suivant:

Corollaire 0.2 (cas du degré impair). *On suppose que l'extension $K/\mathbf{Q}$ est de degré* impair. *Alors, l'ensemble des nombres premiers réductibles pour E est* fini.

De plus, si p un nombre premier réductible pour (E, K), alors, pour tout nombre premier ℓ de bonne réduction, le nombre premier p divise l'entier non nul

$$6D_K N_{K/\mathbf{Q}}(\Delta) B_\ell.$$

La situation est plus compliquée dans le cas des extensions de degré pair. Bien que le critère du théorème ci-dessus s'applique toujours, on n'a plus la garantie, pour une courbe ayant un ensemble réductible fini, qu'il existe un nombre premier ℓ pour lequel l'entier B_ℓ correspondant soit non nul (comme le montre l'exemple 4.4). On démontre alors un critère plus général permettant de contourner cette difficulté, au prix cependant de certaines complications dans son utilisation pratique. Plus précisément, soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$. On pose $R_\mathfrak{q} = 0$ si E a mauvaise réduction en $\mathfrak{q}$. Si, en revanche, E a bonne réduction en $\mathfrak{q}$, on lui associe via un calcul de résultants un certain entier $R_\mathfrak{q}$ dépendant du polynôme minimal sur $\mathbf{Q}$ d'un générateur de $\mathfrak{q}^h$ et de la réduction en $\mathfrak{q}$ de E (cf. Sec. 2.4 pour la construction précise). On montre alors une forme légèrement améliorée du résultat suivant:

Théorème 0.3 ([Théorème 2.8]). *Soit p un nombre premier réductible pour (E, K). Alors, on est dans l'une des situations suivantes*:

(1) *p divise $6D_K N_{K/\mathbf{Q}}(\Delta)$;*
(2) *pour tout idéal premier $\mathfrak{q}$, le nombre premier p divise l'entier $R_\mathfrak{q}$ (si $d = 1$, on suppose que $\mathfrak{q}$ ne divise pas p).*

De plus, si E est sans multiplication complexe sur $\overline{\mathbf{Q}}$, alors $R_\mathfrak{q} \neq 0$ pour une infinité d'idéaux premiers $\mathfrak{q}$.

La démonstration des deux théorèmes principaux 2.4 et 2.8 occupe la Sec. 2. La Sec. 1 contient plusieurs préliminaires utiles. Dans la partie 3, on démontre deux critères «uniformes» pour des ensembles de courbes elliptiques ayant mauvaise réduction additive en une place finie de K et un «défaut de semi-stabilité» particulier. Enfin, la Sec. 4 contient une discussion sur l'utilisation pratique et l'efficacité de l'algorithme fourni par les résultats principaux de la Sec. 2, ainsi que plusieurs exemples numériques concrets.

1. Préliminaires

Dans toute cette section, on fixe un corps de nombres K contenu dans $\overline{\mathbf{Q}}$ et une courbe elliptique E définie sur K. Soit p un nombre premier réductible. Le groupe $E[p]$ possède alors une droite D stable par G_K. Notons λ le caractère donnant l'action de G_K sur D. On l'appelle caractère d'isogénie associé à D. Dans une base convenable de $E[p]$ sur $\mathbf{F}_p$, la représentation ρ_p est représentable matriciellement par

$$\begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix},$$

où λ et λ' s'interprètent comme des caractères de G_K à valeurs dans $\mathbf{F}_p^*$. On a

$$\det \rho_p = \lambda \cdot \lambda' = \chi_p, \tag{1}$$

où χ_p est le caractère donnant l'action de G_K sur les racines p-ièmes de l'unité (caractère cyclotomique).

La représentation ρ_p se factorise à travers le groupe de Galois de l'extension $K(E[p])/K$, où $K(E[p])$ est le corps engendré sur K par les coordonnées des points de p-torsion de E. On note encore ρ_p, λ, λ' et χ_p les morphismes passés au quotient.

Soit $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_K$. On note $I_\mathfrak{q}$ un sous-groupe d'inertie en $\mathfrak{q}$ de $\mathrm{Gal}(K(E[p])/K)$. Si E a bonne réduction en $\mathfrak{q}$ et $\mathfrak{q}$ ne divise pas p, l'extension $K(E[p])/K$ est non ramifiée en $\mathfrak{q}$ par le critère de Néron–Ogg–Shafarevich. On note $\sigma_\mathfrak{q}$ une subsitution de Frobenius en $\mathfrak{q}$ de $\mathrm{Gal}(K(E[p])/K)$ (bien définie à conjugaison près).

Supposons que E ait bonne réduction en $\mathfrak{q}$. On pose alors

$$P_\mathfrak{q}(X) = X^2 - t_\mathfrak{q} X + N(\mathfrak{q}) \in \mathbf{Z}[X]$$

où $N(\mathfrak{q})$ est le cardinal du corps résiduel $\mathcal{O}_K/\mathfrak{q}$ et

$$t_\mathfrak{q} = N(\mathfrak{q}) + 1 - A_\mathfrak{q},$$

avec $A_\mathfrak{q}$ le nombre de points sur le corps $\mathcal{O}_K/\mathfrak{q}$ de la réduction de E en $\mathfrak{q}$. Le résultat suivant est bien connu (cf. [23, Théorème 2.4]) et intervient de façon cruciale dans la démonstration des théorèmes principaux.

Proposition 1.1 (Hasse–Weil). *Les racines complexes de $P_\mathfrak{q}$ sont de module $N(\mathfrak{q})^{1/2}$. En particulier, on a*

$$|t_\mathfrak{q}| \leq 2N(\mathfrak{q})^{1/2}.$$

Si de plus $\mathfrak{q}$ ne divise pas p, le polynôme caractéristique de $\rho_p(\sigma_\mathfrak{q})$ est $\overline{P_\mathfrak{q}} = P_\mathfrak{q} \pmod p \in \mathbf{F}_p[X]$. En particulier, on a

$$\overline{P_\mathfrak{q}}(\lambda(\sigma_\mathfrak{q})) = 0.$$

1.1. *L'ensemble* $\mathbf{Red}(E/K)$

L'objectif de ce paragraphe est de démontrer le résultat suivant.

Proposition 1.2. *Les conditions suivantes sont équivalentes*:

(1) *la courbe E n'a pas de multiplication complexe sur K (i.e.* $\mathrm{End}_K(E) = \mathbf{Z}$);
(2) *l'ensemble* $\mathrm{Red}(E/K)$ *est fini.*

Démonstration. L'implication (1) $\Rightarrow$ (2) résulte du théorème de Šafarevič sur la finitude des classes de K-isomorphisme de courbes elliptiques K-isogènes à une courbe donnée ([23, IX, §6,]). Elle est due à Serre et démontrée dans [20, IV-9].

Réciproquement, si E a des multiplications complexes sur K (i.e. $\mathrm{End}_K(E)$ est de rang 2 comme $\mathbf{Z}$-module), alors

$$\mathrm{End}_K(E) \otimes \mathbf{Q} = \mathrm{End}_{\overline{\mathbf{Q}}}(E) \otimes \mathbf{Q}$$

et K contient le corps quadratique imaginaire $L = \mathrm{End}_K(E) \otimes \mathbf{Q}$. Soit p un nombre premier décomposé dans L. On a

$$p\mathcal{O}_L = \pi \cdot \overline{\pi},$$

où $\mathcal{O}_L$ est l'anneau des entiers de L. Alors, l'ensemble $E[\pi]$ des points de E annulés par les éléments de π est défini sur K et d'ordre p ([15, Chap. 9, §4]). On en déduit que l'ensemble $\mathrm{Red}(E/K)$ est infini. □

Remarque. À partir de cette proposition et de résultats classiques de la théorie de la multiplication complexe, on démontre que les propriétés suivantes sont équivalentes:

(1) le corps K ne contient pas le corps de classes de Hilbert d'un corps quadratique imaginaire;
(2) pour toute courbe elliptique E définie sur K, l'ensemble $\mathrm{Red}(E/K)$ est fini.

1.2. *Ramification et caractère d'isogénie*

On suppose que p est un nombre premier réductible pour E. Le résultat suivant se déduit de l'étude de la restriction de ρ_p aux sous-groupes d'inertie de $\mathrm{Gal}(K(E[p])/K)$ telle qu'elle est faite, par exemple, dans [20, IV], [21, §§1.11–1.12] et [12] (voir également [8, §1] pour une discussion similaire).

Proposition 1.3. *Supposons $p \geq 5$ non ramifié dans K.*

(1) *Le caractère λ^{12} est non ramifié en dehors des idéaux premiers de $\mathcal{O}_K$ divisant p.*
(2) *Soit $\mathfrak{p}$ un idéal de $\mathcal{O}_K$ divisant p. On suppose que E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2 (supersingulière). Alors, il existe un entier $\alpha_\mathfrak{p} \in \{0, 12\}$ tel que*

$$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} .$$

Remarques. (1) Dans une base convenable, la représentation sur les points de p-torsion de la courbe E/D est représentable matriciellement par

$$\begin{pmatrix} \lambda' & * \\ 0 & \lambda \end{pmatrix}.$$

Autrement dit, d'après l'égalité (1), on peut toujours, si on le souhaite, remplacer la famille $\{\alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$ par la famille $\{12 - \alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$.

(2) On peut montrer en utilisant la description locale de ρ_p donnée dans la proposition [12, Proposition 2] que si $\mathfrak{p}$ divise p et E a mauvaise réduction additive en

$\mathfrak{p}$ avec potentiellement bonne réduction supersingulière, alors il existe un entier $\alpha_\mathfrak{p} \in \{4, 6, 8\}$ tel que

$$\lambda^{12} \mid_{I_\mathfrak{p}} = \chi_p^{\alpha_\mathfrak{p}} \mid_{I_\mathfrak{p}} .$$

(3) Dans sa thèse ([8]), A. David démontre que si K ne contient pas le corps de classes de Hilbert d'un corps quadratique imaginaire, il existe alors une constante effective $C(K)$, ne dépendant que de K (et donc pas de E) telle que si $p > C(K)$, on a $\alpha_\mathfrak{p} = 6$ pour *tout* idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p (voir également [17]). Nous n'utiliserons pas ces résultats.

1.3. *Théorie du corps de classes et caractère d'isogénie*

On reprend les hypothèses et notations précédentes. En particulier, p est un nombre premier ≥ 5 non ramifié dans K et on suppose que pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p, E n'a pas mauvaise réduction additive en $\mathfrak{p}$ avec potentiellement bonne réduction de hauteur 2. Étant donné un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus de p, on désigne par

$$N_\mathfrak{p} : (\mathcal{O}_K/\mathfrak{p})^* \longrightarrow \mathbf{F}_p^*$$

le morphisme norme. L'objectif de ce paragraphe 1.3 est de démontrer la proposition ci-dessous, cruciale dans la démonstration des Théorème 2.4 et 2.8. Elle figure également sous une forme légèrement différente dans la thèse de David ([8, Proposition 2.2.1]) ainsi que dans l'article [17, Lemme 1] de Momose (sous l'hypothèse que $K/\mathbf{Q}$ est galoisienne).

Proposition 1.4. *Soit $a \in \mathcal{O}_K$ premier à p et $a\mathcal{O}_K = \prod_\mathfrak{q} \mathfrak{q}^{v_\mathfrak{q}(a)}$ la décomposition de $a\mathcal{O}_K$ en produit d'idéaux premiers de $\mathcal{O}_K$. On suppose que pour tout idéal premier $\mathfrak{q}$ de $\mathcal{O}_K$ divisant a, E a bonne réduction en $\mathfrak{q}$. Alors, on a :*

$$\prod_{\mathfrak{q} \mid a} \lambda(\sigma_\mathfrak{q})^{12 v_\mathfrak{q}(a)} = \prod_{\mathfrak{p} \mid p} N_\mathfrak{p}(a + \mathfrak{p})^{\alpha_\mathfrak{p}},$$

où $\alpha_\mathfrak{p} \in \{0, 12\}$ est défini à la Proposition 1.3.

1.3.1. *Un lemme de la théorie du corps de classes*

Soient L l'extension de K trivialisant le caractère λ^{12} et μ_p le groupe de racines p-ièmes de l'unité dans $\overline{\mathbf{Q}}$. D'après l'accouplement de Weil, on a $\mu_p \subset K(E[p])$. Donc $L(\mu_p)$ est une sous-extension abélienne de $K(E[p])/K$. On note I_K le groupe des idèles de K et

$$r : I_K \longrightarrow \mathrm{Gal}(L(\mu_p)/K),$$

le morphisme de réciprocité global donné par la théorie du corps de classes. Il est surjectif et son noyau contient les idèles principales.

Soit v une place de K. On note K_v le complété de K en v et on identifie K à un sous-corps de K_v. On désigne par

$$r_v : K_v^* \hookrightarrow I_K \longrightarrow \mathrm{Gal}(L(\mu_p)/K)$$

la composée de l'injection de K_v^* dans I_K par le morphisme de réciprocité global.

Si $\mathfrak{q}$ est un idéal premier de $\mathcal{O}_K$ de bonne réduction ne divisant pas p, on rappelle que l'extension $K(E[p])/K$ est non ramifiée en $\mathfrak{q}$. La restriction à $\mathrm{Gal}(L(\mu_p)/K)$ d'une substitution de Frobenius en $\mathfrak{q}$ du groupe $\mathrm{Gal}(K(E[p])/K)$ (bien définie à conjugaison près) est unique. On la note encore $\sigma_\mathfrak{q}$. De même, on note encore χ_p (resp. λ) la restriction du caractère cyclotomique (resp. d'isogénie) à $\mathrm{Gal}(L(\mu_p)/K)$.

Le lemme suivant regroupe plusieurs résultats classiques de la théorie du corps de classes qui seront utiles à la démonstration de la Proposition 1.4. La démonstration du troisième point est tirée de [13, App. 1, Proposition 1].

Lemme 1.5. *Soit v une place de K.*

(1) *Si v est une place infinie de K, on a $\lambda^{12}(r_v(a)) = 1$.*
(2) *Si $v = \mathfrak{q}$ est une place finie de K ne divisant pas p, on a $r_\mathfrak{q}(\mathcal{U}_\mathfrak{q}) = \{1\}$, où $\mathcal{U}_\mathfrak{q}$ est le groupe des unités de l'anneau d'entiers du corps $K_\mathfrak{q}$. Si de plus, $\mathfrak{q}$ divise a, alors $r_\mathfrak{q}(\pi_\mathfrak{q}) = \sigma_\mathfrak{q}$, où $\pi_\mathfrak{q}$ est une uniformisante de $K_\mathfrak{q}$.*
(3) *Si $v = \mathfrak{p}$ est une place finie de K divisant p, alors $r_\mathfrak{p}(a)$ appartient au sous-groupe d'inertie en $\mathfrak{p}$ de $L(\mu_p)/K$ et on a*

$$\chi_p\left(r_\mathfrak{p}(a)\right) = N_\mathfrak{p}(a + \mathfrak{p})^{-1}.$$

Démonstration. Soit v une place de K. On distingue trois cas.

(1) Supposons que v soit une place infinie de K. Soit L' l'extension de K trivialisant le caractère λ,

$$r' : I_K \longrightarrow \mathrm{Gal}(L'(\mu_p)/K),$$

le morphisme de réciprocité global donné par la théorie du corps de classes et

$$r'_v : K_v^* \hookrightarrow I_K \xrightarrow{r'} \mathrm{Gal}(L'(\mu_p)/K).$$

L'image de l'application r'_v est d'ordre ≤ 2. Par ailleurs, l'image par λ^{12} d'un élément de $\mathrm{Gal}(L'(\mu_p)/K)$ ne dépend que de sa restriction à $\mathrm{Gal}(L(\mu_p)/K)$. D'où:

$$\lambda^{12}(r_v(a)) = \lambda^{12}(r'_v(a)),$$

puis

$$\lambda(r'_v(a))^{12} = \lambda(r'_v(a)^{12}) = 1.$$

D'où le résultat.

(2) Supposons que $v = \mathfrak{q}$ soit une place finie de K ne divisant pas p. Alors, d'après [18], l'image par $r_{\mathfrak{q}}$ de $\mathcal{U}_{\mathfrak{q}}$ est un sous-groupe d'inertie en $\mathfrak{q}$ de l'extension $L(\mu_p)/K$. Or celle-ci est non ramifiée en $\mathfrak{q}$ d'après le critère de Néron–Ogg–Šafarevič. D'où l'égalité

$$r_{\mathfrak{q}}(\mathcal{U}_{\mathfrak{q}}) = \{1\}.$$

Si de plus $\mathfrak{q}$ divise a alors E a bonne réduction en $\mathfrak{q}$ par hypothèse et d'après [18], l'image par $r_{\mathfrak{q}}$ de $\pi_{\mathfrak{q}}$ est la substitution de Frobenius en $\mathfrak{q}$ de l'extension $L(\mu_p)/K$. Autrement dit, $r_{\mathfrak{q}}(\pi_{\mathfrak{q}}) = \sigma_{\mathfrak{q}}$.

(3) Supposons que $v = \mathfrak{p}$ soit une place finie de K divisant p. On note $\overline{\mathbf{Q}_p}$ une clôture algébrique de $\mathbf{Q}_p$. Comme p est non ramifié dans K, on identifie $K_{\mathfrak{p}}$ à l'extension non ramifiée de $\mathbf{Q}_p$ contenue dans $\overline{\mathbf{Q}_p}$ dont le degré sur $\mathbf{Q}_p$ est le degré résiduel de $\mathfrak{p}$ sur p. On note K^{ab} la clôture abélienne de K dans $\overline{\mathbf{Q}}$, $K_{\mathfrak{p}}^{ab}$ la clôture abélienne de $K_{\mathfrak{p}}$ dans $\overline{\mathbf{Q}_p}$,

$$\Theta_{\mathfrak{p}} : K_{\mathfrak{p}}^* \longrightarrow \mathrm{Gal}(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}})$$

le morphisme de réciprocité local en $\mathfrak{p}$ et

$$\mathrm{Res}_{\mathfrak{p}} : \mathrm{Gal}(K_{\mathfrak{p}}^{ab}/K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(L(\mu_p)/K)$$

le morphisme de restriction. D'après la compatibilité entre la théorie du corps de classes locale et globale, on a, pour tout $x \in K_{\mathfrak{p}}^*$,

$$\mathrm{Res}_{\mathfrak{p}}(\Theta_{\mathfrak{p}}(x)) = r_{\mathfrak{p}}(x). \tag{2}$$

Or, d'après le corollaire de [13, App. 1, Proposition 1], on a

$$\Theta_{\mathfrak{p}}(a)(\zeta) = \zeta^{n^{-1}},$$

où ζ est une racine primitive p-ième de l'unité dans $\overline{\mathbf{Q}_p}$ et n est un entier tel que

$$N_{\mathfrak{p}}(a + \mathfrak{p}) \equiv n \pmod{p\mathbf{Z}}.$$

D'où le résultat voulu, d'après l'égalité (2).

Cela termine la démonstration du Lemme 1.5. □

1.3.2. *Démonstration de la Proposition 1.4*

L'entier a est non nul car premier à p. L'image par le morphisme de réciprocité global de l'idèle principale $(a)_v$ est triviale:

$$\prod_v r_v(a) = 1. \tag{3}$$

Si v est une place infinie de K, alors d'après le Lemme 1.5, on a

$$\lambda^{12}(r_v(a)) = 1. \tag{4}$$

Si $v = \mathfrak{q}$ est une place finie de K ne divisant ni p, ni a, alors $a \in \mathcal{U}_{K_{\mathfrak{q}}}$. D'après le Lemme 1.5, on a donc $r_{\mathfrak{q}}(a) = 1$.

Si $v = \mathfrak{q}$ est une place finie de K divisant a. Alors, $a = u \cdot \pi_{\mathfrak{q}}^{v_{\mathfrak{q}}(a)}$, où $\pi_{\mathfrak{q}}$ est une uniformisante de $K_{\mathfrak{q}}$ et $u \in \mathcal{U}_{K_{\mathfrak{q}}}$. D'après le Lemme 1.5, on a donc $r_{\mathfrak{q}}(a) = \sigma_{\mathfrak{q}}^{v_{\mathfrak{q}}(a)}$, puis

$$\lambda^{12}(r_{\mathfrak{q}}(a)) = (\lambda^{12}(\sigma_{\mathfrak{q}}))^{v_{\mathfrak{q}}(a)} = \lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(a)}. \tag{5}$$

Si $v = \mathfrak{p}$ est une place finie de K divisant p, alors d'après le Lemme 1.5, $r_{\mathfrak{p}}(a)$ appartient au sous-groupe d'inertie en $\mathfrak{p}$ de $L(\mu_p)/K$ et on a

$$\chi_p(r_{\mathfrak{p}}(a)) = N_{\mathfrak{p}}(a + \mathfrak{p})^{-1}.$$

Or, d'après la Proposition 1.3, on a

$$\lambda^{12} \mid_{I_{\mathfrak{p}}} = \chi_p^{\alpha_{\mathfrak{p}}} \mid_{I_{\mathfrak{p}}} .$$

On en déduit que l'on a

$$\lambda^{12}(r_{\mathfrak{p}}(a)) = N_{\mathfrak{p}}(a + \mathfrak{p})^{-\alpha_{\mathfrak{p}}}. \tag{6}$$

D'après les égalités (3)–(6) ci-dessus, on a

$$\begin{aligned} 1 &= \prod_v \lambda^{12}(r_v(a)) \\ &= \prod_{\mathfrak{q}|a} \lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(a)} \cdot \prod_{\mathfrak{p}|p} N_{\mathfrak{p}}(a + \mathfrak{p})^{-\alpha_{\mathfrak{p}}}. \end{aligned}$$

Cela démontre la Proposition 1.4.

2. Résultats Principaux

Avant de démontrer les théorèmes principaux 2.4 et 2.8, on commence par définir pour tout anneau intègre A, une loi de monoïde commutatif $*$ sur un sous-ensemble de $A[X]$ et par en étudier les propriétés utiles.

2.1. *Loi de monoïde*

Soit A un anneau intègre de corps des fractions L et $\overline{L}$ une clôture algébrique de L. On note M_A le sous-ensemble de $A[X]$ constitué des polynômes unitaires ne s'annulant pas en 0.

Lemme 2.1. *L'application*

$$\begin{aligned} M_A \times M_A &\longrightarrow A[X] \\ (P, Q) &\longmapsto (P * Q)(X) = \mathrm{Res}_Z(P(Z), Q(X/Z)Z^{\deg Q}) \end{aligned}$$

a une image contenue dans M_A. Elle définit une loi de monoïde commutatif sur M_A d'élément neutre $\Psi_1(X) = X - 1$. De plus, si $P, Q \in M_A$ s'écrivent

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \quad et \quad Q(X) = \prod_{j=1}^{m}(X - \beta_j)$$

dans $\overline{L}[X]$, *on a*

$$(P*Q)(X)=\prod_{\substack{1\leq i\leq n\\ 1\leq j\leq m}}(X-\alpha_i\beta_j).$$

En particulier,

$$(P*Q)(0)=(-1)^{\deg P\cdot\deg Q}P(0)^{\deg Q}Q(0)^{\deg P}.$$

Démonstration. Il s'agit de vérifier que pour tout P, Q et $R\in M_A$, on a

(1) $P*Q\in M_A$;
(2) $P*\Psi_1=\Psi_1*P=P$;
(3) $(P*Q)*R=P*(Q*R)$;
(4) $P*Q=Q*P$.

On suppose que le polynôme Q s'écrit

$$Q(X)=X^m+b_{m-1}X^{m-1}+\cdots+b_1X+b_0,\quad \text{avec } b_0\neq 0.$$

Alors,

$$Q\left(\frac{X}{Z}\right)Z^m=b_0Z^m+b_1XZ^{m-1}+\cdots+b_{m-1}X^{m-1}Z+X^m\in A[X][Z]$$

et $\deg_Z(Q(X/Z)Z^m)=m=\deg Q$ (car $b_0\neq 0$). Par définition du résultant de deux polynômes ([4, A, IV.71, §6, Définition 1]), on a donc $P*Q\in A[X]$. Par ailleurs, sur $\overline{L}$, on a

$$Q\left(\frac{X}{Z}\right)Z^m=Q(0)\prod_{j=1}^{m}\left(Z-\frac{1}{\beta_j}X\right)$$

et d'après [4, A, IV.75, §6, Corollaire 1],

$$(P*Q)(X)=Q(0)^n\prod_{i,j}\left(\alpha_i-\frac{1}{\beta_j}X\right).$$

Or, $Q(0)=\prod_{j=1}^{m}(-\beta_j)$, donc

$$(P*Q)(X)=\prod_{i=1}^{n}\prod_{j=1}^{m}(X-\alpha_i\beta_j).$$

C'est la formule de l'énoncé. On en déduit que l'on a:

– $(P*Q)(0)=(-1)^{\deg P\cdot\deg Q}P(0)^{\deg Q}Q(0)^{\deg P}\neq 0$, donc $P*Q\in M_A$;
– $P*\Psi_1=\Psi_1*P=P$;
– $P*Q=Q*P$;

De plus, les polynômes $(P * Q) * R$ et $P * (Q * R)$ ont les mêmes racines dans $\overline{L}$ comptées avec multiplicités. Comme ils sont unitaires, ils sont égaux. D'où le lemme. □

Lemme 2.2. *Soient $r \geq 1$ et $P \in M_A$. Il existe un unique polynôme $P^{(r)} \in M_A$ tel que*

$$P^{(r)}(X^r) = (P * \Psi_r)(X) \tag{7}$$

où $\Psi_r(X) = X^r - 1$. L'application $P \mapsto P^{(r)}$ est un morphisme de monoïdes pour la loi $*$. De plus, si $P \in M_A$ se factorise sur $\overline{L}$ de la façon suivante

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i), \quad \text{on a } P^{(r)}(X) = \prod_{i=1}^{n}(X - \alpha_i^r). \tag{8}$$

Démonstration. Soit $P \in M_A$. L'unicité d'un polynôme $P^{(r)}$ vérifiant la relation (7) est immédiate. Posons

$$P(X) = \prod_{i=1}^{n}(X - \alpha_i) \quad \text{avec } \alpha_i \in \overline{L}$$

et ζ_r une racine r-ième de l'unité dans $\overline{L}$. D'après le Lemme 2.1, on a

$$(P * \Psi_r)(X) = \prod_{i=1}^{n}\prod_{k=0}^{r-1}(X - \zeta_r^k \alpha_i) = \prod_{i=1}^{n}(X^r - \alpha_i^r).$$

Cela démontre qu'il existe bien un polynôme $P^{(r)}$ de $A[X]$ satisfaisant à l'égalité (7) et qu'il est donné par la formule (8). Par ailleurs, d'après le Lemme 2.1, on a $P^{(r)}(0) = (-1)^{(r+1)\deg P} P(0)^r \neq 0$ et comme $P^{(r)}$ est unitaire, on a $P^{(r)} \in M_A$. On en déduit que l'application $P \mapsto P^{(r)}$ est bien définie.

Vérifions enfin qu'il s'agit bien d'un morphisme de monoïdes. On a $\Psi_1^{(r)} = \Psi_1$. Soient P et Q dans M_A. D'après le Lemme 2.1 et la formule (8), les polynômes $(P * Q)^{(r)}$ et $P^{(r)} * Q^{(r)}$ ont les mêmes racines dans $\overline{L}$ comptées avec multiplicités. Ils sont donc égaux. D'où le Lemme 2.2. □

Lemme 2.3. *Soient A et B deux anneaux intègres et $\varphi : A \to B$ un morphisme d'anneaux. L'ensemble*

$$M_A^{\varphi} = \{P \in M_A \mid \varphi(P(0)) \neq 0\}$$

est stable pour la loi $*$. L'application φ induit un morphisme de monoïdes (encore noté φ)

$$\varphi : M_A^{\varphi} \longrightarrow M_B.$$

Soient $P \in M_A^{\varphi}$ et $r \geq 1$. Alors, $P^{(r)} \in M_A^{\varphi}$ et on a $(\varphi(P))^{(r)} = \varphi(P^{(r)})$.

Démonstration. D'après le Lemme 2.1, si $P, Q \in M_A^\varphi \subset M_A$, on a $P*Q \in M_A$ et

$$(P*Q)(0) = (-1)^{\deg P \cdot \deg Q} P(0)^{\deg Q} Q(0)^{\deg P}.$$

D'où

$$\varphi((P*Q)(0)) = (-1)^{\deg P \cdot \deg Q} \varphi(P(0))^{\deg Q} \varphi(Q(0))^{\deg P} \neq 0$$

car $\varphi(P(0)) \neq 0$, $\varphi(Q(0)) \neq 0$ et B est intègre. Donc M_A^φ est bien un sous-ensemble de M_A stable pour la loi $*$. On a $\varphi(\Psi_1) = \Psi_1$. Le résultant de deux polynômes de $A[X]$ est défini par le déterminant d'une certaine matrice (la matrice de Sylvester) à coefficients dans A ([4, A, IV.72, §6]). Comme φ est un morphisme d'anneaux, on a donc:

$$\varphi(P*Q) = \varphi(P) * \varphi(Q), \quad \text{pour } P,\ Q \in M_A^\varphi.$$

Soient $P \in M_A^\varphi$ et $r \geq 1$. Alors, d'après le Lemme 2.2, on a $P^{(r)} \in M_A$ et

$$\varphi(P^{(r)}(0)) = (-1)^{(r+1)\deg P} \varphi(P(0))^r \neq 0$$

car $\varphi(P(0)) \neq 0$ et B est intègre. D'où $P^{(r)} \in M_A^\varphi$. De plus, d'après la formule (7) et la définition du résultant de deux polynômes ([4, A, IV.72, §6]), on a

$$\varphi(P^{(r)}(X^r)) = \varphi((P*\Psi_r)(X)) = (\varphi(P)*\Psi_r)(X) = \varphi(P)^{(r)}(X^r).$$

D'où l'égalité $(\varphi(P))^{(r)} = \varphi(P^{(r)})$ et le Lemme 2.3.

2.2. *Notations*

Étant donnés $P \in M_A$ et $k \geq 1$, on convient de noter

$$P^{*k} = \underbrace{P * \cdots * P}_{k \text{ fois}} \quad \text{et} \quad P^{*0}(X) = X - 1.$$

On désigne par ailleurs par $\varphi : \mathbf{Z} \to \mathbf{Z}/p\mathbf{Z}$ l'application de réduction modulo p. D'après le Lemme 2.3, elle induit un morphisme de monoïdes

$$\begin{aligned} M_{\mathbf{Z}}^\varphi &\longrightarrow M_{\mathbf{F}_p} \\ P &\longmapsto \overline{P}. \end{aligned}$$

En particulier, $\overline{P*Q} = \overline{P} * \overline{Q}$ pour tout $P, Q \in M_{\mathbf{Z}}^\varphi$.

On fixe désormais un corps de nombres K contenu dans $\overline{\mathbf{Q}}$ et une courbe elliptique E définie sur K. On note d le degré de K sur $\mathbf{Q}$, D_K son discriminant, $\mathcal{O}_K$ son anneau d'entiers, h son nombre de classes et $N_{K/\mathbf{Q}}$ la norme de l'extension $K/\mathbf{Q}$.

2.3. *Premier théorème principal*

2.3.1. *Énoncé*

Soit ℓ un nombre premier tel que E ait bonne réduction en tout idéal premier de $\mathcal{O}_K$ divisant ℓ et

$$\ell\mathcal{O}_K = \prod_{\mathfrak{q}|\ell} \mathfrak{q}^{v_\mathfrak{q}(\ell)}$$

sa décomposition en produit d'idéaux premiers de $\mathcal{O}_K$. Par abus de langage, on dit que E a bonne réduction en ℓ. Dans ce cas, on associe à ℓ le polynôme P_ℓ^* à coefficients entiers

$$P_\ell^* = \mathop{\ast}_{\mathfrak{q}|\ell}(P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(\ell))}) \in \mathbf{Z}[X], \tag{9}$$

où les notations $*$ et $P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(\ell))}$ renvoient à celles définies aux paragraphes précédents. On considère de plus l'entier (essentiel dans la suite):

$$B_\ell = \prod_{k=0}^{[\frac{d}{2}]} P_\ell^*(\ell^{12k})$$

où $[d/2]$ désigne la partie entière de $d/2$. Le premier résultat principal que l'on a vue en direction de la détermination explicite de l'ensemble $\mathrm{Red}(E/K)$ est le suivant:

Théorème 2.4. *Soit p un nombre premier réductible pour (E, K). Alors, on est dans l'une des situations suivantes*:

(1) *p divise $6D_K$;*
(2) *il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p en lequel E a mauvaise réduction additive avec potentiellement bonne réduction supersingulière.*
(3) *pour tout nombre premier ℓ, le nombre premier p divise l'entier B_ℓ (si $d = 1$, on suppose $\ell \neq p$).*

La démonstration de ce résultat fait l'objet des paragraphes 2.3.2 et 2.3.3. Supposons que E soit donnée par une équation de Weierstrass à coefficients dans l'anneau $\mathcal{O}_K$ de discriminant Δ. On déduit du théorème 2.4 le corollaire suivant.

Corollaire 2.5. *Soit p un nombre premier réductible pour (E, K). Alors, on est dans l'une des situations suivantes*:

(1) *p divise $6D_K N_{K/\mathbf{Q}}(\Delta)$;*
(2) *pour tout nombre premier ℓ, le nombre premier p divise l'entier B_ℓ (si $d = 1$, on suppose $\ell \neq p$).*

Pour tout nombre premier ℓ de bonne réduction, les racines complexes de P_ℓ^* sont de module ℓ^{6d} (Lemme 2.6), on a, en particulier, l'implication:

$$d \text{ impair } \Longrightarrow B_\ell \neq 0.$$

On en déduit alors le corollaire sur les extensions de degré impair énoncé dans l'introduction.

2.3.2. *Le polynôme P_ℓ^**

On note g_ℓ le cardinal de l'ensemble des idéaux premiers de $\mathcal{O}_K$ divisant ℓ et on suppose que E a bonne réduction en tout idéal premier $\mathfrak{q}$ de $\mathcal{O}_K$ divisant ℓ. Il

s'agit de montrer que p divise B_ℓ. On commence par étudier les propriétés du polynôme P_ℓ^*.

Lemme 2.6. *Le polynôme P_ℓ^* appartient à $M_{\mathbf{Z}}$ et vérifie*:

$$P_\ell^*(0) = \ell^{12\cdot d\cdot 2^{g_\ell-1}}. \tag{10}$$

Ses racines complexes sont de module ℓ^{6d}. Si de plus $\ell \neq p$, alors $P_\ell^* \in M_{\mathbf{Z}}^{\varphi}$ et on a

$$\overline{P_\ell^*}(\Omega) = 0, \quad \text{où } \Omega = \prod_{\mathfrak{q}\mid\ell} \lambda(\sigma_\mathfrak{q})^{12v_\mathfrak{q}(\ell)} \in \mathbf{F}_p.$$

Démonstration. Pour tout $\mathfrak{q} \mid \ell$, le polynôme $P_\mathfrak{q}$ est unitaire, à coefficients entiers et on a (Proposition 1.1):

$$P_\mathfrak{q}(0) = N(\mathfrak{q}) = \ell^{f_\mathfrak{q}}.$$

En particulier, $P_\mathfrak{q} \in M_{\mathbf{Z}}$. D'après les Lemmes 2.1 et 2.2, le polynôme P_ℓ^* est bien défini (la loi $*$ est associative) et indépendant de l'ordre des idéaux premiers dans la décomposition de ℓ dans K (la loi $*$ est commutative). De plus, P_ℓ^* appartient à $M_{\mathbf{Z}} \subset \mathbf{Z}[X]$.

Soient $P_1, \dots, P_n \in M_{\mathbf{Z}}$ de degrés respectifs $d_1, \dots, d_n$. On montre par récurrence sur n, à partir de la formule pour $n = 2$ du Lemme 2.1 que l'on a

$$(P_1 * \cdots * P_n)(0) = (-1)^{(n+1)d_1\cdots d_n} \prod_{i=1}^{n} P_i(0)^{\prod_{j\neq i} d_j}.$$

De plus, d'après le Lemme 2.2, pour tout $P \in M_{\mathbf{Z}}$ et tout entier $r \geq 1$, on a

$$P^{(r)}(0) = (-1)^{(r+1)\deg P} P(0)^r.$$

Comme pour tout idéal $\mathfrak{q} \mid \ell$, on a $\deg P_\mathfrak{q} = 2$, on en déduit

$$\begin{aligned} P_\ell^*(0) &= \prod_{\mathfrak{q}\mid\ell} P_\mathfrak{q}(0)^{12v_\mathfrak{q}(\ell)\cdot 2^{g_\ell-1}} \\ &= \prod_{\mathfrak{q}\mid\ell} (\ell^{f_\mathfrak{q}})^{12v_\mathfrak{q}(\ell)\cdot 2^{g_\ell-1}} = \ell^{12\cdot 2^{g_\ell-1}\sum_{\mathfrak{q}\mid\ell} f_\mathfrak{q} v_\mathfrak{q}(\ell)}. \end{aligned}$$

D'où la formule car $\sum_{\mathfrak{q}\mid\ell} f_\mathfrak{q} v_\mathfrak{q}(\ell) = d$.

Par ailleurs, d'après la Proposition 1.1, les racines complexes de $P_\mathfrak{q}$ sont de module $N(\mathfrak{q})^{1/2} = \ell^{f_\mathfrak{q}/2}$. Donc, d'après le Lemme 2.2, celles de $P_\mathfrak{q}^{(12v_\mathfrak{q}(\ell))}$ sont de module $\ell^{6f_\mathfrak{q}v_\mathfrak{q}(\ell)}$. D'après le Lemme 2.1, celles de P_ℓ^* sont de module

$$\prod_{\mathfrak{q}\mid\ell} \ell^{6f_\mathfrak{q}v_\mathfrak{q}(\ell)} = \ell^{6\sum_{\mathfrak{q}\mid\ell} f_\mathfrak{q} v_\mathfrak{q}(\ell)} = \ell^{6d}.$$

Supposons à présent $\ell \neq p$. Alors, d'après la formule (10), on a $P_\ell^* \in M_{\mathbf{Z}}^{\varphi}$. D'après la Proposition 1.1, on a

$$\overline{P_\mathfrak{q}}(\lambda(\sigma_\mathfrak{q})) = 0.$$

Donc d'après le Lemme 2.2, on a:

$$\overline{P_{\mathfrak{q}}}^{(12v_{\mathfrak{q}}(\ell))}(\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}) \equiv 0 \pmod{p}. \tag{11}$$

Puis,

$$\begin{aligned}\overline{P_\ell^*}(\Omega) &\equiv \overline{\mathop{\ast}_{\mathfrak{q}|\ell} P_{\mathfrak{q}}^{(12v_{\mathfrak{q}}(\ell))}}\left(\prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}\right)\\ &\equiv \left(\mathop{\ast}_{\mathfrak{q}|\ell}\overline{P_{\mathfrak{q}}}^{(12v_{\mathfrak{q}}(\ell))}\right)\left(\prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)}\right) \quad \text{(Lemme 2.3)}\\ &\equiv 0 \pmod{p} \text{ (d'après le Lemme 2.1 et la relation (11))}.\end{aligned}$$

D'où le Lemme 2.6. □

2.3.3. *Fin de la démonstration du Théorème 2.4*

Supposons $p = \ell$. Alors, pour $d \geq 2$, par définition de B_p, il existe un entier $k > 0$ tel que $P_p^*(p^{12k})$ divise B_p. D'où p divise B_p car d'après le Lemme 2.6:

$$P_p^*(p^{12k}) \equiv P_p^*(0) \equiv 0 \pmod{p}.$$

Supposons $p \neq \ell$. D'après la Proposition 1.4 appliquée à $a = \ell$, on a:

$$\Omega = \prod_{\mathfrak{q}|\ell}\lambda(\sigma_{\mathfrak{q}})^{12v_{\mathfrak{q}}(\ell)} = \prod_{\mathfrak{p}|p} N_{\mathfrak{p}}(\ell+\mathfrak{p})^{\alpha_{\mathfrak{p}}}. \tag{12}$$

Or, par définition on a

$$N_{\mathfrak{p}}(\ell+\mathfrak{p}) \equiv \ell^{1+p+\cdots+p^{f_{\mathfrak{p}}-1}} \equiv \ell^{f_{\mathfrak{p}}} \pmod{p}$$

où $N(\mathfrak{p}) = |\mathcal{O}_K/\mathfrak{p}| = \ell^{f_{\mathfrak{p}}}$. D'où

$$\prod_{\mathfrak{p}|p} N_{\mathfrak{p}}(\ell+\mathfrak{p})^{\alpha_{\mathfrak{p}}} \equiv \ell^{\sum_{\mathfrak{p}|p} f_{\mathfrak{p}}\alpha_{\mathfrak{p}}} \pmod{p}. \tag{13}$$

Or, $\alpha_{\mathfrak{p}} \in \{0, 12\}$ d'après la Proposition 1.3 et on pose

$$k = \sum_{\substack{\mathfrak{p}|p\\ \alpha_{\mathfrak{p}}=12}} f_{\mathfrak{p}} \geq 0$$

de sorte que

$$\sum_{\mathfrak{p}|p} f_{\mathfrak{p}}\alpha_{\mathfrak{p}} = 12k. \tag{14}$$

Comme p est non ramifié dans K, on a

$$d = \sum_{\mathfrak{p}|p} f_{\mathfrak{p}}. \tag{15}$$

Or, d'après la Remarque 1.2 suivant la Proposition 1.3, on peut toujours, si on le souhaite, remplacer la famille $\{\alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$ par la famille $\{12-\alpha_\mathfrak{p}\}_{\mathfrak{p}|p}$, donc on peut supposer que l'on a:

$$\sum_{\mathfrak{p}|p} f_\mathfrak{p}\alpha_\mathfrak{p} \leq \sum_{\mathfrak{p}|p} f_\mathfrak{p}(12-\alpha_\mathfrak{p}).$$

Autrement dit, d'après les égalités (14) et (15)

$$12k \leq 12(d-k)$$

soit encore

$$k \leq \left[\frac{d}{2}\right].$$

D'après les égalités (13) et (14) on a

$$\prod_{\mathfrak{p}|p} N_\mathfrak{p}(\ell+\mathfrak{p})^{\alpha_\mathfrak{p}} \equiv \ell^{12k} \pmod{p}. \tag{16}$$

Par ailleurs, d'après le Lemme 2.6, on a $\overline{P_\ell^*}(\Omega)=0$. Donc, d'après les égalités (12) et (16), il vient $\overline{P_\ell^*}\left(\ell^{12k}\right)=0 \pmod{p}$, c'est-à-dire

$$P_\ell^*(\ell^{12k}) \equiv 0 \pmod{p}.$$

D'où le Théorème 2.4.

2.3.4. *Les polynômes P_ℓ^* dans le cas quadratique*

On suppose que K est un corps quadratique, i.e. $d=2$. Pour un ℓ de bonne réduction, on donne une interprétation géométrique de la condition $B_\ell=0$ ainsi qu'une description explicite des polynômes P_ℓ^*. On rappelle au préalable que l'on a $B_\ell = P_\ell^*(1)\cdot P_\ell^*(\ell^{12})$ avec $P_\ell^*(1)\neq 0$ (Lemme 2.6) et que pour tout entier $n\geq 1$, il existe un unique polynôme T_n appartenant à $\mathbf{Z}[X]$ tel que pour tout nombre réel θ, on ait $T_n(\cos\theta)=\cos(n\theta)$. Le polynôme T_n s'appelle le n-ième polynôme de Tchebychev (de première espèce). On a en particulier,

$$T_{12}(X) = 2048X^{12} - 6144X^{10} + 6912X^8 - 3584X^6 + 840X^4 - 72X^2 + 1$$

et $T_{24}(X) = 2T_{12}(X)^2 - 1$.

Proposition 2.7. *On suppose $K/\mathbf{Q}$ quadratique. Soit ℓ nombre premier de bonne réduction. On est dans l'une des situations suivantes.*

(1) *Soit ℓ est ramifié dans K, $\ell\mathcal{O}_K = \mathfrak{q}^2$ et on a*

$$P_\ell^*(X) = P_\mathfrak{q}^{(24)}(X) = X^2 - 2\ell^{12}T_{24}(t_\mathfrak{q}/2\sqrt{\ell})X + \ell^{24}.$$

En particulier, on a

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_\mathfrak{q}^2(t_\mathfrak{q}^2-\ell)^2(t_\mathfrak{q}^2-4\ell)(t_\mathfrak{q}^2-2\ell)^2(t_\mathfrak{q}^2-3\ell)^2(t_\mathfrak{q}^4-4\ell t_\mathfrak{q}^2+\ell^2)^2.$$

Ainsi $B_\ell = 0$ si et seulement si $t_\mathfrak{q} \equiv 0 \pmod{\ell}$, c'est-à-dire si et seulement si E a bonne réduction supersingulière *en $\mathfrak{q}$.*

(2) *Soit ℓ est inerte dans K, $\ell\mathcal{O}_K = \mathfrak{q}$ et on a*

$$P_\ell^*(X) = P_\mathfrak{q}^{(12)}(X) = X^2 - 2\ell^{12}T_{12}\left(t_\mathfrak{q}/2\ell\right)X + \ell^{24}.$$

En particulier, on a

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_\mathfrak{q}^2(t_\mathfrak{q}^2-\ell^2)^2(t_\mathfrak{q}^2-4\ell^2)(t_\mathfrak{q}^2-3\ell^2)^2.$$

Ainsi $B_\ell = 0$ si et seulement si $t_\mathfrak{q} \equiv 0 \pmod{\ell}$, c'est-à-dire si et seulement si E a bonne réduction supersingulière *en $\mathfrak{q}$.*

(3) *Soit ℓ est décomposé dans K, $\ell\mathcal{O}_K = \mathfrak{q}_1\mathfrak{q}_2$ et on a*

$$\begin{aligned} P_\ell^*(X) = (P_{\mathfrak{q}_1} * P_{\mathfrak{q}_2})^{(12)}(X) &= X^4 - 4\ell^{12}T_{12}(t_{\mathfrak{q}_1}/2\sqrt{\ell})T_{12}(t_{\mathfrak{q}_2}/2\sqrt{\ell})X^3 \\ &- 2\ell^{24}(1 - 2(T_{12}(t_{\mathfrak{q}_1}/2\sqrt{\ell})^2 + T_{12}(t_{\mathfrak{q}_2}/2\sqrt{\ell})^2))X^2 \\ &- 4\ell^{36}T_{12}(t_{\mathfrak{q}_1}/2\sqrt{\ell})T_{12}(t_{\mathfrak{q}_2}/2\sqrt{\ell})X + \ell^{48}. \end{aligned}$$

En particulier, on a

$$\begin{aligned} P_\ell^*(\ell^{12}) = \ell^{36}(t_{\mathfrak{q}_1}^2 - t_{\mathfrak{q}_2}^2)^2((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 3\ell)^2 - t_{\mathfrak{q}_1}^2t_{\mathfrak{q}_2}^2)^2(t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - 4\ell)^2 \\ \times ((t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 - \ell)^2 - 3t_{\mathfrak{q}_1}^2t_{\mathfrak{q}_2}^2)^2. \end{aligned}$$

Ainsi $B_\ell = 0$ si et seulement si l'une des conditions suivantes est satisfaite:

$$t_{\mathfrak{q}_1} = \pm t_{\mathfrak{q}_2}; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 \pm t_{\mathfrak{q}_1}t_{\mathfrak{q}_2} = 3\ell; \quad t_{\mathfrak{q}_1}^2 + t_{\mathfrak{q}_2}^2 = 4\ell.$$

Démonstration. La preuve de cette proposition repose sur la proposition 1.1 ainsi que sur les relations de récurrence entre polynômes de Tchebychev. Elle n'est pas difficile. On ne traite que le cas où ℓ est inerte, les autres étant analogues. Supposons donc ℓ inerte dans K avec $\ell\mathcal{O}_K = \mathfrak{q}$ et posons

$$P_\mathfrak{q}(X) = X^2 - t_\mathfrak{q}X + \ell^2 = (X-\alpha)(X-\beta).$$

D'après la Proposition 1.1, on a $|\alpha| = |\beta| = \ell$. Posons donc $\alpha = \ell e^{i\theta}$ avec $\theta \in \mathbf{R}$. D'après le Lemme 2.1, on a

$$P_\ell^*(X) = (X - \alpha^{12})(X - \beta^{12}).$$

D'où

$$P_\ell^*(X) = X^2 - (\alpha^{12} + \beta^{12})X + \ell^{24} = X^2 - 2\ell^{12}\cos(12\theta)X + \ell^{24}.$$

Or, $\cos(12\theta) = T_{12}(\cos\theta)$ et $2\ell\cos\theta = t_{\mathfrak{q}}$, d'où

$$P_\ell^*(X) = X^2 - 2\ell^{12}T_{12}\left(\frac{t_{\mathfrak{q}}}{2\ell}\right)X + \ell^{24}.$$

On en déduit immédiatement

$$P_\ell^*(\ell^{12}) = 2\ell^{24}\left(1 - T_{12}\left(\frac{t_{\mathfrak{q}}}{2\ell}\right)\right).$$

Or, on a $1 - T_{12} = 8(1-T_3)(1+T_3)T_3^2$. D'où la factorisation

$$P_\ell^*(\ell^{12}) = -\ell^{12}t_{\mathfrak{q}}^2(t_{\mathfrak{q}}^2 - \ell^2)^2(t_{\mathfrak{q}}^2 - 4\ell^2)(t_{\mathfrak{q}}^2 - 3\ell^2)^2$$

car

$$T_3(X) = 4X^3 - 3X; \quad 1 - T_3(X) = -(X-1)(2X+1)^2;$$

et

$$1 + T_3(X) = (X+1)(2X-1)^2.$$

On en déduit que l'on a $P_\ell^*(\ell^{12}) = 0$ si et seulement si $t_{\mathfrak{q}} = 0, \pm\ell$ ou $\pm 2\ell$. Autrement dit, $B_\ell = 0$ si et seulement si $t_{\mathfrak{q}} \equiv 0 \pmod{\ell}$ car $|t_{\mathfrak{q}}| \leq 2\ell$. □

2.4. *Second théorème principal*

Le second théorème principal que l'on a en vue est le suivant:

Théorème 2.8. *Soit p un nombre premier réductible pour (E, K). Alors, on est dans l'une des situations suivantes*:

(1) *p divise $6D_K$;*
(2) *il existe un idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ divisant p en lequel E a mauvaise réduction additive avec potentiellement bonne réduction supersingulière.*
(3) *pour tout idéal premier $\mathfrak{q}$ de bonne réduction, le nombre premier p divise l'entier*

$$R_{\mathfrak{q}} = \prod_{k=0}^{[\frac{d}{2}]} \mathrm{Res}(P_{\mathfrak{q}}^{(12h)}, (\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})^{*k}),$$

où $\mathfrak{q}^h = \gamma_{\mathfrak{q}}\mathcal{O}_K$ et $\mathfrak{m}_{\gamma_{\mathfrak{q}}}$ est le polynôme minimal de $\gamma_{\mathfrak{q}}$ sur $\mathbf{Q}$ (si $d = 1$, on suppose que $\mathfrak{q}$ ne divise pas p).

De plus, si E est sans multiplication complexe sur $\overline{\mathbf{Q}}$, alors $R_{\mathfrak{q}} \neq 0$ pour une infinité d'idéaux premiers $\mathfrak{q}$.

Remarque. La démonstration ci-dessous fera apparaître que lorsque l'on a $R_{\mathfrak{q}} = 0$, alors le corps $L^{\mathfrak{q}}$ engendré par les racines du polynôme $P_{\mathfrak{q}}$ est non ramifié hors de $6\ell D_K$ (où $\mathfrak{q}$ divise ℓ). Dans la pratique, il est donc rare d'avoir $R_{\mathfrak{q}} = 0$. On peut même, dans certains cas, préciser la densité de l'ensemble des idéaux premiers $\mathfrak{q}$

pour lesquels $R_{\mathfrak{q}} \neq 0$. Par exemple, si K est galoisien et ne contient pas de corps quadratique imaginaire, il est de densité 1.

Soit $\mathfrak{q}$ un idéal premier de bonne réduction, $\gamma_{\mathfrak{q}}$ un générateur de $\mathfrak{q}^h$ et $\mathfrak{m}_{\gamma_{\mathfrak{q}}}$ son polynôme minimal sur $\mathbf{Q}$. On commence par un lemme préliminaire.

Lemme 2.9. *Le polynôme* $\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}$ *appartient à* $M_{\mathbf{Z}}$ *et vérifie pour* $\mathfrak{p}$ *divisant* p

$$\overline{(\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})^{*f_{\mathfrak{p}}}}(N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p})^{12}) \equiv 0 \pmod{p}.$$

Démonstration. Le polynôme $\mathfrak{m}_{\gamma_{\mathfrak{q}}}$ est irréductible et unitaire. Il appartient donc à $M_{\mathbf{Z}}$ et il en va de même pour $\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}$ d'après le Lemme 2.2. Par définition, on a

$$N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p}) = (\gamma_{\mathfrak{q}}+\mathfrak{p})\cdot(\gamma_{\mathfrak{q}}^{p}+\mathfrak{p})\cdots(\gamma_{\mathfrak{q}}^{p^{f_{\mathfrak{p}}-1}}+\mathfrak{p}) \in \mathbf{Z}/p\mathbf{Z}$$

et

$$\overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}}(\gamma_{\mathfrak{q}}+\mathfrak{p}) \equiv 0 \pmod{\mathfrak{p}}.$$

Or, le polynôme $\mathfrak{m}_{\gamma_{\mathfrak{q}}}$ est à coefficients dans $\mathbf{Z}$, d'où $\overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(p)}} = \overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}}$. On en déduit donc avec les Lemmes 2.1 et 2.2 que l'on a:

$$\begin{aligned}
\overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}}(\gamma_{\mathfrak{q}}^{12}+\mathfrak{p}) &\equiv 0 \pmod{\mathfrak{p}} \\
\vdots &\quad\vdots \\
\overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}}(\gamma_{\mathfrak{q}}^{12p^{f_{\mathfrak{p}}-1}}+\mathfrak{p}) &\equiv 0 \pmod{\mathfrak{p}}.
\end{aligned}$$

Puis avec le Lemme 2.3, il vient

$$\begin{aligned}
&\overline{(\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})^{*f_{\mathfrak{p}}}}(N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p})^{12}) \\
&\quad\equiv \overline{\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}}^{*f_{\mathfrak{p}}}(\gamma_{\mathfrak{q}}^{12}\cdot\gamma_{\mathfrak{q}}^{12p}\cdots\gamma_{\mathfrak{q}}^{12p^{f_{\mathfrak{p}}-1}}+\mathfrak{p}) \\
&\quad\equiv 0 \pmod{p}
\end{aligned}$$

car $N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p}) \in \mathbf{Z}/p\mathbf{Z}$. D'où le lemme. □

Démontrons à présent le Théorème 2.8. Supposons que $\mathfrak{q}$ divise p. Alors, 0 est une racine commune de $P_{\mathfrak{q}}^{(12h)}$ et $\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)}$ modulo p. Donc p divise l'entier $\mathrm{Res}(P_{\mathfrak{q}}^{(12h)}, \mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})$ et par suite, si $d \geq 2$, p divise $R_{\mathfrak{q}}$.

Supposons que $\mathfrak{q}$ ne divise pas p. Alors, d'après la Proposition 1.4 appliquée à $a = \gamma_{\mathfrak{q}}$, on a

$$\lambda(\sigma_{\mathfrak{q}})^{12h} = \prod_{\mathfrak{p}|p} N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p})^{\alpha_{\mathfrak{p}}} = \prod_{\substack{\mathfrak{p}|p \\ \alpha_{\mathfrak{p}}=12}} N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p})^{12}. \tag{17}$$

Or, d'après le Lemme 2.9, on a

$$\overline{(\mathfrak{m}_{\gamma_{\mathfrak{q}}}^{(12)})^{*f_{\mathfrak{p}}}}(N_{\mathfrak{p}}(\gamma_{\mathfrak{q}}+\mathfrak{p})^{12}) \equiv 0 \pmod{p}.$$

On en déduit donc avec le Lemme 2.1 que l'on a

$$\underset{\substack{\mathfrak{p}|p\\ \alpha_{\mathfrak{p}}=12}}{*} \overline{(\mathfrak{m}_{\gamma_\mathfrak{q}}^{(12)})^{*f_\mathfrak{p}}} \left(\prod_{\substack{\mathfrak{p}|p\\ \alpha_{\mathfrak{p}}=12}} N_\mathfrak{p}(\gamma_\mathfrak{q}+\mathfrak{p})^{12} \right) \equiv 0 \pmod{p},$$

puis avec l'égalité (17) ci-dessus et le Lemme 2.3,

$$\overline{(\mathfrak{m}_{\gamma_\mathfrak{q}}^{(12)})^{*k}}(\lambda(\sigma_\mathfrak{q})^{12h}) \equiv 0 \pmod{p},$$

où l'on a posé

$$k = \sum_{\substack{\mathfrak{p}|p\\ \alpha_{\mathfrak{p}}=12}} f_\mathfrak{p} \geq 0.$$

Comme à la Sec. 2.3.3, on peut supposer $k \leq [d/2]$. Par ailleurs, $\lambda(\sigma_\mathfrak{q})^{12h}$ est une racine de $P_\mathfrak{q}^{(12h)} \pmod{p}$. On en déduit donc que p divise $\mathrm{Res}(P_\mathfrak{q}^{(12h)}, (\mathfrak{m}_{\gamma_\mathfrak{q}}^{(12)})^{*k})$ et par suite, p divise $R_\mathfrak{q}$. Cela démontre la première partie du Théorème 2.8. Il reste à voir que si E est sans multiplication complexe sur $\overline{\mathbf{Q}}$, alors $R_\mathfrak{q} \neq 0$ pour une infinité de $\mathfrak{q}$.

Supposons $R_\mathfrak{q} = 0$. Alors, il existe une racine complexe $\alpha_\mathfrak{q}$ de $P_\mathfrak{q}$ telle que $\alpha_\mathfrak{q}^{12h}$ soit racine de $(\mathfrak{m}_{\gamma_\mathfrak{q}}^{(12)})^{*k}$ pour un certain entier $0 \leq k \leq [d/2]$. C'est impossible pour $k = 0$ car $\alpha_\mathfrak{q}^{12h} \neq 1$. On a donc $k \geq 1$ (et par suite $d \geq 2$) et $\alpha_\mathfrak{q}^{12h}$ s'écrit comme un produit de k conjugués de $\gamma_\mathfrak{q}$ élevés à la puissance 12. Notons $L^\mathfrak{q}$ le corps engendré par $\alpha_\mathfrak{q}$. C'est une extension de degré au plus 2 de $\mathbf{Q}$. On distingue deux cas:

(1) soit $\alpha_\mathfrak{q}^{12h} \notin \mathbf{Q}$ et alors $L^\mathfrak{q} = \mathbf{Q}(\alpha_\mathfrak{q}^{12h})$ est inclus dans K^{gal}, la clôture galoisienne de K dans $\overline{\mathbf{Q}}$; en particulier, $L^\mathfrak{q}$ est non ramifié en dehors des premiers divisant D_K.
(2) Soit $\alpha_\mathfrak{q}^{12h} \in \mathbf{Q}$ et alors

$$\zeta = \frac{\overline{\alpha_\mathfrak{q}}}{\alpha_\mathfrak{q}}$$

est une racine $12h$-ième de l'unité contenue dans $L^\mathfrak{q}$. C'est donc une racine primitive 2-ième, 3-ième, 4-ième ou 6-ième de l'unité et l'on a:

(a) soit $\zeta = 1$, $t_\mathfrak{q}^2 = 4N(\mathfrak{q})$ et $L^\mathfrak{q} = \mathbf{Q}$;
(b) soit $\zeta = -1$, $t_\mathfrak{q} = 0$ et $L^\mathfrak{q} = \mathbf{Q}(\sqrt{-1})$ ou $\mathbf{Q}(\sqrt{-\ell})$ (où ℓ est la caractéristique résiduelle de $\mathfrak{q}$);
(c) soit $\zeta = j$ ou j^2 (avec $j^2 + j + 1 = 0$), $t_\mathfrak{q}^2 = N(\mathfrak{q})$, donc $f_\mathfrak{q}$ est pair et $L^\mathfrak{q} = \mathbf{Q}(\sqrt{-3})$;
(d) soit $\zeta = i$ ou $-i$ (avec $i^2 = -1$), $t_\mathfrak{q}^2 = 2N(\mathfrak{q})$, donc $\ell = 2$ et $f_\mathfrak{q}$ est impair. On en déduit $L^\mathfrak{q} = \mathbf{Q}(\sqrt{-1})$;
(e) soit $\zeta = -j$ ou $-j^2$, $t_\mathfrak{q}^2 = 3N(\mathfrak{q})$, donc $\ell = 3$ et $f_\mathfrak{q}$ est impair. On en déduit et $L^\mathfrak{q} = \mathbf{Q}(\sqrt{-3})$.

On en déduit que dans ce cas la courbe E a réduction supersingulière en $\mathfrak{q}$ et que le corps $L^{\mathfrak{q}}$ est non ramifié en dehors de $\{2, 3, \ell\}$.

Autrement dit, on a montré que si $R_{\mathfrak{q}} = 0$, alors le corps $L^{\mathfrak{q}}$ est non ramifié en dehors des nombres premiers divisant $6\ell D_K$. Or, d'après un résultat de Serre ([20, IV-14(d)]), on sait que si E est sans multiplication complexe sur $\overline{\mathbf{Q}}$, alors pour tout ensemble fini P de nombres premiers, il existe une infinité d'idéaux premiers $\mathfrak{q}$ tels que $L^{\mathfrak{q}}$ soit ramifié en tout nombre premier appartenant à P. Compte-tenu de l'étude précédente, on en déduit qu'il existe une infinité d'idéaux premiers $\mathfrak{q}$ pour lesquels on a $R_{\mathfrak{q}} \neq 0$. Cela achève la démonstration du Théorème 2.8.

3. Bornes Uniformes

Dans ce paragraphe, on s'intéresse à la question suivante.

Question. Soient K un corps de nombres et $\mathcal{E}$ un ensemble infini de courbes elliptiques définies sur K tels que pour toute courbe E de l'ensemble $\mathcal{E}$, $\mathrm{Red}(E/K)$ soit fini. Peut-on trouver une constante uniforme $\alpha(\mathcal{E}, K)$ telle que pour toute courbe elliptique E appartenant à $\mathcal{E}$, la représentation ρ_p soit irréductible dès que $p > \alpha(\mathcal{E}, K)$?

Dans le cas où $\mathcal{E}$ est l'ensemble de toutes les courbes elliptiques sans multiplication complexe définies sur K, cette question est une étape (importante) vers la résolution de la question uniforme de Serre (voir [2] pour plus de détails et de nouvelles avancées). Lorsque $K = \mathbf{Q}$ et $\mathcal{E}$ est l'ensemble de toutes les courbes elliptiques définies sur $\mathbf{Q}$, Mazur a montré ([16]) que tel est le cas avec $\alpha(\mathcal{E}, \mathbf{Q}) = 163$. Dans le cas où $\mathcal{E}$ est l'ensemble des courbes semi-stables, Kraus a obtenu des résultats uniformes et effectifs pour différentes familles corps de nombres, notamment les corps quadratiques et cubiques ([11, 13]).

3.1. *Résultats*

Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ de caractéristique résiduelle ℓ. On a

$$N(\mathfrak{q}) = |\mathcal{O}_K/\mathfrak{q}| = \ell^{f_{\mathfrak{q}}},$$

où $f_{\mathfrak{q}}$ est le degré résiduel de $\mathfrak{q}$. On suppose que E a mauvaise réduction additive en $\mathfrak{q}$ avec potentiellement bonne réduction. Alors, pour tout nombre premier $p \geq 3$ tel que $p \neq \ell$, l'action de $I_{\mathfrak{q}}$, sous-groupe d'inertie en $\mathfrak{q}$, sur $E[p]$ se fait par l'intermédiaire d'un certain quotient fini $\Phi_{\mathfrak{q}}$ de $I_{\mathfrak{q}}$ ([22]):

$$I_{\mathfrak{q}} \longrightarrow \Phi_{\mathfrak{q}} \hookrightarrow \mathrm{Aut}(E[p]).$$

Les deux Propositions 3.1 et 3.3 suivantes sont connues pour $K = \mathbf{Q}$ et ont été utilisées par Serre dans [21, §5] pour traiter des exemples numériques. On les généralise ici aux corps de nombres.

Proposition 3.1. *On suppose que le groupe $\Phi_{\mathfrak{q}}$ n'est pas cyclique. Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 5$.*

Démonstration. Soit $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ tel que le sous-groupe $\Phi_\mathfrak{q}$ ne soit pas cyclique. Compte-tenu de la structure des groupes Φ, l'idéal premier $\mathfrak{q}$ a nécessairement caractéristique résiduelle $\ell = 2$ ou 3 ([21, §5.6(a)]) et $|\Phi_\mathfrak{q}| = 8$ ou 24 (resp. 12) si $\ell = 2$ (resp. $\ell = 3$). L'irréductibilité de ρ_p résulte alors du Lemme 3.2 ci-dessous et du fait que $\Phi_\mathfrak{q}$ se plonge dans $\mathrm{Aut}(E[p])$ (car $\ell \neq p$ et $p \geq 3$, [21, §5.6(a)]). □

Lemme 3.2. *Soit H un sous-groupe non abélien de $\mathrm{Gal}(K(E[p])/K)$. Si p ne divise pas l'ordre de H, alors H ne se plonge pas dans un sous-groupe de Borel de $\mathrm{Aut}(E[p])$.*
[*On rappelle qu'un sous-groupe maximal de $\mathrm{Aut}(E[p])$ stabilisant une droite de $E[p]$ est appelé sous-groupe de Borel.*]

Démonstration. Supposons qu'il existe un morphisme injectif ι de H dans un sous-groupe de Borel B de $\mathrm{Aut}(E[p])$. Dans une base convenable de $E[p]$ sur $\mathbf{F}_p$, B est représentable matriciellement par le Borel standard

$$\begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

Il contient alors le sous-groupe S d'ordre p engendré par l'élément

$$u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

C'est un sous-groupe distingué de B. Comme l'ordre de H est premier à p, le morphisme composé

$$H \overset{\iota}{\hookrightarrow} B \to B/S$$

est injectif. Par ailleurs, B/S est abélien. D'où une contradiction car H est supposé non abélien. D'où le Lemme 3.2. □

Proposition 3.3. *On suppose que pour tout entier $n \geq 0$, l'ordre du groupe $\Phi_\mathfrak{q}$ ne divise pas $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$. Alors, la représentation ρ_p est irréductible pour tout nombre premier $p \geq 3$ tel que $p \neq \ell$.*

Démonstration. Soient $p \geq 3$ un nombre premier réductible et $\mathfrak{q}$ un idéal premier de $\mathcal{O}_K$ de caractéristique résiduelle $\ell \neq p$ en lequel E a mauvaise réduction additive avec potentiellement bonne réduction. On souhaite montrer qu'il existe un entier $n \geq 0$ tel que l'ordre du groupe $\Phi_\mathfrak{q}$ divise $N(\mathfrak{q})^n(N(\mathfrak{q})-1)$.

Vu la théorie du corps de classes, le caractère λ s'interprète comme un homomorphisme

$$\lambda : \mathrm{Gal}(K^\mathfrak{m}/K) \longrightarrow \mathbf{F}_p^*,$$

où $\mathfrak{m}$ est le conducteur de λ et $K^{\mathfrak{m}}$ le corps de classes de rayon $\mathfrak{m}$. Alors, le caractère λ est ramifié en $\mathfrak{q}$ (cf. [21, §§ 1.12 et 5.6]) et on a une factorisation du type

$$\mathfrak{m} = \mathfrak{m}' \cdot \mathfrak{q}^{n+1}, \quad \text{où } n \geq 0 \quad \text{et } (\mathfrak{m}', \mathfrak{q}) = 1.$$

L'ordre du groupe $\Phi_{\mathfrak{q}}$ divise l'indice de ramification en $\mathfrak{q}$ de l'extension $K^{\mathfrak{m}}/K$. Or l'extension intermédiaire $K^{\mathfrak{m}'}/K$ est non ramifiée en $\mathfrak{q}$. Donc l'ordre de $\Phi_{\mathfrak{q}}$ divise le cardinal du groupe $\mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathfrak{m}'})$. Notons $h_{\mathfrak{m}}$ (resp. $h_{\mathfrak{m}'}$) le cardinal du groupe $\mathrm{Gal}(K^{\mathfrak{m}}/K)$ (resp. $\mathrm{Gal}(K^{\mathfrak{m}'}/K)$). Alors, d'après [7, Corollaire 3.2.4], on a

$$|\mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathfrak{m}'})| = \frac{h_{\mathfrak{m}}}{h_{\mathfrak{m}'}} = \frac{(\mathcal{U} : \mathcal{U}_{\mathfrak{m}',1})}{(\mathcal{U} : \mathcal{U}_{\mathfrak{m},1})} N(\mathfrak{q})^n (N(\mathfrak{q}) - 1),$$

où $\mathcal{U}_{\mathfrak{m},1}$ (resp. $\mathcal{U}_{\mathfrak{m}',1}$) désigne le sous-groupe du groupe des unités $\mathcal{U}$ de $\mathcal{O}_K$ qui sont congrues à 1 modulo $\mathfrak{m}$ (resp. $\mathfrak{m}'$) au sens de [7, Definition 3.2.2]. Or, comme $\mathfrak{m}'$ divise $\mathfrak{m}$, l'indice de $\mathcal{U}_{\mathfrak{m}',1}$ dans $\mathcal{U}$ divise celui de $\mathcal{U}_{\mathfrak{m},1}$. Donc, l'ordre de $\mathrm{Gal}(K^{\mathfrak{m}}/K^{\mathfrak{m}'})$ divise $N(\mathfrak{q})^n(N(\mathfrak{q}) - 1)$ et il en va de même en particulier pour l'ordre de $\Phi_{\mathfrak{q}}$. D'où la Proposition 3.3. □

Remarque. Lorsque $\ell \geq 5$, on peut remplacer dans l'énoncé, l'hypothèse par: l'ordre du groupe $\Phi_{\mathfrak{q}}$ ne divise pas $N(\mathfrak{q}) - 1$. En effet, on a $|\Phi_{\mathfrak{q}}| = 2$, 3, 4 ou 6 ([21, p. 312]). Or $N(\mathfrak{q})$ est premier à 12, donc $|\Phi_{\mathfrak{q}}|$ divise $N(\mathfrak{q})^n(N(\mathfrak{q}) - 1)$ pour un certain entier n si et seulement si $|\Phi_{\mathfrak{q}}|$ divise $N(\mathfrak{q}) - 1$.

Comme corollaires des propositions ci-dessus, on obtient les résultats suivants dans le cas où $\mathfrak{q}$ divise 2 ou 3.

Corollaire 3.4. *On suppose que* $\mathfrak{q}$ *divise* 2 *et que l'une des conditions suivantes est satisfaite*:

(1) *le groupe* $\Phi_{\mathfrak{q}}$ *est d'ordre* 8 *ou* 24;
(2) *le groupe* $\Phi_{\mathfrak{q}}$ *est d'ordre* 3 *ou* 6 *et le degré résiduel* $f_{\mathfrak{q}}$ *est impair.*

Alors, la représentation ρ_p *est irréductible pour tout nombre premier* $p \geq 5$.

Démonstration. Supposons que $\mathfrak{q}$ divise 2. Lorsque $|\Phi_{\mathfrak{q}}| = 8$ ou 24, le groupe $\Phi_{\mathfrak{q}}$ n'est pas abélien ([21, 5.6(a)]) et la conclusion résulte de la Proposition 3.1. Pour $|\Phi_{\mathfrak{q}}| = 3$ ou 6, supposons la représentation ρ_p réductible. Alors, d'après la Proposition 3.3, l'ordre de $\Phi_{\mathfrak{q}}$ divise $2^{f_{\mathfrak{q}}}(2^{f_{\mathfrak{q}}} - 1)$. Or, $2^{f_{\mathfrak{q}}} - 1 \equiv 1 \pmod 3$ car $f_{\mathfrak{q}}$ est impair. D'où une contradiction et le Corollaire 3.4. □

Lorsque $\mathfrak{q}$ divise 2, l'étude faite dans [1] permet parfois de calculer l'ordre du groupe $\Phi_{\mathfrak{q}}$ directement à partir de la valuation de l'invariant modulaire de E ([1, Théorème 1]). Si K est une extension quadratique de $\mathbf{Q}$ (ou plus généralement si le degré sur $\mathbf{Q}_2$ du complété de K en $\mathfrak{q}$ est ≤ 2), le théorème [1, Théorème 2] et [5] fournissent en toute généralité l'ordre du groupe $\Phi_{\mathfrak{q}}$ en fonction des coefficients d'une équation de Weierstrass de E.

Remarque. La condition de parité dans le corollaire précédent est nécessaire. En effet, soient K l'extension de $\mathbf{Q}$ engendrée par une racine du polynôme

$$(X^2+5X+1)^3(X^2+13X+49)-j_E\cdot X,$$

où $j_E = 2^4\cdot 13^3/3^2$ est l'invariant modulaire de la courbe elliptique E définie sur K par l'équation

$$y^2 = x^3 - x^2 - 4x + 4.$$

Alors, le degré résiduel de K en l'unique idéal $\mathfrak{p}_2$ de $\mathcal{O}_K$ divisant 2, est $f_{\mathfrak{p}_2} = 2$ et la courbe E a un groupe Φ d'ordre 6 en $\mathfrak{p}_2$. Pour autant la représentation $\rho_7 : \mathrm{G}_K \longrightarrow \mathrm{GL}_2(\mathbf{F}_7)$ est *réductible* car K correspond au sous-corps de $\overline{\mathbf{Q}}$ laissé fixe par le stablilisateur dans $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ d'un sous-groupe d'ordre 7 de $E(\overline{\mathbf{Q}})$ ([14, p. 273]).

Lorsque $\mathfrak{q}$ divise 3, on a le corollaire suivant.

Corollaire 3.5. *On suppose que* $\mathfrak{q}$ *divise* 3 *et que l'une des conditions suivantes est satisfaite*:

(1) *le groupe* $\Phi_\mathfrak{q}$ *est d'ordre* 12;
(2) *le groupe* $\Phi_\mathfrak{q}$ *est d'ordre* 4 *et le degré résiduel* $f_\mathfrak{q}$ *est impair.*

Alors, la représentation ρ_p *est irréductible pour tout nombre premier* $p \geq 5$.

Démonstration. Supposons que $\mathfrak{q}$ divise 3. Lorsque $|\Phi_\mathfrak{q}| = 12$, le groupe $\Phi_\mathfrak{q}$ n'est pas abélien ([21, 5.6(a)]) et la conclusion résulte comme ci-dessus de la Proposition 3.1. Pour $|\Phi_\mathfrak{q}| = 4$, supposons la représentation ρ_p réductible. Alors, d'après la Proposition 3.3, l'ordre de $\Phi_\mathfrak{q}$ divise $3^{f_\mathfrak{q}}(3^{f_\mathfrak{q}}-1)$. Or, $3^{f_\mathfrak{q}} - 1 \equiv 2 \pmod 4$ car $f_\mathfrak{q}$ est impair, d'où une contradiction et le Corollaire 3.5. □

3.2. *Exemples numériques*

Dans ce §, on illustre sur deux exemples les résultats uniformes ci-dessus. On adopte les notations standard de Tate ([25]). Pour chaque idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$, on note $v_\mathfrak{p}$ la valuation en $\mathfrak{p}$ de K normalisée par $v_\mathfrak{p}(K^*) = \mathbf{Z}$.

Exemple 3.6. On suppose $K = \mathbf{Q}(\sqrt{5})$. On considère la courbe E d'équation

$$y^2 = x^3 + 2x^2 + \omega x \quad \text{où} \quad \omega = \frac{1+\sqrt{5}}{2}.$$

Alors, $\mathrm{Red}(E/K) = \{2\}$.

Démonstration. On a

$$\begin{cases} c_4 = 2^4(4-3\omega) \\ c_6 = 2^6(-8+9\omega) \\ \Delta = -2^6\omega. \end{cases}$$

Or, ω est une unité de $\mathcal{O}_K$. En particulier, la courbe E a bonne réduction en dehors de (l'idéal premier) $2\mathcal{O}_K$. On a:

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 6, 6).$$

Donc E a mauvaise réduction additive en 2. On note Φ_2 son défaut de semi-stabilité en 2. On a $v_2(j_E) = 6$ et $3v_2(c_4) = 2v_2(c_6)$. L'extension $K/\mathbf{Q}$ étant non ramifié en 2, on a d'après [5], $|\Phi_2| = 4$ ou 8. Or, avec les notations de l'article la condition (C2) n'est pas satisfaite. On en déduit que l'on a $|\Phi_2| = 8$. Et, d'après le Corollaire 3.4, ρ_p est irréductible pour tout nombre premier $p \geq 5$. La courbe E a bonne réduction en l'idéal premier $7\mathcal{O}_K$ et on a $t_7 = -12$. D'où

$$P_7(X) = X^2 - t_7X + 49 \equiv X^2 + 1 \pmod 3.$$

Donc ρ_3 est également irréductible. La représentation ρ_2, en revanche, est réductible car $(0, 0)$ est un point d'ordre 2.

Exemple 3.7. On suppose $K = \mathbf{Q}(\sqrt{13})$. On considère la courbe E d'équation

$$y^2 = x^3 - (313 + 240\omega)x - 17 \quad \text{où} \quad \omega = \frac{1 + \sqrt{13}}{2}.$$

Alors, l'ensemble $\mathrm{Red}(E/K)$ est vide.

Démonstration. On a

$$\begin{cases} c_4 = 2^4 \cdot 3(11 + 8\omega)^2 \\ c_6 = 2^5 \cdot 3^3 \cdot 17 \\ \Delta = 2^4 \cdot 5(11 + 8\omega)^2(213629 + 167568\omega). \end{cases}$$

De plus, $N_{K/\mathbf{Q}}(213629 + 167568\omega) = -1153 \cdot 2430503$ et ni 1153, ni 2430503 ne divisent c_4. Donc la courbe E a mauvaise réduction multiplicative en un idéal premier au-dessus de 1153 et un idéal premier au-dessus de 2430503. Le nombre premier 2 est inerte dans K et

$$(v_2(c_4), v_2(c_6), v_2(\Delta)) = (4, 5, 4).$$

Donc $v_2(j_E) = 8$ et d'après [5], on a $|\Phi_2| = 3$, 6 ou 24. Comme par ailleurs,

$$j'_E = \frac{j_E}{2^8} \equiv -1 \pmod 4,$$

la condition (C3) de l'article est satisfaite avec $\gamma = 1$ et $|\Phi_2| = 3$ ou 6 (en fait $|\Phi_2| = 6$). Puisque $f_2 = 2$ est pair, le cor. 3.4 ne s'applique pas. Cependant, en l'idéal premier $\mathfrak{q}_{17} = (15 + 4\sqrt{13})\mathcal{O}_K$, on a

$$(v_{\mathfrak{q}_{17}}(c_4), v_{\mathfrak{q}_{17}}(c_6), v_{\mathfrak{q}_{17}}(\Delta)) = (2, 1, 2).$$

Donc E a mauvaise réduction additive en $\mathfrak{q}_{17}$ avec potentiellement bonne réduction. Son défaut de semi-stabilité $\Phi_{\mathfrak{q}_{17}}$ est d'ordre 6 ([21, p. 312]). Or, 6 ne divise pas $N(\mathfrak{q}_{17}) - 1 = 16$. Donc, d'après la Proposition 3.3, la représentation ρ_p est

irréductible pour tout nombre premier $p \geq 3$ et $p \neq 17$. Si $\mathfrak{q}_3$ désigne un idéal divisant 3, alors E a bonne réduction en $\mathfrak{q}_3$ et on a $t_{\mathfrak{q}_3} = -3$. Donc le polynôme $P_{\mathfrak{q}_3}(X) = X^2 + 3X + 3$ est irréductible modulo 2 et 17. On en déduit le résultat.

□

4. Algorithme et Exemples Numériques

L'objet de cette section est de discuter l'algorithme de calcul de l'ensemble $\mathrm{Red}(E/K)$ fourni par les résultats du §2 et de l'illustrer sur quelques exemples numériques concrets.

4.1. *L'algorithme*

4.1.1. *Description*

Données: un couple (E, K) constitué:
– d'un corps de nombres K;
– d'une courbe elliptique E sans multiplication complexe sous forme d'une équation de Weierstrass à coefficients dans $\mathcal{O}_K$.

Résultat: l'ensemble $\mathrm{Red}(E/K)$.

À l'aide de ces données, le résultat s'obtient en suivant les étapes ci-dessous.

(1) On calcule l'ensemble S_1 des diviseurs premiers de $6D_K N_{K/\mathbf{Q}}(\Delta)$.
(2) Soit ℓ_0 le plus petit nombre premier n'appartenant pas à S_1. La courbe E a bonne réduction en ℓ_0. On calcule B_{ℓ_0}. Si $B_{\ell_0} \neq 0$, on passe à l'étape 3. Sinon on réitère le procédé avec le plus petit nombre premier ℓ_1 n'appartenant pas à S_1 et $> \ell_0$. Si $B_{\ell_1} \neq 0$, on passe à l'étape 3, etc. Si après plusieurs itérations le procédé n'a toujours pas convergé vers un premier ℓ tel que $B_\ell \neq 0$, on passe à l'étape 3′.
(3) On dispose à présent d'un entier B_ℓ non nul. Pour plus d'efficacité, on peut réitérer l'étape 2 afin d'en obtenir plusieurs. On désigne alors par S_2 l'ensemble des facteurs premiers du Plus Grand Diviseur Commun (pgcd) à ces entiers et on pose $S = S_1 \cup S_2$.
(3′) Comme E est sans multiplication complexe, il existe, d'après le théorème 2.8, un idéal premier $\mathfrak{q}$ de bonne réduction (et même une infinité) tel que $R_\mathfrak{q} \neq 0$. Pour plus d'efficacité, on peut réitérer ce calcul afin d'obtenir plusieurs entiers $R_\mathfrak{q}$ non nuls. On désigne alors par S_2 l'ensemble des facteurs premiers du pgcd à ces entiers et on pose $S = S_1 \cup S_2$.
(4) L'ensemble S contient $\mathrm{Red}(E/K)$ d'après les Théorèmes 2.4 et 2.8, mais vraisemblablement aussi d'autres nombres premiers «parasites». On peut en éliminer certains en calculant les polynômes $P_\mathfrak{q}$ pour quelques idéaux premiers $\mathfrak{q}$ de bonne réduction (ou en reprenant ceux utilisés à l'étape 2): si $P_\mathfrak{q}$ est irréductible modulo p (avec $\mathfrak{q}$ ne divisant pas p), alors p n'appartient pas

à $\mathrm{Red}(E/K)$. Le sous-ensemble S' de S constitué des nombres premiers restants est alors généralement très restreint.

(5) On détermine enfin le sous-ensemble $\mathrm{Red}(E/K)$ de S'.

4.1.2. *Discussion sur l'efficacité et le coût de l'algorithme*

L'algorithme présenté ci-dessus est composé de cinq étapes dont la deuxième est la plus cruciale. L'étape 1 est peu coûteuse en termes de calculs de même que l'étape 4 qui est essentiellement optionnelle et ne sert qu'à alléger la dernière.

L'étape 2 requiert le calcul du polynôme P_ℓ^* pour quelques valeurs de ℓ. Elle nécessite donc de connaître la réduction de E en quelques places finies de K. Cependant, ces calculs (résultants, coefficients de Fourier de la fonction L de E) sont bien implémentés dans `magma` ([3], commande `LGetCoefficients`) ou `sage` ([24]), par exemple, et sont très rapides. En particulier, on n'a besoin d'aucun renseignement profond sur le corps K.

Le choix d'effectuer l'étape 3 ou 3′ dépend du succès de l'étape 2. L'étape 3 n'apporte aucun coût supplémentaire. En revanche, l'étape 3′ peut s'avérer plus lourde puisque le calcul de $R_{\mathfrak{q}}$ nécessite celui de plusieurs résultants, mais surtout de h, d'un générateur de $\mathfrak{q}^h$ et de son polynôme minimal. Cependant, il convient de relativiser la possible «défaillance» de l'étape 2. Dans la pratique, il est très rare d'avoir un couple (E, K) qui échappe au critère du Théorème 2.4. D'une part, une telle courbe E est nécessairement définie sur un corps K de degré pair en raison du Corollaire 0.2. D'autre part, bien qu'il en existe sur des corps biquadratiques (cf. Exemple 4.4), il semble extrêmement peu probable, par exemple, d'en trouver une définie sur un corps quadratique: une telle courbe aurait réduction supersingulière en *tous* les idéaux premiers de degré 2 (cf. Proposition 2.7). Enfin, les seuls exemples trouvés sont tous des cas particuliers de $\mathbf{Q}$-courbes.

L'étape 5, enfin, peut être traitée, lorsque $p = 2, 3, 5, 7$ ou 13, à l'aide de la commande `E.isogenies_prime_degree()` de `sage`. Lorsque $p = 11$ ou $p > 13$, on peut utiliser les tables de polynômes modulaires pour factoriser $F_p(j_E, X)$. Elles sont, par exemple, implémentées dans `magma` (commande `ClassicalModularPolynomial()`) pour $p \leq 59$.

4.2. *Exemples*

Dans ce paragraphe, on détermine les ensembles $\mathrm{Red}(E/K)$ de quelques courbes elliptiques en suivant l'algorithme présenté ci-dessus. On reprend les notations de la Sec. 3.2. Aucun des résultats uniformes de la Sec. 3 ne s'applique aux exemples ci-dessous. Pour les calculs des coefficients de la fonction L de E, on a utilisé `magma`.

Exemple 4.1. On suppose $K = \mathbf{Q}(\sqrt{-1})$. On considère la courbe E d'équation

$$y^2 = x^3 + 2(3 + 2\sqrt{-1})x + 2(3 + 2\sqrt{-1}). \tag{18}$$

Alors, l'ensemble $\mathrm{Red}(E/K)$ est vide.

Démonstration. On a $N_{K/\mathbf{Q}}(\Delta) = 2^{12} \cdot 3^2 \cdot 2857$. Soit p un nombre premier réductible n'appartenant pas à l'ensemble $\{2, 3, 2857\}$. On a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|5} = \{-2, 1\} \quad \text{et} \quad t_7 = 6,$$

puis, d'après le Théorème 2.4 appliqué à $\ell = 5$ et $\ell = 7$, p divise chacun des entiers B_5 et B_7. Or

$$B_5 = 2^{28} \cdot 3^{16} \cdot 5^{39} \cdot 11^2 \cdot 17 \cdot 61 \cdot 73 \cdot 277 \cdot 397 \cdot 557 \cdot 653 \cdot 757 \cdot 23833$$

et

$$B_7 = 2^{14} \cdot 3^8 \cdot 5^2 \cdot 7^{13} \cdot 11 \cdot 13^5 \cdot 37^2 \cdot 2089 \cdot 2689 \cdot 3889,$$

d'où p divise $\operatorname{pgcd}(B_5, B_7) = 2^{14} \cdot 3^8 \cdot 5^2 \cdot 11$. Il ne reste donc plus qu'à traiter les cas $p = 2$, 3, 5, 11 et 2857. Or, E a bonne réduction en l'idéal premier $3\mathcal{O}_K$ et on a

$$P_3(X) = X^2 + 3X + 9.$$

Donc P_3 est irréductible modulo 2, 5 et 11. Et, si $\mathfrak{q}_5$ est un idéal premier au-dessus de 5, on a $t_{\mathfrak{q}_5} = -2$ ou 1, et

$$P_{\mathfrak{q}_5}(X) \equiv X^2 + 2X + 2 \pmod 3.$$

Donc $P_{\mathfrak{q}_5}$ est irréductible modulo 3. Enfin $P_7(X) = X^2 - 6X + 49$ est irréductible modulo 2857. On en déduit le résultat annoncé. □

Exemple 4.2. On suppose $K = \mathbf{Q}(\sqrt{2})$ et on pose

$$\begin{cases} A = -3^3 \cdot 5 \cdot 17^3(428525 + 303032\sqrt{2}) \\ B = 2 \cdot 3^3 \cdot 5 \cdot 17^3(62176502533 + 43965551956\sqrt{2}). \end{cases}$$

On considère la courbe E d'équation

$$y^2 = x^3 + Ax + B.$$

Alors, $\operatorname{Red}(E/K) = \{13\}$.

Démonstration. On vérifie que pour le modèle choisi, on a

$$N_{K/\mathbf{Q}}(\Delta) = -2^{25} \cdot 3^{18} \cdot 5^4 \cdot 7^2 \cdot 17^{15} \cdot 23^6 \cdot 79^6.$$

En particulier, la courbe E a bonne réduction en les idéaux premiers divisant 11, 13, 19, 29 et 41 et on a

$$t_{11} = 4; \quad t_{13} = -14 \quad t_{19} = 26; \quad t_{29} = 1 \quad \text{et} \quad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|41} = \{-3, 2\}.$$

Soit p un nombre premier réductible n'appartenant pas à l'ensemble

$$\{2, 3, 5, 7, 17, 23, 79\}.$$

Alors, d'après le Théorème 2.4 appliqué à $\ell = 11$ et $\ell = 13$, p divise

$$\operatorname{pgcd}(B_{11}, B_{13}) = 2^{12} \cdot 3^8 \cdot 5^2 \cdot 7^4 \cdot 13^2.$$

Autrement dit, il ne reste plus qu'à traiter les cas où $p = 2, 3, 5, 7, 13, 17, 23$ et 79. Or le polynôme P_{11} est irréductible modulo 5, 23 et 79. De même, P_{13} est irréductible modulo 7, P_{19} modulo 17 et P_{29} modulo 2. Si $\mathfrak{q}_{41}$ désigne l'idéal premier de $\mathcal{O}_K$ au-dessus de 41 tel que $t_{\mathfrak{q}_{41}} = 2$, alors $P_{\mathfrak{q}_{41}}$ est irréductible modulo 3. On en déduit que $2, 3, 5, 7, 17, 23$ et 79 ne sont pas réductibles. En revanche 13 est un nombre premier réductible comme on le vérifie à l'aide de la commande `E.isogenies_prime_degree(13)` de `sage`. □

Exemple 4.3. On considère $K = \mathbf{Q}(\cos(\frac{2\pi}{9}))$ le corps cubique cyclique de conducteur 9 et la courbe E d'équation

$$y^2 = x^3 + 2(1+\alpha)^2 x + 24\alpha(2+\alpha),$$

où $\alpha = 2\cos\left(\frac{2\pi}{9}\right)$ est racine du polynôme $X^3 - 3X + 1$. Alors, l'ensemble $\mathrm{Red}(E/K)$ est vide.

Démonstration. On a $D_K = 3^4$ et

$$N_{K/\mathbf{Q}}(\Delta) = -2^{27} \cdot 3^6 \cdot 5^3 \cdot 11^3.$$

Par ailleurs, les nombres premiers 17, 19, 37 et 53 sont (totalement) décomposés dans K et l'on a

$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|17} = \{-3, -3, 3\}; \quad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|19} = \{-5, -5, 5\};$$
$$\{t_{\mathfrak{q}}\}_{\mathfrak{q}|37} = \{-7, -7, 7\}; \quad \{t_{\mathfrak{q}}\}_{\mathfrak{q}|53} = \{-3, 3, 3\}.$$

Soit p un nombre premier réductible n'appartenant pas à l'ensemble $\{2, 3, 5, 11\}$. D'après le Théorème 2.4, appliqué à $\ell = 17$, 19 et 37, p divise

$$\mathrm{pgcd}(B_{17}, B_{19}, B_{37}) = 2^{72} \cdot 3^{42} \cdot 5^{24}.$$

Il ne reste donc plus qu'à traiter les cas où $p = 2, 3$, 5 et 11. Or, si $\mathfrak{q}_{53}$ désigne un idéal premier de $\mathcal{O}_K$ au-dessus de 53, le polynôme $P_{\mathfrak{q}_{53}}$ est irréductible modulo 2, 5 et 11. Par ailleurs, l'idéal $7\mathcal{O}_K$ est premier et $t_7 = -36$, donc le polynôme

$$P_7(X) = X^2 + 36X + 7^3$$

est irréductible modulo 3. On en déduit le résultat annoncé. □

Exemple 4.4. On considère $K = \mathbf{Q}(\sqrt{-3}, \sqrt{-7})$ et E la courbe d'équation

$$y^2 = x^3 + a_4 x + a_6$$

où

$$\begin{cases} a_4 = \dfrac{81}{4} \cdot (69 + 43\sqrt{-3} + 29\sqrt{-7} + 17\sqrt{21}); \\ a_6 = 162 \cdot (207 - 84\sqrt{-3} - 54\sqrt{-7} + 46\sqrt{21}). \end{cases}$$

Alors, $\mathrm{Red}(E/K) = \{2, 3, 5\}$.

Démonstration. La courbe E figure déjà dans [10, Exemple 13] et [9]. Elle a la propriété particulière d'être une $\mathbf{Q}$-courbe, c'est-à-dire, d'être isogène à ses conjuguées galoisiennes. En outre, elle est de conducteur $2\mathcal{O}_K$ et sans multiplication complexe (son invariant modulaire n'est pas entier). En les idéaux au-dessus de 2, elle a mauvaise réduction multiplicative. En particulier, aucun des résultats uniformes de la Sec. 3 ne s'applique. Montrons à présent que le critère du Théorème 2.4 est lui aussi insuffisant pour traiter cette courbe. On doit montrer que pour tout nombre premier $\ell \geq 3$, l'entier B_ℓ est nul, autrement dit, que ℓ^{24} est racine de P_ℓ^* (Lemme 2.6). D'après les propriétés de E rappelées ci-dessus, on a $P_{\mathfrak{q}} = P_{\mathfrak{q}'}$ pour tout couple $(\mathfrak{q}, \mathfrak{q}')$ d'idéaux premiers divisant ℓ. Or $D_K = 3^2 \cdot 7^2$, donc si $\ell \neq 3, 7$, $\ell\mathcal{O}_K$ se décompose en un produit de 2 ou 4 idéaux premiers. On a alors respectivement

$$P_\ell^* = (P_{\mathfrak{q}}^{(12)})^{*2} \quad \text{et} \quad P_\ell^* = (P_{\mathfrak{q}}^{(12)})^{*4}.$$

Or, dans le premier cas, les racines complexes α et β de $P_{\mathfrak{q}}$ satisfont $\alpha\beta = \ell^2$ et dans le second, $\alpha\beta = \ell$. On en déduit le résultat voulu dans ce cas. Par ailleurs, on vérifie que l'on a $P_3^*(X) = (X - 3^{24})^2$ et

$$P_7^*(X) = (X - 7^{24})^2 \cdot (X^2 - 2 \cdot 97 \cdot 193 \cdot 1249 \cdot 5569 \cdot 24097 \cdot 59233X + 7^{48}),$$

d'où la nullité de B_ℓ pour tout ℓ de bonne réduction. Pour cette courbe, on a donc recours au critère du Théorème 2.8. Le nombre de classes h de K est 1. On considère l'idéal premier $\mathfrak{q}_5$ au-dessus de 5 engendré par une racine $\gamma_{\mathfrak{q}_5}$ du polynôme $\mathfrak{m}_{\gamma_{\mathfrak{q}_5}}(X) = X^4 + 17X^2 + 25$. On a alors,

$$P_{\mathfrak{q}_5}(X) = X^2 + 4X + 25 \quad \text{d'où} \quad P_{\mathfrak{q}_5}^{(12)}(X) = X^2 - 2 \cdot 47 \cdot 1163039X + 5^{24}$$

et

$$\mathfrak{m}_{\gamma_{\mathfrak{q}_5}}^{(12)}(X) = (X^2 - 2 \cdot 73 \cdot 19441X + 5^{12})^2$$

puis,

$$\left(\mathfrak{m}_{\gamma_{\mathfrak{q}_5}}^{(12)}\right)^{*2}(X) = \left(X - 5^{12}\right)^8 \cdot \left(X^2 - 2 \cdot 79 \cdot 127 \cdot 337 \cdot 1191313X + 5^{24}\right)^4.$$

On en déduit que l'on a

$$R_{\mathfrak{q}_5} = 2^{126} \cdot 3^{100} \cdot 5^{225} \cdot 7^{21} \cdot 11 \cdot 13^8 \cdot 19 \cdot 37^{11} \cdot 41^8 \cdot 59^{16} \cdot 103 \cdot 109^8 \cdot 149^8 \cdot 193 \cdot 373^2 \cdot 2137 \cdot 4201^2 \cdot 7753^2 \cdot 24061^2.$$

On recommence ensuite ces mêmes calculs avec l'idéal premier $\mathfrak{q}_7$ au-dessus de 7 engendré par une racine $\gamma_{\mathfrak{q}_7}$ du polynôme $\mathfrak{m}_{\gamma_{\mathfrak{q}_7}}(X) = X^4 + 4X^3 + 11X^2 + 14X + 7$. On a alors $P_{\mathfrak{q}_7}(X) = X^2 + 2X + 7$ et

$$R_{\mathfrak{q}_7} = 2^{105} \cdot 3^{59} \cdot 5^{26} \cdot 7^{116} \cdot 11^2 \cdot 13^2 \cdot 17^8 \cdot 23^8 \cdot 31 \cdot 79 \cdot 137^2 \cdot 191^4 \cdot 193 \cdot 463 \cdot 487^2 \cdot 673 \cdot 1033^2 \cdot 1471 \cdot 2953 \cdot 3697.$$

Après ces deux itérations du Théorème 2.8, on a donc montré l'inclusion

$$\mathrm{Red}(E/K) \subset \{2, 3, 5, 7, 11, 13, 193\}.$$

Notons respectivement, $\mathfrak{q}_3$ et $\mathfrak{q}_{17}$ un idéal premier au-dessus de 3 et de 17. Alors, le polynôme $P_{\mathfrak{q}_3}(X) = X^2 + 9$ est irréductible modulo 7 et 11 et le polynôme $P_{\mathfrak{q}_{17}}(X) = X^2 + 10X + 289$ est irréductible modulo 193. De même, le polynôme $P_{\mathfrak{q}_5}$ ci-dessus est irréductible modulo 13. Enfin, $2, 3$ et 5 sont réductibles car ce sont les degrés des isogénies de E vers ses trois conjuguées galoisiennes ([9]). D'où le résultat. □

Remerciements

Don Zagier a accepté de lire une version préliminaire de ce texte. Ses nombreuses remarques ont largement contribué à en améliorer le fond comme la forme. Je l'en remercie vivement. Je dois à John Boxall de nombreux encouragements et de m'avoir suggéré l'énoncé du Théorème 2.8. J'ai eu avec Pierre Charollois et Alain Kraus de nombreuses et fructueuses conversations au sujet de ce travail. Je remercie également le rapporteur de cet article pour sa relecture minutieuse et ses nombreux commentaires. Enfin une partie de cet article a été écrite au sein du département de mathématiques de l'Universität Duisburg-Essen que j'ai plaisir à remercier.

References

[1] N. Billerey, Semi-stabilité des courbes elliptiques, *Dissertationes Math.* **468** (2009), 57 pp.
[2] Y. Bilu and P. Parent, Serre's uniformity problem in the split cartan case, *Ann. of Math.* (*2*) **173**(1) (2011) 569–584.
[3] W. Bosma, J. Cannon and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24**(3–4) (1997) 235–265.
[4] N. Bourbaki, *Éléments de Mathématique*, Lecture Notes in Mathematics, Vol. 864 (Masson, Paris, 1981); Algèbre. Chapitres 4 à 7.
[5] É. Cali, Défaut de semi-stabilité des courbes elliptiques dans le cas non ramifié, *Canad. J. Math.* **56**(4) (2004) 673–698.
[6] H. Cohen, *A Course in Computational Algebraic Number Theory*, Graduate Texts in Mathematics, Vol. 138 (Springer-Verlag, Berlin, 1993).
[7] ———, *Advanced Topics in Computational Number Theory*, Graduate Texts in Mathematics, Vol. 193 (Springer-Verlag, New York, 2000).
[8] A. David, Caractère d'isogénie et borne uniforme pour les homothéties, Thèse de l'université de Strasbourg (2008).
[9] J. González and J. Lario, **Q**-curves and their Manin ideals, *Amer. J. Math.* **123**(3) (2001) 475–503.
[10] E. Gonzalez-Jimenez and X. Guitart, On the modularity level of modular abelian varieties over number fields, *J. Number Theory* **130**(4) (2010) 1560–1570.
[11] A. Kraus, Courbes elliptiques semi-stables et corps quadratiques, *J. Number Theory* **60** (1996) 245–253.
[12] ———, Détermination du poids et du conducteur associés aux représentations des points de p-torsion d'une courbe elliptique, *Dissertationes Math.* **364** (1997), 39 pp.
[13] ———, Courbes elliptiques semi-stables sur les corps de nombres, *Int. J. Number Theory* **3**(4) (2007) 611–633.
[14] A. Kraus and J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* **293** (1992) 259–275.

[15] S. Lang, *Elliptic functions*, Graduate Texts in Mathematics, Vol. 112, 2nd edn. (Springer-Verlag, New York, 1987); With an appendix by J. Tate.
[16] B. Mazur, Rational isogenies of prime degree, *Invent. Math.* **44** (1978) 129–162.
[17] F. Momose, Isogenies of prime degree over number fields, *Compos. Math.* **97**(3) (1995) 329–348.
[18] J. Neukirch, *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], Vol. 280 (Springer-Verlag, Berlin, 1986).
[19] F. Pellarin, Sur une majoration explicite pour un degré d'isogénie liant deux courbes elliptiques, *Acta Arith.* **100**(3) (2001) 203–243.
[20] J.-P. Serre, *Abelian l-Adic Representations and Elliptic Curves* (W. A. Benjamin, Inc., New York-Amsterdam, 1968).
[21] ———, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972) 259–331.
[22] J.-P. Serre and J. Tate, Good reduction of abelian varieties, *Ann. of Math.* **88** (1968) 492–517.
[23] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106 (Springer-Verlag, 1992).
[24] W. A. Stein *et al.*, *Sage Mathematics Software (Version 4.2.1)*, The Sage Development Team (2009); http://www.sagemath.org.
[25] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular Functions of One Variable*, Lect. Notes in Math., Vol. 273 (Springer, 1975), pp. 33–52.

J. London Math. Soc. (2) 89 (2014) 499–523
doi:10.1112/jlms/jdt072

Explicit large image theorems for modular forms

Nicolas Billerey and Luis V. Dieulefait

Abstract

Let f be a (cuspidal) newform of weight $k \geqslant 2$ and level $\Gamma_0(N)$ with $N \geqslant 1$. Ribet proved that, under the assumption that f is non-CM, the residual representations $\bar{\rho}_{f,\lambda}$ attached to f by Deligne have a large image, in a precise sense, for all but finitely many prime ideals λ. In this paper, we make Ribet's theorem explicit by proving that the residue characteristics of these finitely many prime ideals for which the conclusion of Ribet's theorem fails to satisfy some divisibility relation, or are bounded from above by explicit constants, depending on k and N. The results split into different cases according to the possible types for the image, and each of them is illustrated by some numerical examples.

Introduction

Let f be a (cuspidal) newform of weight $k \geqslant 2$, level $N \geqslant 1$ whose Fourier expansion at infinity is given by $f(\tau) = q + \sum_{n \geqslant 2} a_n q^n$, with $q = e^{2i\pi\tau}$ and τ in the complex upper half-plane. We denote by K the number field generated by the coefficients a_n and by $\mathcal{O}$ its ring of integers. Given a prime ideal λ above ℓ in $\mathcal{O}$, we shall denote by $\bar{\rho}_{f,\lambda}$ the unique, up to semi-simplification, mod ℓ Galois representation attached to f by Deligne:

$$\bar{\rho}_{f,\lambda} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2, \mathbf{F}_\lambda),$$

where $\mathbf{F}_\lambda$ is the residue field of $\mathcal{O}$ at λ. Let us denote by $\bar{G}_\lambda$ its image. Using results of Carayol [1], Ribet [25, Theorem 2.1] proved the following theorem (for a definition of forms with complex multiplication see [24] or Definition 1).

Theorem (Ribet). *Assume that f is not a form with complex multiplication. Then, for almost all λ (that is, all but a finite number), the following assertions hold*:

(i) *the representation $\bar{\rho}_{f,\lambda}$ is irreducible*;
(ii) *the order of the group $\bar{G}_\lambda$ is divisible by the residue characteristic of λ.*

In this paper, we shall say that λ is exceptional if it belongs to the finite set of prime ideals for which one of the assertions of Ribet's theorem does not hold. This theorem is a generalization of [23] in the case of $N = 1$, which itself extends pioneering results of Serre [29] and Swinnerton-Dyer [32] in the case of $N = 1$ and $K = \mathbf{Q}$. Although these latter results provide a precise characterization of exceptional prime ideals, the general theorem of Ribet is however non-effective.

The main goal of this paper is to make Ribet's theorem as effective as possible under the additional assumption that f has trivial Nebentypus. Though this further assumption is used in several places in our paper, we believe that our method generalizes to the case of arbitrary characters. Nevertheless, for the sake of conciseness, this generalization will be considered in

Received 3 April 2013; revised 17 August 2013; published online 8 January 2014.

2010 *Mathematics Subject Classification* 11F80, 11F33 (primary).

Research partially supported by MICINN grant MTM2012-33830 and by an ICREA Academia Research Prize.

another paper. More precisely, we prove that the residue characteristic of an exceptional prime satisfies some divisibility relation, or at least is bounded from above by an explicit constant, depending on k and N.

Before describing our main results, we mention that among the special cases covered are a generalization to arbitrary square-free levels of a result of Mazur [18] on the so-called Eisenstein primes for weight 2 and prime level modular forms, and an explicit version of Serre's theorem on the surjectivity of Galois representations attached to elliptic curves over $\mathbf{Q}$ due to Kraus [14] and Cojocaru [4].

Let us denote by $\mathbf{P}(\bar{\rho}_{f,\lambda})$ the projectivization of $\bar{\rho}_{f,\lambda}$ and by $\mathbf{P}(\bar{G}_\lambda)$ its image in $\mathrm{PGL}(2,\mathbf{F}_\lambda)$. According to Dickson's classification of subgroups of $\mathrm{PGL}(2,\mathbf{F}_\lambda)$ (see [9, II.8.27]), if λ is exceptional (we warn the reader that in the literature, the term 'exceptional' sometimes refers to the last situation below only), then we have that one of the following conditions satisfy us:

(I) $\bar{\rho}_{f,\lambda}$ is reducible;
(II) the image $\mathbf{P}(\bar{G}_\lambda)$ in $\mathrm{PGL}(2,\mathbf{F}_\lambda)$ is dihedral;
(III) $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5.

Besides, if λ is non-exceptional, then $\mathbf{P}(\bar{\rho}_{f,\lambda})$ is isomorphic to either $\mathrm{PGL}(2,\mathbf{F})$ or $\mathrm{PSL}(2,\mathbf{F})$ for some subfield $\mathbf{F}$ of $\mathbf{F}_\lambda$, and we shall then say that $\bar{\rho}_{f,\lambda}$ has a large image.

In each of the above cases, we thus provide a divisibility relation, or an upper-bound in terms of k and N satisfied by the residue characteristic ℓ of λ. The last case is the simplest one. Namely, we prove the following theorem.

THEOREM (Theorem 4.1). *If $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5, then either $\ell \mid N$ or $\ell \leqslant 4k-3$.*

In the second case, we give a general upper-bound together with a much finer result in the square-free level case that imply the following theorem.

THEOREM (Theorem 3.2). *Assume $\mathbf{P}(\bar{G}_\lambda)$ to be dihedral. If f does not have complex multiplication, then we have*

$$\ell \leqslant (2(8kN^2(1+\log\log N))^{(k-1)/2})^{g_0^\sharp(k,N)},$$

where $g_0^\sharp(k,N)$ is the number of newforms of weight k and level $\Gamma_0(N)$. Besides, if N is square-free, then either $\ell \mid N$, or $\ell \leqslant k$, or $\ell = 2k-1$.

The first case is by far the most complicated one, and we refer the reader to Theorems 2.4–2.7 for precise and complete statements. Nevertheless, these results, combined with those mentioned in this introduction, yield to (slightly stronger versions of) the following theorems in particular, but important cases where N is square-free and N is a square, respectively.

THEOREM (Square-free level case). *Assume that $N = p_1 \cdots p_t$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes, is square-free, and λ is exceptional. Then we have that one of the following is satisfied:*

(i) $\ell \in \{p_1, \ldots, p_t\}$;
(ii) $\ell \leqslant 4k-3$;
(iii) ℓ *divides*

$$\begin{cases} \gcd_{1\leqslant i\leqslant t}(\mathrm{lcm}(p_i^k-1, p_i^{k-2}-1)) & \text{if } k>2, \\ \mathrm{lcm}_{1\leqslant i\leqslant t}(p_i^2-1) & \text{if } k=2. \end{cases}$$

THEOREM (Square level case). *Assume that $N = c^2$ is a square, f does not have complex multiplication and λ is exceptional. Then we have that one of the following is satisfied*:

(i) $\ell \mid N$;
(ii) $\ell \leqslant (2(8kN^2(1+\log\log N))^{(k-1)/2})^{g_0^\sharp(k,N)}$, *where $g_0^\sharp(k,N)$ is the number of (cuspidal) newforms of weight k and level $\Gamma_0(N)$*;
(iii) *there exists a primitive Dirichlet character $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that*:
  (a) *either ℓ divides the norm of $p^k - \epsilon^{-1}(p)$ for some prime $p \mid c$*;
  (b) *or ℓ divides the numerator of the norm of $B_{k,\epsilon}/2k$*;
  where c_0 divides c, $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2 and $B_{k,\epsilon}$ is the kth Bernoulli number attached to ϵ.

Apart from (III) which is slightly different, the main idea used in proving the results of the paper is to interpret situations (I) and (II) above in terms of congruences between modular forms. In the case of reducible representations $\bar\rho_{f,\lambda}$, the original form f is then shown to be congruent modulo ℓ to a suitable Eisenstein series whose construction depends on the weight and level. The theory of modular forms modulo ℓ of Serre and Katz enables us to interpret this congruence as an equality. The desired bound then follows from a careful study of the constant term of these Eisenstein series at various cusps. Besides, in the case of dihedral projective image, the congruent modular form is a specific twist of the original form f. In that case, the upper-bound follows from those of Sturm and Deligne.

Ghate and Parent recently addressed the question of whether the residual Galois representations attached to rational simple non-CM modular abelian varieties have 'uniform' large images (see [8, Question 1.2] for a precise statement). One of the main results of their paper is that, in the weight 2 situation, there exists a uniform bound (depending on $[K : \mathbf{Q}]$, but not on the level) for the residue characteristic of prime ideals in the A_4, S_4 or A_5 case. While we are in contrary working with a fixed level, their work is still quite relevant for us.

The first section of the paper is devoted to classical facts about modular Galois representations and their local behaviors. The next three sections deal with cases (I), (II) and (III) above, respectively. Finally, some numerical examples illustrating our results are presented in the last section.

1. *Preliminaries*

For simplicity, we shall write $\bar\rho$ for $\bar\rho_{f,\lambda}$. We further denote by $\bar\rho^{ss}$ the semi-simplification of $\bar\rho$. In this section, we also assume $\ell \nmid N$.

1.1. *Local decomposition at Steinberg primes*

Let p be a prime dividing N exactly once. We shall write $p \| N$. Define $\bar\rho_p$ to be the restriction of $\bar\rho$ to a decomposition group G_p at p. For any $x \in \mathcal{O}$, let us denote by $\lambda(x)$ the unramified character of G_p that maps a Frobenius element to $x \pmod\lambda$. Langlands has proved that [16, Proposition 2.8]

$$\bar\rho_p \simeq \begin{pmatrix} \mu\bar\chi_\ell^{k/2-1} & \star \\ 0 & \mu\bar\chi_\ell^{-k/2} \end{pmatrix}, \tag{1.1}$$

where $\mu = \lambda(a_p/p^{k/2-1})$ is trivial or quadratic since $a_p = \pm p^{k/2-1}$ [20, Theorem 4.6.17]. In particular, if $\mathrm{Frob}_p \in G_p$ is a Frobenius element at p, then the roots of the characteristic polynomial of $\bar\rho(\mathrm{Frob}_p)$ are $a_p \pmod\lambda$ and $pa_p \pmod\lambda$.

1.2. *Classification of degenerate cases*

Let $N(\bar{\rho}^{ss})$ be the Artin conductor of $\bar{\rho}^{ss}$. It was proved by Carayol [1] that $N(\bar{\rho}^{ss})$ is a divisor of N. Moreover, Carayol [2, §§ 1.2–1.3] and Livné [15] have (independently) classified the 'degenerate' cases (in Carayol's terminology), that is, when $e_p \overset{\text{def}}{=} v_p(N) - v_p(N(\bar{\rho}^{ss})) > 0$ for some prime p. They proved that when $e_p > 0$, we are in one of the situations described in Table 1.

Moreover, it follows from their classification that, in the first and third cases, p satisfies certain congruences modulo ℓ. Namely, we have the following proposition (which we deduce from [2, § 1.5] using the fact that, in these cases, $\bar{\rho}^{ss}$ is the semi-simplification of the reduction of an ℓ-adic degenerate representation of type (i), (iii) or (iv) with the terminology of [2, Proposition 2]).

PROPOSITION 1.1 (Carayol–Livné). *Assume $e_p > 0$ and $v_p(N) \geqslant 2$. Then we have $p \equiv \pm 1 \pmod{\ell}$.*

1.3. *Local description at ℓ*

Assume $2 \leqslant k \leqslant \ell + 1$. Let G_ℓ be a decomposition group at ℓ and I_ℓ be its inertia subgroup. Then Deligne and Fontaine [7] have, respectively, proved that

(i) if f is ordinary at λ (that is, if $a_\ell \not\equiv 0 \pmod{\lambda}$), then $\bar{\rho}_{|G_\ell}$ is reducible and

$$\bar{\rho}_{|I_\ell} \simeq \begin{pmatrix} \bar{\chi}_\ell^{k-1} & \star \\ 0 & 1 \end{pmatrix};$$

(ii) if f is not ordinary at λ, then $\bar{\rho}_{|G_\ell}$ is irreducible and

$$\bar{\rho}_{|I_\ell} \simeq \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix},$$

where $\{\psi, \psi'\} = \{\psi, \psi^\ell\}$ is the set of fundamental characters of level 2 ([7, § 2.4]).

The following lemma is immediate.

LEMMA 1.2. *Assume $\ell > k$.*

(i) *The image of $\bar{\chi}_\ell^{k-1}$ is cyclic of order $n = (\ell - 1)/\gcd(\ell - 1, k - 1) \geqslant 2$. In particular, we have $n = 2$ if and only if $\ell = 2k - 1$. Moreover, if $\ell > 4k - 3$, then $n > 5$.*

(ii) *The image of $\psi^{(\ell-1)(k-1)}$ is cyclic of order $m = (\ell + 1)/\gcd(\ell + 1, k - 1) \geqslant 2$. In particular, we have $m = 2$ if and only if $\ell = 2k - 3$. Moreover, if $\ell > 4k - 5$, then $m > 5$.*

TABLE 1. *Classification of the degenerate cases.*

$v_p(N)$	$b + 1 \geqslant 2$	1	2
$v_p(N(\bar{\rho}^{ss}))$	$b \geqslant 1$	0	0
e_p	1	1	2

2. *Reducible representations*

2.1. *Preliminaries: Gauss sums and Bernoulli numbers*

Let $\psi : (\mathbf{Z}/f\mathbf{Z})^\times \to \mathbf{C}^\times$ be a primitive Dirichlet character of modulus $f \geqslant 1$. The Gauss sum attached to ψ is defined by

$$W(\psi) = \sum_{n=1}^{f} \psi(n)\, e^{2i\pi n/f}.$$

LEMMA 2.1. *We have $|W(\psi)| = \sqrt{f}$. Moreover, as an algebraic integer, the norm of $W(\psi)$ is a power of f.*

Proof. The first part of the lemma is [20, Lemma 3.1.1]. Let σ be a $\bar{\mathbf{Q}}$-automorphism and $m \in \mathbf{Z}$ such that $\sigma(e^{2i\pi/f}) = e^{2i\pi m/f}$. Then, by Miyake [20], we have

$$\sigma(W(\psi)) = \sum_{n=1}^{f} \psi^\sigma(n)\, e^{2i\pi nm/f} = \bar{\psi}^\sigma(m) W(\psi^\sigma)$$

and thus $|\sigma(W(\psi))| = |W(\psi^\sigma)| = \sqrt{f}$. This completes the proof of the lemma. □

The Bernoulli numbers attached to ψ are defined by

$$\sum_{n=1}^{f} \psi(n) \frac{t\, e^{nt}}{e^{ft} - 1} = \sum_{m \geqslant 0} B_{m,\psi} \frac{t^m}{m!}.$$

In particular, if ψ is the trivial character, then $B_{m,\psi}$ is the classical Bernoulli number B_m, except when $m = 1$, in which case $B_{1,\psi} = -B_1 = \frac{1}{2}$. The following proposition is a well-known result of van Staudt–Clausen.

PROPOSITION 2.2 (van Staudt–Clausen). *Let $m \geqslant 2$ be an even integer. The denominator of B_m is $\prod_{p-1|m} p$, where the product runs over the primes p such that $p - 1$ divides m.*

The Bernoulli numbers are also related to certain special values of the L-function $L(s, \psi)$ attached to ψ. More precisely, we have the following proposition [34, Chapter 4].

PROPOSITION 2.3. *Assume that ψ to be even. Let $m \geqslant 2$ be an even integer. Then we have*

$$L(m, \psi) = -W(\psi) \frac{C_m}{f^m} \cdot \frac{B_{m,\psi^{-1}}}{2m} \neq 0, \quad \text{where } C_m = \frac{(2i\pi)^m}{(m-1)!}.$$

2.2. *Statement of the results*

THEOREM 2.4. *Assume $\bar{\rho}_{f,\lambda}$ to be reducible. If $v_2(N) = 2$ or $v_2(N) \geqslant 3$ is odd, then either ℓ divides N, or $\ell < k - 1$, or $\ell = 3$.*

Put $c = \max\{d \geqslant 1;\ d^2 \mid N\}$. The following result is a generalization of Ribet's [23, Lemma 5.2] on the level 1 case to higher levels.

THEOREM 2.5 (main result). *Assume $\bar{\rho}_{f,\lambda}$ to be reducible. Then one of the following assertions holds.*

(i) *The prime ℓ divides N or $\ell < k-1$.*
(ii) *The level N is not a square and there exists an even Dirichlet character $\eta : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that, for every prime p dividing N with odd valuation $v_p(N)$, we have:*
  (a) *either $v_p(N) \geqslant 3$ and $p \equiv \pm 1 \pmod{\ell}$;*
  (b) *or $v_p(N) = 1$ and ℓ divides the norm of either $p^k - \eta(p)$, or $p^{k-2} - \eta(p)$.*
(iii) *The level N is a square (that is, $N = c^2$) and one of the following holds:*
  (a) *either there exists a prime p such that $v_p(N) = 2$ and $p \equiv \pm 1 \pmod{\ell}$;*
  (b) *or there exists a primitive Dirichlet character $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that, for $\ell > k+1$, we have:*
    (1) *either ℓ divides the norm of $p^k - \epsilon^{-1}(p)$ for some prime $p \mid c$;*
    (2) *or ℓ divides the numerator of the norm of $B_{k,\epsilon}/2k$;*
    where c_0 divides c and $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2.

Note that these two results give an effective bound for ℓ in terms of N and k unless $k = 2$ and $N = p_1 \cdots p_t c^2$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes not dividing c, and c is odd or divisible by 4 (as in particular condition (2.5) in Theorem 2.5 might be vacuous if $k = 2$). In the square-free level case (namely, when $c = 1$), we, however, have the following theorem whose first part is an immediate corollary of Theorem 2.5, and whose second part follows from a generalization of a result of Mazur on the weight 2 and prime level case (cf. [**18**; **19**, Proposition 1]).

THEOREM 2.6 (Square-free level case). *Assume that $\bar{\rho}_{f,\lambda}$ is reducible and $N = p_1 \cdots p_t$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes.*

(i) *If $k > 2$, then one of the following assertions holds:*
  (a) *either ℓ divides N or $\ell < k-1$;*
  (b) *ℓ divides the following non-zero integer*

$$\gcd(\operatorname{lcm}(p_i^k - 1, p_i^{k-2} - 1), 1 \leqslant i \leqslant t).$$

(ii) *If $k = 2$ and $\ell \nmid 6N$, then the following assertions hold:*
  (a) *for any $1 \leqslant i \leqslant t$ with $a_{p_i} = -1$, we have $p_i \equiv -1 \pmod{\ell}$;*
  (b) *we have $(a_{p_1}, \ldots, a_{p_t}) \neq (-1, \ldots, -1)$;*
  (c) *if $(a_{p_1}, \ldots, a_{p_t}) = (+1, \ldots, +1)$, then ℓ divides the non-zero integer $\prod_{i=1}^t (p_i - 1)$.*

We point out that Ribet already proved (but did not publish) the second part of this theorem as well as 'converse results' (see the notes [**27**] on his homepage).

The last theorem of this section deals with the cases not covered by the previous results.

THEOREM 2.7. *Assume that $\bar{\rho}_{f,\lambda}$ is reducible. If $k = 2$ and N is of the form $N = p_1 \cdots p_t c^2$, where $c \neq 1$, $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes not dividing c, and c is odd or divisible by 4, then one of the following are satisfied:*

(i) *$\ell \mid N$;*
(ii) *$\ell < k-1$;*
(iii) *there exists a prime p such that $v_p(N) = 2$ and $p \equiv \pm 1 \pmod{\ell}$;*

(iv) *there exists a primitive Dirichlet character* $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ *such that, for* $\ell > 3$, *we have that any one of the following is satisfied*:
(a) ℓ *divides the norm of* $p_i^2 - \nu^2(p_i)$ *for some* $1 \leqslant i \leqslant t$;
(b) ℓ *divides the norm of* $p^2 - \epsilon^{-1}(p)$ *for some prime* $p \mid c$;
(c) ℓ *divides* $p_i - 1$ *for some* $1 \leqslant i \leqslant t$;
(d) ℓ *divides the numerator of the norm of* $B_{2,\epsilon}/4$;
where $c_0 \mid c$ *and* $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ *is the inverse of the primitive Dirichlet character attached to* ν^2.

2.3. *The Eisenstein series E*

Assume $\ell \nmid N$. For simplicity, let us denote $\bar\rho$ for $\bar\rho_{f,\lambda}$ and assume $\bar\rho$ to be reducible. The semi-simplification $\bar\rho^{ss}$ of $\bar\rho$ is the direct sum of two characters ϵ_1 and ϵ_2. Each of them may be decomposed as a product $\bar\nu_i\bar\chi_\ell^{\alpha_i}$ with $\bar\nu_i$ unramified at ℓ and $0 \leqslant \alpha_i < \ell - 1$ $(i = 1, 2)$. Using that f has trivial Nebentypus, we obtain that $\bar\rho^{ss}$ has determinant $\bar\chi_\ell^{k-1}$. Hence, we have $\alpha_1 + \alpha_2 \equiv k - 1 \pmod{\ell - 1}$ and $\bar\nu_2 = \bar\nu_1^{-1}$.

Let us further assume that $\ell + 1 \geqslant k$. Using the results of § 1.3, one sees that $\{\alpha_1, \alpha_2\} = \{0, k - 1\}$ and thus

$$\bar\rho^{ss} \simeq \bar\nu \oplus \bar\nu^{-1}\bar\chi_\ell^{k-1}, \tag{2.1}$$

with $\bar\nu \in \{\bar\nu_1, \bar\nu_2\}$. Moreover, according to Carayol's theorem of § 1.2, the conductor $\mathfrak{c}$ of $\bar\nu$ satisfies

$$N(\bar\rho^{ss}) = \mathfrak{c}^2 \mid N. \tag{2.2}$$

In particular, $N(\bar\rho^{ss})$ is a square dividing N.

Let ν be the Teichmüller lift of $\bar\nu$. We may identify it with a primitive Dirichlet character modulo $\mathfrak{c}$. From now on, assume that:

(1) either $k > 2$;
(2) or, $k = 2$ and $\mathfrak{c} \neq 1$.

Under this assumption, we may consider the Eisenstein series in $\mathcal{M}_k(\Gamma_0(\mathfrak{c}^2))$ whose Fourier expansion is given by

$$E(\tau) = -\vartheta(\mathfrak{c})\frac{B_k}{2k} + \sum_{n \geqslant 1} \sigma_{k-1}^{\nu}(n)q^n,$$

where

$$\vartheta(\mathfrak{c}) = \begin{cases} 1 & \text{if } \mathfrak{c} = 1, \\ 0 & \text{otherwise,} \end{cases} \qquad \sigma_{k-1}^{\nu}(n) = \sum_{0<m|n} \nu(n/m)\nu^{-1}(m)m^{k-1}$$

and B_k is the kth Bernoulli number. Note also that our notation E differs from the notation $E_k^{\nu,\nu^{-1}}$ of [5, Chapter 4] by a factor 2: $E_k^{\nu,\nu^{-1}} = 2E$.

The following proposition gives the constant term of the Fourier expansion of E at the various cusps of $\Gamma_0(\mathfrak{c}^2)$.

PROPOSITION 2.8. *The Eisenstein series* E *is defined over* $\mathcal{O}_L$, *where* L *is the field generated by the values of* ν, *unless* $\mathfrak{c} = 1$ *(and* $k > 2$*), in which case* E *is the classical Eisenstein series* $E_k(\tau) = -B_k/2k + \sum_{n \geqslant 1} \sigma_{k-1}(n)q^n$ *of weight* k *and level* 1. *Let* $s = u/v$ *(where* $\gcd(u, v) = 1$, $v \mid \mathfrak{c}^2$ *and* u *varies through a set of representatives of the integers modulo* $\gcd(v, \mathfrak{c}^2/v)$*) be a cusp of* $\Gamma_0(\mathfrak{c}^2)$, *and let* $\gamma \in \mathrm{SL}(2, \mathbf{Z})$ *such that* $\gamma\infty = s$. *Then the constant term* Υ *of* $E|_k\gamma$ *is*

independent of the choice of such a γ and satisfies

$$\Upsilon \neq 0 \Leftrightarrow v = \mathfrak{c}.$$

In that case, we have

$$\Upsilon = -\nu(-u)\left(\frac{\mathfrak{c}}{c_0}\right)^k \frac{W((\nu^2)_0)}{W(\nu)} \frac{B_{k,(\nu^2)_0^{-1}}}{2k} \prod_{p|\mathfrak{c}} (1-(\nu^2)_0(p)p^{-k}),$$

where $(\nu^2)_0$ is the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. Moreover, if $\mathfrak{c} > 1$, then $E|_k\gamma \in \mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})[\![q^{1/\mathfrak{c}^2}]\!]$, where $\mu_{\mathfrak{c}^2}$ is the group of $\mathfrak{c}^2$th roots of unity.

Proof. The proposition is immediate when $\mathfrak{c} = 1$. Assume therefore $\mathfrak{c} > 1$. Then, by construction, the Fourier expansion of E has coefficients in $\mathcal{O}_L$, and therefore E is defined over $\mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})$ (see [**11**, § 1.6]).

Let $s = u/v$ as in the proposition be a cusp of $\Gamma_0(\mathfrak{c}^2)$ (for the description of a set of representatives of the cusps of $\Gamma_0(\mathfrak{c}^2)$, see [**10**, Proposition 2.6]) and $\gamma \in \mathrm{SL}(2,\mathbf{Z})$ such that $\gamma\infty = s$. The last assertion follows from the q-expansion principle, and the fact that the Fourier expansion of E at ∞ has coefficients in $\mathcal{O}_L$ (see [**11**, Corollary 1.6.2.]).

Since k is even, the constant term of E at s is well defined (that is, it does not depend on the choice of such a γ). Put

$$\gamma = \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z}) \quad \text{and} \quad G = \frac{C_k W(\nu)}{\mathfrak{c}^k} E, \ \text{where } C_k = \frac{(2i\pi)^k}{(k-1)!}. \tag{2.3}$$

The constant part of $G|_k\gamma$ is then given by the following sum (see [**5**, Chapter 4] and [**28**, § VII.3] for a justification in the weight 2 case; the factor $\frac{1}{2}$ comes from our normalization for E):

$$\Upsilon_0 = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij)\vartheta(\overline{i\mathfrak{c}u + v(j+l\mathfrak{c})})\zeta^{\overline{\mathfrak{c}i\beta+(j+l\mathfrak{c})\delta}}(k),$$

where the bar means reduction modulo $\mathfrak{c}^2$,

$$\vartheta(\bar{n}) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{\mathfrak{c}^2}, \\ 0 & \text{otherwise,} \end{cases} \qquad \zeta^{\bar{n}}(k) = \sum_{m \equiv n \pmod{\mathfrak{c}^2}}{}' \frac{1}{m^k},$$

and the primed summation notation means to sum over non-zero integers.

Assume Υ_0 to be non-zero. Then there exist $i,j,l \in \{0,\dots,\mathfrak{c}-1\}$ such that

$$\nu(ij)\vartheta(\overline{i\mathfrak{c}u + v(j+l\mathfrak{c})}) \neq 0.$$

In other words, $\gcd(ij,\mathfrak{c}) = 1$ and $i\mathfrak{c}u + v(j+l\mathfrak{c}) \equiv 0 \pmod{\mathfrak{c}^2}$. It follows that $vj \equiv 0 \pmod{\mathfrak{c}}$. But j is co-prime to $\mathfrak{c}$ by assumption. So $v \equiv 0 \pmod{\mathfrak{c}}$ and u is invertible modulo $\mathfrak{c}$. The congruence $i \equiv -(j/u)(v/\mathfrak{c}) \pmod{\mathfrak{c}}$ follows easily and, therefore, we have

$$\nu(ij) = \nu\left(-\frac{vj^2}{u\mathfrak{c}}\right) = \nu\left(-\frac{j^2}{u}\right)\nu\left(\frac{v}{\mathfrak{c}}\right) \neq 0.$$

So $\gcd(v/\mathfrak{c},\mathfrak{c}) = 1$ and since $\mathfrak{c} \mid v$ and $v \mid \mathfrak{c}^2$, we obtain $v = \mathfrak{c}$.

Conversely, assume $v = \mathfrak{c} > 1$. Then $\gcd(u,\mathfrak{c}) = 1$ and, on one hand, we have

$$i\mathfrak{c}u + v(j+l\mathfrak{c}) \equiv 0 \pmod{\mathfrak{c}^2} \Longleftrightarrow i \equiv -j/u \pmod{\mathfrak{c}};$$

on the other hand

$$\begin{aligned}\mathfrak{c}i\beta+(j+l\mathfrak{c})\delta&=\frac{1}{u}(u\mathfrak{c}i\beta+(j+l\mathfrak{c})u\delta)\\&\equiv\frac{1}{u}(-vj\beta+(j+l\mathfrak{c})(1+\beta v))\ (\mathrm{mod}\,\mathfrak{c}^2)\\&\equiv\frac{1}{u}(j+l\mathfrak{c})\ (\mathrm{mod}\,\mathfrak{c}^2).\end{aligned}$$

Combining these two facts, we find that

$$\begin{aligned}2\Upsilon_0&=\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu(-j^2/u)\zeta^{\overline{(j+l\mathfrak{c})/u}}(k)\\&=\nu(-u)\sum_{l=0}^{c-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu(j^2/u^2)\sum_{m\equiv(j+l\mathfrak{c})/u\ (\mathrm{mod}\,\mathfrak{c}^2)}{}'\frac{1}{m^k}\\&=\nu(-u)\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\sum_{m\equiv j/u\ (\mathrm{mod}\,\mathfrak{c})}{}'\frac{\nu^2(m)}{m^k}\\&=2\nu(-u)\sum_{m\geqslant 1}\frac{\nu^2(m)}{m^k}=2\nu(-u)L(k,\nu^2),\end{aligned}\tag{2.4}$$

where ν^2 is viewed as a character modulo $\mathfrak{c}$. Let $(\nu^2)_0$ be the primitive Dirichlet character attached to ν^2. It is an even character modulo $c_0 \mid \mathfrak{c}$ and we have

$$L(k,\nu^2)=L(k,(\nu^2)_0)\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-k}).\tag{2.5}$$

Applying Proposition 2.3 to $\psi=(\nu^2)_0$ and $m=k$, we obtain

$$L(k,(\nu^2)_0)=-W((\nu^2)_0)\frac{C_k}{c_0^k}\frac{B_{k,(\nu^2)_0^{-1}}}{2k}\neq 0.\tag{2.6}$$

According to Equations (2.4)–(2.6) together with (2.3), when $v=\mathfrak{c}$, the constant term of the Fourier expansion of E at s is thus the non-zero algebraic number

$$\Upsilon=\frac{\mathfrak{c}^k}{C_kW(\nu)}\Upsilon_0=-\nu(-u)\left(\frac{\mathfrak{c}}{c_0}\right)^k\frac{W((\nu^2)_0)}{W(\nu)}\frac{B_{k,(\nu^2)_0^{-1}}}{2k}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-k}),$$

as claimed. □

2.4. *Proof of Theorems* 2.4 *and* 2.5

Assume $\bar\rho$ to be reducible with $\ell\nmid N$ and $\ell+1\geqslant k$. We keep the notation of § 2.3. In particular, we have (cf. (2.1) and (2.2))

$$\bar\rho^{ss}\simeq\bar\nu\oplus\bar\nu^{-1}\bar\chi_\ell^{k-1},\tag{2.7}$$

where $\bar\nu$ is a character of conductor $\mathfrak{c}$ such that $\mathfrak{c}^2\mid N$. So, in particular, we have $\mathfrak{c}\mid c$.

Assume $v_2(N)=2$. Then $v_2(c)=1$ and $\mathfrak{c}$ is odd since there is no primitive Dirichlet character modulo twice an odd integer. Therefore, we are in a degenerate case at $p=2$ as described in § 1.2. By Proposition 1.1, we have $2\equiv\pm1\ (\mathrm{mod}\,\ell)$, namely $\ell=3$.

If N is not a square, then let us consider a prime p dividing N with odd valuation $v_p(N)$. Once again, we necessarily are in one of the degenerate cases. If $v_p(N)\geqslant 3$, then, by Proposition 1.1, we obtain $p\equiv\pm1\ (\mathrm{mod}\,\ell)$. This completes the proof of Theorem 2.4.

Assume now that, for some prime p, we have $v_p(N) = 1$ and let us denote by η the Teichmüller lift of $\bar{\nu}^2$. Since $\mathfrak{c}$ is a divisor of c, we may identify η with an even Dirichlet character modulo c. Comparing the restriction to a decomposition group at p of $\bar{\rho}^{ss}$ given by (2.1) with the local representation given by (1.1), we obtain the following equality between sets of characters of G_p:

$$\{\bar{\nu}, \bar{\nu}^{-1}\bar{\chi}_\ell^{k-1}\} = \{\mu\bar{\chi}_\ell^{k/2}, \mu\bar{\chi}_\ell^{k/2-1}\},$$

where $\mu = \lambda(a_p/p^{k/2-1})$ is the at most quadratic character defined in § 1.1. We thus are in one of the following situations:

(1) either $\bar{\nu} = \mu\bar{\chi}_\ell^{k/2}$ and then $\bar{\nu}^2 = \bar{\chi}_\ell^k$. Applying this equality to a Frobenius element at p, we obtain that $\bar{\nu}^2(\mathrm{Frob}_p) = p^k \pmod{\ell}$ and therefore ℓ divides the norm of $p^k - \eta(p)$;

(2) or $\bar{\nu} = \mu\bar{\chi}_\ell^{k/2-1}$ and then $\bar{\nu}^2 = \bar{\chi}_\ell^{k-2}$. Again we have $\bar{\nu}^2(\mathrm{Frob}_p) = p^{k-2} \pmod{\ell}$ and we conclude as before that ℓ divides the norm of $p^{k-2} - \eta(p)$.

It remains to prove Theorem 2.5 when N is a square, namely, when $N = c^2$. Assume first that $\mathfrak{c} \neq c$. Then we are in a degenerate case as described in § 1.2 for some prime number p. Moreover, $N(\bar{\rho}^{ss}) = \mathfrak{c}^2$ is a square and therefore we have $v_p(N) = 2$ and $v_p(N(\bar{\rho}^{ss})) = 0$. By Proposition 1.1, it follows that $p \equiv \pm 1 \pmod{\ell}$.

In other words, if, for every prime p dividing N with valuation 2, we have $p \not\equiv \pm 1 \pmod{\ell}$, then $\mathfrak{c} = c$, $N = \mathfrak{c}^2$ and there is no degeneration at all. Assume now that we are in this situation. Since the space of weight 2 and level 1 modular forms are trivial, it follows that either $k > 2$, or $k = 2$ and $\mathfrak{c} \neq 1$. Therefore, we may consider the Eisenstein series E of § 2.3. Let M denote the compositum of K and L (the field generated by the values of ν).

LEMMA 2.9. *The Eisenstein series E is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$. Moreover, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that*

$$a_r \equiv a_r(E) \pmod{\mathcal{L}} \quad \textit{for all primes } r \neq \ell.$$

Proof. The fact that E is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$ follows, for instance, from [**5**, Proposition 5.2.3]. Moreover, by isomorphism (2.7) there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that

$$a_r \equiv a_r(E) \pmod{\mathcal{L}} \quad \text{for all primes } r \nmid \ell N.$$

If now r is a prime dividing N, then $r^2 \mid N$ and $a_r = 0$ (see [**20**, Theorem 4.6.17]). Besides, $\nu(r) + \nu^{-1}(r)r^{k-1} = 0$. Hence, $a_r = 0 = a_r(E)$. This proves the lemma. □

Let now Θ be the Katz's operator on modular forms over $\bar{\mathbf{F}}_\ell$, whose action on q-expansions is given by $q(d/dq)$ (denoted by $A\theta$ in [**12**]). Assume $\ell > k + 1$. Then the constant term of E at ∞ is non-zero only if $\mathfrak{c} = 1$ and $k > 2$. In that case it is $-B_k/2k$, which is ℓ-integral by Proposition 2.2. We denote by $\bar{f}$ and $\bar{E}$ the modular forms over $\bar{\mathbf{F}}_\ell$ obtained by reduction modulo $\mathcal{L}$ of f and E, respectively. Lemma 2.9 implies that $\Theta(\bar{f}) = \Theta(\bar{E})$. Moreover, Katz has proved that if $\ell > k + 1$, then Θ is injective [**12**, Corollary (3)]. Under this assumption, it thus follows that the Eisenstein series E becomes cuspidal after reduction.

If $\mathfrak{c} = 1$, then we immediately obtain that ℓ divides the numerator of $B_k/2k$ as stated in the theorem. Assume therefore that $\mathfrak{c} > 1$. Then ℓ divides the numerator of the norm of the constant term of E at each cusp of $\Gamma_0(\mathfrak{c}^2)$, namely by Proposition 2.8:

$$\Upsilon = \pm\left(\frac{\mathfrak{c}}{c_0}\right)^k \frac{W(\epsilon^{-1})}{W(\nu)} \frac{B_{k,\epsilon}}{2k} \prod_{p\mid\mathfrak{c}} (1 - \epsilon^{-1}(p)p^{-k}),$$

where $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2. By Lemma 2.1, the prime divisors of the norm of $W(\epsilon^{-1})/W(\nu)$ divide N and therefore are co-prime to ℓ. The same obviously holds for $\mathfrak{c}/c_0$. Therefore, we eventually obtain that ℓ divides the norm of either $p^k - \epsilon^{-1}(p)$ for some p dividing $\mathfrak{c}$ (and thus c) or the norm of the numerator of $B_{k,\epsilon}/2k$. This completes the proof of Theorem 2.5.

2.5. *Proof of Theorem* 2.6

As already mentioned, the first part of Theorem 2.6 is a direct corollary of Theorem 2.5. So let us assume $k = 2$ and $\ell \nmid 6N$. By the reasoning at the beginning of § 2.3, we may write

$$\bar{\rho}^{ss} \simeq \mathbf{1} \oplus \bar{\chi}_\ell, \tag{2.8}$$

where $\mathbf{1}$ is the trivial character of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. In particular, we have $\mathfrak{c}^2 = N(\bar{\rho}^{ss}) = 1$, hence $\mathfrak{c} = 1$. Let now $p \in \{p_1, \ldots, p_t\}$ be a prime dividing N. By § 1.1, the local representation $\bar{\rho}_p$ at p semi-simplifies to

$$\lambda(a_p) \oplus \lambda(a_p)\bar{\chi}_\ell. \tag{2.9}$$

Comparing (2.8) and (2.9), we obtain the following equality between sets of characters of G_p:

$$\{\mathbf{1}, \bar{\chi}_\ell\} = \{\lambda(a_p)\bar{\chi}_\ell, \lambda(a_p)\}.$$

Moreover, if $a_p = -1$, then the character $\lambda(a_p)$ is non-trivial and, therefore, we must have $\lambda(a_p) = \bar{\chi}_\ell$ as characters of G_p. In other words, $p \equiv -1 \pmod{\ell}$. This proves assertion ((ii)(a)) of Theorem 2.6.

Before proving the next two assertions, note that we precisely are in the excluded situation of § 2.3, namely $k = 2$ and $\mathfrak{c} = 1$. For that reason, we cannot use the Eisenstein series E as in the proof of Theorem 2.5 (cf. § 2.4).

To circumvent the lack of weight 2 level 1 Eisenstein series, it will be more convenient to directly work with modular forms over $\bar{\mathbf{F}}_\ell$. Let E_2 be the classical series in characteristic 0 defined by

$$E_2(\tau) = -\frac{1}{24} + \sum_{n \geqslant 1} \sigma_1(n) q^n.$$

Recall that E_2 is not a modular form (it is a quasi-modular form). However, its reduction modulo ℓ (recall that $\ell \geqslant 5$), denoted by $\bar{E}_2$, is a well-defined modular form over $\bar{\mathbf{F}}_\ell$. Moreover, as a modular form over $\bar{\mathbf{F}}_\ell$ of level N (which is co-prime to ℓ by assumption), $\bar{E}_2$ has filtration $\ell + 1$ (see [**29**]). Put

$$E' = \left[\prod_{p|N} (a_p U_p - p\mathrm{Id})\right] \bar{E}_2,$$

where U_p denotes the usual Hecke operator at p. The following proposition summarizes the main properties of E'.

PROPOSITION 2.10. *As a modular form over $\bar{\mathbf{F}}_\ell$, E' is a well-defined normalized $(a_1(E') = 1)$ eigenform for all the Hecke operators at level $\Gamma_0(N)$ such that*

$$\begin{cases} T_r E' = (1 + r)E' & \text{for all primes } r \nmid N, \\ U_p E' = a_p E' & \text{for any prime } p \mid N. \end{cases}$$

Moreover, E' has filtration 2 unless $(a_{p_1}(f),\dots,a_{p_t}(f))=(-1,\dots,-1)$ when it has filtration $\ell+1$. The constant term of its Fourier expansion at infinity is given by

$$a_0(E')=\begin{cases}(-1)^{t+1}\dfrac{(p_1-1)\cdots(p_t-1)}{24} & \text{if } (a_{p_1}(f),\dots,a_{p_t}(f))=(+1,\dots,+1),\\ 0 & \text{otherwise.}\end{cases}$$

Proof. By the commutativity of the Hecke algebra, E' is a well-defined modular form over $\bar{\mathbf{F}}_\ell$ of level N. Let r be a prime not dividing N. Since $T_r\bar{E}_2=(1+r)\bar{E}_2$, we obtain that $T_rE'=(1+r)E'$, as claimed.

Let $u\neq 1$ be an integer dividing N. We denote by $\bar{E}_{2,u}$ the reduction modulo ℓ of the classical characteristic-0 Eisenstein series $E_{2,u}\in\mathcal{M}_2(\Gamma_0(u))$ defined by

$$E_{2,u}(\tau)=E_2(\tau)-uE_2(u\tau)=\frac{u-1}{24}+\sum_{n\geqslant 1}\left(\sum_{\substack{0<m|n\\ u\nmid m}}m\right)q^n. \tag{2.10}$$

If p is a prime divisor of N, then recall that we have

$$U_p\bar{E}_2=\bar{E}_{2,p}+p\bar{E}_2;$$
$$U_p\bar{E}_{2,u}=\begin{cases}\bar{E}_{2,p}+(1+p)\bar{E}_{2,u}-\bar{E}_{2,pu} & \text{if } p\nmid u,\\ \bar{E}_{2,p}+p\bar{E}_{2,u/p} & \text{if } p\mid u \text{ and } p\neq u,\\ \bar{E}_{2,p} & \text{if } p=u.\end{cases}$$

So let p be a prime divisor of N. We have

$$\begin{aligned}(a_pU_p-p\mathrm{Id})U_p\bar{E}_2&=((a_pU_p-p\mathrm{Id}))(\bar{E}_{2,p}+p\bar{E}_2)\\ &=p^2(a_p-1)\bar{E}_2+(a_p-p+pa_p)\bar{E}_{2,p}.\end{aligned}$$

If $a_p=+1$, then we obtain $(a_pU_p-p\mathrm{Id})U_p\bar{E}_2=\bar{E}_{2,p}=(a_pU_p-p\mathrm{Id})\bar{E}_2$, which is the desired result. On the other hand, if $a_p=-1$, then, by the assertion ((ii)(a)) proved above, we have $p\equiv -1\pmod{\ell}$ and the previous equality between forms over $\bar{\mathbf{F}}_\ell$ thus gives

$$(a_pU_p-p\mathrm{Id})U_p\bar{E}_2=-2\bar{E}_2+\bar{E}_{2,p}=-(a_pU_p-p\mathrm{Id})\bar{E}_2.$$

To complete the proof, it now remains to compute the filtration of E' and the first two terms of its Fourier expansion at infinity. Let $s=\sharp\{1\leqslant i\leqslant t\mid a_{p_i}(f)=+1\}$. If $0<s<t$, then we may assume, without loss of generality, that

$$N=p_1\cdots p_s\cdot p_{s+1}\cdots p_t\quad\text{with}\quad\begin{cases}U_{p_i}f=f & \text{for all } 1\leqslant i\leqslant s,\\ U_{p_i}f=-f & \text{for all } s+1\leqslant i\leqslant t.\end{cases}$$

By induction on t, we prove that

$$E'=\delta_{(s=0)}2^t\bar{E}_2+\sum_{\substack{(k,l)\in\{0,\dots,s\}\times\{0,\dots,t-s\}\\ (k,l)\neq(0,0)}}(-1)^{k+1}\sum_{\substack{1\leqslant i_1<\cdots<i_k\leqslant s\\ s+1\leqslant j_1<\cdots<j_l\leqslant t}}\bar{E}_{2,p_{i_1}\cdots p_{i_k}\cdot p_{j_1}\cdots p_{j_l}},$$

where

$$\delta_{(s=0)}=\begin{cases}1 & \text{if } s=0,\\ 0 & \text{otherwise,}\end{cases}$$

and the condition $1\leqslant i_1<\cdots<i_k\leqslant s$ or $s+1\leqslant j_1<\cdots<j_l\leqslant t$ is empty if $s=0$ or $s=t$, respectively. From this equality the assertion about the filtration follows. Moreover, an easy computation using Newton's binomial theorem and (2.10) proves the assertions about the first two Fourier coefficients. □

Let us now complete the proof of Theorem 2.6. According to (2.8) and the previous proposition, we have

$$a_n(\bar{f}) = a_n(E') \quad \text{for all prime-to-}\ell \text{ integers } n,$$

where $\bar{f}$ denotes the modular form over $\bar{\mathbf{F}}_\ell$ obtained by reduction of f modulo λ. Since $\ell \geqslant 5 > k+1 = 3$, Katz's theory [**12**, Corollary (3)] actually shows that $\bar{f} = E'$. Thus, E' has filtration 2 and we cannot have $(a_{p_1}(f), \dots, a_{p_t}(f)) = (-1, \dots, -1)$. Moreover, the constant term of E' at infinity must vanish and when $(a_{p_1}(f), \dots, a_{p_t}(f)) = (+1, \dots, +1)$, this gives the congruence stated in the theorem.

2.6. *Proof of Theorem* 2.7

Assume $\bar{\rho}$ to be reducible with $\ell \nmid N$ and $\ell + 1 \geqslant k$. As in § 2.4, we have

$$\bar{\rho}^{ss} \simeq \bar{\nu} \oplus \bar{\nu}^{-1}\bar{\chi}_\ell, \tag{2.11}$$

where $\bar{\nu}$ is a character of conductor $\mathfrak{c}$ such that $N(\bar{\rho}^{ss}) = \mathfrak{c}^2 \mid N$. So, in particular, we have $\mathfrak{c} \mid c$.

If $\mathfrak{c} \neq c$, then we necessarily are in a degenerate case as described in § 1.2, with $e_p = 2$ at some prime divisor p of c. Therefore, $v_p(N) = 2$ and, by Proposition 1.1, we have $p \equiv \pm 1 \pmod{\ell}$.

We can thus assume, from now on, that $\mathfrak{c} = c$. Let us denote by ν the Teichmüller lift of $\bar{\nu}$, viewed as a primitive Dirichlet character modulo c.

Let $1 \leqslant i \leqslant t$. Comparing the restriction to a decomposition group at p_i of $\bar{\rho}^{ss}$ with the local representation given by (1.1), we obtain the following equality between sets of characters of G_{p_i}:

$$\{\bar{\nu}, \bar{\nu}^{-1}\bar{\chi}_\ell\} = \{\lambda(a_{p_i})\bar{\chi}_\ell, \lambda(a_{p_i})\},$$

where $\lambda(a_{p_i})$ is the quadratic character defined in § 1.1.

Assume that, for some $1 \leqslant i \leqslant t$, we have $\bar{\nu} = \lambda(a_{p_i})\bar{\chi}_\ell$ (again, as characters of G_{p_i}). Since $a_{p_i} = \pm 1$, it then follows that ℓ divides the norm of $\nu(p_i)^2 - p_i^2$.

From now on, we will therefore assume that $\bar{\nu} = \lambda(a_{p_i})$ for every $1 \leqslant i \leqslant t$. It then follows that $\bar{\nu}(p_i) = a_{p_i} \pmod{\ell}$. Since $\mathfrak{c} > 1$, we may consider the Eisenstein series

$$E(\tau) = \sum_{n \geqslant 1} \sigma_1^\nu(n) q^n \in \mathcal{M}_2(\Gamma_0(\mathfrak{c}^2))$$

introduced in § 2.3. This is an eigenform for all the Hecke operators at level $\Gamma_0(\mathfrak{c}^2)$.

2.6.1. *The Eisenstein series* E'

Put

$$E'(\tau) = \left[\prod_{i=1}^{t} (U_{p_i} - p_i \nu^{-1}(p_i)\mathrm{Id})\right] E(p_1 \cdots p_t \tau) \in \mathcal{M}_2(\Gamma_0(N)),$$

where U_{p_i} denotes the p_ith Hecke operator acting on $\mathcal{M}_2(\Gamma_0(N))$. In expanded form, we have

$$E'(\tau) = E + \sum_{j=1}^{t} (-1)^j \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant t} p_{i_1} \cdots p_{i_j} \nu^{-1}(p_{i_1} \cdots p_{i_j}) E(p_{i_1} \cdots p_{i_j} \tau). \tag{2.12}$$

As before, let us denote by L the field generated by the values of ν and by M the compositum of L and K. The following lemma is crucial.

LEMMA 2.11. *The Eisenstein series E' is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$. Moreover, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that*

$$a_r \equiv a_r(E') \pmod{\mathcal{L}} \quad \textit{for all primes } r \neq \ell.$$

Proof. The Eisenstein series E' is clearly normalized and, since ℓ is co-prime to N, this is an eigenfunction for the T_ℓ-operator acting on $\mathcal{M}_2(\Gamma_0(N))$. By isomorphism (2.11) and assumption $\bar{\nu}(p_i) = a_{p_i} \pmod{\ell}$, $1 \leqslant i \leqslant t$, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that

$$\nu(r) + \nu^{-1}(r)r \equiv a_r \pmod{\mathcal{L}} \quad \text{for every prime } r \nmid \ell N$$

and $\nu(p_i) \equiv a_{p_i} \pmod{\mathcal{L}}$ for any $1 \leqslant i \leqslant t$. Let r be a prime. If r does not divide ℓN, then E' is a T_r-eigenfunction with eigenvalue $a_r(E') = \nu(r) + \nu^{-1}(r)r$, which is congruent to a_r modulo $\mathcal{L}$. Otherwise, if r divides c (and thus N), then E' is a U_r-eigenfunction with corresponding eigenvalue $0 = a_r$. Finally, if $r = p_j \in \{p_1, \dots, p_t\}$, then we have

$$(U_{p_j}E')(\tau) = \left(\prod_{\substack{i=1 \\ i \neq j}}^{t} (U_{p_i} - p_i\nu^{-1}(p_i)\mathrm{Id}) \right) \cdot (U_{p_j}^2 - p_j\nu^{-1}(p_j)U_{p_j})E(p_1 \cdots p_t\tau).$$

Besides, according to [**5**, Proposition 5.2.2], we have

$$\begin{aligned}
&(U_{p_j}^2 - p_j\nu^{-1}(p_j)U_{p_j})E(p_1 \cdots p_t\tau) \\
&\quad = (\nu(p_j) + \nu^{-1}(p_j)p_j)E(\widehat{p_1 \cdots p_t}\tau) - p_jE(p_1 \cdots p_t\tau) - p_j\nu^{-1}(p_j)E(\widehat{p_1 \cdots p_t}\tau) \\
&\quad = \nu(p_j)(U_{p_j} - p_j\nu^{-1}(p_j)\mathrm{Id})E(p_1 \cdots p_t\tau),
\end{aligned}$$

where $\widehat{p_1 \cdots p_t} = \prod_{\substack{i=1 \\ i \neq j}}^{t} p_i$. This equality proves that E' is a U_{p_j}-eigenfunction with corresponding eigenvalue $\nu(p_j)$ and the congruence $\nu(p_j) \equiv a_{p_j} \pmod{\mathcal{L}}$ eventually completes the proof of the lemma. □

2.6.2. *Constant term at $1/\mathfrak{c}$ and end of the proof of Theorem* 2.7 Since E' vanishes at ∞, we compute its constant term at another specific cusp, where it is non-vanishing, namely $1/\mathfrak{c}$. Put

$$\gamma = \begin{pmatrix} 1 & 0 \\ \mathfrak{c} & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}).$$

We postpone the proof of the following proposition to § 2.6.3.

Proposition 2.12. *The constant term of the Fourier expansion of $E'|_2\gamma$ is the non-zero algebraic number in $\mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})$:*

$$\Upsilon' = -\nu(-1)\left(\frac{\mathfrak{c}}{c_0}\right)^2 \frac{W((\nu^2)_0)}{W(\nu)} \frac{B_{2,(\nu^2)_0^{-1}}}{4} \left(\prod_{i=1}^{t} (1 - p_i^{-1}) \right) \cdot \left(\prod_{p \mid \mathfrak{c}} (1 - (\nu^2)_0(p)p^{-2}) \right),$$

where the second product runs over the primes and $(\nu^2)_0$ is the primitive Dirichlet character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$.

Using this proposition, we now complete the proof of Theorem 2.7. Let Θ be the Katz's operator on modular forms over $\bar{\mathbf{F}}_\ell$, whose action on q-expansions is given by $q(d/dq)$ (denoted by $A\theta$ in [**12**]). Assume $\ell > k + 1 = 3$. Lemma 2.11 implies that $\Theta(\bar{f}) = \Theta(\bar{E})$, where $\bar{f}$ and $\overline{E'}$ are the modular forms over $\bar{\mathbf{F}}_\ell$ obtained by reduction modulo $\mathcal{L}$ of f and E', respectively. Moreover, Katz has proved that if $\ell > 3$, then Θ is injective [**12**, Corollary (3)]. Under this assumption, it thus follows that the Eisenstein series E' becomes cuspidal after reduction.

Put $\epsilon = (\nu^2)_0^{-1}$. By Proposition 2.12 and using the assumption $\mathfrak{c} = c$, we therefore have that ℓ divides the numerator of the norm of

$$\Upsilon' = \pm \left(\frac{c}{c_0}\right)^2 \frac{W(\epsilon^{-1})}{W(\nu)} \frac{B_{2,\epsilon}}{4} \left(\prod_{i=1}^{t}(1-p_i^{-1})\right) \cdot \left(\prod_{p|c}(1-\epsilon^{-1}(p)p^{-2})\right).$$

By Lemma 2.1, the prime divisors of the norm of $W(\epsilon^{-1})/W(\nu)$ divide N and therefore are co-prime to ℓ. The same obviously holds for c/c_0. It thus follows that either $p_i \equiv 1 \pmod{\ell}$ for some $1 \leqslant i \leqslant t$, or ℓ divides the norm of either $p^2 - \epsilon^{-1}(p)$ for some p dividing c, or the norm of the numerator of $B_{2,\epsilon}/4$. This completes the proof of Theorem 2.7.

2.6.3. *Proof of Proposition* 2.12 Let us first introduce notation as in the proof of Proposition 2.8. Put

$$G = \frac{C_2 W(\nu)}{\mathfrak{c}^2} E, \quad \text{where } C_2 = -4\pi^2,$$

and similarly

$$G' = \frac{C_2 W(\nu)}{\mathfrak{c}^2} E'.$$

For simplicity, we shall denote by $\underline{i}$ the elements of

$$\mathcal{N} = \{(i_1, \ldots, i_j) \text{ such that } j \in \{1, \ldots, t\} \text{ and } 1 \leqslant i_1 < \cdots < i_j \leqslant t\}.$$

If $\underline{i} = (i_1, \ldots, i_j) \in \mathcal{N}$, we put

$$p_{\underline{i}} = p_{i_1} \cdots p_{i_j} \quad \text{and} \quad a_{\underline{i}} = a_{p_{i_1}} \cdots a_{p_{i_j}}.$$

Let $v = \overline{(c_v, d_v)} \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$. Following [5, § 4.6], define

$$G_2^v(\tau) = \frac{1}{(c_v\tau + d_v)^2} + \frac{1}{\mathfrak{c}^4} \sum_{d \in \mathbf{Z}}{}' \frac{1}{((c_v\tau + d_v)/\mathfrak{c}^2 - d)^2} + \frac{1}{\mathfrak{c}^4} \sum_{c \neq 0} \sum_{d \in \mathbf{Z}} \frac{1}{((c_v\tau + d_v)/\mathfrak{c}^2 - c\tau - d)^2}, \tag{2.13}$$

where the primed summation notation means to sum over non-zero integers. For any $\underline{i} \in \mathcal{N}$ and any $v \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$, put

$$G_2^{v,p_{\underline{i}}}(\tau) = G_2^v(p_{\underline{i}}\tau) \quad \text{and} \quad G^{p_{\underline{i}}}(\tau) = G(p_{\underline{i}}\tau).$$

According to [5, § 4.2] and the definition of E (cf. § 2.3), we have

$$G = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij) G_2^{\overline{(i\mathfrak{c}, j+l\mathfrak{c})}}$$

and therefore

$$G^{p_{\underline{i}}} = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij) G_2^{\overline{(i\mathfrak{c}, j+l\mathfrak{c})}, p_{\underline{i}}}. \tag{2.14}$$

Lemma 2.13. *Let $v = \overline{(c_v, d_v)} \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$. The constant term of $G_2^{v,p_{\underline{i}}}|_2\gamma$ is*

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v \mathfrak{c}}) \left(\frac{1}{p_{\underline{i}}}\right)^2 \zeta^{\overline{d_v/p_{\underline{i}}}}(2),$$

where the bar means reduction modulo $\mathfrak{c}^2$,

$$\vartheta(\bar{n}) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{\mathfrak{c}^2}, \\ 0 & \text{otherwise,} \end{cases} \qquad \zeta^{\bar{n}}(2) = \sum_{m \equiv n \pmod{\mathfrak{c}^2}}{}' \frac{1}{m^2},$$

and the primed summation notation means to sum over non-zero integers.

Proof. We first compute $G_2^{v,p_{\underline{i}}}|_2\gamma$ using (2.13). We find

$$(G_2^{v,p_{\underline{i}}}|_2\gamma)(\tau) = \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1))^2} + \sum_{d\in\mathbf{Z}}{}' \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1) - \mathfrak{c}^2 d(\mathfrak{c}\tau+1))^2} + \sum_{c\neq 0}\sum_{d\in\mathbf{Z}} \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1) - \mathfrak{c}^2(cp_{\underline{i}}\tau + d(\mathfrak{c}\tau+1)))^2}.$$

In other words, we have $(G_2^{v,p_{\underline{i}}}|_2\gamma)(\tau) = A + B$, where

$$A = \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c})\tau + d_v)^2} + \sum_{d\in\mathbf{Z}}{}' \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c} - \mathfrak{c}^2 d\mathfrak{c})\tau + d_v - \mathfrak{c}^2 d)^2}$$

and

$$B = \sum_{c\neq 0}\sum_{d\in\mathbf{Z}} \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c} - \mathfrak{c}^2(cp_{\underline{i}} + d\mathfrak{c}))\tau + d_v - \mathfrak{c}^2 d)^2}.$$

Since $\gcd(p_{\underline{i}}, \mathfrak{c}) = 1$, we may assume, without loss of generality, that $0 \leqslant c_v p_{\underline{i}} + d_v\mathfrak{c} < \mathfrak{c}^2$. Therefore, the constant term of A is given by

$$\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\frac{1}{d_v^2}$$

and the one of B by

$$\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\neq 0}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0}} \frac{1}{(d_v - \mathfrak{c}^2 d)^2}.$$

Therefore, the constant term of $G_2^{v,p_{\underline{i}}}|_2\gamma$ is

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\in\mathbf{Z}}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0}} \frac{1}{(d_v - \mathfrak{c}^2 d)^2}.$$

Note that if $\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}}) = 1$, then $d_v \not\equiv 0 \pmod{\mathfrak{c}^2}$ since v is of order $\mathfrak{c}^2$. A change of variable yields

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\in\mathbf{Z}}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0 \\ (c,d)\equiv v \ (\mathfrak{c}^2)}} \frac{1}{d^2}$$

and thus

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{\substack{d\neq 0 \\ d\equiv d_v \ (\mathfrak{c}^2) \\ p_{\underline{i}}|d}} \frac{1}{d^2} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{\substack{m\neq 0 \\ m\equiv d_v/p_{\underline{i}} \ (\mathfrak{c}^2)}} \frac{1}{(p_{\underline{i}} m)^2}.$$

Finally, we obtain $\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})/p_{\underline{i}}^2 \cdot \zeta^{\overline{d_v/p_{\underline{i}}}}(2)$, as asserted. □

Using this lemma and formula (2.14), we are now able to compute the constant term of $G^{p_{\underline{i}}}|_2\gamma$.

LEMMA 2.14. *The constant term of* $G^{p_{\underline{i}}}|_2\gamma$ *is*

$$\Upsilon_{\underline{i}} = \nu(p_{\underline{i}})\frac{1}{p_{\underline{i}}^2}\cdot\Upsilon_0, \quad \text{with } \Upsilon_0 = -\nu(-1)W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}),$$

where $(\nu^2)_0$ *is the primitive Dirichlet character associated to* ν^2 *of modulus* $c_0 \mid \mathfrak{c}$.

Proof. The proof of this lemma is quite similar to the proof of Proposition 2.8. According to (2.14), we have

$$\Upsilon_{\underline{i}} = \frac{1}{2}\sum_{i,j,l=0}^{\mathfrak{c}-1}\nu(ij)\Upsilon_{\overline{(i\mathfrak{c},j+l\mathfrak{c})},\underline{i}}$$

and thus, by Lemma 2.13,

$$\Upsilon_{\underline{i}} = \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\sum_{i,j,l=0}^{\mathfrak{c}-1}\nu(ij)\vartheta(\overline{i\mathfrak{c}p_{\underline{i}}+\mathfrak{c}(j+l\mathfrak{c})})\zeta^{\overline{d_v/p_{\underline{i}}}}(2).$$

This yields

$$\begin{aligned}\Upsilon_{\underline{i}} &= \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu\left(-\frac{j^2}{p_{\underline{i}}}\right)\zeta^{\overline{d_v/p_{\underline{i}}}}(2)\\ &= \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu((j^2/p_{\underline{i}})^2)\sum_{m\equiv(j+l\mathfrak{c})/p_{\underline{i}}\ (\mathfrak{c}^2)}{}'\frac{1}{m^2}\\ &= \frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)L(2,\nu^2).\end{aligned}$$

Let $(\nu^2)_0$ be the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. We have

$$L(2,\nu^2) = L(2,(\nu^2)_0)\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}).$$

Applying Proposition 2.3 to $\psi = (\nu^2)_0$ and $m = k$, we obtain

$$L(2,(\nu^2)_0) = -W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4} \neq 0$$

and thus

$$\Upsilon_{\underline{i}} = -\frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}),$$

as claimed. □

Let us now complete the proof of Proposition 2.12. With the notation introduced at the beginning of this paragraph and Equation (2.12), we have

$$G'|_2\gamma = G|_2\gamma + \sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})G^{p_{\underline{i}}}|_2\gamma.$$

Therefore, according to Proposition 2.8 and Lemma 2.14, the constant term of $G'|_2\gamma$ is

$$\Upsilon_0 + \sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})\Upsilon_{\underline{i}} = \Upsilon_0\left(1+\sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})\nu(p_{\underline{i}})\frac{1}{p_{\underline{i}}^2}\right) = \Upsilon_0\prod_{i=1}^{t}(1-p_i^{-1}),$$

where $(\nu^2)_0$ is the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. Proposition 2.12 now follows from the normalization $E' = (\mathfrak{c}^2/(C_2 W(\nu)))G'$.

3. *Dihedral representations*

3.1. *Preliminaries: twisting and CM forms*

Let M be an integer, $F(\tau) = \sum_{n\geqslant 1} a_n(F)q^n \in \mathcal{S}_k(\Gamma_0(M))$ and ψ be a Dirichlet character of modulus $f \geqslant 1$. Define

$$(F \otimes \psi)(\tau) = \sum_{n\geqslant 1} a_n(F)\psi(n)q^n.$$

The following result is a special case of [**30**, Proposition 3.64].

LEMMA 3.1. *With the notation above, assume ψ to be a quadratic primitive Dirichlet character. Then $F \otimes \psi$ belongs to $\mathcal{S}_k(\Gamma_0(\mathrm{lcm}(M, f^2)))$. Moreover, if F is a normalized Hecke eigenform for the Hecke operators $\{T_p\}_{p\nmid M}$, then $F \otimes \psi$ is a normalized Hecke eigenform for the Hecke operators $\{T_p\}_{p\nmid fM}$ with corresponding eigenvalues $\{a_p(F)\psi(p)\}_{p\nmid fM}$.*

We take the following definition for CM forms [**24**].

DEFINITION 1. Assume that ψ is not the trivial character. The form F has complex multiplication (or, F is a CM form) by ψ if $a_p(F) = a_p(F)\psi(p)$ for all p in a set of primes of density 1.

3.2. *Statement of the result*

Recall that

$$\mathbf{P}(\bar{\rho}_{f,\lambda}) : G_{\mathbf{Q}} \xrightarrow{\bar{\rho}_{f,\lambda}} \mathrm{GL}(2, \mathbf{F}_\lambda) \longrightarrow \mathrm{PGL}(2, \mathbf{F}_\lambda),$$

where $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, and put $\mathbf{P}(\bar{G}_\lambda) = \mathbf{P}(\bar{\rho}_{f,\lambda})(G_{\mathbf{Q}})$.

The following result is a generalization to arbitrary weights and fields of coefficients of a theorem on the surjectivity of Galois representations attached to elliptic curves over $\mathbf{Q}$ independently proved by Kraus [**14**] and Cojocaru [**4**]. In particular, it implies that, in the case of dihedral projective image, ℓ is explicitly bounded in terms of k and N.

THEOREM 3.2. *Assume that $\mathbf{P}(\bar{G}_\lambda)$ is dihedral. If f does not have complex multiplication, then we have*

$$\ell \leqslant (2(8kN^2(1 + \log\log N))^{(k-1)/2})^{[K:\mathbf{Q}]}.$$

Besides, if N is square-free, then either $\ell \mid N$, or $\ell \leqslant k$, or $\ell = 2k - 1$.

REMARK 1. (i) The integer $[K : \mathbf{Q}]$ is bounded from above by the dimension $g_0^\sharp(k, N)$ of the new subspace of $\mathcal{S}_k(\Gamma_0(N))$. A closed formula in terms of k and N for $g_0^\sharp(k, N)$ as well as asymptotic estimates can be found in [**17**].

(ii) When $N = 1$, the result goes back to Ribet (see the proof of (ii) p. 264 and the remark after [**23**, Corollary 4.5]). Moreover, our argument for the case of arbitrary square-free level is a combination of tricks from [**25**, **26**].

(iii) A newform of square-free level and trivial Nebentypus is automatically non-CM (see, for example, [**33**, § 4]).

3.3. *Proof of Theorem* 3.2

Assume $\ell \nmid N$ and $\mathbf{P}(\bar{G}_\lambda)$ dihedral. Then $\mathbf{P}(\bar{G}_\lambda)$ is an extension of $\{\pm 1\}$ by a cyclic group C, and every element of $\bar{G}_\lambda$ that does not map to C has trace 0. Hence, we may consider the following quadratic character:

$$\epsilon_\lambda : G_{\mathbf{Q}} \overset{\mathbf{P}(\bar{\rho}_{f,\lambda})}{\longrightarrow} \mathbf{P}(\bar{G}_\lambda) \longrightarrow \{\pm 1\}.$$

Let L_λ be the number field cut out by $\mathbf{P}(\bar{\rho}_{f,\lambda})$ and $K_\lambda/\mathbf{Q}$ its quadratic subextension fixed by the kernel of ϵ_λ. The extension $L_\lambda/\mathbf{Q}$ has Galois group isomorphic to $\mathbf{P}(\bar{G}_\lambda)$ while $C \simeq \mathrm{Gal}(L_\lambda/K_\lambda)$. Clearly, ϵ_λ is unramified outside ℓN. The following proposition describes more precisely the ramification set of ϵ_λ.

PROPOSITION 3.3. *Assume* $2 < \ell \nmid N$.

(i) *Let* $p \neq \ell$ *be a ramified prime for* ϵ_λ. *Then* $p^2 \mid N$.
(ii) *Assume* $\ell > k$ *and*
  (a) *either* f *is ordinary at* λ *and* $\ell \neq 2k-1$;
  (b) *or* f *is not ordinary at* λ *and* $\ell \neq 2k-3$.

Then ϵ_λ *is unramified at* ℓ.

Proof. Let p be a prime dividing N exactly once. By § 1.1, we know that the inertia subgroup I_p at p acts unipotently in $\bar{\rho}$. Since $\bar{G}_\lambda$ has prime-to-ℓ order, it follows that I_p acts trivially. So $\bar{\rho}$ and, hence, ϵ_λ are unramified at p. This proves the first part of the proposition.

Assume now $\ell > k$. Let I_ℓ be the inertia group of a decomposition subgroup at ℓ and recall that $\ell \nmid N$. We prove that ϵ_λ is unramified at ℓ under conditions (a) and (b) in turn.

(a) Assume that f is ordinary at λ and $\ell \neq 2k-1$. By § 1.3, we have

$$\bar{\rho}_{|I_\ell} \simeq \begin{pmatrix} \bar{\chi}_\ell^{k-1} & \star \\ 0 & 1 \end{pmatrix}.$$

But $\bar{G}_\lambda$ has prime-to-ℓ order and therefore $\star = 0$. In particular, $\mathbf{P}(\bar{\rho}_{f,\lambda})(I_\ell)$ is isomorphic to the image of $\bar{\chi}_\ell^{k-1}$ which is, by Lemma 1.2, cyclic of order $(\ell-1)/\gcd(\ell-1, k-1) > 2$. Therefore, it has to be included in C, and hence ϵ_λ is unramified at ℓ.

(b) Assume that f is not ordinary at λ and $\ell \neq 2k-3$. By § 1.3, $\mathbf{P}(\bar{\rho}_{f,\lambda})(I_\ell)$ is isomorphic to the image of I_ℓ under $\psi^{(\ell-1)(k-1)}$, where ψ is a fundamental character of level 2. By the assumption $\ell \neq 2k-3$ and Lemma 1.2, it is therefore cyclic of order $(\ell+1)/\gcd(\ell+1, k-1) > 2$. We conclude as before. □

Assume N to be square-free and $\ell > k$. Then, by the above proposition, K_λ is the unique quadratic extension of $\mathbf{Q}$ ramified at ℓ only and $\ell \in \{2k-1, 2k-3\}$. The case $\ell = 2k-3$, however, does not occur. This is proved in [**6**, Lemma 3.2]. Hence, Theorem 3.2 in the square-free level case.

Assume now that N is any integer not divisible by ℓ, and that $\ell > k$ satisfies $\ell \neq 2k-1$ and $\ell \neq 2k-3$. We may identify ϵ_λ with a Dirichlet character. Let us denote by $\mathfrak{c}$ its conductor. It is co-prime to ℓ by the above proposition. We then have $\mathfrak{c} = |D_{K_\lambda}|$, where D_{K_λ} is the fundamental discriminant of the quadratic field K_λ fixed by the kernel of ϵ_λ (see [**22**, VII. § 11]). In particular, if $K_\lambda = \mathbf{Q}(\sqrt{D_0})$ with D_0 square-free, then $\mathfrak{c} = D_0$ or $4D_0$ depending on whether

$D_0 \equiv 1 \pmod 4$ or not. Moreover, if $\ell > 2k-1$, then by the proposition above, $\mathfrak{c}^2 \mid 2^4 N$. Put $g = f \otimes \epsilon_\lambda$. By the Lemma 3.1, $g \in \mathcal{S}_k(\Gamma_0(2^4 N))$ and, for any prime $p \nmid 2N$, g is an eigenform for the T_p Hecke operator with corresponding eigenvalue $a_p(g) = a_p \epsilon_\lambda(p)$. Let $D_0' = \varepsilon \prod_{3 \leqslant p \mid N} p$ be the product of all odd primes dividing N with a sign $\varepsilon \in \{\pm 1\}$ chosen so that $D_0' \equiv 3 \pmod 4$. Then $4D_0'$ is a fundamental discriminant and the Kronecker symbol $\psi = (4D_0'/\cdot)$ is a primitive quadratic Dirichlet character of modulus $4D_0'$ (see [**3**, Theorem 2.2.15]) precisely ramified at the primes dividing $2N$. Put

$$\tilde{f} = f \otimes \psi \quad \text{and} \quad \tilde{g} = g \otimes \psi.$$

Since $(4D_0')^2 \mid 2^4 N^2$, it follows from Lemma 3.1 that $\tilde{f}, \tilde{g} \in \mathcal{S}_k(\Gamma_0(2^4 N^2))$ and, for any integer n, we have

$$\begin{cases} a_n(\tilde{f}) = a_n \psi(n), \\ a_n(\tilde{g}) = a_n \epsilon_\lambda(n) \psi(n). \end{cases} \tag{3.1}$$

Since f is assumed to be non-CM (in the sense of Definition 1), we have $\tilde{f} \neq \tilde{g}$ and by Murty [**21**, Theorem 1], there exists an integer

$$n \leqslant \frac{4k}{3} N^2 \prod_{p \mid 2N} \left(1 + \frac{1}{p}\right) \leqslant 2kN^2 \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \tag{3.2}$$

such that $a_n(\tilde{f}) \neq a_n(\tilde{g})$. According to (3.1), it follows that we have

$$\psi(n) \neq 0, \quad a_n \neq 0 \text{ and } \epsilon_\lambda(n) = -1.$$

From the condition $\epsilon_\lambda(n) = -1$, we deduce that there exists a prime divisor q of n together with an odd integer t such that $q^t \mid n$, but $q^{t+1} \nmid n$ and $\epsilon_\lambda(q) = -1$. If $q = \ell$, then we are done in bounding ℓ in terms of k and N. Assume therefore $q \neq \ell$. The multiplicativity of the Fourier coefficients of f gives that $a_{q^t} \mid a_n$, and hence (since t is odd) that $a_q \neq 0$. Besides, since $\epsilon_\lambda(q) = -1$, the image under $\bar{\rho}_{f,\lambda}$ of a Frobenius at q has trace 0 modulo λ. In other words, ℓ divides the norm of the non-zero algebraic integer a_q. Applying Deligne's estimate on the Fourier coefficients of f and its Galois conjugates by $\bar{\mathbf{Q}}$-automorphisms, we obtain that

$$\ell \leqslant \mathrm{N}_{K/\mathbf{Q}}(a_q) = \prod_{\sigma : K \hookrightarrow \mathbf{C}} |\sigma(a_q)| \leqslant (2q^{(k-1)/2})^{[K:\mathbf{Q}]}. \tag{3.3}$$

Besides, using [**14**, Lemma 2] and inequality (3.2), we obtain the following estimate for q:

$$q \leqslant 8kN^2(1 + \log\log N). \tag{3.4}$$

The theorem follows from (3.3) and (3.4).

4. *Projective image isomorphic to A_4, S_4 or A_5*

The following result is proved in a different way in [**25**].

THEOREM 4.1. *If $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5, then either $\ell \mid N$ or $\ell \leqslant 4k-3$.*

Proof. Assume that $\ell \nmid N$ and $\ell > k$. Then, by § 1.3, $\mathbf{P}(\bar{G}_\lambda)$ has a cyclic subgroup given the image of inertia at ℓ. In the case of ordinariness, this cyclic subgroup is isomorphic to the image of $\bar{\chi}_\ell^{k-1}$ which has order > 5 if $\ell > 4k-3$ by Lemma 1.2. Else, if f is not ordinary at λ, then it has order $(\ell+1)/\gcd(\ell+1, k-1)$ which is also > 5 if $\ell > 4k-3$.

In any case, if $\ell > 4k-3$, then $\mathbf{P}(\bar{G}_\lambda)$ has an element of order > 5. This rules out the possibility for $\mathbf{P}(\bar{G}_\lambda)$ to be isomorphic to A_4, S_4 or A_5. □

REMARK 2. In [8, Theorem 1.4(a)], Ghate and Parent give an explicit upper-bound in the weight 2 case and projective image isomorphic to A_4, S_4 or A_5, depending only (and necessarily) on $[K : \mathbf{Q}]$, but *not* on the level.

5. *Numerical examples*

In this section, we give some examples illustrating the theorems of the paper. All the computations were performed on SAGE [31].

5.1. *Reducible representations*

Before dealing with examples, let us first recall that, for the representations $\bar{\rho}_{f,\lambda}$, irreducibility is equivalent to absolute irreducibility.

5.1.1. *Square level case* Fix $(k, N) = (6, 81)$. The new subspace in $\mathcal{S}_6(\Gamma_0(81))$ is eighteen-dimensional and splits into five Galois conjugacy classes labeled 81.6a,...,81.6e in SAGE [31]. According to Theorem 2.5, the prime ideals λ such that $\bar{\rho}_{f,\lambda}$ is reducible for some newform $f \in \mathcal{S}_6(\Gamma_0(81))$ have residue characteristic ℓ in $\{2, 3, 5, 7, 43, 1171\}$. Let us first show that 2, 3, 7, 43 and 1171 are indeed the residue characteristics of some prime ideals λ, for which $\bar{\rho}_{f,\lambda}$ is reducible for the specific (up to Galois conjugacy) modular form f labeled 81.6c. We have

$$f(\tau) = q + \alpha q^2 + (\alpha^2 - 32)q^4 + (-\tfrac{1}{4}\alpha^3 - \tfrac{9}{4}\alpha^2 + \tfrac{25}{2}\alpha + 54)q^5 + O(q^5),$$

where α is a root of $X^4 + 3X^3 - 84X^2 - 72X + 792$.

Let us denote by K the number field generated by α. We call ν the primitive Dirichlet character modulo 9 sending 2 to ζ_3, where ζ_3 is a primitive third root of unity and $L = \mathbf{Q}(\zeta_3)$. Since ν has order 3, we have $\epsilon = \nu$ with the notation of Theorem 2.5. Moreover, we have $B_{6,\nu}/12 = (751\zeta_3 + 1172)/3$, which has norm $3^{-1} \cdot 7 \cdot 43 \cdot 1171$.

Then we show more precisely that, for each $\ell \in \{2, 3, 7, 43, 1171\}$, there are prime ideals λ_ℓ and $\mathfrak{p}_\ell$ above ℓ in $\mathcal{O}$ and $\mathbf{Z}[\zeta_3]$, respectively, such that $\bar{\rho}^{ss}_{f,\lambda_\ell} \simeq \bar{\rho}_{E,\mathfrak{p}_\ell}$, where E is the following Eisenstein series:

$$E(\tau) = \sum_{n \geqslant 1} \sigma_5^\nu(n)q^n = q - (31\zeta_3 + 32)q^2 + (1023\zeta_3 + 31)q^4 + (3124\zeta_3 - 1)q^5 + O(q^5).$$

Such an isomorphism is proved to hold by checking that, for all integers n up to the Sturm bound (which, here, equals 54), we have a congruence

$$a_n \equiv a_n(E) \pmod{\mathcal{L}_\ell},$$

for some prime ideal $\mathcal{L}_\ell$ above ℓ in the integer ring of the compositum KL. For instance, if $\ell = 43$, we can take

$$\mathcal{L}_{43} = (43, \alpha + \zeta_3 - 6).$$

Therefore, we have $\bar{\rho}^{ss}_{f,\lambda_\ell} \simeq \bar{\nu}_\ell \oplus \bar{\nu}_\ell^{-1}\bar{\chi}_\ell^5$ where

$$\bar{\nu}_\ell \ : G_{\mathbf{Q}} \twoheadrightarrow (\mathbf{Z}/9\mathbf{Z})^\times \xrightarrow{\nu} \mathbf{Z}[\zeta_3] \twoheadrightarrow \mathbf{Z}[\zeta_3]/\mathfrak{p}_\ell$$

is ν modulo $\mathfrak{p}_\ell$ viewed as a character of $G_{\mathbf{Q}}$. For each ℓ as above, the corresponding ideals λ_ℓ and $\mathfrak{p}_\ell$ are listed in Table 2 (as given in SAGE).

Let us now see what happens for the remaining prime, namely $\ell = 5$. For the specific newform above with coefficients field K, we have $5\mathcal{O} = \lambda_5\lambda_5'$, where $\lambda_5 = (5, \alpha + 4)$ and $\lambda_5' = (5, \alpha^3 + 4\alpha^2 + 3)$. Then λ_5 and λ_5' have inertia degree 1 and 3, respectively. Besides, if Frob_2 denotes a Frobenius at 2, the characteristic polynomial of $\bar{\rho}_{f,\lambda_5}(\mathrm{Frob}_2)$ and $\bar{\rho}_{f,\lambda_5'}(\mathrm{Frob}_2)$ is $X^2 - \alpha X + 2^5$.

TABLE 2. *Congruence primes between f and E.*

ℓ	λ_ℓ	$\mathfrak{p}_\ell$
2	$(2, \alpha^3/36 + \alpha^2/4 - 7\alpha/6 - 7)$	(2)
3	$(3, -\alpha^3/36 + \alpha^2/12 + 7\alpha/6 - 7)$	$(2\zeta_3 + 1)$
7	$(7, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 + 2)$	$(3\zeta_3 + 1)$
43	$(43, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 - 20)$	$(7\zeta_3 + 6)$
1171	$(1171, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 - 586)$	$(39\zeta_3 + 25)$

TABLE 3. *Smallest prime $p \neq 3, 5$ and $\leqslant 100$ such that $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ acts irreducibly.*

f	$K = \mathbf{Q}(\alpha)$	λ	p
81.6a	$\alpha^2 + 3\alpha - 30 = 0$	$(-6\alpha + 25)$	2
		$(-6\alpha - 43)$	7
81.6b	$\alpha^2 - 3\alpha - 30 = 0$	$(-6\alpha - 25)$	2
		$(-6\alpha + 43)$	7
81.6c	$\alpha^4 + 3\alpha^3 - 84\alpha^2 - 72\alpha + 792 = 0$	$(5, \alpha + 4)$	2
		$(5, \alpha^3 + 4\alpha^2 + 3)$	2
81.6d	$\alpha^4 - 3\alpha^3 - 84\alpha^2 + 72\alpha + 792 = 0$	$(5, \alpha + 1)$	2
		$(5, \alpha^3 + \alpha^2 + 2)$	2
81.6e	$\alpha^6 - 171\alpha^4 + 7128\alpha^2 - 432 = 0$	$(5, \alpha^2 + 1)$	$\emptyset$
		$(5, \alpha^2 + 3\alpha + 3)$	7
		$(5, \alpha^2 + 2\alpha + 3)$	7

Such a polynomial being irreducible modulo λ_5 and λ_5' as one checks, we obtain that $\bar{\rho}_{f,\lambda_5}$ and $\bar{\rho}_{f,\lambda_5'}$ are both irreducible.

For each pair (f, λ), where f is a newform in $\mathcal{S}_6(\Gamma_0(81))$ and λ is a prime ideal in $\mathcal{O}$ above 5, we give in Table 3 the smallest prime number $p \neq 3, 5$ and $\leqslant 100$ for which the characteristic polynomial of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is irreducible.

Therefore, all the representations $\bar{\rho}_{f,\lambda}$ are irreducible unless perhaps if f is the form 81.6e and $\lambda = (5, \alpha^2 + 1)$. But this latter representation is also proved to be irreducible by noting that the eigenvalues of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_2)$ and $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_{19})$ in $\mathbf{F}_\lambda$ are $\{3\beta, 3\beta\}$ and $\{2\beta + 1, 3\beta + 1\}$, respectively, where β is the image of α in $\mathbf{F}_\lambda$ (since if it were reducible, we would have $\bar{\rho}_{f,\lambda}^{ss} \simeq \epsilon_1 \oplus \epsilon_2$, where both ϵ_1 and ϵ_2 factor through $(\mathbf{Z}/45\mathbf{Z})^\times$). This eventually proves the following proposition.

PROPOSITION 5.1. *There exists a newform $f \in \mathcal{S}_6(\Gamma_0(81))$ together with a prime ideal λ in $\mathcal{O}$ such that $\bar{\rho}_{f,\lambda}$ is reducible if and only if ℓ belongs to $\{2, 3, 7, 43, 1171\}$.*

5.1.2. *Square-free level case* Fix $(k, N) = (4, 11)$. The new subspace in $\mathcal{S}_4(\Gamma_0(11))$ is two-dimensional and generated by one Galois orbit labeled 11.4a in SAGE [31]. Let f be a representative of this Galois orbit. We have

$$f(\tau) = q + \alpha q^2 + (-4\alpha + 3)q^3 + (2\alpha - 6)q^4 + (8\alpha - 7)q^5 + O(q^5),$$

where α is a root of $X^2 - 2X - 2$. The field $K = \mathbf{Q}(\alpha)$ is the coefficients field of f. According to Theorem 2.6, if $\bar{\rho}_{f,\lambda}$ is reducible, then λ has residue characteristic ℓ in the set $\{2, 3, 5, 11, 61\}$.

For each prime ℓ in $\{2,3,5,11,61\}$, we give in Table 4 the smallest prime $p \neq 11, \ell$ and $p \leqslant 100$ such that the characteristic polynomial of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is irreducible.

Therefore, all such Galois representations are irreducible, except perhaps $\bar{\rho}_{f,(2\alpha-1)}$ and $\bar{\rho}_{f,(\alpha-9)}$. These latter representations turn out to be reducible and we have

$$\bar{\rho}^{ss}_{f,(2\alpha-1)} \simeq \bar{\chi}_{11} \oplus \bar{\chi}_{11}^2 \quad \text{and} \quad \bar{\rho}^{ss}_{f,(\alpha-9)} \simeq \mathbf{1} \oplus \bar{\chi}_{61}^3 \simeq \bar{\rho}_{E_4,61}.$$

This eventually proves the following proposition.

PROPOSITION 5.2. *There exists a newform $f \in \mathcal{S}_4(\Gamma_0(11))$ together with a prime ideal λ in $\mathcal{O}$ such that $\bar{\rho}_{f,\lambda}$ is reducible if and only if $\ell = 11$ or $\ell = 61$.*

5.2. *Dihedral representation*

In this section, we discuss an example of dihedral projective representation attached to some specific newform. The new subspace in $\mathcal{S}_2(\Gamma_0(1888))$ has dimension 58 and is split into 16 Galois orbits. Among them let us consider the newform f (up to Galois conjugacy) labeled 1888.10a whose first terms in its Fourier expansion at infinity are

$$f(\tau) = q + \tfrac{1}{2}\alpha q^3 + (-\tfrac{1}{16}\alpha^4 + \tfrac{3}{2}\alpha^2 - \alpha - 2)q^5 + O(q^6),$$

where α is a root of $X^5 + 6X^4 - 20X^3 - 128X^2 + 48X + 320$. The prime 5 is definitely smaller than the (huge) bound given in Theorem 3.2 and one proves that there is a mod 5 representation attached to f which has dihedral projective image. Namely, let us consider the prime ideal $\lambda = (5, \alpha/2)$ above 5 in $\mathcal{O}$. Then one checks that the representation $\bar{\rho}_{f,\lambda}$ is isomorphic to $\bar{\rho}_{\mathcal{E},5}$ where $\mathcal{E}$ is the rational CM elliptic curve of conductor 32 given by the equation $y^2 = x^3 - x$. Since $5 \equiv 1 \pmod 4$, one knows by the theory of complex multiplication that $\bar{\rho}_{\mathcal{E},5}$ has image included in the normalizer of a split Cartan subgroup of $\mathrm{GL}(2, \mathbf{F}_5)$. The same conclusion for $\bar{\rho}_{f,\lambda}$ thus follows.

5.3. *Projective image isomorphic to A_4, S_4 or A_5*

As an illustration of Theorem 4.1, we report here on an example due to Ribet [**26**, Remark 2, p. 283] and recalled in [**13**, Example 3.2, p. 244] (we warn the reader that the term 'exceptional' therein refers to a modular representation with projective image isomorphic to A_4, S_4 or A_5). The new subspace in $\mathcal{S}_2(\Gamma_0(23))$ is two-dimensional and generated by one Galois orbit labeled 23.4a in SAGE, with coefficients field $K = \mathbf{Q}(\alpha)$, where α is a root of $X^2 + X - 1$. Let λ be the unique prime ideal above 3 in $\mathcal{O}$. It is shown in [**13**] that the corresponding projective representation has image isomorphic to A_5 and that the field cut out by its kernel is the A_5-extension of $\mathbf{Q}$ given as the splitting field of the polynomial $X^5 + 3X^3 + 6X^2 + 9$.

Several other examples may also be found in [**13**] such as a mod 19 representation of projective image isomorphic to S_4 attached to the unique cusp form of weight 6, level 4 and trivial Nebentypus. The authors also discuss an effective procedure that, given a newform f and a prime ℓ, determines whether some mod ℓ representation attached to f has projective image isomorphic to A_4, S_4 or A_5.

TABLE 4. *Smallest prime $p \neq 11, \ell$ and $\leqslant 100$ such that $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ acts irreducibly.*

ℓ	2	3	5	11		61	
λ	(α)	$(\alpha-1)$	(5)	$(2\alpha-3)$	$(2\alpha-1)$	$(\alpha-9)$	$(\alpha+7)$
p	3	2	2	2	$\emptyset$	$\emptyset$	2

Acknowledgements. The first-named author is indebted to Mladen Dimitrov, David Loeffler, Filippo Nuccio, Nick Ramsey and Panagiotis Tsaknias for helpful conversations. Gabor Wiese deserves special thanks for his constant support and advice, as well as for invaluable comments and suggestions. Part of this work was done when Nicolas Billerey was a postdoc at the Institut für Experimentelle Mathematik in Essen. He is grateful to its members for a pleasant and stimulative working environment.

References

1. H. Carayol, 'Sur les représentations l-adiques associées aux formes modulaires de Hilbert', *Ann. Sci. École Norm. Sup.* (4) 19 (1986) 409–468.
2. H. Carayol, 'Sur les représentations galoisiennes modulo l attachées aux formes modulaires', *Duke Math. J.* 59 (1989) 785–801.
3. H. Cohen, *Number theory. Vol. I. Tools and diophantine equations*, Graduate Texts in Mathematics 239 (Springer, New York, 2007).
4. A. C. Cojocaru, 'On the surjectivity of the Galois representations associated to non-CM elliptic curves', *Canad. Math. Bull.* 48 (2005) 16–31. With an appendix by Ernst Kani.
5. F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics 228 (Springer, New York, 2005).
6. L. V. Dieulefait, 'Automorphy of $\mathrm{Symm}^5(\mathrm{GL}(2))$ and base change', Preprint, 2012, arXiv:1208.3946.
7. B. Edixhoven, 'The weight in Serre's conjectures on modular forms', *Invent. Math.* 109 (1992) 563–594.
8. E. Ghate and P. Parent, 'On uniform large Galois images for modular abelian varieties', *Bull. London Math. Soc.* 44 (2012) 1169–1181.
9. B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 (Springer, Berlin, 1967).
10. H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics 17 (American Mathematical Society, Providence, RI, 1997).
11. N. M. Katz, 'p-adic properties of modular schemes and modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 69–190.
12. N. M. Katz, 'A result on modular forms in characteristic p', *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 53–61.
13. I. Kiming and H. A. Verrill, 'On modular mod l Galois representations with exceptional images', *J. Number Theory* 110 (2005) 236–266.
14. A. Kraus, 'Une remarque sur les points de torsion des courbes elliptiques', *C. R. Acad. Sci. Paris Sér. I Math.* 321 (1995) 1143–1146.
15. R. Livné, 'On the conductors of mod l Galois representations coming from modular forms', *J. Number Theory* 31 (1989) 133–141.
16. D. Loeffler and J. Weinstein, 'On the computation of local components of a newform', *Math. Comp.* 81 (2012) 1179–1200.
17. G. Martin, 'Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$', *J. Number Theory* 112 (2005) 298–331.
18. B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* 47 (1977/78) 33–186.
19. B. Mazur and J.-P. Serre, 'Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg)', *Séminaire Bourbaki (1974/1975), Exp. No. 469*, Lecture Notes in Mathematics 514 (Springer, Berlin, 1976) 238–255.
20. T. Miyake, *Modular forms*, Springer Monographs in Mathematics (Springer, Berlin, English edition, 2006). Translated from the 1976 Japanese original by Yoshitaka Maeda.
21. M. R. Murty, 'Congruences between modular forms', *Analytic number theory (Kyoto, 1996)*, London Mathematical Society Lecture Note Series 247 (Cambridge University Press, Cambridge, 1997) 309–320.
22. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 322 (Springer, Berlin, 1999). Translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.
23. K. A. Ribet, 'On l-adic representations attached to modular forms', *Invent. Math.* 28 (1975) 245–275.
24. K. A. Ribet, 'Galois representations attached to eigenforms with Nebentypus', *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 17–51.
25. K. A. Ribet, 'On l-adic representations attached to modular forms. II', *Glasgow Math. J.* 27 (1985) 185–194.
26. K. A. Ribet, 'Images of semistable Galois representations', *Pacific J. Math.* (Special Issue) (1997) 277–297. Olga Taussky-Todd: in memoriam.
27. K. A. Ribet, 'Non-optimal levels of mod l reducible Galois representations or Modularity of residually reducible representations', 9 July 2010. Notes of a talk given at the Centre de Recerca Matemàtica (Barcelona).

28. B. Schoeneberg, *Elliptic modular functions: an introduction* (Springer, 1974). Translated from the German by J. R. Smart and E. A. Schwandt; Die Grundlehren der mathematischen Wissenschaften, Band 203.
29. J.-P. Serre, 'Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]', *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, Lecture Notes in Mathematics 317 (Springer, Berlin, 1973) 319–338.
30. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan 11 (Princeton University Press, Princeton, NJ, 1994). Reprint of the 1971 original, Kanô Memorial Lectures, 1.
31. W. A. Stein *et al. Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. http://www.sagemath.org.
32. H. P. F. Swinnerton-Dyer, 'On l-adic representations and congruences for coefficients of modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 1–55.
33. P. Tsaknias, 'A possible generalization of Maeda's conjecture', Preprint, 2012, arXiv:1205.3420.
34. L. C. Washington, *Introduction to cyclotomic fields*, 2nd edn. Graduate Texts in Mathematics 83 (Springer, New York, 1997).

Nicolas Billerey
Laboratoire de Mathématiques
Université Blaise Pascal – Clermont-Ferrand 2
Campus Universitaire des Cézeaux
63177 Aubière cedex
France
nicolas.billerey@math.univ-bpclermont.fr

Luis V. Dieulefait
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
Spain
ldieulefait@ub.edu

Math. Res. Lett.
Volume 23, Number 1, 15–41, 2016

On the modularity of reducible mod l Galois representations

Nicolas Billerey and Ricardo Menares

Given an odd, semisimple, reducible, 2-dimensional mod l Galois representation, we investigate the possible levels of the modular forms giving rise to it. When the representation is the direct sum of the trivial character and a power of the mod l cyclotomic character, we are able to characterize the primes that can arise as levels of the associated newforms. As an application, we determine a new explicit lower bound for the highest degree among the fields of coefficients of newforms of trivial Nebentypus and prime level. The bound is valid in a subset of the primes with natural (lower) density at least 3/4.

Introduction

Let l be a rational prime number. In this paper we are interested in 2-dimensional mod l Galois representations, that is, continuous homomorphisms

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l). \tag{0.1}$$

Work of Deligne, extending earlier results by Eichler and Shimura, shows that such representations arise naturally in the theory of modular forms. More precisely, let us take $\overline{\mathbb{Q}}$ to be the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and fix a place w of $\overline{\mathbb{Q}}$ over l. We denote by $a \mapsto \widetilde{a}$ the reduction map modulo w from the ring of integers $\overline{\mathbb{Z}}$ of $\overline{\mathbb{Q}}$ to the residue field $\overline{\mathbb{F}}_l$. Let us denote by $\mathcal{S}_k(\Gamma_1(N))$ the $\mathbb{C}$-vector space of cuspidal modular forms of weight $k \geq 2$ for $\Gamma_1(N)$. Then, attached to any form $f \in \mathcal{S}_k(\Gamma_1(N))$ that is an eigenform for the Hecke operators $\{T_p\}_{p\nmid N}$ with corresponding set of eigenvalues $\{a_p\}_{p\nmid N}$, there is a Dirichlet character χ of modulus N and an odd

2010 Mathematics Subject Classification: Primary 11F80, 11F33. Secondary 11N25.

semisimple Galois representation

$$\rho_f \ : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l),$$

unique up to isomorphism, that is unramified outside Nl and satisfies for every prime $p \nmid Nl$

$$\begin{cases} \mathrm{tr}(\rho_f(\mathrm{Frob}_p)) = \widetilde{a_p} \\ \det(\rho_f(\mathrm{Frob}_p)) = \widetilde{\chi(p)}p^{k-1} \end{cases}$$

where Frob_p denotes a Frobenius element at p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

A natural problem is then to understand which mod l Galois representations ρ are modular, meaning that ρ is isomorphic to some ρ_f as above. We shall say in this case that ρ arises from the cuspidal eigenform f. Since ρ does not uniquely determine f, it is equally important to determine the set of possible values of the level, weight and character of f. In this article, we will focus on the level aspect.

In the case where ρ is *irreducible*, these questions are addressed by Serre's modularity conjecture ([31]), which is now a theorem of Khare and Wintenberger ([18, 19]). Thanks to these works (building on several deep results by many people), it is known that every odd, irreducible Galois representation ρ as in (0.1) arises from a cuspidal eigenform. Let $N(\rho)$ be the prime-to-l part of the Artin conductor of ρ. Carayol ([5]) and Livné ([20]) independently proved that $N(\rho)$ is minimal (for divisibility) among all possible prime-to-l levels of modular forms giving rise to ρ. Ribet's famous level-lowering theorem ([27, Thm. 1.1]) shows that a modular ρ indeed arises from a Hecke eigenform of this 'optimal' level. On the other hand, Diamond and Taylor soon thereafter ([10]) completely described the set of prime-to-l integers $M > N(\rho)$ such that ρ arises from a weight-k *newform* of level M, in terms of the ramification theory of ρ. They called such integers *non-optimal levels* attached to ρ.

In this paper we focus on the case where ρ is *reducible*. Given an even integer $k \geq 2$, we have that, if $l \geq k-1$, then every modular mod l reducible representation arising from a weight-k newform with squarefree level and trivial Nebentypus is of the form $\mathbf{1} \oplus \chi_l^{k-1}$, where χ_l is the mod l cyclotomic character (cf. Proposition 3.1). The results of this paper are most precise when ρ is of this form.

The representation $\mathbf{1} \oplus \chi_l^{k-1}$ is unramified outside l, hence the prime-to-l part of its Artin conductor is 1. Because of this fact, we will say that $\mathbf{1} \oplus \chi_l^{k-1}$ is *modular of optimal level* if it arises from a cuspidal eigenform of weight

k and level 1. Contrary to what happens in the irreducible case, in spite of the fact that $\mathbf{1} \oplus \chi_l^{k-1}$ is odd and semi-simple, this representation need not be modular of optimal level for every choice of k and l. Indeed, when $k = 2$, there are no cusp forms of level one and weight two and hence $\mathbf{1} \oplus \chi_l$ is not modular of optimal level. On the other hand, in (even) weight $k \geq 4$, Ribet has proved that, if $l > k + 1$, then the representation $\mathbf{1} \oplus \chi_l^{k-1}$ is modular of optimal level if and only if l divides the numerator of B_k/k where B_k denotes the k-th Bernoulli number (more precisely, the direct implication of this assertion results from [25, Lem. 5.2] and the reverse implication is mentioned in [15, Prop. 1]).

Our goal is to study the set of integers $N \geq 2$, prime to l, such that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform of weight k, level N and trivial Nebentypus. Following the terminology that Diamond and Taylor introduced in the irreducible case, we call such integers *non-optimal levels* attached to this representation.

Our main concern is the classification of the squarefree, non-optimal levels attached to $\mathbf{1} \oplus \chi_l^{k-1}$. In weight $k = 2$, the first step in this study is a well-known result of Mazur ([23, Prop. (5.12)]), asserting that $\mathbf{1} \oplus \chi_l$ arises from a weight-2 cusp form of prime level N and trivial Nebentypus if and only if l divides the numerator of $(N-1)/12$. Then, Ribet classified the squarefree non-optimal levels having exactly two prime factors, under the assumption $l > 3$ (cf. [28]). His results have been very recently extended to the case of three prime factors by his student Hwajong Yoo in his Ph.D. thesis (Spring 2013). These works show that the classical level-raising condition does not suffice to determine the non-optimal levels.

Our main theorem treats the case $k \geq 4$ and is an interpolation of Mazur's and Ribet's results quoted above in the following sense.

Theorem 1. *Let k be an even integer ≥ 4 and assume $l > k + 1$. Then the representation $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a weight-k newform of prime level N, $N \neq l$, and trivial Nebentypus if and only if at least one of the following conditions holds :*

1) $N^k \equiv 1 \pmod{l}$
2) $N^{k-2} \equiv 1 \pmod{l}$ *and l divides the numerator of B_k/k.*

We conjecture that, when $k \geq 4$ is even, the level-raising condition at a prime p is actually sufficient for the representation $\mathbf{1} \oplus \chi_l^{k-1}$ to arise from a newform of squarefree level divisible by p. This leads to a conjectural description of the set of squarefree levels of weight-k newforms with trivial

Nebentypus that give rise to $\mathbf{1} \oplus \chi_l^{k-1}$ (cf. Conjecture 3.2 and the ensuing remarks). Theorem 1 confirms this description for prime non-optimal levels. We discuss in Section 3.3 how hypothesis (1) and (2) relate to the level-raising condition.

We stress the fact that the statement of Theorem 1 considers not only eigenforms, but newforms (in Mazur's and Ribet's statements this distinction is unnecessary). We deduce this statement from explicit computations of the constant term of various Eisenstein series at the cusps of an appropriate modular curve. We carry on these computations in Section 1, following a classical analytic approach. These calculations refine related constant term computations appearing in the work of Faltings and Jordan [13], who use algebraic geometry methods through the interpretation of modular forms as sections of a line bundle on a modular curve (cf. Remark 1.3). Our proof of the reverse implication in Theorem 1 proceeds by first constructing, using Eisenstein series modulo l and the Deligne-Serre lemma, a cuspidal eigenform satisfying the necessary congruences. We then use a theorem of Diamond in [8] to show that we can take the eigenform to be a newform of level N.

We shall prove in Section 2 that every odd representation which is the sum of two characters arises from a cuspidal modular form (Theorem 2.1). This fact is presumably well-known to experts, but our methods allow us to provide an elementary and self-contained proof and we include it here because we could not locate a proof in the literature. A related general question is to decide whether a given odd, reducible, but not necessarily semisimple, mod l Galois representation is the reduction of a l-adic representation attached to some cuspidal eigenform. We refer the interested reader to the work of Ramakrishna [24], and the references therein, for a collection of important results on this question.

We apply our results to the following situation. To a normalized eigenform $f \in \mathcal{S}_k(\Gamma_0(N))^{\mathrm{new}}$ with q-expansion at infinity

$$f(z) = \sum_{n \geq 1} a_n(f) q^n, \quad q = e^{2\pi i z},$$

we attach the number field $K_f := \mathbb{Q}\big(a_n(f) : (n, N) = 1\big)$. Put

$$d_k^{\mathrm{new}}(N) := \max\{[K_f : \mathbb{Q}] : f \in \mathcal{S}_k(\Gamma_0(N))^{\mathrm{new}}, \\ \text{normalized Hecke eigenform}\}.$$

A Theorem of Royer[1] ([29]) implies that

$$d_k^{\mathrm{new}}(N) \gg_k \sqrt{\log\log N}, \quad N \to \infty, \quad N \text{ prime}. \tag{0.2}$$

As an application of Theorem 1, we obtain, in the spirit of [11], a lower bound for $d_k^{\mathrm{new}}(N)$. As a new ingredient, we use results from analytic number theory on the density of prime numbers p for which $p-1$ has a large prime factor (cf. [16], [22]). We then manage to obtain a bound which is better than (0.2) but is only valid in a restricted class of prime numbers.

Theorem 2. *There exists an explicit set of primes $\mathcal{P}$ of (natural) lower density at least $\frac{3}{4}$ with the property that, for every even integer $k \geq 2$, there exists a constant $c_k > 0$ such that the inequality*

$$d_k^{\mathrm{new}}(N) \geq c_k \log N$$

holds for all $N \in \mathcal{P}$ with $N \geq (k+1)^4$. The constant c_k can be taken as

$$c_k = \left(8 \log\left(1 + 2^{(k-1)/2}\right)\right)^{-1}.$$

If we assume the truth of Conjecture 3.2, then it is possible to extend the validity of the above bound to appropriate squarefree integers (cf. Theorem 4.2).

In the spirit of Maeda's conjecture, Tsaknias has proposed a conjectural lower bound for $d_k^{\mathrm{new}}(N)$ for N fixed and varying k [33]. His conjecture implies that there exists a constant $c > 0$ such that, for all prime numbers N, there is an integer $k(N)$ such that $d_k^{\mathrm{new}}(N) > cN$ for all $k \geq k(N)$. Further numerical data, that he has generously shared with us, suggest that $k(N)$ is a bounded function of N. If this were true, then $d_k^{\mathrm{new}}(N)$ would grow linearly with N if k is fixed.

1. Preliminaries on Eisenstein series

In this section we recall some classical definitions and compute the constant term of the q-expansion at various cusps of some specific Eisenstein series that will be used in the sequel.

[1]Royer's theorem holds for arbitrary levels N with a constant depending on a fixed prime not dividing N. It is however stated only in the case $k = 2$ in *loc. cit.* but the proof undoubtedly extends to weights ≥ 2.

1.1. Gauss sums and Bernoulli Numbers

For an integer $m \geq 2$, we set

$$C_m = \frac{(-2i\pi)^m}{(m-1)!}.$$

Let $\psi : (\mathbb{Z}/c\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character of modulus $c \geq 1$. The Gauss sum attached to ψ is defined by

$$W(\psi) = \sum_{n=1}^{c} \psi(n) e^{2i\pi n/c}$$

and the Bernoulli numbers $(B_{m,\psi})_{m\geq 1}$ by

$$\sum_{n=1}^{c} \psi(n) \frac{te^{nt}}{e^{ct}-1} = \sum_{m\geq 0} B_{m,\psi} \frac{t^m}{m!}.$$

In particular, if ψ is the trivial character (of modulus 1), then $B_{m,\psi}$ is the classical Bernoulli number B_m, except when $m = 1$ in which case we have $B_{1,\psi} = -B_1 = 1/2$.

The Bernoulli numbers are related to certain special values of the L-function $L(s, \psi)$ attached to ψ. More precisely, we have the following proposition (which follows, for instance, from [34], Theorem 4.2 and the functional equation on p. 30 of *loc. cit.*).

Proposition 1.1. *Let $m \geq 2$ be an integer such that $\psi(-1) = (-1)^m$. Then, we have that*

$$L(m, \psi) = -W(\psi) \frac{C_m}{c^m} \cdot \frac{B_{m,\overline{\psi}}}{2m} \neq 0,$$

where $\overline{\psi}$ means the complex conjugate of ψ.

1.2. Constant term computations

For a positive real number A, let us denote by α_A the operator acting on complex valued functions f on the upper half-plane $\mathfrak{h}$ by

$$\alpha_A(f)(z) = f(Az).$$

1.2.1. General computations. Let $k \geq 3$ be an integer and $\varepsilon_0 : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be a primitive Dirichlet character of modulus $N \geq 1$ such that $\varepsilon_0(-1) = (-1)^k$. We denote by $E_k^{\mathbf{1},\varepsilon_0}$ the Eisenstein series in $\mathcal{M}_k(\Gamma_1(N), \varepsilon_0)$ given by the following q-expansion :

$$E_k^{\mathbf{1},\varepsilon_0}(z) = -\frac{B_{k,\varepsilon_0}}{2k} + \sum_{n\geq 1}\Big(\sum_{m|n}\varepsilon_0(m)m^{k-1}\Big)q^n, \quad \text{where } q = e^{2\pi iz}. \tag{1.3}$$

Note that when $N = 1$, $E_k^{\mathbf{1},\varepsilon_0} = E_k^{\mathbf{1},\mathbf{1}}$ is nothing but the classical level 1 Eisenstein series of weight k

$$E_k = -\frac{B_k}{2k} + \sum_{n\geq 1}\Big(\sum_{m|n} m^{k-1}\Big)q^n. \tag{1.4}$$

Note also that our function $E_k^{\mathbf{1},\varepsilon_0}$ differs from that of [9, Thm. 4.5.1] by a factor 2 (that is, their function $E_k^{\mathbf{1},\varepsilon_0}$ is twice ours). The main goal of this paragraph is to compute the constant term of the q-expansion of $\big(\alpha_M E_k^{\mathbf{1},\varepsilon_0}\big)|_k\gamma$ where $M \geq 1$ is an integer coprime to N, $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ and the notation $|_k$ means the classical slash operator on modular forms.

Proposition 1.2. *Let ε_0 and k as above. Let M be an integer ≥ 1 coprime to N and $\gamma = \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. The constant term of the q-expansion of $\big(\alpha_M E_k^{\mathbf{1},\varepsilon_0}\big)|_k\gamma$ is*

$$\begin{cases} 0 & \text{if } N \nmid \dfrac{v}{r} \\ -\dfrac{\overline{\varepsilon_0}(M')\varepsilon_0(\delta)}{M'^k}\dfrac{B_{k,\varepsilon_0}}{2k} \neq 0 & \text{otherwise} \end{cases}$$

where $r = \gcd(v, M)$ and $M' = M/r$.

Remark 1.3. The constant term of this kind of Eisenstein series plays a role in the work of Faltings and Jordan (cf. [13], Definition 3.16 and Theorem 3.20). However, they compute these constant terms only up to a unit in an appropriate ring of integers.

Proof. With the notations of Section 1.1 put

$$G = \frac{2C_k W(\overline{\varepsilon_0})}{N^k} E_k^{\mathbf{1},\varepsilon_0}.$$

According to the remark above, the function $G_k^{\mathbf{1},\varepsilon_0}$ of [9, Thm. 4.5.1] is twice our function G. It then follows from the definition of this function on page 127 of *loc. cit.* that

$$G = \sum_{\substack{j=0 \\ \gcd(j,N)=1}}^{N-1} \overline{\varepsilon_0}(j) G_k^{\overline{(0,j)}},$$

where the bar over $(0,j)$ means reduction modulo N (while $\overline{\varepsilon_0}$ means the complex conjugate of ε_0 as in Section 1.1) and

$$G_k^{\overline{(0,j)}}(z) = \sum_{\substack{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ (c,d)\equiv(0,j) \pmod N}} \frac{1}{(cz+d)^k}.$$

Therefore for any $0 \leq j \leq N-1$ coprime to N, we have

$$\left(\alpha_M G_k^{\overline{(0,j)}}\right)|_k\gamma(z) = \sum_{\substack{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ (c,d)\equiv(0,j) \pmod N}} \frac{1}{((cMu+dv)z+cM\beta+d\delta)^k}.$$

Hence its constant term is given by

$$\Upsilon_j = \sum_{\substack{(c,d)\in\mathbb{Z}^2\setminus\{(0,0)\} \\ (c,d)\equiv(0,j) \pmod N \\ cMu+dv=0}} \frac{1}{(cM\beta+d\delta)^k}.$$

Let $r = \gcd(v,M)$. Then $cMu+dv=0$ if and only if $cM'u+dv'=0$ where $M' = M/r$ and $v' = v/r$.

If $u=0$, then $\Upsilon_j = 0$ (for any j) unless $N=1$ in which case $j=0$ and

$$\Upsilon_0 = \sum_{c\in\mathbb{Z}} \frac{1}{(cM\beta)^k} = 2\frac{1}{M^k}\zeta(k)$$

since in this case $\beta = \pm 1$ and k is even. Therefore, according to Proposition 1.1, the constant term Υ of $(\alpha_M G)|_k\gamma$ is 0 if $N>1$ (and thus $N \nmid v = \pm 1$) and is $-\dfrac{C_k}{M^k}\dfrac{B_k}{k}$ when $N=1$. Hence the result in this case.

Assume now $u \neq 0$. Given $d \in \mathbb{Z}$, $d \equiv j \pmod N$, the following conditions are then equivalent :

1) there exists $c \in \mathbb{Z}$, $c \equiv 0 \pmod N$ such that $cMu+dv=0$;

2) we have $N \mid v'$ and $M'u \mid d$.

Indeed, if the first condition is satisfied, we have $cM'u + dv' = 0$ and thus $M'u \mid dv'$. But $M'u$ and v' are coprime hence $M'u \mid d$. Besides, $0 = cM'u + dv' \equiv dv' \pmod N$ and since $d \equiv j \pmod N$ and $\gcd(j, N) = 1$, we get that $N \mid v'$.

On the other hand, if the second condition holds, put $c = -\frac{d}{M'u}v' = -\frac{d}{Mu}v$. Then $c \in \mathbb{Z}$ satisfies $cMu + dv = 0$ and since $N \mid v'$ by assumption, we get $c \equiv 0 \pmod N$.

Moreover if these equivalent conditions are satisfied, then we have

$$cM\beta + d\delta = \frac{1}{u}(cu\beta M + du\delta) = \frac{1}{u}(du\delta - dv\beta) = \frac{d}{u}.$$

Therefore the constant term Υ of $(\alpha_M G)|_k\gamma$ is 0 when $N \nmid v'$ and is otherwise given by

$$\begin{aligned}
\Upsilon &= \sum_{\substack{j=0\\ \gcd(j,N)=1}}^{N-1} \overline{\varepsilon_0}(j)\Upsilon_j = \sum_{\substack{j=0\\ \gcd(j,N)=1}}^{N-1} \overline{\varepsilon_0}(j) \sum_{\substack{d\in\mathbb{Z}\setminus\{0\}\\ d\equiv j \pmod N\\ M'u\mid d}} \left(\frac{u}{d}\right)^k \\
&= \sum_{\substack{j=0\\ \gcd(j,N)=1}}^{N-1} \overline{\varepsilon_0}(j) \sum_{\substack{d\in\mathbb{Z}\setminus\{0\}\\ d\equiv j/(M'u) \pmod N}} \frac{1}{(M'd)^k} \\
&= \frac{\overline{\varepsilon_0}(M'u)}{M'^k} \sum_{\substack{j=0\\ \gcd(j,N)=1}}^{N-1} \sum_{\substack{d\in\mathbb{Z}\setminus\{0\}\\ d\equiv j/(M'u) \pmod N}} \frac{\overline{\varepsilon_0}(d)}{d^k} \\
&= \frac{\overline{\varepsilon_0}(M'u)}{M'^k} \sum_{d\in\mathbb{Z}\setminus\{0\}} \frac{\overline{\varepsilon_0}(d)}{d^k} \\
&= 2\frac{\overline{\varepsilon_0}(M'u)}{M'^k} L(k, \overline{\varepsilon_0})
\end{aligned}$$

as $\overline{\varepsilon_0}(-1) = (-1)^k$. Besides, since $N \mid v$ and $u\delta - v\beta = 1$, we have $\overline{\varepsilon_0}(u) = \varepsilon_0(\delta)$. Using Proposition 1.1, we therefore find that in this case the constant term Υ of $(\alpha_M G)|_k\gamma$ is non-zero and given by

$$\Upsilon = -\frac{2C_k W(\overline{\varepsilon_0})}{N^k} \frac{\overline{\varepsilon_0}(M')\varepsilon_0(\delta)}{M'^k} \frac{B_{k,\varepsilon_0}}{2k}.$$

Hence the result in this case as well. □

1.2.2. A useful Eisenstein series. In this paragraph we state some results about Eisenstein series that will be used in Section 3. Let N be a squarefree integer and k be an even integer ≥ 4. We denote by $\mathcal{E}_k(\Gamma_0(N))$ the space spanned by the Eisenstein series of weight k and level $\Gamma_0(N)$.

For each prime divisor p of N, let $\delta_p \in \{1, p^{k-1}\}$. Put

$$E(z) = \left[\prod_{\substack{p|N \\ p \text{ prime}}} (U_p - \delta_p \mathrm{Id}) \right] \alpha_N E_k(z) \in \mathcal{E}_k(\Gamma_0(N)),$$

where U_p (for p a prime divisor of N) is the p-th Hecke operator acting on $\mathcal{E}_k(\Gamma_0(N))$. We remark that, even if it is not included in the notation, the function E does depend on the choice of the parameters $\{\delta_p : p|N\}$. For a prime number p not dividing N, we denote by T_p the classical p-th Hecke operator acting on $\mathcal{E}_k(\Gamma_0(N))$. The following proposition summarizes the main properties of E.

Proposition 1.4. *The Eisenstein series E is a normalized Hecke eigenform of level $\Gamma_0(N)$ such that*

$$\begin{cases} T_p E = (1 + p^{k-1})E & \text{if } p \nmid N \\ U_p E = (p^{k-1}/\delta_p)E & \text{otherwise.} \end{cases}$$

We have that

$$E = \sum_{M|N} (-1)^{|M|} \delta_M \alpha_M E_k, \tag{1.5}$$

where $|M|$ is the number of prime divisors of M and

$$\delta_M = \prod_{\substack{p|M \\ p \text{ prime}}} \delta_p.$$

Let s be a cusp of $X_0(N)$. It is then $\Gamma_0(N)$-equivalent to $1/v$ for some $v \mid N$ and the constant term of the Fourier expansion of E at the cusp s is

$$-\frac{B_k}{2k} \prod_{p|N} \left(1 - \delta_p \left(\frac{\gcd(p, v)}{p} \right)^k \right),$$

where the product runs over the prime divisors of N.

Proof. The Eisenstein series E_k is a normalized Hecke eigenform of level 1 with eigenvalue $1 + p^{k-1}$ for each prime number p. Let p be a prime not dividing N. It then follows from the action of Hecke operators on q-expansions of modular forms (see, for instance, [9, Prop. 5.2.2]) that $T_p \alpha_N E_k = \alpha_N T_p E_k$. Since the Hecke algebra spanned by $\{T_p : p \nmid N, U_p : p|N\}$ is commutative, we get $T_p E = (1 + p^{k-1})E$.

Let now p be a prime dividing N and M an integer dividing N. We have that

$$U_p \alpha_M E_k = \begin{cases} \alpha_{M/p} E_k & \text{if } p \mid M \\ (1 + p^{k-1})\alpha_M E_k - p^{k-1}\alpha_{Mp} E_k & \text{otherwise.} \end{cases} \tag{1.6}$$

Indeed, the case $p|M$ follows from *loc. cit.* (note however that Diamond and Shurman use the notation T_p in the case $p \mid N$ as well) and the case $p \nmid M$ follows from a direct calculation using the q-expansion (1.4) of E_k..

Since N is squarefree, we therefore get

$$\begin{aligned} U_p(U_p - \delta_p \mathrm{Id})\alpha_N E_k &= (U_p^2 - \delta_p U_p)\alpha_N E_k \\ &= U_p \alpha_{N/p} E_k - \delta_p \alpha_{N/p} E_k \\ &= (1 + p^{k-1})\alpha_{N/p} E_k - p^{k-1}\alpha_N E_k - \delta_p \alpha_{N/p} E_k \\ &= \frac{p^{k-1}}{\delta_p}\alpha_{N/p} E_k - p^{k-1}\alpha_N E_k \\ &= \frac{p^{k-1}}{\delta_p}\left(\alpha_{N/p} E_k - \delta_p \alpha_N E_k\right) \\ &= \frac{p^{k-1}}{\delta_p}(U_p - \delta_p \mathrm{Id})\alpha_N E_k. \end{aligned}$$

Hence the result in this case as well.

Using Equation (1.6), we easily prove by induction on the number of prime divisors of N the 'expanded form' (1.5) for E.

Let s be a cusp of $X_0(N)$. Since N is squarefree, we have that s is $\Gamma_0(N)$-equivalent to $1/v$ where $v \mid N$. Let M be a divisor of N. Then, according to Proposition 1.2 the constant term of the Fourier expansion of $\alpha_M E_k$ at the cusp s is

$$-\frac{B_k}{2k}\left(\frac{\gcd(v, M)}{M}\right)^k.$$

Since N is squarefree, the constant term of the Fourier expansion of E at the cusp $1/v$ is then

$$-\frac{B_k}{2k}\sum_{M|N}(-1)^{|M|}\delta_M\left(\frac{\gcd(v,M)}{M}\right)^k=-\frac{B_k}{2k}\prod_{\substack{p|N\\ p \text{ prime}}}\left(1-\delta_p\left(\frac{\gcd(p,v)}{p}\right)^k\right).$$

This proves the result. □

2. Modularity of odd reducible semisimple representations

The following theorem is presumably well-known to experts, but we provide a proof due to lack of suitable reference.

Theorem 2.1. *Every odd representation which is the direct sum of two characters arises from a cuspidal eigenform.*

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$ be such a representation and fix a place w of $\overline{\mathbb{Q}}$ above l, as in the Introduction. Assume first that $\rho \simeq \mathbf{1} \oplus \varepsilon\chi_l^b$ where ε is unramified at l and $0 \leq b \leq l-2$. The oddness condition here means $\varepsilon(-1) = (-1)^{b+1}$. We now define two integers $N \geq 1$ and $k \geq 2$ and a character ε_0.

Let us denote by N the Artin conductor of ε. It is coprime to l by assumption. Moreover if we denote by ε_0 the Teichmüller lift (with respect to w) of ε we may identify it with a primitive Dirichlet character of conductor N. It satisfies $\varepsilon_0(-1) = (-1)^{b+1}$ unless $l = 2$, in which case we have $\varepsilon_0(-1) = 1$.

We define a 'weight' k attached to $\mathbf{1} \oplus \varepsilon\chi_l^b$ as follows :

$$k = \begin{cases} 4 & \text{if } b = 0 \text{ and } l = 2 \\ l & \text{if } b = 0 \text{ and } l \geq 3 \\ l+1 & \text{if } b = 1 \\ b+1 & \text{if } b \geq 2 \end{cases}.$$

Note that $\varepsilon_0(-1) = (-1)^k$ and $k - 1 \equiv b \pmod{l-1}$. Hence $\rho \simeq \mathbf{1} \oplus \varepsilon\chi_l^{k-1}$.

Remark 2.2. Serre's recipe (see [31, Eq. (2.3.2)]) for the weight of such a representation is (with Edixhoven's notation, [12])

$$k_\rho = \begin{cases} l & \text{if } b = 0 \\ b+1 & \text{if } b \geq 1 \end{cases}$$

while Edixhoven's definition gives $k(\rho) = b + 1$ (*loc. cit.*). Our definition is motivated by the fact that we want to avoid working with Eisenstein series of weight 1 or 2 in the proof of Theorem 2.3 below.

Let λ be the prime ideal induced by our fixed place w in the ring of integers of the number field generated by the values of ε_0. We can now state a special case of Theorem 2.1.

Theorem 2.3. *Let (N, k, ε_0) as above. Then, the representation $\mathbf{1} \oplus \varepsilon\chi_l^b$ arises from an eigenform in $\mathcal{S}_k(\Gamma_1(Np), \varepsilon_0)$ for every prime number $p \nmid Nl$ such that λ divides the non-zero algebraic number $\dfrac{B_{k,\varepsilon_0}}{2k}(\varepsilon_0(p)p^k - 1)$.*

Proof. Let p be a prime number not dividing Nl. We consider

$$E = E_k^{\mathbf{1},\varepsilon_0} - \alpha_p E_k^{\mathbf{1},\varepsilon_0}$$

where $E_k^{\mathbf{1},\varepsilon_0}$ is the Eisenstein series defined in Equation (1.3) and compute the constant term, say a_γ, of the q-expansion of $E|_k\gamma$ for any $\gamma = \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. By construction we have $\varepsilon_0(-1) = (-1)^k$. According to Proposition 1.2, if $N \nmid v$, then $a_\gamma = 0$. Besides, if $Np \mid v$, then $\gamma \in \Gamma_0(Np)$ and $E|_k\gamma = \varepsilon_0(\delta)E$. Hence $a_\gamma = 0$ in this case as well. Finally, if $N \mid v$ and $p \nmid v$, then Proposition 1.2 gives

$$a_\gamma = -\varepsilon_0(\delta)\frac{B_{k,\varepsilon_0}}{2k}\left(1 - \frac{\overline{\varepsilon_0}(p)}{p^k}\right).$$

Therefore, under the assumption that λ divides $(\varepsilon_0(p)p^k - 1)B_{k,\varepsilon_0}/2k$, the reduction of E modulo λ is a cuspidal eigenform with coefficients in $\overline{\mathbb{F}}_l$ and eigenvalues $1 + \varepsilon(q)q^{k-1}$ for every prime $q \nmid Np$. According to Lem. 6.11 of [7] we can find a form $f \in \mathcal{S}_k(\Gamma_1(Np), \varepsilon_0)$ which is an eigenform for the Hecke operators $\{T_q\}_{q\nmid Np}$ with corresponding eigenvalues $\{a_q\}_{q\nmid Np}$ satisfying (for $q \neq l$) $\widetilde{a_q} = 1 + \varepsilon(q)q^{k-1}$. Hence the representation $\mathbf{1} \oplus \varepsilon\chi_l^b = \mathbf{1} \oplus \varepsilon\chi_l^{k-1}$ arises from an eigenform in $\mathcal{S}_k(\Gamma_1(Np), \varepsilon_0)$ as claimed. □

Proof of Theorem 2.1: let ρ be an odd representation which is the direct sum of two characters, say $\rho = \nu \oplus \nu'$. We thus have $(\nu\nu')(-1) = -1$. Put $\mu = \nu^{-1}\nu'$ and write $\mu = \varepsilon\chi_l^b$ where ε is unramified at l and $0 \leq b \leq l - 2$. It satisfies $\mu(-1) = -1$ (or, equivalently $\varepsilon(-1) = (-1)^{b+1}$). Let N, k and ε_0 be the invariants as defined above attached to the representation $\mathbf{1} \oplus \mu = \mathbf{1} \oplus \varepsilon\chi_l^b$. By the previous theorem the representation $\mathbf{1} \oplus \mu$ arises from a

Hecke eigenform f in $\mathcal{S}_k(\Gamma_1(Np), \varepsilon_0)$ for infinitely many primes $p \nmid Nl$. Let us now consider some characteristic 0 lift ν_0 of ν with finite image. It may be identified with some primitive Dirichlet character of modulus r, say. Put $g = f \otimes \nu_0$. By a result of Shimura [32, Prop. 3.64], we have that g belongs to $\mathcal{S}_k(\Gamma_1(\mathrm{lcm}(Np, r^2, rN)), \varepsilon_0\nu_0^2)$. Moreover g is an eigenform for the Hecke operators outside Npr (see [26, p. 34]) and its attached mod l Galois representation is isomorphic to $\rho_f \otimes \nu \simeq \rho$. We thus have proved Theorem 2.1.

3. Non-optimal levels of $\mathbf{1} \oplus \boldsymbol{\chi}_l^{k-1}$

The following proposition justifies our study of reducible representations of the special form $\mathbf{1} \oplus \chi_l^{k-1}$.

Proposition 3.1. *Let f be a newform of weight $k \geq 2$, squarefree level N and trivial Nebentypus. For a prime l, if $l \geq k-1$ and ρ_f is reducible, we have that ρ_f is isomorphic to $\mathbf{1} \oplus \chi_l^{k-1}$.*

Proof. By assumption, ρ_f is the direct sum of two characters ν_1 and ν_2. We decompose each of them as a product of a character ε_i $(i = 1, 2)$, which is unramified at l, and some power of the cyclotomic character. The local description of the representation ρ_f at l ([12, Thm. 2.5-2.6]) shows that, under the assumption $l \geq k-1$, the exponents of the cyclotomic characters are 0 and $k-1$. On the other hand, the product $\varepsilon_1\varepsilon_2$ is trivial (as the form f has trivial Nebentypus) and by the squarefreeness assumption the characters ε_i are also unramified at the primes dividing N and hence trivial. □

In the rest of this section we fix an even integer $k \geq 2$ and focus our attention on the level-raising problem for (odd) representations of the form $\mathbf{1} \oplus \chi_l^{k-1}$ with $2 \leq k \leq l-3$. With regards to the problem of classifying the squarefree non-optimal levels attached to $\mathbf{1} \oplus \chi_l^{k-1}$, we propose the following conjecture.

Conjecture 3.2. *Let k be an even integer ≥ 4 and assume $l > k+1$. Then the representation $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a weight-k newform of squarefree level N, with $l \nmid N$, and trivial Nebentypus if and only if at least one of the following conditions holds :*

1) *we have $(p^k - 1)(p^{k-2} - 1) \equiv 0 \pmod{l}$ for every prime number p dividing N and there exists a prime divisor p_0 of N such that $p_0^k \equiv 1 \pmod{l}$;*

2) *we have* $p^{k-2} \equiv 1 \pmod{l}$ *for every prime number* p *dividing* N *and* l *divides the numerator of* B_k/k*, where* B_k *denotes the* k*-th Bernoulli number.*

We are able to show the direct implication in this conjecture (see Theorem 3.3). Concerning the reverse implication, we prove a weaker statement (see Theorem 3.5). On the other hand, Theorem 1 settles the conjecture in the case where N is prime. The case $N = 1$ follows in one direction from a result of Ribet ([25, Lem. 5.2]) and from Deligne-Serre's lifting lemma ([7, Lem. 6.11]) in the other (cf. Corollary 3.7 and Remark 3.8).

We can prove that Conjecture 3.2 is actually equivalent to saying that the classical (necessary) level-raising condition at a prime (away from the level) is sufficient (cf. Section 3.3). In Section 3.2 we combine Theorems 3.3 and 3.5 with a result of Diamond ([8]) to prove the prime-level case of the conjecture. Using magma ([4]), we have computationally checked the validity of the conjecture for fixed weights and levels in various ranges. In particular it holds true for $k = 4$ and $N < 5000$ and for $6 \leq k < 32$ and $N < 50$.

3.1. Necessary conditions

In this paragraph we prove the following statement which corresponds to the direct implication in Conjecture 3.2.

Theorem 3.3. *Let* k *be an even integer and* N *be a non-negative squarefree integer. Assume* $k \geq 4$*,* $l > k + 1$ *and* $l \nmid N$*. If the representation* $\mathbf{1} \oplus \chi_l^{k-1}$ *arises from a weight-*k *newform of level* N *and trivial Nebentypus, then at least one of the following assertions holds :*

1) *we have* $(p^k - 1)(p^{k-2} - 1) \equiv 0 \pmod{l}$ *for every prime number* p *dividing* N *and there exists a prime divisor* p_0 *of* N *such that* $p_0^k \equiv 1 \pmod{l}$*;*

2) *we have* $p^{k-2} \equiv 1 \pmod{l}$ *for every prime number* p *dividing* N *and* l *divides the numerator of* B_k/k*.*

The proof splits into two steps. We first deduce some weaker conditions from the local description of modular representations at primes dividing exactly once the level. In a slightly different form, this was already done in a joint paper by Dieulefait and the first author ([3]), but we briefly repeat the argument here for the sake of conciseness. We then strengthen these

conditions using some (new) computations about Eisenstein series from Section 1.2.2 to obtain Theorem 3.3.

Let k, l and N as in the theorem. Recall that we have fixed a place w of $\overline{\mathbb{Q}}$ above l. Assume that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from some newform f of weight k and level $\Gamma_0(N)$. Let p be a prime dividing N. By [21, Prop. 2.8], the restriction of ρ_f to a decomposition group D_p at p is $\mu\chi_l^{k/2} \oplus \mu\chi_l^{k/2-1}$ where μ is the (at most) quadratic unramified character thats maps a Frobenius at p to the reduction modulo w of $a_p(f)/p^{k/2-1}$. Therefore, we have the following equality between sets of characters of D_p :

$$\{\mathbf{1}, \chi_l^{k-1}\} = \{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\}.$$

1) Assume that $\mathbf{1} = \mu\chi_l^{k/2}$. Then, in particular $p^k \equiv 1 \pmod{l}$.
2) Assume that $\mathbf{1} = \mu\chi_l^{k/2-1}$. Then, $\widetilde{a_p(f)} = 1$ and in particular, $p^{k-2} \equiv 1 \pmod{l}$.

Let us now assume that the first assertion of the theorem is not satisfied. According to the above discussion we have

$$p^{k-2} \equiv 1 \pmod{l}; \quad p^k \not\equiv 1 \pmod{l} \quad \text{and} \quad \widetilde{a_p(f)} = 1$$

for every prime p dividing N and we must show that l divides the numerator of B_k/k. This will be achieved using a careful study of the constant term of the Fourier expansion at various cusps of a specific Eisenstein series which we now introduce.

Let us consider the Eisenstein series E as in Section 1.2.2 with parameters $\delta_p = p^{k-1}$ for every prime $p \mid N$ and write $E(z) = \sum_{n\geq 0} a_n(E)q^n$, where $q = e^{2i\pi z}$. Then by assumption and Proposition 1.4, we have :

$$\widetilde{a_p(f)} = \widetilde{a_p(E)}, \quad \text{for all primes } p \neq l.$$

Besides, both E and f are normalized Hecke eigenforms. Therefore, we get

$$\widetilde{a_n(f)} = \widetilde{a_n(E)}, \quad \text{for all prime-to-}l \text{ integers } n.$$

We denote by $\widetilde{f}$ and $\widetilde{E}$ the reductions modulo w of f and E respectively. Applying the operator $\Theta = q\frac{d}{dq}$ (see [30]) we obtain the equality $\Theta(\widetilde{f}) = \Theta(\widetilde{E})$. Since the Θ operator is injective under the assumption $l > k+1$ ([17, Cor. 3]), we conclude that $\widetilde{E} = \widetilde{f}$. In particular, w divides the numerator of the constant term of E at the cusp ∞. By Proposition 1.4, this means that

l divides the numerator of $\frac{B_k}{2k}\prod_{p|N}(1-p^{k-1})$. Since $p^{k-1} \equiv 1 \pmod{l}$ would imply $p^k \equiv 1 \pmod{l}$ (as $p^{k-2} \equiv 1 \pmod{l}$), contrary to the hypotheses, we get the desired result. This ends the proof of Theorem 3.3.

Remark 3.4. According to Proposition 1.4, the vanishing modulo l of the constant terms of E at the other cusps of $X_0(N)$ does not give additional information.

3.2. Weaker converse statement and the prime level case

In what follows we present a weaker statement in the direction of the reverse implication of Conjecture 3.2. We will finish this paragraph with a proof of Theorem 1.

Theorem 3.5. *Let N be a positive squarefree integer. Let k be an even integer ≥ 4 and assume $l > k+1$. Assume that at least one of the following conditions holds :*

1) *we have $(p^k-1)(p^{k-2}-1) \equiv 0 \pmod{l}$ for every prime number p dividing N and there exists a prime divisor p_0 of N such that $p_0^k \equiv 1 \pmod{l}$;*
2) *we have $p^{k-2} \equiv 1 \pmod{l}$ for every prime number p dividing N and l divides the numerator of B_k/k.*

Then the representation $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a weight-k eigenform of level N and trivial Nebentypus.

Remark 3.6. This statement is weaker than the reverse implication in Conjecture 3.2 because it is not guaranteed that the eigenform is a newform.

Proof. Assume that either condition of the theorem is satisfied and let us consider the Eisenstein series E of Section 1.2.2 with the following choice of parameters :

$$\delta_p = \begin{cases} 1 & \text{if } p^k \equiv 1 \pmod{l} \\ p^{k-1} & \text{otherwise} \end{cases}.$$

Recall from Equation (1.5) that we have

$$E = \sum_{M|N} (-1)^{|M|} \delta_M \alpha_M E_k, \tag{3.7}$$

where $|M|$ is the number of prime divisors of M and

$$\delta_M = \prod_{\substack{p|M \\ p \text{ prime}}} \delta_p.$$

According to the assumptions $l > k+1$, $l \nmid N$ and the Van Staudt-Clausen theorem, the series E has l-integral rational Fourier coefficients at ∞. Let us denote by F its reduction modulo l. It is a well-defined modular form over $\mathbb{F}_l$.

We now prove that F is actually cuspidal. By Proposition 1.4, this is clear under assumption (2) (as in particular, l divides the numerator of B_k/k). Else, if we assume assumption (1), then there exists a prime divisor p_0 of N such that $\delta_{p_0} = 1$. Let s be a cusp of $X_0(N)$. It is $\Gamma_0(N)$-equivalent to some cusp of the form $1/v$ with $v \mid N$ and $1 \leq v \leq N$. Then

$$1 - \delta_{p_0} \left(\frac{\gcd(p_0, v)}{p_0} \right)^k = \begin{cases} 0 & \text{if } \gcd(p_0, v) = p_0 \\ 1 - p_0^{-k} & \text{otherwise.} \end{cases}$$

is congruent to 0 modulo l. Hence the result by Proposition 1.4.

As it is already the case for E, the cuspidal form F is a Hecke eigenform at level N. Therefore according to the Deligne-Serre lifting lemma, there exist a finite extension $K/\mathbb{Q}_l$ with ring of integers $\mathcal{O}$ and uniformizer $\mathcal{L}$ and a normalized Hecke eigenform $f \in \mathcal{S}_k(\Gamma_0(N); \mathcal{O})$ with system of eigenvalues $\{c_p\}_p$ where p runs over the primes, such that

$$c_p \equiv 1 + p^{k-1} \pmod{\mathcal{L}} \text{ if } p \nmid N \text{ and } c_p \equiv p^{k-1}/\delta_p \pmod{\mathcal{L}} \text{ otherwise.}$$

Moreover f is a classical modular form (as its Fourier coefficients are roots of the characteristic polynomials of the Hecke operators). □

By a direct combination of Theorems 3.3 and 3.5 we get a new proof of the result of Ribet mentioned in the Introduction, which constitutes the level 1 case of Conjecture 3.2.

Corollary 3.7. *Let k be an even integer ≥ 4 and l be a prime $> k+1$. Then the representation $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a weight-k eigenform of level 1 if and only if l divides the numerator of B_k/k.*

Remark 3.8. The direct implication of this result is due to Ribet [25, Lem. 5.2]. The reverse implication is mentioned in [15, Prop. 1].

Proof of Theorem 1: The direct implication is a particular case of Theorem 3.3.

Now we prove the reverse implication. By Theorem 3.5, we have that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from an eigenform $f_0 \in \mathcal{S}_k(\Gamma_0(N))$. If f_0 is a newform, then we are done. Hence, in what follows we will assume that f_0 is an oldform. We denote by f its associated (normalized) level 1 eigenform. By a standard application of the Cebotarev density theorem, the mod l representations ρ_f and ρ_{f_0} are isomorphic.

Let K be the number field spanned by the Fourier coefficients of f. Since ρ_{f_0} is isomorphic to $\mathbf{1} \oplus \chi_l^{k-1}$ and $l \nmid N$, we have that there is an integral prime ideal $\lambda \subset O_K$ above l such that $a_N(f) \equiv 1 + N^{k-1} \pmod{\lambda}$. We claim that

$$a_N(f)^2 \equiv N^{k-2}(1+N)^2 \pmod{\lambda}. \tag{3.8}$$

Indeed,

$$a_N(f) \equiv 1 + N^{k-1} \equiv \begin{cases} 1 + N^{-1} \pmod{\lambda} & \text{if } N^k \equiv 1 \pmod{l} \\ 1 + N \pmod{\lambda} & \text{if } N^{k-2} \equiv 1 \pmod{l}. \end{cases}$$

Since

$$N^{k-2}(1+N)^2 \equiv \begin{cases} (1+N^{-1})^2 \pmod{l} & \text{if } N^k \equiv 1 \pmod{l} \\ (1+N)^2 \pmod{l} & \text{if } N^{k-2} \equiv 1 \pmod{l} \end{cases}$$

this proves the claim.

Relation (3.8) allows us to use a theorem of Diamond ([8, Thm. 1][2]), to ensure that there exists a normalized newform $f_1 \in S_k\big(\Gamma_0(N)\big)^{\text{new}}$ with eigenvalues in a finite extension K'/K and an ideal $\lambda' \subset O_{K'}$ above λ such that

$$a_p(f) \equiv a_p(f_1) \pmod{\lambda'} \text{ for all primes } p \nmid Nl.$$

Then, ρ_{f_1} is isomorphic to $\mathbf{1} \oplus \chi_l^{k-1}$, concluding the proof.

3.3. Relationship with the level-raising condition

Let

$$\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

be an odd semisimple Galois representation of conductor $N(\rho)$ (coprime to l). We shall say that ρ satisfies the level-raising condition at a prime

[2]Note that Diamond's (N, l, p) in *loc. cit.* is $(1, N, l)$ in our notation.

number $p \nmid N(\rho)l$ if

$$p\,(\mathrm{tr}\rho(\mathrm{Frob}_p))^2 = (1+p)^2 \det\rho(\mathrm{Frob}_p) \quad \text{in } \overline{\mathbb{F}}_l,$$

where Frob_p denotes a Frobenius element at p in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Such a condition is satisfied if the representation ρ arises from a newform in $\mathcal{S}_k(\Gamma_1(Np))$ with $(N,p)=1$. In particular, it is a necessary condition to raise the level of a modular representation from N to Np. In their paper [10], Diamond and Taylor prove that this is also sufficient when ρ is assumed to be irreducible.

In the special case of the representation $\mathbf{1} \oplus \chi_l^{k-1}$, with even $k \geq 2$, the level-raising condition at a prime $p \neq l$ is merely

$$(p^k-1)(p^{k-2}-1) \equiv 0 \pmod{l}. \tag{3.9}$$

If $k=2$, the congruence (3.9) is automatically fulfilled for every p, even though there are primes p such that $\mathbf{1} \oplus \chi_l$ is not modular of weight 2 and level p. However, we believe that the case $k \geq 4$ is different and by analogy with the irreducible case, we propose the following conjecture:

Conjecture 3.9. *Let $k \geq 4$ be an even integer and l be a prime $> k+1$. Assume that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform in $\mathcal{S}_k(\Gamma_0(N))$ with N squarefree and coprime to l and that $p \nmid Nl$ is a prime number at which $\mathbf{1} \oplus \chi_l^{k-1}$ satisfies the level raising condition, namely $(p^k-1)(p^{k-2}-1) \equiv 0 \pmod{l}$. Then, the representation $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform in $\mathcal{S}_k(\Gamma_0(Np))$.*

Using Theorems 3.3 and 3.5 above we now prove the following result.

Proposition 3.10. *Conjectures 3.2 and 3.9 are equivalent.*

Proof. Assume Conjecture 3.2 and the hypothesis of Conjecture 3.9. Then Theorem 3.3 ensures that the squarefree integer Np satisfies the hypothesis of Conjecture 3.2, thus proving Conjecture 3.9.

Assume conversely Conjecture 3.9 and let us show that Conjecture 3.2 holds. The direct implication therein corresponds to Theorem 3.3. Let us now prove the reverse implication. Let N be a prime-to-l squarefree integer that satisfies at least one of the conditions in the statement of Conjecture 3.2. According to Theorem 3.5, $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform in $\mathcal{S}_k(\Gamma_0(M))$ for some integer $M \mid N$. If $M \neq N$, we want to show that we can now raise the level from M to N. Let p be a prime dividing N/M. Then one clearly has $(p^k-1)(p^{k-2}-1) \equiv 0 \pmod{l}$ and Conjecture 3.9 shows that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform in $\mathcal{S}_k(\Gamma_0(pM))$. If $pM = N$, we are done. Otherwise

we can repeat this process until we reach N. Hence, we have proved Conjecture 3.2. □

Remark 3.11. As for irreducible representations, we deduce from Conjecture 3.2 that if the representation $\mathbf{1} \oplus \chi_l^{k-1}$ for $k \geq 4$ arises from newforms in $\mathcal{S}_k(\Gamma_0(M))$ and in $\mathcal{S}_k(\Gamma_0(N))$ for squarefree integers $M \mid N$, then it also arises from a newform in $\mathcal{S}_k(\Gamma_0(N'))$ for any intermediate level $M \mid N' \mid N$. As noticed by Ribet, such a result is false for $k = 2$. The representation $\mathbf{1} \oplus \chi_5$ for instance arises in levels 11 and 66 but neither in level 22 nor in level 33.

4. Lower bound for the highest degree of the coefficient field of newforms

In this section we prove Theorem 2. For a nonzero integer m, let $P^+(m)$ be the largest prime factor of m. Let

$$\mathcal{P} := \{N \text{ prime such that } P^+(N-1) > N^{1/4}\}. \tag{4.10}$$

That is, for every $N \in \mathcal{P}$, there exists a prime l with

$$N \equiv 1 \pmod{l} \text{ and } l > N^{1/4}. \tag{4.11}$$

Let $A \subset \mathbb{N}$ be a set consisting only of prime numbers. For $x \in \mathbb{R}$, let

$$A(x) = |\{a \in A : a \leq x\}|, \quad \pi(x) = |\{p \leq x : p \text{ is prime}\}|.$$

We recall that the quantity

$$\liminf_{x \to \infty} \frac{A(x)}{\pi(x)}$$

is called the natural lower density of A.

Lemma 4.1. *The set $\mathcal{P}$ has natural lower density at least $3/4$.*

Proof. In [22], Theorem 1, it is proved that

$$\mathcal{P}(x) \geq \frac{3}{4} \cdot \frac{x}{\log x} + O\Big(\frac{x}{(\log x)^{5/3}}\Big), \quad \text{as } x \to \infty. \tag{4.12}$$

Using (4.12) and the prime number theorem we obtain

$$\liminf_{x\to\infty} \frac{S(x)}{\pi(x)} \geq \frac{3}{4},$$

as desired. □

Proof of Theorem 2: Let $\mathcal{P}$ be defined by (4.10). Take $N \in \mathcal{P}$ and a prime l as in (4.11). Assume $N \geq (k+1)^4$. Then $N^k \equiv 1 \pmod{l}$ and $l > k+1$. Hence, Theorem 1 and Mazur's Theorem [23, Prop. (5.12)]) ensure that $\mathbf{1} \oplus \chi_l^{k-1}$ arises from a newform $f = q + \sum_{n\geq 2} a_n q^n$ of trivial Nebentypus, level N and weight k if $k \geq 4$ and $k = 2$ respectively. Put $K = K_f$ and $d = [K_f : \mathbb{Q}]$. Take a prime ideal $\lambda \subset O_K$ with $\lambda | l$ such that

$$a_p \equiv 1 + p^{k-1} \pmod{\lambda}, \qquad \text{for all primes } p \nmid Nl.$$

Moreover, Nl is odd, so that we may consider this congruence for $p = 2$. Deligne's bound ([6], Théorème 8.2) implies that, for every archimedean place τ of K, we have that $|\tau(a_2)| \leq 2 \cdot 2^{(k-1)/2}$. Hence, the algebraic integer $b := a_2 - 1 - 2^{k-1} \in O_K$ is nonzero, belongs to λ and satisfies $|\tau(b)| \leq (1 + 2^{(k-1)/2})^2$ for all τ as before. In particular, we have that

$$|N_{K/\mathbb{Q}}(b)| \leq \left(1 + 2^{(k-1)/2}\right)^{2d}.$$

Since $l | N_{K/\mathbb{Q}}(b)$, we conclude that $l \leq (1 + 2^{(k-1)/2})^{2d}$, implying

$$d_k^{\text{new}}(N) \geq d \geq \frac{\log l}{2\log(1 + 2^{(k-1)/2})} \geq \frac{\log N}{8\log(1 + 2^{(k-1)/2})}.$$

This ends the proof of Theorem 2.

4.1. Final remarks

The basic idea of using a_2 comes from the proof of a similar statement in weight 2 by Dieulefait, Jimenez Urroz and Ribet ([11, §2]). We are able to obtain a more general result because of our Theorem 1 (that generalizes Mazur's theorem to higher weight) and the information on primes p with large prime factors of $p-1$ given by Theorem 1 from [22].

It is conjectured that for any $\varepsilon > 0$, the set prime numbers p such that $P^+(p-1) \geq p^{1-\varepsilon}$ has a positive lower density $\kappa(\varepsilon) > 0$. The bound $\kappa(3/4) \geq 3/4$ is established in [22] by extending a method of Goldfeld who had previously obtained $\kappa(1/2) \geq 1/2$ ([16]). Much effort has been invested

in solving this conjecture for values of ε as small as possible (cf. [14], [1]). For the purposes of Theorem 2, progress in this difficult problem would improve on the value of the constant c_k. However, such improvements would not change the fact that our method produces a constant c_k that tends to zero with k.

On the other hand, any value of ε *bigger than* $3/4$ for which one could prove $\kappa(\varepsilon) > 3/4$ would enlarge the set of primes for which our bound is valid (at the expense of a small loss in the constant c_k), thus improving Theorem 2 in an interesting way. For a nice compilation of conjectures and results about the density of this and related sets, see Section 2 of [2].

If we assume Conjecture 3.2, it is possible to show an analogous lower bound for $d_k^{\mathrm{new}}(N)$ for N in an appropriate family of squarefree integers. Let r be a non-negative integer. Put

$$\mathcal{N}_r = \left\{ N \in \mathbb{N} : N = p_1 p_2 \cdots p_r, \omega(N) = r, P^+ \left(\gcd_{1 \le i \le r} (p_i - 1) \right) > N^{\frac{1}{2r}} \right\},$$

where $\omega(m)$ is number of different prime factors of the integer m and $p_1, \ldots, p_r$ denote primes. It is shown in [22] Theorem 2, that, as $x \to \infty$, we have :

$$\frac{x^{\frac{1}{2}+\frac{1}{2r}}}{(\log x)^{r+1}} \ll_r |\{N \in \mathcal{N}_r : N \le x\}| \ll_r \frac{x^{\frac{1}{2}+\frac{1}{2r}} (\log\log x)^{r-1}}{(\log x)^2}.$$

These estimates show that the set $\mathcal{N}_r$ is infinite and that, if $r \ge 2$, this set has density zero when regarded as a subset of squarefree numbers with exactly r prime divisors.

Mimicking the argument given above when N is prime, we finally prove the following result.

Theorem 4.2. *Assume Conjecture 3.2 and let q be a fixed prime number. Then, for every integer $r \ge 2$ and every even $k \ge 4$, we have that*

$$d_k^{\mathrm{new}}(N) \gg_{k,q} \frac{1}{r} \log N, \quad \text{as } N \to \infty, N \in \mathcal{N}_r \text{ coprime to } q.$$

Sketch of proof. Consider $N \in \mathcal{N}_r$. By assumption, there exists a prime l such that $N \equiv 1 \pmod{l}$ and $l > N^{\frac{1}{2r}}$. Moreover, if N is large enough, then $l > k+1$. By Conjecture 3.2, there exists a newform $f \in \mathcal{S}_k(\Gamma_0(N))$

with eigenvalues $\{a_p\}_p$ giving rise to $\mathbf{1} \oplus \chi_l^{k-1}$, that is :

$$a_p \equiv 1 + p^{k-1} \pmod{\lambda}, \qquad \text{for all primes } p \nmid Nl,$$

where λ is some prime ideal in $\overline{\mathbb{Q}}$ above l. Besides, N is coprime to q by assumption and thus for large enough N we have $q \nmid Nl$. We then conclude as in the proof of Theorem 2 using a_q instead of a_2.

Acknowledgements

The authors benefited from the warm hospitality of the mathematics department at Universidad Técnica Federico Santa María. We also received from É. Fouvry, F. Luca and E. Royer explanations and concrete suggestions on the analytic number theory surrounding Theorem 2. We thank K. Ribet and G. Wiese for interesting comments and references. P. Tsaknias has kindly shared numerical data with us. We are grateful to the anonymous referee, whose careful reading of the manuscript greatly helped to improve it. R. Menares is partially supported by FONDECYT grant 11110225 and CONICYT grant Inserción en la academia

References

[1] R. C. Baker and G. Harman, *The Brun-Titchmarsh theorem on average*. In: Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Vol. 138 of *Progr. Math.*, 39–103, Birkhäuser Boston, Boston, MA (1996).

[2] W. D. Banks, J. B. Friedlander, C. Pomerance, and I. E. Shparlinski, *Multiplicative structure of values of the Euler function*. In: High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams, Vol. 41 of *Fields Inst. Commun.*, 29–47, Amer. Math. Soc., Providence, RI (2004).

[3] N. Billerey and L. V. Dieulefait, *Explicit large image theorems for modular forms*. J. Lond. Math. Soc. (2), **89** (2014), no. 2, 499–523.

[4] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*. J. Symbolic Comput., **24** (1997), no. 3–4, 235–265. Computational algebra and number theory (London, 1993).

[5] H. Carayol, *Sur les représentations galoisiennes modulo l attachées aux formes modulaires*. Duke Math. J., **59** (1989), no. 3, 785–801.

[6] P. Deligne, *La conjecture de Weil. I.* Inst. Hautes Études Sci. Publ. Math., (1974), no. 43, 273–307.

[7] P. Deligne and J.-P. Serre, *Formes modulaires de poids* 1. Ann. Sci. École Norm. Sup. (4), **7** (1974), 507–530 (1975).

[8] F. Diamond, *Congruence primes for cusp forms of weight* $k \geq 2$. Astérisque, **196–197** (1991), 205–213. Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[9] F. Diamond and J. Shurman, *A first course in modular forms*. Vol. 228 of *Graduate Texts in Mathematics*, Springer-Verlag, New York (2005), ISBN 0-387-23229-X.

[10] F. Diamond and R. Taylor, *Nonoptimal levels of mod l modular representations*. Invent. Math., **115** (1994), no. 3, 435–462.

[11] L. V. Dieulefait, J. Jimenez Urroz, and K. A. Ribet, *Modular forms with large coefficient fields via congruences*. `arXiv:1111.5592` (2011)

[12] B. Edixhoven, *The weight in Serre's conjectures on modular forms*. Invent. Math., **109** (1992), no. 3, 563–594.

[13] G. Faltings and B. W. Jordan, *Crystalline cohomology and* $\mathrm{GL}(2, \mathbf{Q})$. Israel J. Math., **90** (1995), no. 1–3, 1–66.

[14] É. Fouvry, *Théorème de Brun-Titchmarsh: application au théorème de Fermat*. Invent. Math., **79** (1985), no. 2, 383–407.

[15] E. Ghate, *An introduction to congruences between modular forms*. In: Currents trends in number theory (Allahabad, 2000), 39–58, Hindustan Book Agency, New Delhi (2002).

[16] M. Goldfeld, *On the number of primes p for which* $p + a$ *has a large prime factor*. Mathematika, **16** (1969) 23–27.

[17] N. M. Katz, *A result on modular forms in characteristic p*. In: Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 53–61. Lecture Notes in Math., Vol. 601, Springer, Berlin (1977).

[18] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture. I.* Invent. Math., **178** (2009), no. 3, 485–504.

[19] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture. II.* Invent. Math., **178** (2009), no. 3, 505–586.

[20] R. Livné, *On the conductors of mod l Galois representations coming from modular forms*. J. Number Theory, **31** (1989), no. 2, 133–141.

[21] D. Loeffler and J. Weinstein, *On the computation of local components of a newform*. Math. Comp., **81** (2012), no. 278, 1179–1200.

[22] F. Luca, R. Menares, and A. Pizarro-Madariaga, *On shifted primes with large prime factors and their products*. Bull. Belg. Math. Soc. Simon Stevin, **22** (2015), no. 1, 39–47.

[23] B. Mazur, *Modular curves and the Eisenstein ideal*. Inst. Hautes Études Sci. Publ. Math., (1977), no. 47, 33–186 (1978).

[24] R. Ramakrishna, *Deformations of certain reducible Galois representations*. J. Ramanujan Math. Soc., **17** (2002), no. 1, 51–63.

[25] K. A. Ribet, *On l-adic representations attached to modular forms*. Invent. Math., **28** (1975) 245–275.

[26] K. A. Ribet, *Galois representations attached to eigenforms with Nebentypus*. In: Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), 17–51. Lecture Notes in Math., Vol. 601, Springer, Berlin (1977).

[27] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*. Invent. Math., **100** (1990), no. 2, 431–476.

[28] K. A. Ribet, *Non-optimal levels of mod l reducible Galois representations or Modularity of residually reducible representations* (July 9, 2010) Notes of a talk given at the Centre de Recerca Matemàtica (Barcelona).

[29] E. Royer, *Facteurs* $\mathbf{Q}$*-simples de* $J_0(N)$ *de grande dimension et de grand rang*. Bull. Soc. Math. France, **128** (2000), no. 2, 219–248.

[30] J.-P. Serre, *Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]*. In: Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416, 319–338. Lecture Notes in Math., Vol. 317, Springer, Berlin (1973).

[31] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J., **54** (1987), no. 1, 179–230.

[32] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Vol. 11 of *Publications of the Mathematical Society of Japan*. Princeton University Press, Princeton, NJ (1994), ISBN 0-691-08092-5. Reprint of the 1971 original, Kanô Memorial Lectures, 1.

[33] P. Tsaknias, *A possible generalization of Maeda's conjecture*. In: Computations with Modular Forms (Proceedings of a Summer School and Conference, Heidelberg, August/September 2011), Vol. 6 of *Contributions in Mathematical and Computational Sciences*, 317–329, Springer, Berlin (2014).

[34] L. C. Washington, *Introduction to cyclotomic fields*. Vol. 83 of *Graduate Texts in Mathematics*, Springer-Verlag, New York, second edition (1997), ISBN 0-387-94762-0.

Université Clermont Auvergne, Université Blaise Pascal
Laboratoire de Mathématiques, BP 10448
F-63000 Clermont-Ferrand, France
& CNRS, UMR 6620, LM, F-63171 Aubière, France
E-mail address: Nicolas.Billerey@math.univ-bpclermont.fr

Instituto de Matemáticas
Pontificia Universidad Católica de Valparaíso
Blanco Viel 596, Cerro Barón, Valparaíso, Chile
E-mail address: ricardo.menares@pucv.cl

Received January 15, 2014

MATHEMATICS OF COMPUTATION
Volume 86, Number 305, May 2017, Pages 1375–1401
http://dx.doi.org/10.1090/mcom/3129
Article electronically published on August 18, 2016

SUMS OF TWO S-UNITS VIA FREY-HELLEGOUARCH CURVES

MICHAEL A. BENNETT AND NICOLAS BILLEREY

Abstract. In this paper, we develop a new method for finding all perfect powers which can be expressed as the sum of two rational S-units, where S is a finite set of primes. Our approach is based upon the modularity of Galois representations and, for the most part, does not require lower bounds for linear forms in logarithms. Its main virtue is that it enables us to carry out such a program explicitly, at least for certain small sets of primes S; we do so for $S = \{2, 3\}$ and $S = \{3, 5, 7\}$.

1. Introduction

If $S = \{p_1, p_2, \ldots, p_k\}$ is a finite set of primes, we define the set of *S-units* to be those integers of the shape $\pm p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, with exponents α_i integers. The arithmetic of such sets has been frequently studied due to its connections to a wide variety of problems in Number Theory and Arithmetic Geometry. In the latter direction, equations of the shape

$$x + y = z^2, \tag{1.1}$$

where x and y are integer S-units for certain specific sets S, arise naturally when one wishes to make effective a theorem of Shafarevich on the finiteness of isomorphism classes of elliptic curves over a number field K with good reduction outside a given finite set of primes. By way of a simple example, if we wish to find all elliptic curves $E/\mathbb{Q}$ with nontrivial rational 2-torsion and good reduction outside $\{p_1, p_2, \ldots, p_k\}$, we are led to consider curves E of the shape

$$E \ : \ y^2 = x^3 + ax^2 + bx,$$

where a and b are rational integers satisfying

$$b^2(a^2 - 4b) = \pm 2^{\alpha_0} p_1^{\alpha_1} \cdots p_k^{\alpha_k},$$

for nonnegative integers α_i. Writing $|b| = 2^{\beta_0} p_1^{\beta_1} \cdots p_k^{\beta_k}$, we thus seek to solve equation (1.1), with $z = a$ and $S = \{2, p_1, p_2, \ldots, p_k\}$.

An algorithm for computing all solutions to equations of the shape (1.1), over $\mathbb{Q}$, can be found in Chapter 7 of de Weger [25], where, for instance, one can find a complete characterization of the solutions to equation (1.1) in case $S = \{2, 3, 5, 7\}$. This algorithm combines lower bounds for linear forms in complex and p-adic logarithms with lattice basis reduction for p-adic lattices.

Received by the editor July 21, 2015 and, in revised form, October 19, 2015.
2010 *Mathematics Subject Classification.* Primary 11D61; Secondary 11G05.
The first-named author was supported in part by a grant from NSERC.
The second-named author acknowledges the financial support of CNRS and ANR-14-CE25-0015 Gardio. He also warmly thanks PIMS and the Mathematics Department of UBC for hospitality and excellent working conditions.

More generally, for a given set of primes S, we may consider equations of the shape

$$x + y = z^n, \tag{1.2}$$

with $n \geq 2$ an integer, x and y integer S-units, and z a nonzero integer. We will call such a quadruple (x, y, z, n) a *primitive* solution of (1.2) if $\gcd(x, y)$ is nth-power free. Such equations are the main topic of discussion in Chapter 9 of Shorey and Tijdeman [20], due to their connections to the problem of characterizing perfect powers in nondegenerate binary recurrence sequences of algebraic numbers. If we write $y = y_0 y_1^n$ in equation (1.2), with y_0 nth-power free (whereby there are at most $2n^{|S|}$ choices for y_0), then it follows from the theory of Thue-Mahler equations that, for a fixed value of $n \geq 3$, the set of primitive solutions (x, y, z, n) of (1.2) is finite (see [20, Thm. 7.2]). A stronger statement still is the following (essentially Theorem 9.2 of [20]):

Theorem 1.1. *There are only finitely many coprime integer S-units x, y and w for which there exist integers $n \geq 2$ and $z \neq 0$ such that $x + y = wz^n$.*

The aim of this paper is to illustrate the use of Frey-Hellegouarch curves in solving equations like (1.1) and, more generally, (1.2). Specifically, we will apply such an approach to provide a new proof of Theorem 1.1 that *a priori* avoids the use of lower bounds for linear forms in logarithms, instead combining Frey-Hellegouarch curves, modularity and level-lowering with the aforementioned theorem of Shafarevich. In fairness, it must be mentioned that effective versions of the latter result have typically depended fundamentally on linear forms in logarithms; for recent papers along these lines, see the work of Fuchs, von Känel and Wüstholz [12] and von Känel [14]. The benefit of our approach is it enables us to, in Section 7, explicitly solve equation (1.2) for a pair of sets S with cardinality $|S| \geq 2$. To the best of our knowledge, this is the first time this has been carried out. Indeed, it is unclear whether the classical approach to Theorem 1.1 via only lower bounds for linear forms in logarithms can be made practical with current technology in any nontrivial situations.

The outline of our paper is as follows. Section 2 introduces our basic notation. In Section 3, we show how to obtain various finiteness results currently proved with techniques from Diophantine approximation, via Frey-Hellegouarch curves over $\mathbb{Q}$. Philosophically, this bears a strong resemblance to recent work of von Känel [14] and of Murty and Pasten [17]. Section 4 contains explicit details of the connections between Frey-Hellegouarch curves and modular forms. In Sections 5 and 6, we carry out such a "modular" approach quite explicitly for exponents $n = 2$ and $n = 3$ respectively. As an illustration of our methods, we completely solve (1.2) for $S = \{2, 3, 5, 7\}$ and $n \in \{2, 3\}$ (hence recovering de Weger's aforementioned result), and also for $S = \{2, 3, p\}$ and $n \in \{2, 3\}$, for every prime $p < 100$. It should be emphasized that this is not a "serious" application of our method, but merely meant as an illustration of a partial converse of the connection between solving equations of the shape (1.2) and computing elliptic curves. The reader may wish to omit these sections at first (and, for that matter, subsequent) readings. A more interesting result along these lines is due to Kim [15], where the connection between the more general cubic Thue-Mahler equation and Shafarevich's theorem is mapped out.

Section 7 contains, as previously mentioned, the main result of the paper, namely an explicit solution of equation (1.2) for the sets $S = \{2, 3\}$ and $\{3, 5, 7\}$. The

techniques we employ to prove these results, besides the aforementioned use of Frey-Hellegouarch curves and their associated modular forms, are local methods and appeal to computer algebra packages for solving Thue and Thue-Mahler equations; for the last of these, we rely extensively upon the computational number theory packages MAGMA [5], PARI [18] and SAGE [22].

We thank Rafael von Känel and Benjamin Matschke for pointing out to us a missing solution in a previous version of Proposition 5.4, and Nikos Tzanakis for helping us formulate our notation more precisely.

2. Notation

In what follows, we will let p be a prime number and m a nonzero integer. We denote by $\mathrm{rad}(m)$ the radical of $|m|$, i.e. the product of distinct primes dividing m, and by $\mathrm{ord}_p(m)$ the largest nonnegative integer k such that p^k divides m. We write $\mathrm{rad}_p(m)$ for the prime-to-p part of the radical of $|m|$, that is, the largest divisor of $\mathrm{rad}(m)$ that is relatively prime to p.

We will begin by noting some basic results on modular forms and connections between them and elliptic curves. Suppose that the q-expansion

$$f = q + \sum_{i \geq 2} c_i q^i \tag{2.1}$$

defines a weight 2, level N_0 (cuspidal) newform, with coefficients c_i generating a number field $K/\mathbb{Q}$. Further, let $E/\mathbb{Q}$ be an elliptic curve of conductor N and n a rational prime. If l is a prime satisfying $l \nmid N$, we define

$$a_l(E) = l + 1 - \#E(\mathbb{F}_l).$$

We say that E *arises modulo* n *from the newform* f and write $E \sim_n f$ if there exists a prime ideal $\mathfrak{N} \mid n$ of K such that, given any prime $l \neq n$, we have either

$$a_l(E) \equiv c_l \pmod{\mathfrak{N}}, \text{ if } l \nmid nNN_0 \tag{2.2}$$

or

$$l + 1 \equiv \pm c_l \pmod{\mathfrak{N}}, \text{ if } l \nmid nN_0 \text{ and } \mathrm{ord}_l(N) = 1. \tag{2.3}$$

3. Finiteness results via modularity and level-lowering

Throughout this section, we will let S denote a finite set of primes and a a positive integer. The second part of the following lemma is a classical and easy application of the theory of linear forms in logarithms (see Corollary 1.2 of [20]). We here give a complete proof of the result below using instead Frey-Hellegouarch curves and Shafarevich's theorem (Theorem IX.6.1 of [21]).

Lemma 3.1. *There are only finitely many integer S-units x, y, w with $\gcd(x, y) \leq a$ for which there exists a nonzero integer z such that $x + y = wz^2$. In particular, if x, y are integer S-units with $\gcd(x, y) \leq a$ such that $x + y$ is again an S-unit, then $\max\{|x|, |y|\}$ is bounded by a constant depending on S and a.*

Proof. Let x, y and w be integer S-units and let $z \neq 0$ be an integer such that $x+y = wz^2$. Consider the elliptic curve

$$E \ : \ Y^2 = X^3 + 2wzX^2 + ywX$$

with discriminant

$$\Delta(E) = 2^6 x^2 y^2 w^3.$$

It follows that E has good reduction outside $S \cup \{2\}$. By Shafarevich's theorem, there are only finitely many isomorphism classes of rational elliptic curves having good reduction outside a finite set of primes. This forces

$$j(E) = j(x,y) = 2^6 \cdot \frac{(4x+y)^3}{y^2 x}$$

to take only finitely many values when x and y range over all S-units. But then, since $j(x,y) = j(x/y, 1)$, the quotient x/y also takes finitely many different values and therefore $\max\{|x|, |y|\}$ is bounded whenever $\gcd(x,y) \leq a$. □

We next prove a version of Theorem 9.1 of [20] through appeal to (various) Frey-Hellegouarch curves and level-lowering.

Theorem 3.2. *Let x, y and w be integer S-units with $\gcd(x,y) \leq a$. Let $n \geq 2$ and $|z| > 1$ be integers. If $x + y = wz^n$, then n is bounded by a constant depending only on S and a.*

Proof. Assume $z \neq \pm 1$. If z is an integer S-unit, then, by the previous lemma, $\max\{|x|, |y|\}$ and thus n is bounded by a constant depending only on S and a. Therefore, one may assume that z is not an S-unit, and, in particular, we may choose a prime $q \notin S$ dividing z. Define an elliptic curve $E/\mathbb{Q}$ as follows. If $q \neq 2$, then consider

$$E \,:\, Y^2 = X(X-x)(X+y)$$

whose discriminant and c_4-coefficient are given by

$$\Delta(E) = 2^4 (xywz^n)^2 \quad \text{and} \quad c_4(E) = 2^4(w^2 z^{2n} - xy).$$

If however $q = 2$, we take

$$E \,:\, Y^2 + 3xXY - x^2 yY = X^3$$

with discriminant and c_4-coefficient given by

$$\Delta(E) = -3^3 x^8 y^3 wz^n \quad \text{and} \quad c_4(E) = 3^2 x^3 (9wz^n - y).$$

In both cases, E has multiplicative reduction at q with $\mathrm{ord}_q(\Delta(E))$ divisible by n. Let us then further assume that $n \geq 7$, $n \notin S$, and that the mod n representation attached to E is absolutely irreducible. By classical bounds on conductors (see [7] for instance), modularity of elliptic curves over $\mathbb{Q}$ ([6]) and Ribet's level-lowering theorem ([19]), the elliptic curve E arises modulo n from a weight 2 newform $f(z) = \sum_{m \geq 1} c_m e^{2i\pi mz}$ of (trivial Nebentypus and) level $N_0 \mid 2^8 \cdot 3^5 \cdot \prod_{\substack{p \in S \\ p \neq 2,3}} p^2$ such that N_0 is coprime to q. Therefore, N_0 is bounded by a constant depending only on S, and there exists a prime ideal $\mathfrak{N}$ above n in the ring of integers of the coefficient field K of f such that

$$c_q \equiv \pm(q+1) \pmod{\mathfrak{N}}.$$

By Deligne's bounds, $c_q \pm (q+1)$ is a nonzero algebraic integer in K whose Galois conjugates are all less than $(1+\sqrt{q})^2$ in absolute value and whose norm is divisible by n. Therefore we have $n \leq (1+\sqrt{q})^{2[K:\mathbb{Q}]}$. Since $[K:\mathbb{Q}]$ is bounded by the dimension of the space of weight-2 cuspforms of level N_0, it follows that n is bounded from above by a constant depending only on S, as desired. □

Combining these results with the finiteness of the number of solutions to Thue-Mahler equations (see, for instance, Theorem 7.1 of [20]) allows us to prove the following.

Theorem 3.3. *There are only finitely many integer S-units x, y, w with $\gcd(x, y) \leq a$ for which there exist integers $n \geq 2$ and $z \neq 0$ such that $x + y = wz^n$.*

Proof. By Lemma 3.1, the equation $x + y = \pm w$ has only finitely many solutions in integer S-units x, y and w, with $\gcd(x, y) \leq a$. Further, if x, y and w are integer S-units with $\gcd(x, y) \leq a$ such that there exist integers $n \geq 2$ and z with $|z| > 1$ satisfying $x + y = wz^n$, then, by the previous theorem, n is bounded by a constant depending only on S and a. But, for a fixed value of $n \geq 2$, the finiteness of solutions to equation $x + y = wz^n$ in S-units x, y, w with $\gcd(x, y) \leq a$ and integer z follows from Lemma 3.1 and from the finiteness of the set of solutions to Thue-Mahler equations for $n = 2$ and $n \geq 3$ respectively. □

Given a primitive solution (x, y, z, n) of (1.2), let us denote by d the gcd of x and y. Then d divides z^n and, without loss of generality, we may write $z^n/d = wz'^n$ where z' is a nonzero integer and w is an nth-power free positive integer S-unit. If $x' = x/d$ and $y' = y/d$, then one has

$$x' + y' = wz'^n. \tag{3.1}$$

Conversely, let x', y', w be pairwise coprime integer S-units with w positive satisfying the above equation and let w' be a positive S-unit such that $ww' = \mathrm{rad}(w)^n$. Put $x = w'x'$, $y = w'y'$ and $z = \mathrm{rad}(w)z'$. Then, (x, y, z, n) is a primitive solution of (1.2).

Therefore, all the primitive solutions of equation (1.2) can be deduced from the finite set of S-units satisfying the condition of Theorem 3.3 with $a = 1$. Moreover, combining this remark with the previous results, we have the following:

Corollary 3.4. *For a fixed value of $n \geq 2$, there are only finitely many triples (x, y, z) such that $x + y = z^n$ with z a nonzero integer, x, y integer S-units and $\gcd(x, y)$ nth-power free. Moreover, there are only finitely many primitive solutions to equation (1.2) if and only if $2 \notin S$.*

Proof. According to the discussion above, the first part of the corollary is a direct consequence of Theorem 3.3 (with $a = 1$). If, however, $2 \in S$, then $(2^{n-1}, 2^{n-1}, 2, n)$ is a primitive solution to (1.2) for any $n \geq 2$.

Conversely, if $2 \notin S$, consider a primitive solution (x, y, z, n) to (1.2). Dividing the equation by $\gcd(x, y)$ leads, as explained earlier, to an equation of the shape $x' + y' = wz'^n$ where x', y', w are coprime integer S-units and $z' \mid z$. By assumption, x', y', w are odd and therefore z' is even. In particular, we have $|z'| > 1$, and by Theorem 3.2, n is bounded independently of x, y and z. The desired finiteness result now follows from the first part of the corollary. □

In the proof of Lemma 3.1 we have appealed to $(n, n, 2)$-Frey-Hellegouarch curves, and for Theorem 3.2 to (n, n, n) and $(n, n, 3)$-Frey-Hellegouarch curves. The main goal of this paper is to make the statements of this section completely explicit in a number of situations. For this purpose, we will have use of refined information on Frey-Hellegouarch curves of the above signatures.

4. Background on Frey-Hellegouarch curves and modular forms

We recall some (by now) classical but useful results on Frey-Hellegouarch curves associated with generalized Fermat equations of signature (n, n, n), $(n, n, 2)$ and $(n, n, 3)$, and the newforms from which they arise.

4.1. **Signature** (n, n, n)**.** Let A, B and C be nth-power free pairwise coprime nonzero integers and let a, b and c be pairwise coprime nonzero integers such that

$$Aa^n + Bb^n = Cc^n. \tag{4.1}$$

We make the additional simplifying assumptions (which are not without loss of generality, but will be satisfied in the cases of interest to us) that

$$Aa^n \equiv -1 \pmod 4 \quad \text{and} \quad Bb^n \equiv 0 \pmod{16}.$$

Define an elliptic curve $E_{n,n,n}^{A,B,C}(a, b, c)$ via

$$E_{n,n,n}^{A,B,C}(a, b, c) \ : \ Y^2 + XY = X^3 + \frac{Bb^n - Aa^n - 1}{4}X^2 - \frac{AB(ab)^n}{16}X.$$

We summarize the properties of $E_{n,n,n}^{A,B,C}(a, b, c)$ that will be useful to us in the following result (see Kraus [16]).

Proposition 4.1. *If $n \geq 5$ is prime and $n \nmid ABC$, we have that*

$$E = E_{n,n,n}^{A,B,C}(a, b, c) \ \sim_n f,$$

for f a weight 2 cuspidal newform of level

$$N_0 = \begin{cases} 2\,\mathrm{rad}_2(ABC) & \text{if} \quad 0 \leq \mathrm{ord}_2(B) \leq 3 \text{ or } \mathrm{ord}_2(B) \geq 5, \\ \mathrm{rad}_2(ABC) & \text{if} \quad \mathrm{ord}_2(B) = 4. \end{cases}$$

Further, if l is prime with $l \nmid ABCabc$, then

$$a_l(E) \equiv l + 1 \pmod 4.$$

4.2. **Signature** $(n, n, 2)$**.** Next let a, b, c, A, B and C be nonzero integers such that

$$Aa^n + Bb^n = Cc^2, \tag{4.2}$$

with aA, bB and cC pairwise coprime, C squarefree and $n \geq 7$ prime. Without loss of generality, we may suppose that A and B are nth-power free and that we are in one of the following situations :

(1) $abABC \equiv 1 \pmod 2$ and $b \equiv -BC \pmod 4$;

(2) $ab \equiv 1 \pmod 2$ and either $\mathrm{ord}_2(C) = 1$ or $\mathrm{ord}_2(B) = 1$;

(3) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) = 2$ and $c \equiv -bB/4 \pmod 4$;

(4) $ab \equiv 1 \pmod 2$, $\mathrm{ord}_2(B) \in \{3, 4, 5\}$ and $c \equiv C \pmod 4$;

(5) $\mathrm{ord}_2(Bb^n) \geq 6$ and $c \equiv C \pmod 4$.

In cases (1) and (2), we will consider the curve

$$E^{A,B,C}_{(1),n,n,2}(a,b,c)\ :\ Y^2 = X^3 + 2cCX^2 + BCb^nX.$$

In cases (3) and (4), we will instead consider

$$E^{A,B,C}_{(2),n,n,2}(a,b,c)\ :\ Y^2 = X^3 + cCX^2 + \frac{BCb^n}{4}X,$$

and in case (5),

$$E^{A,B,C}_{(3),n,n,2}(a,b,c)\ :\ Y^2 + XY = X^3 + \frac{cC-1}{4}X^2 + \frac{BCb^n}{64}X.$$

These are all elliptic curves defined over $\mathbb{Q}$.

The following lemma summarizes some useful facts about these curves. Apart from its (easy-to-check) assertion (2) and up to some slight differences of notation, this is Lemma 2.1 of [3].

Lemma 4.2. *Let $i = 1, 2$ or 3 and $E = E^{A,B,C}_{(i),n,n,2}(a,b,c)$.*

(1) *The discriminant $\Delta(E)$ of the curve E is given by*

$$\Delta(E) = 2^{\delta_i}C^3B^2A(ab^2)^n, \quad \text{where } \delta_i = \begin{cases} 6 & \text{if } i = 1, \\ 0 & \text{if } i = 2, \\ -12 & \text{if } i = 3. \end{cases}$$

(2) *The j-invariant $j(E)$ of the curve E is given by*

$$j(E) = 2^6\frac{(4Aa^n + Bb^n)^3}{Aa^n(Bb^n)^2}.$$

(3) *The conductor $N(E)$ of the curve E is given by*

$$N(E) = 2^{\alpha}\mathrm{rad}_2(C)^2\mathrm{rad}_2(abAB),$$

where

$$\alpha = \begin{cases} 5 & \text{if } i = 1, \text{ case (1)}, \\ 8 & \text{if } i = 1, \text{ case (2) and } \mathrm{ord}_2(C) = 1, \\ 7 & \text{if } i = 1, \text{ case (2) and } \mathrm{ord}_2(B) = 1, \\ 2 & \text{if } i = 2, \text{ case (3)}, \mathrm{ord}_2(B) = 2 \text{ and } b \equiv -BC/4 \pmod 4, \\ 3 & \text{if } i = 2, \text{ case (3)}, \mathrm{ord}_2(B) = 2 \text{ and } b \equiv BC/4 \pmod 4, \\ 5 & \text{if } i = 2, \text{ case (4) and } \mathrm{ord}_2(B) = 3, \\ 3 & \text{if } i = 2, \text{ case (4) and } \mathrm{ord}_2(B) \in \{4, 5\}, \\ 0 & \text{if } i = 3, \text{ case (5) and } \mathrm{ord}_2(Bb^n) = 6, \\ 1 & \text{if } i = 3, \text{ case (5) and } \mathrm{ord}_2(Bb^n) \geq 7. \end{cases}$$

In particular, E has multiplicative reduction at each odd prime p dividing $abAB$. Also, E has multiplicative reduction at 2 if $\mathrm{ord}_2(Bb^n) \geq 7$.

(4) *The curve E has a $\mathbb{Q}$-rational point of order 2.*

For the purposes of our applications, we will have need of an analog of Proposition 4.1, essentially Lemma 3.3 of [3].

Proposition 4.3. *If $n \geq 7$ is prime and $ab \neq \pm 1$, we have, for each $i \in \{1,2,3\}$, that*

$$E = E^{A,B,C}_{(i),n,n,2}(a,b,c) \ \sim_n f,$$

for f a weight 2 cuspidal newform of level $N_0 = 2^{\alpha'}\mathrm{rad}_2(C)^2\mathrm{rad}_2(AB)$ where

$$\alpha' = \begin{cases} 1 & \text{if } ab \equiv 0 \pmod 2 \text{ and } AB \equiv 1 \pmod 2, \\ \alpha & \text{otherwise,} \end{cases}$$

where α is as defined in Lemma 4.2.

4.3. **Signature $(n,n,3)$.** Let us suppose that a,b,c,A,B and C are nonzero integers such that

$$Aa^n + Bb^n = Cc^3 \tag{4.3}$$

with $n \geq 5$ prime. Assume Aa, Bb, and Cc are pairwise coprime and, without loss of generality, that $Aa \not\equiv 0 \pmod 3$ and $Bb^n \not\equiv 2 \pmod 3$. Further, suppose that C is cubefree and that A and B are nth-power free. We consider the elliptic curve

$$E^{A,B,C}_{n,n,3}(a,b,c) : \ Y^2 + 3CcXY + C^2Bb^nY = X^3.$$

With the above assumptions, we have the following result (Lemma 2.1 of [4]).

Lemma 4.4. *Let $E = E^{A,B,C}_{n,n,3}(a,b,c)$.*

(1) *The discriminant $\Delta(E)$ of the curve E is given by*

$$\Delta(E) = 3^3AB^3C^8(ab^3)^n.$$

(2) *The j-invariant of E is given by*

$$j(E) = 3^3\frac{Cc^3(9Aa^n + Bb^n)^3}{AB^3(ab^3)^n}.$$

(3) *The conductor $N(E)$ of the curve E is*

$$N(E) = 3^\alpha\mathrm{rad}_3(ABab)\mathrm{rad}_3(C)^2$$

where

$$\alpha = \begin{cases} 2 & \text{if } 9 \mid (2 + C^2Bb^n - 3Cc), \\ 3 & \text{if } 3 \parallel (2 + C^2Bb^n - 3Cc), \\ 4 & \text{if } \mathrm{ord}_3(Bb^n) = 1, \\ 3 & \text{if } \mathrm{ord}_3(Bb^n) = 2, \\ 0 & \text{if } \mathrm{ord}_3(Bb^n) = 3, \\ 1 & \text{if } \mathrm{ord}_3(Bb^n) > 3, \\ 5 & \text{if } 3 \mid C. \end{cases}$$

In particular, E has split multiplicative reduction at each prime $p \neq 3$ dividing Bb, split multiplicative reduction at each prime dividing Aa congruent to 1, 4, 5, 7, 16, 17 or 20 modulo 21, and nonsplit multiplicative reduction at all other primes dividing Aa, except 3. Also, E has split multiplicative reduction at 3 if $\mathrm{ord}_3(Bb^n) > 3$, and good reduction if $\mathrm{ord}_3(Bb^n) = 3$.

(4) *The curve E has a $\mathbb{Q}$-rational point of order 3.*

In what follows, we will apply Frey-Hellegouarch curves of signature $(n, n, 3)$ more frequently than other signatures. The following result, essentially Proposition 4.2 of [4] (though it is worth noting that the value $N_n(E)$ as defined in Lemma 3.4 of that paper is actually stated incorrectly for the cases where $n \mid ABC$), will be of particular use to us.

Proposition 4.5. *If $n \geq 5$ is prime, $ab \neq \pm 1$ and $E^{A,B,C}_{n,n,3}(a,b,c)$ does not correspond to the identities*

$$1 \cdot 2^5 + 27 \cdot (-1)^5 = 5 \cdot 1^3 \quad \text{or} \quad 1 \cdot 2^7 + 3 \cdot (-1)^7 = 1 \cdot 5^3,$$

then we have that

$$E = E^{A,B,C}_{n,n,3}(a,b,c) \ \sim_n f,$$

for $f = \sum_{m \geq 1} c_m q^m$ a weight 2 cuspidal newform of level

$$N_0 = 3^{\alpha'} \mathrm{rad}_3(AB)\mathrm{rad}_3(C)^2,$$

where $\alpha' = \alpha$ with α as defined in Lemma 4.4 unless $\mathrm{ord}_3(Bb^n) \geq 3$, in which case we have

$$\alpha' = \begin{cases} 0 & \text{if } \mathrm{ord}_3(B) = 3, \\ 1 & \text{otherwise.} \end{cases}$$

More precisely, if l is a prime, coprime to nN_0, then n divides $\mathrm{Norm}_{K/\mathbb{Q}}(c_l - a_l)$ where K is the number field generated by the Fourier coefficients of f and $a_l \in S_l$, with

$$S_l = \{x \colon |x| < 2\sqrt{l},\ x \equiv l+1 \pmod 3\} \cup \{l+1\},$$

if $l \equiv 1, 4, 5, 7, 16, 17, 20 \pmod{21}$, and

$$S_l = \{x \colon |x| < 2\sqrt{l},\ x \equiv l+1 \pmod 3\} \cup \{-l-1, l+1\},$$

otherwise.

5. The case $n = 2$

In this section, we consider equation (1.1) (as treated by de Weger in [25] and [26]), via an $(n, n, 2)$ Frey-Hellegouarch curve approach. According to the discussion of Section 3, the corresponding equations to treat are of the shape

$$x + y = wz^2 \tag{5.1}$$

where x, y and w are pairwise coprime integer S-units. Define $a = b = 1$, $c = z$, $A = x$, $B = y$ and $C = w$. Then we have $Aa^n + Bb^n = Cc^2$ and may assume, without loss of generality, that we are in one of the situations (1)-(5) of §4.2. Consider the associated elliptic curve $E/\mathbb{Q}$ of Lemma 4.2. It has good reduction outside $S' = S \cup \{2\}$. Therefore, if we know representatives $F/\mathbb{Q}$ of all (the finitely many) isomorphism classes of rational elliptic curves (with a nontrivial two-torsion subgroup) having good reduction outside S', all that remains to do to solve (5.1) is to check for an equality

$$j(E) = j(F), \quad \text{where } j(E) = 2^6 \cdot \frac{(4x+y)^3}{y^2 x}$$

and $j(F)$ denote the j-invariants of E and F respectively. Computing such representatives is a classical but challenging problem that has only been achieved for a rather restrictive list of sets, including $\{2, 3, 5, 7\}$, $\{2, 3, 11\}$, $\{2, 13\}$, $\{2, 17\}$, $\{2, 19\}$ and $\{2, 23\}$ (see [9]).

Nevertheless, the precise information on the conductor $N(E)$ of E provided by Lemma 4.2, namely $N(E) = 2^{\alpha}\mathrm{rad}_2(w)^2\mathrm{rad}_2(xy)$ where

$$\alpha = \begin{cases} 5 & \text{if } xyw \equiv 1 \pmod 2 \text{ and } yw \equiv -1 \pmod 4, \\ 8 & \text{if } \mathrm{ord}_2(w) = 1, \\ 7 & \text{if } \mathrm{ord}_2(y) = 1, \\ 2 & \text{if } \mathrm{ord}_2(y) = 2 \text{ and } z \equiv w \equiv -y/4 \pmod 4, \\ 3 & \text{if } \mathrm{ord}_2(y) = 2 \text{ and } z \equiv -w \equiv -y/4 \pmod 4, \\ 5 & \text{if } \mathrm{ord}_2(y) = 3 \text{ and } z \equiv w \pmod 4, \\ 3 & \text{if } \mathrm{ord}_2(y) \in \{4, 5\} \text{ and } z \equiv w, \\ 0 & \text{if } \mathrm{ord}_2(y) = 6 \text{ and } z \equiv w \pmod 4, \\ 1 & \text{if } \mathrm{ord}_2(y) \geq 7 \text{ and } z \equiv w \pmod 4, \end{cases}$$

allows us to sometimes show, for some specific sets S, that we have $N(E) \leq 350000$ except for some precisely identified quadruples (x, y, w, z). In that situation, we can therefore appeal, via the SAGE package `database_cremona_ellcurve` ([22], [8]), to Cremona's tables, which, at the time of writing (Spring 2015), contain representatives for all rational elliptic curves of conductor less than 350000.

By way of example, consider $S = \{2, 3, 5, 7\}$ or $S = \{2, 3, p\}$ with p prime, $11 \leq p < 100$. We stress the fact that, for most of these latter sets, we presently do not know a complete list of representatives of the isomorphism classes of rational elliptic curves having good reduction outside S. Nevertheless, the strategy outlined above does apply and this allows us to easily recover de Weger's result mentioned in the Introduction and to solve equations that remained unsolved in a recent paper by Terai [24] (see Corollary 5.5). We carry out the details in the next two subsections; the SAGE code used for our computations is available at

`http://www.math.ubc.ca/~bennett/Sum_Of_Two_S-units.pdf`.

5.1. **The case $S = \{2, 3, 5, 7\}$.** Specializing the approach above to the case $S = \{2, 3, 5, 7\}$ considered by de Weger, we note that *a priori* we must consider conductors of the shape

$$N(E) = 2^{\alpha} \cdot 3^{\delta_3} \cdot 5^{\delta_5} \cdot 7^{\delta_7},$$

where $\delta_i = \mathrm{ord}_i(N(E)) \leq 2$, $i = 3, 5, 7$, and $\alpha = \mathrm{ord}_2(N(E)) \in \{0, 1, 2, 3, 5, 7, 8\}$. However, we have the following easy result.

Lemma 5.1. *In each case $N(E) \leq 350000$. Further, if $(\delta_3, \delta_5, \delta_7) \in \{0, 2\}$, then either*

$$(x, y, w, z) \in \{(-1, 8, 7, -1), (-1, 64, 7, 3), (1, 4, 5, -1), (-1, 16, 15, -1), \\ (1, 2, 3, \pm 1), (-1, 4, 3, -1), (-1, 2, 1, \pm 1), (1, 8, 1, -3), (1, 1, 2, \pm 1)\}$$

or $(\delta_3, \delta_5, \delta_7) \in \{(0, 0, 0), (0, 0, 2), (2, 2, 0)\}$ and $\alpha = 1$.

Proof. If $\delta_3, \delta_5, \delta_7 \in \{0, 2\}$, we have a solution to an equation of the shape

$$2^k + \epsilon = wz^2,$$

where k is nonnegative, $\epsilon = \pm 1$ and $\mathrm{rad}(w) \mid 2 \cdot 3 \cdot 5 \cdot 7$. The solutions to this equation for $k \leq 6$ correspond to those listed in the lemma. Moreover, if $k \geq 7$, none of these equations have a solution modulo 840 unless we have $w = 1, 7$ or 15, that is, $(\delta_3, \delta_5, \delta_7) \in \{(0, 0, 0), (0, 0, 2), (2, 2, 0)\}$.

Similarly, it is easy to check that $N(E) \leq 350000$, unless we have

$$\alpha = 8 \text{ and } (\delta_3, \delta_5, \delta_7) = (2,2,2), (2,2,1), (2,1,2), (1,2,2),$$
$$\alpha = 7 \text{ and } (\delta_3, \delta_5, \delta_7) = (2,2,2), (1,2,2),$$

or

$$\alpha = 5 \text{ and } (\delta_3, \delta_5, \delta_7) = (2,2,2).$$

Of these, only the cases

$$(\alpha, \delta_3, \delta_5, \delta_7) = (8,2,2,1), (8,2,1,2), (8,1,2,2), (7,1,2,2)$$

may correspond to solutions to (5.1), namely to equations of the shape

$$7^k \pm 1 = 2 \cdot 3 \cdot 5z^2, \quad 5^k \pm 1 = 2 \cdot 3 \cdot 7z^2, \quad 3^k \pm 1 = 2 \cdot 5 \cdot 7z^2, \quad 3^k \pm 2 = 5 \cdot 7z^2,$$

and $2 \cdot 3^k \pm 1 = 5 \cdot 7z^2$. Each of these equations, however, is insoluble modulo 840. □

From Lemma 5.1 and the above discussion, we may thus appeal to Cremona's SAGE package to reproduce de Weger's results (with a slightly faster search provided by the restrictions on the exponents given in the above lemma). In particular, if $S = \{2,3,5,7\}$, as noted in [25, Thm. 7.2], there are precisely 388 solutions (x,y,z) to (1.1) with $\gcd(x,y)$ squarefree and $x \geq |y| > 0$ and $z > 0$. We list these solutions in the file `http://www.math.ubc.ca/~bennett/2-3-5-7.pdf`.

As an obvious byproduct, we also obtain a complete list of solutions to (1.1) with $S = \{2,3\}$ and $S = \{3,5,7\}$. As we will consider these sets again in Section 7, we state these results here.

Proposition 5.2. *The only primitive integer solutions to equation (1.1) with $S = \{2,3\}$ and with, say, $x \geq |y| > 0$ are given by*

$$(x,y) = (2,-1), (2,2), (3,-2), (3,1), (4,-3), (6,-2), (6,3), (8,1), (9,-8), (12,-3),$$
$$(16,9), (18,-2), (24,1), (27,-2), (48,1), (81,-32), (288,1) \text{ and } (486,-2).$$

Proposition 5.3. *The only primitive integer solutions to equation (1.1) with $S = \{3,5,7\}$ and with, say, $x \geq |y| > 0$ are given by*

$$(x,y) = (3,1), (5,-1), (7,-3), (9,-5), (9,7), (15,1), (21,-5), (21,15), (25,-21),$$
$$(25,-9), (35,1), (49,-45), (49,15), (63,1), (105,-5), (135,-35), (147,-3),$$
$$(175,21), (175,81), (189,-125), (189,7), (343,-243), (405,-5), (625,-49),$$
$$(675,1), (729,-245), (1029,-5), (3375,2401), (3969,-125), (9375,1029),$$
$$(15625,-1701), (59535,1), (688905,-5) \text{ and } (4782969,4375).$$

5.2. **The case $S = \{2,3,p\}$.** We now turn our attention to the case $S = \{2,3,p\}$ where p is a prime in the range $11 \leq p < 100$. Once again, we must *a priori* consider conductors of the shape

$$N(E) = 2^\alpha \cdot 3^{\delta_3} \cdot p^{\delta_p},$$

where $\delta_i = \mathrm{ord}_i(N(E)) \leq 2$, $i = 3, p$, and $\alpha = \mathrm{ord}_2(N(E)) \in \{0,1,2,3,5,7,8\}$; many of these conductors exceed the limits of the current Cremona database. However, we have the following result.

Proposition 5.4. *In each case $N(E) \leq 350000$, unless (x,y,w,z) corresponds to one of the following equations:*

$$3^4 + 1 = 2 \cdot 41, \quad 2 \cdot 3^3 - 1 = 53, \quad 3^{10} - 1 = 2 \cdot 61 \cdot 22^2, \quad 3^4 + 2 = 83, \quad 3^4 - 2 = 79,$$
$$3^5 + 1 = 61 \cdot 2^2, \quad 2^3 \cdot 3^2 + 1 = 73, \quad 2^3 \cdot 3^2 - 1 = 71, \quad 3^4 + 2^3 = 89, \quad 3^4 - 2^3 = 73.$$

Proof. It is easy to check that we have $N(E) \leq 350000$ unless we are in one of the following situations:

$(\alpha, \delta_3, \delta_p)$	$(8,2,2)$	$(7,2,2)$	$(8,1,2)$	$(7,1,2)$	$(8,0,2)$
p	≥ 13	≥ 19	≥ 23	≥ 31	≥ 37
$(\alpha, \delta_3, \delta_p)$	$(5,2,2)$	$(7,0,2)$	$(5,1,2)$	$(3,2,2)$	
p	≥ 37	≥ 53	≥ 61	≥ 71	

Of these, only the cases $(\alpha, \delta_3, \delta_p) \in \{(8,1,2), (7,1,2), (5,1,2)\}$ may actually correspond to our equations. We are therefore led to solve the following equations, where $\epsilon = \pm 1$ and k is a positive integer:

$$3^k + \epsilon = 2pz^2, \quad \text{for } p \geq 23,$$

$$2 \cdot 3^k + \epsilon = pz^2 \quad \text{and} \quad 3^k + 2\epsilon = pz^2, \quad \text{for } p \geq 31,$$

and

$$3^k + \epsilon = pz^2, \quad 2^3 \cdot 3^k + \epsilon = pz^2 \quad \text{and} \quad 3^k + 2^3\epsilon = pz^2, \quad \text{for } p \geq 61.$$

We deal with each of these in turn. Considering first the equation $3^k + \epsilon = 2pz^2$, we readily check that it has no solution modulo $8p$ for odd values of k and $23 \leq p < 100$. Assume therefore that k is even. If moreover $\epsilon = -1$, then by factorization, we end up with an equation of the shape $3^m \pm 1 = z'^2$ or $3^m \pm 1 = 2z'^2$ for some integer z'. According to [3, Thm. 1.1], this leads to a unique solution to our equation, namely $3^{10} - 1 = 2 \cdot 61 \cdot 22^2$.

Finally, if k is even and $\epsilon = +1$, the equation $3^k + 1 = 2pz^2$ has no solution modulo $24p$ unless $p = 29, 41, 53$ or 89. However, for $p = 29, 53$ and 89, it has no solution modulo pq where $q = 43, 313$ and 23 respectively. In the remaining case, namely $p = 41$, write $3^k = 3^\beta x^3$ with $0 \leq \beta \leq 2$ and $x \in \mathbb{Z}$. Then, $(X, Y) = (2 \cdot 3^\beta \cdot 41x, 2^2 3^\beta \cdot 41^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 + 2^3 \cdot 3^{3\beta} \cdot 41^3.$$

Computing its integral points using the aforementioned SAGE command thus leads to the unique solution $3^4 + 1 = 2 \cdot 41$.

We now turn our attention to the equation $2 \cdot 3^k + \epsilon = pz^2$. We easily check that for p in the range $31 \leq p < 100$, this equation has no solution modulo $24p$ unless we have

$$(\epsilon, p) = (1, 31),\ (1, 43),\ (1, 79),\ (-1, 53) \text{ or } (-1, 89).$$

For $p = 31, 43, 79$ and 89, the corresponding equation has no solution modulo pq where $q = 13, 7, 13$ and 23 respectively. For the remaining case, that is, $(\epsilon, p) = (-1, 53)$, reducing modulo 53, we find that $k \equiv 0 \pmod 3$. Writing $k = 3k_0$, $(X, Y) = (2 \cdot 3^{k_0} \cdot 53, 2 \cdot 53^2 z)$ is thus an integral point on the elliptic curve

$$Y^2 = X^3 - 2^2 \cdot 53^3.$$

As before, we compute its integral points on SAGE and deduce the unique solution $2 \cdot 3^3 - 1 = 53$.

Consider now equation $3^k + 2\epsilon = pz^2$ for p in the range $31 \leq p \leq 100$. We check that there is no solution modulo $24p$ unless we have

$$(\epsilon, p) = (1, 53),\ (1, 59),\ (1, 83),\ (-1, 31),\ (-1, 79) \text{ and } (-1, 97).$$

For $p = 53, 59, 31$ and 97, we however have that the corresponding equation has no solution modulo pq where $q = 2887, 523, 13$ and 7 respectively. It remains to deal

with the cases $(\epsilon, p) = (1, 83)$ and $(-1, 79)$. In the latter case, we find that $k \equiv 1 \pmod 3$ by reducing modulo 79. Writing $k = 3k_0+1$, $(X, Y) = (3^{k_0+1} \cdot 79, 3^1 \cdot 79^2 z)$ is necessarily an integral point on the elliptic curve

$$Y^2 = X^3 - 2 \cdot 3^2 \cdot 79^3.$$

This again leads to a unique solution, namely $3^4 - 2 = 79$. In the former case, that is, $(\epsilon, p) = (1, 83)$, write $3^k = 3^\beta x^3$ with $0 \le \beta \le 2$ and $x \in \mathbb{Z}$. Then, $(X, Y) = (3^\beta \cdot 83x, 3^\beta \cdot 83^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 + 2 \cdot 3^{2\beta} \cdot 83^3.$$

Computing its integral points using the command `IntegralPoints` in MAGMA ([5]) leads to a unique solution which is $3^4 + 2 = 83$. We note here that the corresponding routine in SAGE has marked difficulty with this equation.

We now consider equation $3^k + \epsilon = pz^2$. If $\epsilon = +1$, then we have no solution modulo $24p$ unless $p = 61, 67$ or 79. For $p = 67$ or 79, however, we have that the corresponding equation has no solution modulo pq where $q = 23$ or 2341 respectively. If $p = 61$, write $3^k = 3^\beta x^3$ with $0 \le \beta \le 2$ and $x \in \mathbb{Z}$. Then, $(X, Y) = (3^\beta \cdot 61x, 3^\beta \cdot 61^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 + 3^{2\beta} \cdot 61^3.$$

Computing its integral points using SAGE leads to the unique solution $3^5 + 1 = 61 \cdot 2^2$. If now $\epsilon = -1$, then reducing $3^k - 1 = pz^2$ modulo 8 shows that k is necessarily even. Write $k = 2k_0$ and $3^{k_0} = 3^\beta x^3$ with $0 \le \beta \le 2$ and $x \in \mathbb{Z}$. Then, for some divisor z_1 of z, either $(X, Y) = (2 \cdot 3^\beta x, 2^2 \cdot 3^\beta z_1)$ or $(X, Y) = (2 \cdot 3^\beta x, 2 \cdot 3^\beta z_1)$ is an integral point on one of the elliptic curves

$$Y^2 = X^3 \pm 2^3 \cdot 3^{2\beta}.$$

However none of their integral points (which we have already computed) corresponds to a solution of our equation.

Let us now consider the equation $2^3 \cdot 3^k + \epsilon = pz^2$. If $\epsilon = +1$, then the corresponding equation has no solution modulo $24p$ unless $p = 73$ or 97. Moreover in the former case, we have $k \equiv 2 \pmod 3$. If $p = 97$, we check that $2^3 \cdot 3^k + 1 = 97z^2$ has no solution modulo $13 \cdot 97$. Assume thus that $p = 73$ and write $k = 3k_0 + 2$. Then $(X, Y) = (2 \cdot 3^{2+k_0} \cdot 73, 3^2 \cdot 73^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 + 3^4 \cdot 73^3.$$

We therefore find that there is only one solution corresponding to $2^3 \cdot 3^2 + 1 = 73$. Similarly, if $\epsilon = -1$, then the corresponding equation has no solution modulo $24p$ unless $p = 71$. Write $3^k = 3^\beta x^3$ with $x \in \mathbb{Z}$ and $0 \le \beta \le 2$. Then, $(X, Y) = (2 \cdot 3^\beta \cdot 71x, 3^\beta \cdot 71^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 - 3^{2\beta} \cdot 71^3.$$

This gives rise to the unique solution $2^3 \cdot 3^2 - 1 = 71$.

We finally deal with the last equation, namely $3^k + 2^3\epsilon = pz^2$. If $\epsilon = +1$, then the corresponding equation has no solution modulo $24p$ unless $p = 83$ or 89. If $p = 83$, we find a local obstruction modulo $2^3 \cdot 7 \cdot 13$. If $p = 89$, we write $3^k = 3^\beta x^3$ with $x \in \mathbb{Z}$ and $0 \le \beta \le 2$, whereby $(X, Y) = (3^\beta \cdot 89x, 3^\beta \cdot 89^2 z)$ is an integral point on the elliptic curve

$$Y^2 = X^3 + 2^3 \cdot 3^{2\beta} \cdot 89^3.$$

We therefore conclude that there is only one solution corresponding to $3^4+2^3=89$. Similarly, if $\epsilon=-1$, then the corresponding equation has no solution modulo $24p$ unless $p=67$ or $p=73$. Moreover, in that latter case, we have $k\equiv 1 \pmod 3$, and it is easy to check that $3^k-2^3=67z^2$ has no solution modulo $23\cdot 67$. Assume therefore that $p=73$ and write $k=3k_0+1$. Then $(X,Y)=(3^{k_0+1}\cdot 73, 3\cdot 73^2 z)$ is an integral point on the elliptic curve

$$Y^2=X^3-2^3 3^2\cdot 73^3.$$

This gives rise to the unique solution $3^4-2^3=73$, which completes the proof of the proposition. □

Utilizing Proposition 5.4, we can again appeal to Cremona's SAGE package to compute primitive solutions to equation (1.1). For each set $S=\{2,3,p\}$, we have tabulated these solutions at `http://www.math.ubc.ca/~bennett/2-3-p.pdf`. By quick examination of this table for $p=23$ and $p=47$, we immediately deduce the following result about equations that remained unsolved in Proposition 3.3 of Terai [24] (but have been recently solved via rather different methods by Deng [11]).

Proposition 5.5. *The only solutions to* $x^2+23^m=12^n$ *and* $x^2+47^m=24^n$ *are* $(x,m,n)=(\pm 11,1,2)$ *and* $(x,m,n)=(\pm 23,1,2)$ *respectively.*

6. The case $n=3$

We now deal with equation (1.2) when $n=3$ using a $(p,p,3)$ Frey-Hellegouarch curve approach. The corresponding equations to treat are of the shape

$$x+y=wz^3 \tag{6.1}$$

where x,y and w are pairwise coprime integer S-units. We may assume, without loss of generality, that w is cubefree and positive and that we have $x\not\equiv 0 \pmod 3$ and $y\not\equiv 2 \pmod 3$. With the notation of §4.3, we attach to such a solution the elliptic curve $E=E_{n,n,3}^{x,y,w}(1,1,z)$:

$$E:\ Y^2+3wzXY+w^2yY=X^3.$$

As in Section 5, all that remains to do to solve equation (6.1) is to check for an equality

$$j(E)=j(F),\quad \text{where } j(E)=3^3\frac{(x+y)(9x+y)^3}{xy^3}$$

and $j(F)$ denote the j-invariants of E and F respectively, with F ranging over all representatives of the isomorphism classes of elliptic curves having good reduction outside $S\cup\{3\}$ (and a nontrivial 3-torsion subgroup). To circumvent the difficulty of computing representatives and make this approach work for a broader list of sets S (including some for which we do not know a complete list of such representatives), we also make use of the precise formula for the conductor of E given by Lemma 4.4,

namely $N(E) = 3^{\alpha}\mathrm{rad}_3(xy)(\mathrm{rad}_3(w))^2$ where

$$\alpha = \begin{cases} 2 & \text{if } w^2y - 3wz \equiv -2 \pmod 9, \\ 3 & \text{if } w^2y - 3wz \equiv 1 \text{ or } 4 \pmod 9, \\ 4 & \text{if } \mathrm{ord}_3(y) = 1, \\ 3 & \text{if } \mathrm{ord}_3(y) = 2, \\ 0 & \text{if } \mathrm{ord}_3(y) = 3, \\ 1 & \text{if } \mathrm{ord}_3(y) > 3, \\ 5 & \text{if } 3 \mid w. \end{cases}$$

As in the previous section, we now apply this approach to the sets $S = \{2, 3, 5, 7\}$ and $S = \{2, 3, p\}$ with p prime, $11 \le p \le 100$.

6.1. **The case $S = \{2, 3, 5, 7\}$.** Specializing to $S = \{2, 3, 5, 7\}$, we *a priori* need to consider all conductors of the shape

$$N(E) = 2^{\delta_2} \cdot 3^{\alpha} \cdot 5^{\delta_5} \cdot 7^{\delta_7}$$

with $\delta_i(N) = \mathrm{ord}_i \in \{0, 1, 2\}$, $i = 2, 5, 7$ and $\alpha = \mathrm{ord}_3(N) \in \{0, 1, 2, 3, 4, 5\}$. However, we have, as before, the following result.

Lemma 6.1. *In each case $N(E) < 350000$.*

Proof. It is easy to check that we have the desired inequality for $N(E)$, unless

$$(\alpha, \delta_2, \delta_5, \delta_7) \in \{(5, 1, 2, 2), (5, 2, 2, 2), (4, 2, 2, 2)\}.$$

Among these possibilities, only the case $(\alpha, \delta_2, \delta_5, \delta_7) = (5, 1, 2, 2)$ may correspond to solutions. Since each of the equations

$$2^k \pm 1 = 3^{\delta_3}5^{\delta_5}7^{\delta_7}z^3, \quad \text{with each } \delta_i \in \{1, 2\}$$

is insoluble modulo 840, we obtain the stated result. □

As explained previously, we can therefore appeal to Cremona's table of elliptic curves to solve equation (6.1) and thus (1.2) with $n = 3$ and $S = \{2, 3, 5, 7\}$. It turns out that there are exactly 207 triples (x, y, z) such that $x+y = z^3$ with x and y $\{2, 3, 5, 7\}$-units, with $\gcd(x, y)$ cubefree and, say, $x \ge |y| > 0$, and z a positive integer. They are listed in the file `http://www.math.ubc.ca/~bennett/2-3-5-7.pdf`. From there we easily extract the latter solutions to this equation for $S = \{2, 3\}$ and $S = \{3, 5, 7\}$. We list them here for later use.

Proposition 6.2. *The only primitive solutions to equation (1.2) with $n = 3$, $S = \{2, 3\}$ and, say, $x \ge |y| > 0$ are given by*

$$(x, y) = (2, -1),\ (3, -2),\ (4, -3),\ (4, 4),\ (6, 2),\ (9, -8),\ (9, -1),\ (12, -4),\ (18, 9),\ (24, 3),\ (36, -9) \quad \textit{and} \quad (128, -3).$$

Proposition 6.3. *The only primitive solutions to equation (1.2) with $n = 3$, $S = \{3, 5, 7\}$ and, say, $x \ge |y| > 0$ are given by*

$$(x, y) = (5, 3),\ (7, 1),\ (9, -1),\ (15, -7),\ (35, -27),\ (49, 15),\ (63, 1),\ (189, -125),\ (225, -9),\ (441, -225),\ (1225, -225),\ (1875, -147) \quad \textit{and} \quad (3969, -1225).$$

6.2. **The case $S = \{2, 3, p\}$.** We now turn our attention to the case $S = \{2, 3, p\}$ where $11 \leq p < 100$ is prime. Once again, we *a priori* need to consider all conductors of the shape

$$N(E) = 2^{\delta_2} \cdot 3^{\alpha} \cdot p^{\delta_p}$$

with $\delta_i = \mathrm{ord}_i(N) \in \{0, 1, 2\}$, $i = 2, p$ and $\alpha = \mathrm{ord}_3(N) \in \{0, 1, 2, 3, 4, 5\}$. However, we have the following result, the proof of which, it being quite similar to that of Proposition 5.4, we omit for the sake of concision.

Proposition 6.4. *We have $N(E) \leq 350000$ unless (x, y, w, z) corresponds to one of the following equations:*

$$2^7 + 1 = 3 \cdot 43, \quad 3 \cdot 2^4 - 1 = 47, \quad 3 \cdot 2^5 + 1 = 97,$$

$$2^6 + 3 = 67 \quad \textit{and} \quad 2^6 - 3 = 61.$$

Combining this proposition with Cremona's tables of elliptic curves then allows us to compute all the solutions to (1.2) with $n = 3$, $S = \{2, 3, p\}$ and p as above. We list them in the file `http://www.math.ubc.ca/~bennett/2-3-p.pdf`.

7. The general equation

In this last section, we completely solve equation (1.2) for two specific sets of primes, namely $S = \{2, 3\}$ and $S = \{3, 5, 7\}$, using a variety of Frey-Hellegouarch curves, level-lowering and heavy computations involving modular forms and Thue-Mahler equations. It is only through careful combination of a variety of Frey-Hellegouarch curves, in conjunction with local arguments, that we are able to reduce these problems to a feasible collection of Thue-Mahler equations (in our case, all of degree 5). This is, in essence, the main feature of our approach that distinguishes it from one purely reliant upon lower bounds for linear forms in logarithms. This latter method is, in our opinion, at least with current technology, impractical for explicitly solving equation (1.2) for any set S with at least two elements.

7.1. **The case $S = \{2, 3\}$.** We prove the following result.

Theorem 7.1. *The only primitive solutions to equation (1.2) with $S = \{2, 3\}$ and, say, $x \geq |y| > 0$ and $z > 0$ are given by the following infinite families:*

$$(x, y, z, n) = (2, -1, 1, n), (3, -2, 1, n), (4, -3, 1, n), (9, -8, 1, n), (2^{n-1}, 2^{n-1}, 2, n),$$
$$(3 \cdot 2^{n-2}, 2^{n-2}, 2, n), (3 \cdot 2^{n-1}, -2^{n-1}, 2, n), (2 \cdot 3^{n-1}, 3^{n-1}, 3, n),$$
$$(2^2 \cdot 3^{n-1}, -3^{n-1}, 3, n), (2^3 \cdot 3^{n-2}, 3^{n-2}, 3, n), \quad \textit{all with } n \geq 2,$$
$$(x, y, z, n) = (3^2 \cdot 2^{n-3}, -2^{n-3}, 2, n) \quad \textit{for } n \geq 3$$

and by

$$(x, y, z, n) = (16, 9, 5, 2),\ (18, -2, 4, 2),\ (24, 1, 5, 2),\ (27, -2, 5, 2),\ (81, -32, 7, 2),$$
$$(48, 1, 7, 2),\ (128, -3, 5, 3),\ (288, 1, 17, 2) \textit{ and } (486, -2, 22, 2).$$

The cases where $n \leq 4$ were covered in the previous two sections. We may therefore assume, without loss of generality, that $n \geq 5$ is prime. The corresponding equation to treat is

$$x + y = wz^n \tag{7.1}$$

with x, y and w coprime integer $\{2, 3\}$-units and w nth-power free.

Assume first that $\mathrm{ord}_2(xyw) \geq 4$. Since precisely one of x, y and wz is even, we may suppose, without loss of generality, that $x \equiv -1 \pmod 4$ and that

$$\max\{\mathrm{ord}_2(y), \mathrm{ord}_2(w)\} \geq 4.$$

We write $(Aa^n, Bb^n) = (x, y)$ or $(x, -wz^n)$ if y or w is even, respectively, and set $Cc^n = Aa^n + Bb^n$, for A, B and C nth-power free integers. With the notation of §4.1, considering the elliptic curve $E = E^{A,B,C}_{n,n,n}(a, b, c)$, we thus have that n fails to divide ABC and $\mathrm{ord}_2(ABC) \geq 4$, and hence, in the notation of Proposition 4.1, $E \sim_n f$ where f is a weight 2 newform of level $N_0 \mid 6$. The resulting contradiction implies that necessarily $\mathrm{ord}_2(xyw) \leq 3$.

Assume next that $\mathrm{ord}_3(xyw) \geq 4$. Without loss of generality, we may suppose that $x \not\equiv 0 \pmod 3$, $y \not\equiv 2 \pmod 3$ and that

$$\max\{\mathrm{ord}_3(y), \mathrm{ord}_3(w)\} \geq 4.$$

We define

$$(Aa^n, Bb^n, Cc^3) = (-wz^n, y, -x) \text{ or } (-x, wz^n, y),$$

depending on whether $3 \mid y$ or w, respectively, where, in either case, A and B are chosen to be nth-power free and C is cubefree. In both cases, we have $n \not| ABC$ and $|ab| \geq |z|$.

If $|z| \geq 2$, then with the notation of Proposition 4.5, we have $E^{A,B,C}_{n,n,3}(a, b, c) \sim_n f$ where f is a weight 2 newform of level $N_0 \mid 12$ and hence a contradiction. We therefore have $z = \pm 1$ and we are led to solve $3^k - 2^l = \pm 1$ with $k \geq 4$. Both equations have no solution for $l \leq 2$, and, by reducing modulo 8, we see that the equation $3^k - 2^l = -1$ has no solution for $l \geq 3$ as well. If $3^k - 2^l = +1$ and $l \geq 3$, then k is necessarily even, whereby both $3^{k/2} - 1$ and $3^{k/2} + 1$ are powers of 2. Hence $k < 4$ and this is again a contradiction.

We are left, then, to consider equation (7.1) with

$$\max\{\mathrm{ord}_2(xyw), \mathrm{ord}_3(xyw)\} \leq 3.$$

A short calculation leads to the families indicated in Theorem 7.1.

7.2. **The case $S = \{3, 5, 7\}$.** The following result is the main theorem of the paper. As we shall observe, despite the apparently small size of S and its elements, the computations involved here are really approaching the limits of current "off the shelf" technology (though coming refinements in computational tools for modular forms will alleviate this somewhat).

Theorem 7.2. *The only primitive solutions to equation (1.2) with $S = \{3, 5, 7\}$ and $x > |y| > 0$ are given by*

$$(x, y) = (3, 1), (5, -1), (5, 3), (7, -3), (7, 1), (9, -5), (9, -1), (9, 7), (15, -7), (15, 1),$$
$$(21, -5), (21, 15), (25, -21), (25, -9), (25, 7), (27, 5), (35, -27), (35, -3), (35, 1),$$
$$(49, -45), (49, 15), (63, 1), (81, -49), (105, -5), (125, 3), (135, -35), (135, -7),$$
$$(147, -3), (175, 21), (175, 81), (189, -125), (189, 7), (225, -9), (343, -243),$$
$$(375, -343), (405, -5), (441, -225), (625, -49), (675, 1), (729, -245), (1029, -5),$$
$$(1225, -225), (1323, -27), (1875, -147), (3375, 2401), (3969, -1225), (3969, -125),$$
$$(9375, 1029), (10125, -125), (15625, -1701), (50625, -3969), (59535, 1),$$
$$(540225, -2401), (688905, -5), (4782969, 4375) \text{ and } (24310125, -10125).$$

Before proving our main theorem, we first state some useful preliminary results starting with a standard factorization lemma.

Lemma 7.3. *Let x and y be coprime integers and n an odd prime number. If we write*

$$\phi_n(x,y) = \frac{x^n + y^n}{x+y},$$

then we have that

$$\gcd(x+y, \phi_n(x,y)) \in \{1, n\}$$

and, moreover, that

$$\gcd(x+y, \phi_n(x,y)) = n \Leftrightarrow n \mid x^n + y^n \Leftrightarrow n \mid \phi_n(x,y) \Leftrightarrow n \mid x+y.$$

Further, $n^2 \nmid \phi_n(x,y)$ and if ℓ is a prime dividing $x^n + y^n$, then either $\ell \mid x+y$ or $\ell \equiv 1 \pmod{n}$.

Proof. Apart from its very last assertion, this lemma is proved in [10, Lemma 2.1]. Suppose that ℓ is a prime dividing $x^n + y^n$. Then, by coprimality, ℓ does not divide y. We may thus find an integer y' such that $yy' \equiv -1 \pmod{\ell}$, whence $(xy')^n \equiv 1 \pmod{\ell}$. If $xy' \equiv 1 \pmod{\ell}$, it follows that

$$xy' + yy' = y'(x+y) \equiv 0 \pmod{l},$$

so that $l \mid x+y$. Otherwise, since n is prime, xy' has order n modulo l, so that $n \mid l-1$, i.e. $l \equiv 1 \pmod{n}$. □

This lemma is a key tool in the proof of the following result.

Lemma 7.4. *Let x, y be coprime nonzero integers and $n \geq 5$ be a prime number. Then*

$$P(x^n + y^n) \geq 11$$

unless $|x| = |y| = 1$.

Proof. Assume $P(x^n + y^n) \leq 7$ and $|x| \neq |y|$. Then, with the above notation, we have that $|\phi_n(x,y)| > 1$, since, if $x^n + y^n = \pm(x+y)$, then necessarily $|x| = |y|$. It follows that there exists a prime $l \in \{2,3,5,7\}$ such that $l \mid \phi_n(x,y)$ and hence, by Lemma 7.3, $l \mid x+y$, whereby $l = n \in \{5,7\}$. We thus have

$$x^n + y^n = \pm n(x+y), \quad \text{for } n = 5 \text{ or } 7,$$

which again has no solutions with $|x| \neq |y|$. This contradiction completes the proof of the lemma. □

The next result will be of use in proving a special case of Theorem 7.2 (see Proposition 7.6).

Proposition 7.5. *The only solutions to $C^4 - 1 = p^\alpha q^\beta z^n$ and $D^2 - 1 = p^\alpha z^n$ for C, D and z positive integers with z even, $n \geq 5$ prime, and $\{p,q\} \subset \{3,5,7\}$ are with*

$$n = 5, \quad C = 7 \quad \text{and} \quad D \in \{15, 17\}.$$

Proof. We first deal with $C^4 - 1 = p^\alpha q^\beta z^n$. Since z is even, we have that C is odd and by factorization (up to permutation of p and q) that either

$$C^2 + 1 = 2z_1^n, \; C^2 + 1 = 2p^\alpha z_1^n \; \text{ or } \; C^2 + 1 = 2p^\alpha q^\beta z_1^n,$$

for some odd integer z_1. By a classical result of Störmer ([23, p. 168]), the first case holds only for $z_1 = C = 1$. Similarly in the third case, we deduce that

$C^2-1=2^{n-1}z_2^n$ for some nonzero integer z_2 which in turn contradicts Corollary 1.4 of [1]. We therefore end up in the situation where

$$C^2+1=2p^\alpha z_1^n \quad \text{and} \quad C^2-1=2^{n-1}q^\beta z_2^n,$$

for some positive integer z_2. By factorization, $C\pm 1=2q^\beta w_1^n$ and $C\mp 1=2^{n-2}w_2^n$ for some positive integers w_1 and w_2, whereby we have

$$q^\beta w_1^n-2^{n-3}w_2^n=\pm 1.$$

We may thus appeal to Theorem 1.1 of [2] with (in the notation of that paper) $S=\{2,q\}$ to conclude that $n=5$ and $w_1=w_2=1$, whence $C=7$ as claimed.

We now turn our attention to the equation $D^2-1=p^\alpha z^n$. By factorization, for some positive integers w_1 and w_2, we have either

$$w_1^n-2^{n-2}p^\alpha w_2^n=\pm 1 \quad \text{or} \quad p^\alpha w_1^n-2^{n-2}w_2^n=\pm 1.$$

According to *loc. cit.* applied to $S=\{2,p\}$, the former equation has no such solutions, whereas the only solutions to the latter are with $n=5$, $p^\alpha\in\{7,3^2\}$ and $w_1=w_2=1$. This gives rise to $D\in\{15,17\}$, as claimed. □

With those preliminary results in hand, we now turn to the actual proof of Theorem 7.2. Once again, recall that we have to solve

$$x+y=wz^n, \tag{7.2}$$

where x,y,w are coprime $\{3,5,7\}$-units with x,w positive, $n\geq 5$ prime and z nonzero.

Our first result is concerned with the case $y=\pm 1$ in equation (7.2) above.

Proposition 7.6. *Let x and w be coprime positive integer $\{3,5,7\}$-units, let $y=\pm 1$ and let $n\geq 5$ be a prime number such that $x+y=wz^n$ for some positive integer z. Then, $y=-1$, $n=5$, $z=2$ and*

$$(x,w)=(7^4,3\cdot 5^2) \quad \text{or} \quad (3^2\cdot 5^2,7).$$

Proof. According to Lemma 7.4, we may assume, without loss of generality, that $w\neq 1$. Similarly by applying [2, Thm. 1.1] to each subset of $\{3,5,7\}$ of cardinality 2, we may also assume that $\mathrm{rad}(xw)=3\cdot 5\cdot 7$. Besides, sieving modulo $2^4\mathrm{rad}(w)$ shows that we necessarily have $y=-1$ and that either x is a 4th power and w has two distinct prime factors (in $\{3,5,7\}$) or that x is a square and w has only one prime factor. We finally conclude using Proposition 7.5. □

According to Lemma 7.4 and Proposition 7.6 above, in order to prove Theorem 7.2, it remains to solve each equation of the shape

$$3^\alpha 5^\beta+(-1)^\delta 7^\gamma=z^n, \quad \text{with } (\alpha,\beta)\not\equiv(0,0) \pmod n \text{ and } \gamma\not\equiv 0 \pmod n, \tag{7.3}$$

$$3^\alpha 7^\gamma+(-1)^\delta 5^\beta=z^n, \quad \text{with } (\alpha,\gamma)\not\equiv(0,0) \pmod n \text{ and } \beta\not\equiv 0 \pmod n, \tag{7.4}$$

$$5^\beta 7^\gamma+(-1)^\delta 3^\alpha=z^n, \quad \text{with } (\beta,\gamma)\not\equiv(0,0) \pmod n \text{ and } \alpha\not\equiv 0 \pmod n, \tag{7.5}$$

$$3^\alpha+(-1)^\delta 5^\beta=7^\gamma z^n, \quad \text{with } \alpha,\beta>0 \text{ and } 0<\gamma\leq n-1, \tag{7.6}$$

$$3^\alpha+(-1)^\delta 7^\gamma=5^\beta z^n, \quad \text{with } \alpha,\gamma>0 \text{ and } 0<\beta\leq n-1, \tag{7.7}$$

$$5^\beta+(-1)^\delta 7^\gamma=3^\alpha z^n, \quad \text{with } \beta,\gamma>0 \text{ and } 0<\alpha\leq n-1, \tag{7.8}$$

where α,β and γ are nonnegative integers, $n\geq 5$ is prime and $\delta\in\{0,1\}$.

In the remainder of this section, we prove the following precise result on these equations. Combining it with Proposition 7.6 and results from Sections 5 and 6 completes the proof of Theorem 7.2.

Theorem 7.7. *The solutions to equations (7.3) – (7.8) in nonnegative integers α, β and γ, prime $n \geq 5$ and $\delta \in \{0,1\}$ correspond to the identities*

$$2^5 = 3 \cdot 5^3 - 7^3 = 3^4 - 7^2 = 5 \cdot 7 - 3 = 3^3 + 5 = 5^2 + 7,$$
$$2^{10} = 3 \cdot 7^3 - 5 \quad \text{and} \quad 2^7 = 5^3 + 3 = 3^3 \cdot 5 - 7.$$

Suppose that we have a solution to one of equations (7.3) – (7.8) in nonnegative integers α, β and γ, prime $n \geq 5$ and $\delta \in \{0,1\}$, and rewrite this in the shape (4.3) for suitable choices of A, B, C, a, b and c. Applying Proposition 4.5, we thus have that $E \sim_n f$ for some weight 2 cuspidal newform of level N_0 where, crudely, we have that $N_0 \mid 3^5 \cdot 5^2 \cdot 7^2$. Since $2 \mid z$ and hence necessarily $2 \mid ab$, we may apply congruence (2.3) with $l = 2$ to conclude that

$$n \leq \left(3 + 2\sqrt{2}\right)^{g_0(N_0)} \leq \left(3 + 2\sqrt{2}\right)^{(N_0+1)/12} < 10^{18991},$$

where $g_0(N_0)$ denotes the number of cuspidal weight-2 newforms of level N_0.

In what follows, we will in fact show that this upper bound can, through somewhat refined arguments using various Frey-Hellegouarch curves, local computations and Thue(-Mahler) solvers, be replaced by the assertion that $n \in \{5, 7\}$, corresponding to the solutions noted in Theorem 7.7. In the case $n = 5$, an approach via Frey-Hellegouarch curves, while theoretically of value, in practice appears to work poorly. Instead, we will use MAGMA code for solving Thue-Mahler equations due to K. Hambrook [13]; documentation for this may be found at

`http://www.math.ubc.ca/~bennett/hambrook-thesis-2011.pdf`.

The result we deduce by appealing to this code is the following:

Proposition 7.8. *The solutions to equations (7.3) – (7.8) in nonnegative integers α, β, γ and $\delta \in \{0,1\}$, with $n = 5$ correspond to the identities*

$$2^5 = 3 \cdot 5^3 - 7^3 = 3^4 - 7^2 = 5 \cdot 7 - 3 = 3^3 + 5 = 5^2 + 7 \quad \text{and} \quad 2^{10} = 3 \cdot 7^3 - 5.$$

Proof. According to the shapes of the equations and the noted restrictions on α, β and γ, it suffices to solve the following Thue-Mahler equations (some of which may be treated locally):

$$\begin{aligned}
z^5 - 3^a 5^b y^5 &= 7^c, \quad \text{with } 0 \leq a, b \leq 4 \text{ and } (a,b) \neq (0,0),\\
z^5 - 3^a 7^c y^5 &= 5^b, \quad \text{with } 0 \leq a, c \leq 4 \text{ and } (a,c) \neq (0,0),\\
z^5 - 5^b 7^c y^5 &= 3^a, \quad \text{with } 0 \leq b, c \leq 4 \text{ and } (b,c) \neq (0,0),\\
7^c z^5 - 5^b y^5 &= 3^a, \quad \text{with } 0 < b, c \leq 4,\\
3^a z^5 - 5^b y^5 &= 7^c, \quad \text{with } 0 < a, b \leq 4.
\end{aligned}$$

This is easily achieved using Hambrook's code and leads to the solutions mentioned. □

It is worth noting at this point in the proceedings that, at least as currently implemented, the Thue-Mahler solver we are using has severe difficulties with equations

of degree 7 and higher. In particular, we will need to work very carefully in order to avoid its use for the remaining cases under consideration.

We will now deal with each of equations (7.3)–(7.8) in turn, assuming $n \geq 7$ and that we have a solution satisfying the conditions mentioned. We will make repeated use of Proposition 4.5, explicitly using MAGMA to calculate newforms of all relevant levels N_0.

The results are as follows. We list in Table 1 the triples $(\delta_3, \delta_5, \delta_7)$ of interest to us for which the space of weight 2 cuspidal newforms of level

$$N_0 = 3^{\delta_3} \cdot 5^{\delta_5} \cdot 7^{\delta_7} \tag{7.9}$$

is nontrivial, together with the list of all primes $n \geq 7$ for which there exists at least one form f of level N_0 satisfying both (2.3) with $l = 2$ and the congruences of Proposition 4.5 for all primes $3 \leq l < 50$. The MAGMA code used for this computation (when $N_0 < 10000$) is available at `http://www.math.ubc.ca/~bennett/nn3.m`.

For the larger levels $N_0 = 3^4 \cdot 5^2 \cdot 7 = 14175$ and $N_0 = 3^4 \cdot 5 \cdot 7^2 = 19845$, we have first used Wiese's MAGMA function `Decomposition` (from his package `ArtinAlgebras` available on his homepage) to compute the characteristic polynomials of the first few Fourier coefficients. The output can be found in

`http://www.math.ubc.ca/~bennett/14175.m`

and in

`http://www.math.ubc.ca/~bennett/19845.m`,

respectively.

TABLE 1. Triples $(\delta_3, \delta_5, \delta_7)$ and corresponding values of n.

$(\delta_3, \delta_5, \delta_7)$	n
$(0,0,2),\ (0,2,1),\ (1,0,1),\ (1,1,0),\ (1,2,0),\ (1,2,1),$ $(3,0,0),\ (3,0,1),\ (3,0,2),\ (4,0,0),\ (4,1,0),\ (5,0,1)$	none
$(0,1,2),\ (0,2,2),\ (1,0,2),\ (1,1,2),$ $(4,0,2),\ (4,2,1),\ (5,1,0)$	7
$(1,2,2),\ (3,2,1),\ (4,1,2)$	7, 11
$(5,0,0)$	17
$(5,1,1)$	7, 17

In the next six subsections we deal with each equation in turn. Full details on the computations can be found in the file

`http://www.math.ubc.ca/~bennett/Last_Equations.pdf`

7.2.1. *The equation* $3^\alpha 5^\beta + (-1)^\delta 7^\gamma = z^n$. By reducing the equation modulo 8, we see that α and β have the same parity, and that α is odd if and only if we have $\delta \equiv \gamma \pmod 2$. We begin by assuming that α and β are even and $n \geq 7$. If, further, $\beta > 0$, we consider the curve

$$E = E_{(3),n,n,2}^{(-1)^{\delta+1}7^{\gamma_0},1,1}(7^{\gamma_1}, z, (-1)^{\alpha/2}3^{\alpha/2} \cdot 5^{\beta/2}),$$

where $\gamma = n\gamma_1 + \gamma_0$, with $0 \leq \gamma_0 \leq n-1$. It has good reduction at 5 and is of the shape

$$E \ : \ Y^2 + XY = X^3 + AX^2 + BX$$

where $A, B \in \mathbb{Z}$ with $A \equiv 1 \pmod 5$ and $B \not\equiv 0 \pmod 5$, whereby $a_5(E) \in \{\pm 2, \pm 4\}$. On the other hand, by Proposition 4.3, $E \sim_n f$ where f is a weight-2

newform of level 14. Since there is a unique such newform and it satisfies $c_5 = 0$, we obtain a contradiction from (2.3) for $l = 5$. Assume next that α is even, $\beta = 0$ and $n = 7$. If $\gamma \geq 2$, then we have $3^\alpha \equiv z^7 \pmod{49}$ and, since $z \not\equiv 0 \pmod 7$, $3^{6\alpha} \equiv 1 \pmod{49}$. This leads to the conclusion that $\alpha \equiv 0 \pmod 7$ and hence a contradiction. If $\gamma = 1$, then we have $\delta = 0$ and the equation to solve is $3^\alpha + 7 = z^7$. However we check that there is no value of $\alpha \pmod{42}$ such that

$$(3^\alpha + 7)^6 \equiv 1 \pmod{49} \quad \text{and} \quad (3^\alpha + 7)^6 \equiv 0 \text{ or } 1 \pmod{43},$$

and hence obtain a contradiction in this case as well. We therefore may assume that α is even, $\beta = 0$ and $n \geq 11$, and consider the curve

$$E = E_{n,n,3}^{1,-3^{\alpha_0},(-1)^\delta 7^{\gamma_0}}(z, 3^{\alpha_1}, 7^{\gamma_1}),$$

where $\alpha = n\alpha_1 + \alpha_0$, with $0 < \alpha_0 \leq n-1$ and $\gamma = 3\gamma_1 + \gamma_0$, with $0 \leq \gamma_0 \leq 2$. Then, by Proposition 4.5, $E \sim_n f$ where f is a weight 2 newform of level N_0 with $N_0 \mid 3 \cdot 7^2$ or $3^3 \mid N_0 \mid 3^3 \cdot 7^2$ if $\alpha \geq 3$ or $\alpha = 2$ respectively. Since $n \geq 11$, we therefore reach a contradiction upon appealing to Table 1.

Next, suppose that α and β are odd. If $n = 7$ and $\gamma \geq 2$, we simply note that there is no solution modulo $2^3 \cdot 7^2 \cdot 29 \cdot 43 \cdot 71$. If $n = 7$ and $\gamma = 1$, then $\delta = 1$ and modulo $2^3 \cdot 7^2 \cdot 29 \cdot 43 \cdot 113$, we have that $\alpha \equiv 3 \pmod 7$ and $\beta \equiv 1 \pmod 7$. We are therefore led to solve the Thue equation

$$z^7 - 3^3 5 y^7 = 7$$

using PARI/GP. This gives rise to a unique solution to our equation, namely $3^3 \cdot 5 - 7 = 2^7$. If, however, we assume that $n \geq 11$, we begin by considering the following $(n, n, 3)$ Frey-Hellegouarch curve

$$E = E_{n,n,3}^{1,-3^{\alpha_0}5^{\beta_0},(-1)^\delta 7^{\gamma_0}}(z, 3^{\alpha_1}5^{\beta_1}, 7^{\gamma_1})$$

where

$$\begin{cases} \alpha = n\alpha_1 + \alpha_0, & 0 \leq \alpha_0 \leq n-1, \\ \beta = n\beta_1 + \beta_0, & 0 \leq \beta_0 \leq n-1, \\ \gamma = 3\gamma_1 + \gamma_0, & 0 \leq \gamma_0 \leq 2. \end{cases}$$

Then, by Proposition 4.5, $E \sim_n f$ where f has level N_0 with $N_0 \mid 3 \cdot 5 \cdot 7^2$ or $N_0 = 3^4 \cdot N_1$, where $N_1 \mid 3^4 \cdot 5 \cdot 7^2$, if $\alpha \geq 3$ or $\alpha = 1$ respectively. According to Table 1, since $n \geq 11$, we necessarily have level $N_0 = 3^4 \cdot 5 \cdot 7^2$, whence

$$\alpha = 1, \quad \beta \equiv 1 \pmod 2, \quad n = 11 \quad \text{and} \quad \beta \not\equiv 0 \pmod{11}.$$

To treat this remaining case, we now consider the (n, n, n) Frey-Hellegouarch curve

$$E = E_{11,11,11}^{3\cdot 5^{\beta_0},-1,(-1)^{\delta+1}7^{\gamma_0}}(5^{\beta_1}, z, 7^{\gamma_1}),$$

where $\beta = 11\beta_1 + \beta_0$ and $\gamma = 11\gamma_1 + \gamma_0$ with $0 < \beta_0, \gamma_0 \leq 10$ (recall that $\beta, \gamma \not\equiv 0 \pmod{11}$). According to Proposition 4.1, E arises from a weight-2 newform f of level 210 and f corresponds to an elliptic curve $F/\mathbb{Q}$ such that

$$a_q(F) \not\equiv \pm 2 \pmod{11}, \quad \text{for } q = 23 \text{ and } 67.$$

This implies that F has good reduction at 23 and 67, or, in other words, that neither 23 nor 67 divides z. We may thus sieve locally at these primes to show that there is no triple (β, δ, γ) (with β odd and $\delta \equiv \gamma \pmod 2$) such that

$$3 \cdot 5^\beta + (-1)^\delta 7^\gamma \in \left(\mathbb{F}_q^\times\right)^{11}$$

simultaneously for $q = 23$ and 67. This leads to the desired contradiction, whereby we may conclude that the only solution to (7.3) for $n \geq 7$ prime corresponds to $3^3 \cdot 5 - 7 = 2^7$.

7.2.2. *The equation* $3^\alpha 7^\gamma + (-1)^\delta 5^\beta = z^n$. By reducing modulo 8, we see that α and β necessarily have the same parity, and that α is odd precisely when we have $\delta \equiv \gamma \pmod 2$. Assume first that α and β are even and $n \geq 7$. Let us consider

$$E = E_{(3),n,2}^{-3^{\alpha_0}7^{\gamma_0},1,(-1)^\delta}(3^{\alpha_1}7^{\gamma_1}, z, (-1)^\delta 5^{\beta/2}),$$

where $\alpha = n\alpha_1 + \alpha_0$, $\gamma = n\gamma_1 + \gamma_0$, with $0 \leq \alpha_0, \gamma_0 \leq n-1$. Since $\beta > 0$, E has good reduction at 5. Moreover, if $\delta = 0$, then it satisfies $a_5(E) = \pm 4$. From Proposition 4.3, E arises modulo n from a weight 2 newform of level 42 (recall that $\alpha > 0$). But there is a unique newform at level 42 corresponding to an elliptic curve $F/\mathbb{Q}$ with $a_5(F) = -2$, a contradiction. It follows that we have $\delta = 1$, which in turn implies γ even. We may thus consider instead

$$E = E_{(3),n,2}^{5^{\beta_0},1,1}(5^{\beta_1}, z, (-1)^{(\alpha+\gamma)/2}3^{\alpha/2}7^{\gamma/2}),$$

where $\beta = n\beta_1 + \beta_0$ with $0 < \beta_0 \leq n-1$. Then, by Proposition 4.3, E arises from a weight 2 newform of level 10. This is an obvious contradiction.

Next, assume that α and β are odd and $n \geq 7$. We consider the elliptic curve $E = E_{n,n,3}^{A,B,C}(a,b,c)$ with

$$A = 1,\ B = -3^{\alpha_0}7^{\gamma_0},\ C = (-1)^\delta 5^{\beta_0}, a = z,\ b = 3^{\alpha_1}7^{\gamma_1} \text{ and } c = 5^{\beta_1},$$

where $\alpha = n\alpha_1 + \alpha_0$, $\gamma = n\gamma_1 + \gamma_0$ with $0 \leq \alpha_0, \gamma_0 \leq n-1$ and $\beta = 3\beta_1 + \beta_0$ with $0 \leq \beta_0 \leq 2$. Then $E \sim_n f$ where f is a weight 2 newform of level, say, N_0 which we may compute using Proposition 4.5. If $\alpha \geq 3$, we find that $N_0 \mid 3 \cdot 5^2 \cdot 7$ and hence reach a contradiction from consideration of Table 1. Assume therefore that $\alpha = 1$ and that (A, B, C, a, b, c) does not correspond to the solution $3 + 5^3 = 2^7$. Then, necessarily, $n = 7$ and $N_0 = 3^4 \cdot 5^2 \cdot 7$. In particular, we have $\gamma_0 \neq 0$, i.e., $\gamma \not\equiv 0 \pmod 7$. We now use local arguments to conclude. Indeed, if $\gamma \geq 2$, then by reducing mod 49, we obtain that $\beta \equiv 0 \pmod 7$, a contradiction. If, however, $\gamma = 1$, then $\delta = 1$ and we check that there is no value of β (odd) such that $\beta \not\equiv 0 \pmod 7$ and

$$(3 \cdot 7 - 5^\beta)^{(p-1)/7} \equiv 0 \text{ or } 1 \pmod p$$

holds for $p = 29$ and 71 simultaneously.

This gives the desired contradiction and hence proves that the only solution to (7.4) for $n \geq 7$ prime corresponds to $3 + 5^3 = 2^7$.

7.2.3. *The equation* $5^\beta 7^\gamma + (-1)^\delta 3^\alpha = z^n$. By reducing modulo 8, we see that α and β have the same parity and that α is odd if and only if we have $\delta \equiv \gamma \pmod 2$. From the preceding two subsections, we may suppose that $\beta\gamma \neq 0$. If $n = 7$ and $\gamma \geq 2$, then considering the equation modulo 7^2, we conclude that $\alpha \equiv 0 \pmod 7$, a contradiction. If, however, $n = 7$ and $\gamma = 1$, we can easily check that there is no solution modulo $2^3 \cdot 7^2 \cdot 29 \cdot 43 \cdot 127 \cdot 379$. We may thus suppose that $n \geq 11$. Further, if α, β and γ are all even (so that $\delta = 1$), we can consider the elliptic curve

$$E = E_{(3),n,2}^{3^{\alpha_0},1,1}(3^{\alpha_1}, z, (-1)^{\gamma/2}5^{\beta/2}7^{\gamma/2})$$

where $\alpha = n\alpha_1 + \alpha_0$ with $0 < \alpha_0 \leq n-1$. By Proposition 4.3, it arises at level 6, a contradiction. We may thus suppose that at least one of α, β or γ is odd.

If $\alpha \geq 3$, then we consider

$$E = E_{n,n,3}^{1,(-1)^{\delta+1}3^{\alpha_0},5^{\beta_0}7^{\gamma_0}}(z, 3^{\alpha_1}, 5^{\beta_1}7^{\gamma_1})$$

where

$$\begin{cases} \alpha = n\alpha_1 + \alpha_0, & 0 < \alpha_0 \leq n-1, \\ \beta = 3\beta_1 + \beta_0, & 0 \leq \beta_0 \leq 2, \\ \gamma = 3\gamma_1 + \gamma_0, & 0 \leq \gamma_0 \leq 2. \end{cases}$$

By Proposition 4.5, we have $E \sim_n f$ where f has level $N_0 \mid 3 \cdot 5^2 \cdot 7^2$; from Table 1, we necessarily have $n = 11$.

We now use an (n, n, n) Frey-Hellegouarch curve argument to treat this remaining case. Consider either elliptic curve

$$E = E_{11,11,11}^{-5^{\beta_0}7^{\gamma_0},1,(-1)^{\delta}3^{\alpha_0}}(5^{\beta_1}7^{\gamma_1}, z, 3^{\alpha_1})$$

or

$$E = E_{11,11,11}^{5^{\beta_0}7^{\gamma_0},-1,(-1)^{\delta+1}3^{\alpha_0}}(5^{\beta_1}7^{\gamma_1}, z, 3^{\alpha_1})$$

where

$$\begin{cases} \alpha = 11\alpha_1 + \alpha_0 & 0 < \alpha_0 \leq 10, \\ \beta = 11\beta_1 + \beta_0 & 0 \leq \beta_0 \leq 10, \\ \gamma = 11\gamma_1 + \gamma_0 & 0 \leq \gamma_0 \leq 10, \end{cases}$$

if γ is even or odd, respectively. Then, by Proposition 4.1, $E \sim_n f$ where f has level $N_0 \in \{30, 42, 210\}$. It follows that the newform f corresponds to an elliptic curve $F/\mathbb{Q}$ for which there are unique isogeny classes at level $N_0 \in \{30, 42\}$ and five isogeny classes at level 210. For $q \in \{23, 67, 89, 199\}$, we compute $a_q(F)$ to show that E has good reduction at q (i.e., $q \nmid z$) unless, perhaps, if either $q = 89$ and f corresponds to the isogeny class `210c` (in Cremona's notation) or $q = 199$ and f corresponds to the isogeny class `210d`. We finally sieve over α, β and γ (not all even) to show that we do not have

$$5^{\beta}7^{\gamma} + (-1)^{\delta}3^{\alpha} \in \left((\mathbb{Z}/q\mathbb{Z})^{\times}\right)^{11} \quad \text{and} \quad a_q(E) \equiv a_q(F) \pmod{11},$$

for $q = 23, 67$ and 89 simultaneously if the isogeny class of F is not `210c` and for $q = 23, 67$ and 199 simultaneously otherwise.

Assume now $\alpha \in \{1, 2\}$. We basically follow the same strategy we used for the case $\alpha \geq 3$ applying first an $(n, n, 3)$ and then an (n, n, n) argument, though the details are somewhat simpler. Indeed, we first consider

$$E = E_{n,n,3}^{5^{\beta_0}7^{\gamma_0},-1,(-1)^{\delta+1}3}(5^{\beta_1}7^{\gamma_1}, z, 1)$$

or

$$E = E_{n,n,3}^{-5^{\beta_0}7^{\gamma_0},1,(-1)^{\delta}3^2}(5^{\beta_1}7^{\gamma_1}, z, 1)$$

where

$$\begin{cases} \beta = n\beta_1 + \beta_0, & 0 \leq \beta_0 \leq n-1, \\ \gamma = n\gamma_1 + \gamma_0, & 0 \leq \gamma_0 \leq n-1, \end{cases}$$

if $\alpha = 1$ or $\alpha = 2$, respectively. Then, by Proposition 4.5, $E \sim_n f$ where f has level $3^5 \cdot N_1$, where $N_1 \mid 5 \cdot 7$. From appeal to Table 1, we conclude that $n = 17$ (and $\beta, \gamma \not\equiv 0 \pmod{17}$).

We now use an (n, n, n) Frey-Hellegouarch curve argument to deal with the case $n = 17$. As before, we consider the elliptic curve

$$E = E_{17,17,17}^{-5^{\beta_0}7^{\gamma_0},1,(-1)^{\delta}3^{\alpha}}(5^{\beta_1}7^{\gamma_1}, z, 1)$$

or

$$E = E_{17,17,17}^{5^{\beta_0}7^{\gamma_0},-1,(-1)^{\delta+1}3^{\alpha}}(5^{\beta_1}7^{\gamma_1}, z, 1)$$

with $\beta_0, \beta_1, \gamma_0, \gamma_1$ as above, if γ is even or odd, respectively. Then E arises mod 17 from an elliptic curve F of conductor $N_0 \in \{30, 42, 210\}$ and for $q \in \{103, 137\}$, we check, by computing $a_q(E) \pmod{17}$ that E has good reduction at q (i.e., that $q \nmid z$). For $\alpha \in \{1, 2\}$, we finally sieve over β and γ to show that

$$5^{\beta}7^{\gamma} + (-1)^{\delta}3^{\alpha} \in \left((\mathbb{Z}/q\mathbb{Z})^{\times}\right)^{17} \quad \text{and} \quad a_q(E) \equiv a_q(F) \pmod{17}$$

do not hold for $q = 103$ and 137 simultaneously. This finishes the proof that equation (7.5) has no solution for $n \geq 7$.

7.2.4. *The equation* $3^{\alpha} + (-1)^{\delta}5^{\beta} = 7^{\gamma}z^n$. Considering equation (7.6), we conclude that α and β have the same parity and that α is odd if and only if we have $\delta = 0$. If α and β are odd, then $\delta = 0$ and, since $\gamma > 0$, we have $3^{\alpha} + 5^{\beta} \equiv 0 \pmod 7$ and hence a contradiction. Next, assume that α and β are even and $n \geq 7$. The equation to treat is now

$$3^{\alpha} - 5^{\beta} = 7^{\gamma}z^n.$$

We thus consider the elliptic curve

$$E = E_{n,n,3}^{-7^{\gamma},3^{\alpha_0},5^{\beta_0}}(z, 3^{\alpha_1}, 5^{\beta_1})$$

where

$$\begin{cases} \alpha = n\beta_1 + \alpha_0, & 0 \leq \beta_0 \leq n-1, \\ \beta = 3\beta_1 + \beta_0, & 0 \leq \gamma_0 \leq 2. \end{cases}$$

By Proposition 4.5, we have $E \sim_n f$ where f has level $N_0 = 3^k \cdot 5^{\delta_5} \cdot 7$ with $\delta_5 \in \{0, 2\}$ and

$$k = \begin{cases} 3 & \text{if } \alpha = 2, \\ 0 & \text{if } \alpha \equiv 3 \pmod n, \\ 1 & \text{if } \alpha \geq 3 \text{ and } \alpha \not\equiv 3 \pmod n. \end{cases}$$

Using Table 1, it then follows that $\alpha = 2$ and $n \in \{7, 11\}$. We first consider the $(n, n, 3)$ Frey-Hellegouarch curve

$$E = E_{n,n,3}^{7^{\gamma},5^{\beta_0},3^2}(z, 5^{\beta_1}, 1),$$

where $\beta = n\beta_1 + \beta_0$ with $0 \leq \beta_0 \leq n-1$. By Proposition 4.5, the curve E arises modulo n from a newform f of level $N_0 = 3^5 \cdot N_1$, where $N_1 \mid 5 \cdot 7$. Hence, using Table 1, we deduce that $n \in \{7, 17\}$ and, in particular, that $n \neq 11$.

If, however, $n = 7$, then we use local arguments to get a contradiction. If $\gamma \geq 2$, we check that there is no solution modulo $2^3 \cdot 7^2 \cdot 43$. Similarly, if $\gamma = 1$, then there is no solution modulo $2^3 \cdot 7^2 \cdot 43 \cdot 127$. This shows that equation (7.6) has no solution for $n \geq 7$ prime.

7.2.5. *The equation* $3^{\alpha} + (-1)^{\delta}7^{\gamma} = 5^{\beta}z^n$. By reducing mod $2^4 \cdot 5$, we conclude that $\alpha \equiv 0 \pmod 4$, $\gamma \equiv 0 \pmod 4$ and $\delta = 1$. Write $\alpha = 2\alpha_0$ and $\gamma = 2\gamma_0$. Then, there exist nonzero integers z_1, z_2 with z_2 odd such that either

$$\begin{cases} 3^{\alpha_0} - 7^{\gamma_0} = 2^{n-1}5^{\beta}z_1^n, \\ 3^{\alpha_0} + 7^{\gamma_0} = 2z_2^n, \end{cases} \quad \text{or} \quad \begin{cases} 3^{\alpha_0} - 7^{\gamma_0} = 2^{n-1}z_1^n, \\ 3^{\alpha_0} + 7^{\gamma_0} = 2 \cdot 5^{\beta}z_2^n. \end{cases}$$

Adding these equations and recalling that α_0 is even yields either

$$\left(3^{\alpha_0/2}\right)^2 = 2^{n-2}5^{\beta}z_1^n + z_2^n \quad \text{or} \quad \left(3^{\alpha_0/2}\right)^2 = 2^{n-2}z_1^n + 5^{\beta}z_2^n.$$

If $n \geq 11$, we consider the $(n, n, 2)$ Frey-Hellegouarch curve

$$E = E^{1,2^{n-2}5^{\beta},1}_{(3),n,n,2}(z_2, z_1, (-3)^{\alpha_0/2}) \quad \text{or} \quad E = E^{5^{\beta},2^{n-2},1}_{(3),n,n,2}(z_2, z_1, (-3)^{\alpha_0/2})$$

according to whether we are in the first or second case above, respectively. Then, by Proposition 4.3, the curve E arises at level 10, an immediate contradiction. We may therefore assume that $n = 7$ and sieve over α, β and γ to show that there is no solution modulo $2^4 \cdot 7^2 \cdot 29 \cdot 43 \cdot 71 \cdot 113 \cdot 127 \cdot 211 \cdot 337 \cdot 421$. This shows that equation (7.7) has no solution for $n \geq 7$ prime.

7.2.6. *The equation* $5^{\beta} + (-1)^{\delta}7^{\gamma} = 3^{\alpha}z^n$. By reducing mod $2^4 \cdot 3$, we find that $\beta \equiv 0 \pmod 4$, $\gamma \equiv 0 \pmod 2$ and $\delta = 1$. We then consider the $(n, n, 2)$ Frey-Hellegouarch curve

$$E = E^{5^{\beta_0},-3^{\alpha},1}_{(3),n,n,2}(5^{\beta_1}, z, (-7)^{\gamma/2}),$$

where $\beta = n\beta_1 + \beta_0$ with $0 \leq \beta_0 \leq n - 1$. It has good reduction at 7 and satisfies $a_7(E) = 0$. On the other hand, the curve E arises from the (unique) newform f at level 30, which satisfies $c_7(f) = -4$. This gives us the desired contradiction and hence proves that equation (7.8) has no solution for $n \geq 7$ prime.

References

[1] M. A. Bennett, *Products of consecutive integers*, Bull. London Math. Soc. **36** (2004), no. 5, 683–694, DOI 10.1112/S0024609304003480. MR2070445 (2005e:11034)

[2] M. A. Bennett, K. Győry, M. Mignotte, and Á. Pintér, *Binomial Thue equations and polynomial powers*, Compos. Math. **142** (2006), no. 5, 1103–1121, DOI 10.1112/S0010437X06002181. MR2264658 (2007h:11044)

[3] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54, DOI 10.4153/CJM-2004-002-2. MR2031121 (2005c:11035)

[4] M. A. Bennett, V. Vatsal, and S. Yazdani, *Ternary Diophantine equations of signature* $(p, p, 3)$, Compos. Math. **140** (2004), no. 6, 1399–1416, DOI 10.1112/S0010437X04000983. MR2098394 (2005i:11036)

[5] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, DOI 10.1006/jsco.1996.0125. Computational algebra and number theory (London, 1993). MR1484478

[6] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic), DOI 10.1090/S0894-0347-01-00370-8. MR1839918 (2002d:11058)

[7] A. Brumer and K. Kramer, *The conductor of an abelian variety*, Compositio Math. **92** (1994), no. 2, 227–248. MR1283229 (95g:11055)

[8] J. E. Cremona, *Database of elliptic curves*, 2014. SAGE package available at `http://www.sagemath.org/packages/`.

[9] J. E. Cremona and M. P. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experiment. Math. **16** (2007), no. 3, 303–312. MR2367320 (2008k:11057)

[10] S. R. Dahmen and S. Siksek, *Perfect powers expressible as sums of two fifth or seventh powers*, Acta Arith. **164** (2014), no. 1, 65–100, DOI 10.4064/aa164-1-5. MR3223319

[11] M.-J. Deng, *A note on the Diophantine equation* $x^2 + q^m = c^{2n}$, Proc. Japan Acad. Ser. A Math. Sci. **91** (2015), no. 2, 15–18, DOI 10.3792/pjaa.91.15. MR3310965

[12] C. Fuchs, R. von Känel, and G. Wüstholz, *An effective Shafarevich theorem for elliptic curves*, Acta Arith. **148** (2011), no. 2, 189–203, DOI 10.4064/aa148-2-5. MR2786163 (2012h:11085)

[13] K. Hambrook, *Implementation of a Thue-Mahler solver*, M.Sc. thesis, University of British Columbia, 2011.

[14] R. von Känel, *Modularity and integral points on moduli schemes*, preprint.

[15] D. Kim, *A modular approach to Thue-Mahler equations*, preprint.

[16] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée* (French, with French summary), Canad. J. Math. **49** (1997), no. 6, 1139–1161, DOI 10.4153/CJM-1997-056-2. MR1611640 (99g:11039)
[17] M. R. Murty and H. Pasten, *Modular forms and effective Diophantine approximation*, J. Number Theory **133** (2013), no. 11, 3739–3754, DOI 10.1016/j.jnt.2013.05.006. MR3084298
[18] The PARI Group, Bordeaux, *PARI/GP version* `2.7.1`, 2014, available at `http://pari.math.u-bordeaux.fr/`.
[19] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476, DOI 10.1007/BF01231195. MR1047143 (91g:11066)
[20] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Mathematics, vol. 87, Cambridge University Press, Cambridge, 1986. MR891406 (88h:11002)
[21] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR2514094 (2010i:11005)
[22] W. A. Stein et al., *Sage Mathematics Software (Version 5.13)*. The Sage Development Team, 2013. `http://www.sagemath.org`.
[23] C. Störmer, *Solution complète en nombres entiers de l'équation* $m \arctan \frac{1}{x} + n \arctan \frac{1}{y} = k\frac{\pi}{4}$ (French), Bull. Soc. Math. France **27** (1899), 160–170. MR1504340
[24] N. Terai, *A note on the Diophantine equation* $x^2 + q^m = c^n$, Bull. Aust. Math. Soc. **90** (2014), no. 1, 20–27, DOI 10.1017/S0004972713000981. MR3227126
[25] B. M. M. de Weger, *Algorithms for Diophantine Equations*, CWI Tract, vol. 65, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Amsterdam, 1989. MR1026936 (90m:11205)
[26] B. M. M. de Weger, *The weighted sum of two S-units being a square*, Indag. Math. (N.S.) **1** (1990), no. 2, 243–262, DOI 10.1016/0019-3577(90)90007-A. MR1060828 (91j:11017)

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada
E-mail address: `bennett@math.ubc.edu`

Laboratoire de Mathématiques, Université Clermont Auvergne, Université Blaise Pascal, BP 10448, F-63000 Clermont-Ferrand, France — and — CNRS, UMR 6620, LM, F-63171 Aubière, France
E-mail address: `Nicolas.Billerey@math.univ-bpclermont.fr`

TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 370, Number 2, February 2018, Pages 967–986
http://dx.doi.org/10.1090/tran/6979
Article electronically published on August 15, 2017

STRONG MODULARITY OF REDUCIBLE GALOIS REPRESENTATIONS

NICOLAS BILLEREY AND RICARDO MENARES

Abstract. Let $\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathrm{GL}_2(\overline{\mathbf{F}}_l)$ be an odd, semi-simple Galois representation. Here, $l \geq 5$ is prime and $\overline{\mathbf{F}}_l$ is an algebraic closure of the finite field $\mathbf{Z}/l\mathbf{Z}$. When the representation is irreducible, the strongest form of Serre's original modularity conjecture (which is now proved) asserts that ρ arises from a cuspidal eigenform of type (N, k, ε) over $\overline{\mathbf{F}}_l$, where N, k and ε are, respectively, the level, weight and character attached to ρ by Serre.

In this paper we characterize, under the assumption $l > k + 1$, reducible semi-simple representations, that we call strongly modular, such that the same result holds. This characterization generalizes a classical theorem of Ribet pertaining to the case $N = 1$. When the representation is not strongly modular, we give a necessary and sufficient condition on primes p not dividing Nl for which ρ arises in level Np, hence generalizing a classical theorem of Mazur concerning the case $(N, k) = (1, 2)$.

The proofs rely on the classical analytic theory of Eisenstein series and on local properties of automorphic representations attached to newforms.

Introduction

Let l be a prime number. We denote by $\overline{\mathbf{F}}_l$ and $\overline{\mathbf{Q}}$ algebraic closures of $\mathbf{F}_l = \mathbf{Z}/l\mathbf{Z}$ and the rational field $\mathbf{Q}$, respectively. In this article we are interested in Galois representations of the form

$$\rho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_l), \tag{1}$$

where ρ is a continuous homomorphism. Let $N \geq 1$ and $k \geq 2$ be two integers with N coprime to l and let $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ be a character. Let f be a cusp form of type (N, k, ε) over $\overline{\mathbf{F}}_l$ (in the sense of [Ser87, Déf., p. 193]) which is an eigenfunction for the p-th Hecke operator with eigenvalue a_p in $\overline{\mathbf{F}}_l$ for each prime number p. By work of Deligne, to such a form f, one can attach a (unique up to isomorphism) semi-simple odd Galois representation ρ_f which is unramified outside Nl and satisfies the following property : If Frob_p denotes a Frobenius element at a prime $p \nmid Nl$, then the characteristic polynomial of $\rho_f(\mathrm{Frob}_p)$ is given by

$$X^2 - a_p X + \varepsilon(p)p^{k-1}.$$

According to a standard terminology, a Galois representation ρ is called *modular* if it is isomorphic to ρ_f for some f as above. In that case, we also say that ρ arises from f.

Received by the editors April 11, 2016, and, in revised form, May 12, 2016.
2010 *Mathematics Subject Classification.* Primary 11F80, 11F33; Secondary 11F70.
The first author was partially supported by CNRS and ANR-14-CE-25-0015 Gardio.
The second author was partially supported by PUCV grant 037.469/2015.

Moreover, to any given Galois representation ρ, Serre attaches in [Ser87, §§1-2] a triple (N, k, ε), which we refer to as the Serre type of ρ, consisting of an integer $N \geq 1$ coprime to l, an integer $k \geq 2$ and a group homomorphism $\varepsilon\colon (\mathbf{Z}/N\mathbf{Z})^\times \to \overline{\mathbf{F}}_l^\times$ which are called the conductor, weight and character of ρ, respectively.

In this paper, we shall say that a Galois representation ρ is *strongly modular* if it arises from a cuspidal eigenform f over $\overline{\mathbf{F}}_l$ of type (N, k, ε) where (N, k, ε) is the Serre type of ρ.

With this terminology, the strong form ([Ser87, (3.2.4$_?$)]) of Serre's modularity conjecture, asserts that any odd, irreducible Galois representation ρ as in (1), with $l \geq 5$, is strongly modular. This conjecture has now been proved through the combined work of many mathematicians (see [KW09a, KW09b] and the references therein).

We remark that the results of Carayol (cf. [Car86, Thm. (A)] and the considerations in [Car89, **1.-2.**]), ensure that whenever ρ is strongly modular, the eigenform f can be taken to be the reduction of a newform F (in characteristic zero) of level N.

In this article, we address the case where ρ is reducible. Let

$$\nu_1, \nu_2\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \overline{\mathbf{F}}_l^\times$$

be continuous characters and assume that $\rho = \nu_1 \oplus \nu_2$ defines an odd (semi-simple) Galois representation of Serre type (N, k, ε). Then, ρ is modular (e.g. see [BM15, Thm. 2.1]) but need not be strongly modular. Our task is to provide a necessary and sufficient condition for such a reducible Galois representation to be strongly modular. Thanks to Ribet, such a characterization is known in the case $N = 1$ under the assumption $l > k + 1$ (see [Rib75, Lem. 5.2] or [BM15, Cor. 3.7] for a reformulation in this context). Under the same assumption, we prove in this paper a generalization of this result to arbitrary conductors.

Let $\eta\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ be a character unramified at l. For any integer $k \geq 2$ satisfying $l > k+1$, we define in subsection 1.2 a mod l Bernoulli number $B_{k,\eta} \in \overline{\mathbf{F}}_l$ associated with η (our $B_{k,\eta}$ is essentially the reduction of a classical k-th Bernoulli number attached to a lift of η, but some care has to be taken due to denominators and the choice of place). For every prime number p, set

$$\eta(p) = \begin{cases} \eta(\mathrm{Frob}_p) & \text{if } \eta \text{ is unramified at } p, \\ 0 & \text{if } \eta \text{ is ramified at } p. \end{cases}$$

In this notation, the following is the main result of the paper.

Theorem 1. *Let $\nu_1, \nu_2\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ be characters defining an odd (semi-simple) Galois representation $\rho = \nu_1 \oplus \nu_2$ of Serre type (N, k, ε) with $l > k + 1$. Then, there exist characters $\varepsilon_1, \varepsilon_2\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ unramified at l such that $\rho = \varepsilon_1 \oplus \varepsilon_2 \chi_l^{k-1}$, where χ_l is the* mod l *cyclotomic character. Set $\eta = \varepsilon_1^{-1}\varepsilon_2$. The representation ρ is strongly modular if and only if*

$$\textit{either } B_{k,\eta} = 0 \quad \textit{or} \quad \eta(p)p^k = 1 \textit{ for some prime } p \textit{ dividing } N.$$

If the representation ρ alluded to above is not strongly modular, we give in Theorem 2 a precise characterization (under the same assumption as before) of the primes $M \nmid Nl$ for which ρ arises from a cusp form of type (NM, k, ε). Such a theorem extends a result of Mazur ([Maz77, Prop. 5.12]), that handles the case $(N, k) = (1, 2)$, to arbitrary weights and conductors.

Theorem 2. *In the same notation and under the same assumptions as in Theorem 1, assume moreover that ρ is not strongly modular. Let M be a prime number not dividing Nl. Then ρ arises from a modular form of type (NM, k, ε) if and only if*

$$\begin{cases} M \equiv 1 \pmod{l} & \text{if } (N,k) = (1,2) \quad \textit{(Mazur)}, \\ \eta(M)M^k = 1 & \text{if } (N,k) \neq (1,2). \end{cases}$$

In particular, there are infinitely many such primes.

We remark that, due to the results of Carayol already mentioned, the modular form over $\overline{\mathbf{F}}_l$ in Theorem 2 can be taken to be the reduction of a newform of level NM (cf. subsection 3.2 of this article).

Although the details need to be treated separately, the overall strategy for proving both results is the same and relies on properties of characteristic zero eigenforms and their attached automorphic representations. Let us briefly describe this strategy in the case of Theorem 1. Let ρ be as the statement of the theorem. Attached to such a reducible representation is a specific Eisenstein series E. If ρ is strongly modular, then there must occur a congruence between E and a certain cuspidal (new) eigenform of weight k and level N. This in turn implies that the constant terms of E vanish at all cusps after reduction modulo l, leading to the necessary conditions of the theorem. Conversely, if these conditions hold, then we prove that the reduction of E modulo l is a cusp form f over $\overline{\mathbf{F}}_l$ of the same type as ρ such that $\rho \simeq \rho_f$.

The paper is organized as follows. In Section 1, we define the Bernoulli numbers attached to mod l Galois characters that appear in the statement of Theorem 1 above and compute the constant term at the various cusps of a particular Eisenstein series which is of crucial use in the proofs of our results. After quickly recalling in Section 2 some background on cuspidal eigenforms and Hecke operators in the adelic setting, we prove in Section 3 our two main theorems.

1. Bernoulli numbers and Eisenstein series

In this section we recall some classical definitions and integrality results on Bernoulli numbers attached to Dirichlet characters. Also, we compute the constant term in the q-expansion at the cusps of the modular curve $X_1(N)$ of some specific Eisenstein series that will be used in the sequel. The final computation is stated in Proposition 4 below.

1.1. **Notation and definitions.** Let ϕ be a primitive Dirichlet character of conductor $\mathfrak{f} \geq 1$. The Gauss sum attached to ϕ is defined by

$$W(\phi) = \sum_{n=1}^{\mathfrak{f}} \phi(n) e^{2i\pi n/\mathfrak{f}}.$$

It is a non-zero algebraic integer whose norm is a power of $\mathfrak{f}$. The (generalized) Bernoulli numbers $(B_{m,\phi})_{m\geq 1}$ associated with ϕ are defined by the following expansion:

$$\sum_{n=1}^{\mathfrak{f}} \phi(n) \frac{te^{nt}}{e^{\mathfrak{f}t} - 1} = \sum_{m\geq 0} B_{m,\phi} \frac{t^m}{m!}. \tag{2}$$

Note that when $\phi = \mathbf{1}$ is the trivial character (of conductor 1), then, for every integer $m \geq 2$, we have $B_{m,\phi} = B_m$, where B_m denotes the classical m-th Bernoulli number.

1.2. **Bernoulli numbers of mod l characters.** Let $\eta\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ be a Galois character unramified at l. Denote by $\mathfrak{c}_0$ the conductor of η (coprime to l by assumption) and identify η with a character:

$$\eta\colon (\mathbf{Z}/\mathfrak{c}_0\mathbf{Z})^\times \longrightarrow \overline{\mathbf{F}}_l^\times.$$

The aim of this subsection is to define the k-th Bernoulli number attached to η for any integer $k \geq 2$ such that $l > k+1$. This definition relies on integrality properties of Bernoulli numbers attached to Dirichlet characters which we now recall.

Let w be a place of $\overline{\mathbf{Q}}$ above l and let $\overline{\mathbf{Z}}_w$ be the local ring of w-integral algebraic numbers in $\overline{\mathbf{Q}}$. The residue field k_w of w identifies with an algebraic closure of $\mathbf{F}_l$. Fix an isomorphism $\iota\colon k_w \to \overline{\mathbf{F}}_l$ and consider the composition map

$$\nu_w\colon \overline{\mathbf{Z}}_w \to k_w \xrightarrow{\iota} \overline{\mathbf{F}}_l.$$

We may then consider the multiplicative lift

$$\psi\colon (\mathbf{Z}/\mathfrak{c}_0\mathbf{Z})^\times \longrightarrow \overline{\mathbf{Z}}^\times$$

of η with respect to w. That is, ψ is the unique character with values in the roots of unity of prime-to-l order such that

$$\nu_w(\psi(x)) = \eta(x), \quad \text{for all } x \in (\mathbf{Z}/\mathfrak{c}_0\mathbf{Z})^\times.$$

We now state the integrality result we need to define our Bernoulli numbers associated to η.

Lemma 3. *For any integer $k \geq 2$ such that $l > k+1$, the Bernoulli number $B_{k,\psi}$ is w-integral.*

Proof. Let k be an integer as in the statement of the lemma. We easily check on the definition (2) that if $\psi(-1) \neq (-1)^k$, then $B_{k,\psi} = 0$. Assume therefore that $\psi(-1) = (-1)^k$. If ψ is the trivial character, then k must be an even integer and the corresponding Bernoulli number $B_{k,\psi}$ is nothing but the classical Bernoulli number B_k. The Van Staudt-Clausen theorem ensures that the prime divisors p of the denominator of B_k satisfy $p-1 \mid k$. Since $l > k+1$, the prime number l does not divide the denominator of B_k, as desired.

Assume therefore ψ is non-trivial. Let

$$d = \begin{cases} 1 & \text{if } \mathfrak{c}_0 \text{ admits two different prime divisors,} \\ 2 & \text{if } \mathfrak{c}_0 = 4, \\ 1 & \text{if } \mathfrak{c}_0 = 2^n, n > 2, \\ k\mathfrak{c}_0 & \text{if } \mathfrak{c}_0 > 2 \text{ is a prime number,} \\ 1 - \psi(1+p) & \text{if } \mathfrak{c}_0 = p^n, p > 2, n > 1, p \text{ is a prime number.} \end{cases}$$

By a theorem of Carlitz (see [Car59a] and [Car59b]), $dk^{-1}B_{k,\psi}$ is an algebraic integer. Hence, we are reduced to verify that w does not divide d.

Assume that $\mathfrak{c}_0 = p^n$, where p is an odd prime number and $n \geq 2$. We assume by contradiction that w divides $d = 1 - \psi(1+p)$. Let $H \subseteq (\mathbf{Z}/p^n\mathbf{Z})^\times$ be the subgroup spanned by $1+p$. Taking the reduction map ν_w attached to w, we conclude that η is trivial on H. Since H is the kernel of the natural map $(\mathbf{Z}/p^n\mathbf{Z})^\times \to (\mathbf{Z}/p\mathbf{Z})^\times$,

we conclude that η can be factored through $(\mathbf{Z}/p\mathbf{Z})^\times$, contradicting the primitivity of η.

If $\mathfrak{c}_0 \geq 3$ is not of the form discussed in the previous paragraph, the fact that $l \nmid d$ clearly follows from the definition of d and the hypothesis on k, l and $\mathfrak{c}_0$. □

Using this result, we now set, for any integer k as above,

$$B_{k,\eta} = \nu_w\left(B_{k,\psi}\right) \in \overline{\mathbf{F}}_l. \tag{3}$$

Let w' be another place of $\overline{\mathbf{Q}}$ over l. There exists $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ such that $w' = \sigma(w)$ and we identify the residue field $k_{w'}$ (of the ring of w'-integral algebraic numbers in $\overline{\mathbf{Q}}$) with $\overline{\mathbf{F}}_l$ via $\iota \circ \sigma^{-1}$. Then $\sigma(\psi)$ is the multiplicative lift of η with respect to the place $w' = \sigma(w)$ and since we have

$$B_{k,\sigma(\psi)} = \sigma\left(B_{k,\psi}\right)$$

the definition (3) is independent of the choice of the place w. We refer to $B_{k,\eta} \in \overline{\mathbf{F}}_l$ as the k-th Bernoulli number associated with η.

1.3. **The setting.** In this subsection we set some notation and definitions that will be used in the rest of this section. Let $k \geq 2$ be an integer. We set

$$C_k = \frac{(-2i\pi)^k}{(k-1)!}.$$

Let

$$\chi_i \colon (\mathbf{Z}/\mathfrak{c}_i\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times, \quad i = 1, 2,$$

be primitive Dirichlet characters such that $\chi_1(-1)\chi_2(-1) = (-1)^k$. Denote by $\overline{\chi_i}$ the complex conjugate of χ_i, $i = 1, 2$. Put $N = \mathfrak{c}_1\mathfrak{c}_2$. For $k \geq 3$ and z in the complex upper half-plane $\mathfrak{H}$, let

$$G_k^{\chi_1,\chi_2}(z) = \sum_{(m,n)\in\mathbf{Z}^2\setminus\{(0,0)\}} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mz+n)^k}.$$

On the other hand, for any $\varepsilon > 0$, we consider

$$G_{2,\varepsilon}^{\chi_1,\chi_2}(z) = \sum_{(m,n)\in\mathbf{Z}^2\setminus\{(0,0)\}} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mz+n)^2|mz+n|^{2\varepsilon}} \quad (z \in \mathfrak{H}).$$

We remark that our functions $G_k^{\chi_1,\chi_2}(z)$ $(k \geq 3)$ and $G_{2,\varepsilon}^{\chi_1,\chi_2}(z)$ correspond to the functions $E_k(z;\chi,\psi)$ and $E_2(z,\varepsilon;\chi,\psi)$, respectively, defined in Eqs. (7.1.1) and (7.2.1) of [Miy06] with $(\chi,\psi) = (\chi_1, \overline{\chi_2})$.

From now on, and until the end of this section, assume that either $N > 1$ or $k > 2$ and denote by $E_k^{\chi_1,\chi_2}$ the function defined by

$$E_k^{\chi_1,\chi_2}(z) = -\delta(\chi_1)\frac{B_{k,\chi_2}}{2k} + \sum_{n\geq 1}\sigma_{k-1}^{\chi_1,\chi_2}(n)q^n \quad (q = e^{2\pi iz}, z \in \mathfrak{H}), \tag{4}$$

where

$$\sigma_{k-1}^{\chi_1,\chi_2}(n) = \sum_{m|n}\chi_1(n/m)\chi_2(m)m^{k-1}, \quad \delta(\chi_1) = \begin{cases} 1 & \text{if } \chi_1 \text{ is trivial,} \\ 0 & \text{otherwise,} \end{cases}$$

and B_{k,χ_2} denotes the k-th Bernoulli number associated with χ_2 (see subsection 1.1).

According to [Miy06, Thm. 7.1.3 and Eq. (7.1.13)], we have

$$G_k^{\chi_1,\chi_2}(\mathfrak{c}_2 z) = \frac{2C_k W(\overline{\chi_2})}{\mathfrak{c}_2^k} E_k^{\chi_1,\chi_2}(z), \quad \text{for } k \geq 3, \tag{5}$$

and similarly using Theorem 7.2.12, we have

$$\lim_{\varepsilon \to 0^+} G_{2,\varepsilon}^{\chi_1,\chi_2}(\mathfrak{c}_2 z) = \frac{2C_2 W(\overline{\chi_2})}{\mathfrak{c}_2^2} E_2^{\chi_1,\chi_2}(z). \tag{6}$$

According to loc. cit., §7.1 and §7.2 for $k \geq 3$ and $k = 2$, respectively, together with Theorem 4.7.1, we have that $E_k^{\chi_1,\chi_2}$ is an Eisenstein series of weight k, level N and Nebentypus character $\chi_1\chi_2$.

1.4. **Computation of the constant terms.** We keep the notation and assumptions of the previous subsection and moreover denote by $\mathfrak{c}_0$ the conductor of the primitive character $(\overline{\chi_1}\chi_2)_0$ associated with $\overline{\chi_1}\chi_2$. For any integer M we denote by α_M the usual degeneracy operator given by $\alpha_M f(z) = f(Mz)$.

For a given matrix $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, we let

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \lim_{\mathrm{Im}(z)\to\infty} \left((\alpha_M E_k^{\chi_1,\chi_2}) \,|_k \gamma \right)(z)$$

be the constant term of the Fourier expansion at ∞ of $(\alpha_M E_k^{\chi_1,\chi_2}) \,|_k \gamma$. Here, the notation $|_k$ refers to the classical slash operator acting on weight k modular forms.

The main goal of this section is the computation, embodied in Proposition 4 below, of the constant term $\Upsilon_k^{\chi_1,\chi_2}(\gamma, M)$.

Proposition 4. *Let $\gamma = \left(\begin{smallmatrix} u & \beta \\ v & \delta \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ and let $M \geq 1$ be an integer. Put $r = \gcd(v, M)$, $v' = v/r$ and $M' = M/r$. If $\mathfrak{c}_2 \nmid v'$, then we have that $\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = 0$. Otherwise, if $\mathfrak{c}_2 \mid v'$, then*

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) \neq 0 \iff \gcd\left(\frac{v'}{\mathfrak{c}_2}, \mathfrak{c}_1\right) = 1.$$

Moreover, in that case, we have that $\Upsilon_k^{\chi_1,\chi_2}(\gamma, M)$ is given by the non-zero algebraic number

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \xi \cdot \left(\frac{\mathfrak{c}_2}{M'\mathfrak{c}_0}\right)^k \cdot \frac{W\left((\chi_1\overline{\chi_2})_0\right)}{W\left(\overline{\chi_2}\right)} \cdot \frac{B_{k,(\overline{\chi_1}\chi_2)_0}}{2k} \prod_{p \mid N} \left(1 - (\chi_1\overline{\chi_2})_0(p) p^{-k}\right),$$

where $\xi = -\chi_2(\delta)\overline{\chi_2}(M')\chi_1(-v'/\mathfrak{c}_2)$ is a root of unity and p runs over the prime divisors of N.

Remark 1. The result above generalizes the special cases $(\chi_1, \chi_2, M) = (\chi_1, \chi_1^{-1}, 1)$ and $(\chi_1, k) = (\mathbf{1}, \geq 3)$ stated in [BD14, Prop. 2.8] and [BM15, Prop. 1.2] respectively. In this paper, we not only need the above statement in its full generality and precision, but we also provide a unified and (slightly) simplified proof of these previous results.

The following result is easily deduced from the above proposition and will be of use in Section 3.

Corollary 5. *In the notation of Proposition 4, assume M and N are coprime. Then, we have*

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \left(\frac{r}{M}\right)^k \overline{\chi_1}(r)\chi_2(r)\overline{\chi_2}(M)\Upsilon_k^{\chi_1,\chi_2}(\gamma, 1).$$

We break the proof of Proposition 4 in several steps. The proof is given at the end of this paragraph, except for the justification of an intermediary step in the case $k = 2$, which is dealt with in the next subsection.

Lemma 6. *Under the same hypothesis as in Proposition 4, we have that*

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \frac{\mathfrak{c}_2^k}{2C_k W(\overline{\chi_2})} \cdot \sum_{(m,n)\in C} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mM\mathfrak{c}_2\beta + n\delta)^k},$$

where $C = \{(m,n) \in \mathbf{Z}^2 \backslash \{(0,0)\} : mM\mathfrak{c}_2 u + nv = 0\}$.

Proof of Lemma 6 in the case $k > 2$. Using (5), we have that

$$\frac{2C_k W(\overline{\chi_2})}{\mathfrak{c}_2^k} \Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \lim_{\mathrm{Im}(z)\to\infty} \Big((\alpha_{M\mathfrak{c}_2} G_k^{\chi_1,\chi_2}) \,|_k \gamma \Big)(z).$$

Also, we have

$$\Big((\alpha_{M\mathfrak{c}_2} G_k^{\chi_1,\chi_2}) \,|_k \gamma \Big)(z) = \sum_{\substack{(m,n)\in\mathbf{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\chi_1(m)\overline{\chi_2}(n)}{(z(mM\mathfrak{c}_2 u + nv) + mM\mathfrak{c}_2\beta + n\delta)^k},$$

where the above sum is absolutely convergent since $k \geq 3$. We can therefore exchange limit and summation, yielding the result. □

Remark 2. When $k = 2$, the sum in the last equation of the previous proof is not absolutely convergent and it becomes necessary to give additional considerations, that we present in subsection 1.5, in order to justify the interchange of limit and summation. The full proof of Lemma 6 is thus achieved in Lemma 10 below.

We now prove the following key result assuming the validity of Lemma 6 for any $k \geq 2$.

Lemma 7. *Under the same hypothesis as in Proposition 4. If $\mathfrak{c}_2 \nmid v'$, then we have $\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = 0$. Otherwise, if $\mathfrak{c}_2 \mid v'$, then we have*

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma, M) = \frac{\overline{\chi_2}(M'u)\chi_1(-v'/\mathfrak{c}_2)}{M'^k} \cdot \frac{\mathfrak{c}_2^k}{C_k W(\overline{\chi_2})} \cdot L(k, \chi_1\overline{\chi_2}),$$

where $L(k, \chi_1\overline{\chi_2}) = \sum_{n\geq 1} (\chi_1\overline{\chi_2})(n) n^{-k}$.

Proof. For simplicity, put $\Upsilon = \Upsilon_k^{\chi_1,\chi_2}(\gamma, M)$.

(i) Assume $u = 0$. Then, $-v\beta = 1$, implying $v \in \{\pm 1\}$, $M' = M$ and $v' = v$. Also, the set C in Lemma 6 satisfies $C = (\mathbf{Z} \setminus \{0\}) \times \{0\}$. If $\chi_2 \neq \mathbf{1}$ (that is, if $\mathfrak{c}_2 \nmid v'$), we have that $\chi_2(0) = 0$ and then $\Upsilon = 0$ as claimed.

Assume now that $\chi_2 = \mathbf{1}$. Then, $\mathfrak{c}_2 = W(\overline{\chi_2}) = 1$ and $\chi_1(-1) = (-1)^k$. These relations imply $\chi_1(-v) = \beta^{-k}$. On the other hand, Lemma 6 ensures that

$$2C_k\Upsilon = \sum_{\substack{m\in\mathbf{Z} \\ m\neq 0}} \frac{\chi_1(m)}{(mM\beta)^k} = \frac{2}{(\beta M)^k} L(k, \chi_1) = \frac{2\chi_1(-v)}{M^k} L(k, \chi_1),$$

concluding the proof in this case.

(ii) Assume $u \neq 0$. We have the following.

Claim. Let $n \in \mathbf{Z} \setminus \{0\}$ with $\gcd(n, \mathfrak{c}_2) = 1$. Then, there exists $m \in \mathbf{Z}$ such that $(m, n) \in C$ if and only if $M'u | n$ and $\mathfrak{c}_2 \mid v'$. Furthermore, in this case we have that

$$m = -\frac{n}{M'u} \cdot \frac{v'}{\mathfrak{c}_2} \quad \text{and} \quad mM\mathfrak{c}_2\beta + n\delta = \frac{n}{u}. \tag{7}$$

Proof of the claim. If $(m, n) \in C$, then $mM'\mathfrak{c}_2 u + nv' = 0$. We have that $\gcd(M', v') = 1$ by definition. Moreover, $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ implies $\gcd(u, v) = 1$, hence $M'u \mid n$. On the other hand, since $\gcd(\mathfrak{c}_2, n) = 1$, we have that $\mathfrak{c}_2 \mid v'$.

Conversely, if $M'u \mid n$ and $\mathfrak{c}_2 \mid v'$, then the integer $m = -\frac{n}{M'u} \cdot \frac{v'}{\mathfrak{c}_2}$ satisfies $(m, n) \in C$.

Finally, if the equivalence is satisfied, we easily check using the relation $u\delta - v\beta = 1$, that the second relation in (7) holds. □

Using the claim and Lemma 6, we have that $\Upsilon = 0$ if $\mathfrak{c}_2 \nmid v'$. Otherwise, if $\mathfrak{c}_2 \mid v'$, then we have

$$\begin{aligned}
\frac{2C_k W(\overline{\chi_2})}{\mathfrak{c}_2^k}\Upsilon &= \sum_{\substack{M'u|n \\ n\neq 0}} \frac{\chi_1(n/M'u)\chi_1(-v'/\mathfrak{c}_2)\overline{\chi_2}(n)}{\left(\frac{n}{u}\right)^k} \\
&= \chi_1(-v'/\mathfrak{c}_2) \sum_{\substack{t\in\mathbf{Z} \\ t\neq 0}} \frac{\chi_1(t)\overline{\chi_2}(M'ut)}{(M't)^k} \quad (n = M'ut) \\
&= \frac{\chi_1(-v'/\mathfrak{c}_2)\overline{\chi_2}(M'u)}{M'^k} \sum_{\substack{t\in\mathbf{Z} \\ t\neq 0}} \frac{\chi_1(t)\overline{\chi_2}(t)}{t^k} \\
&= \frac{\chi_1(-v'/\mathfrak{c}_2)\overline{\chi_2}(M'u)}{M'^k} 2L(k, \chi_1\overline{\chi_2}),
\end{aligned}$$

since $\chi_1(-1)\overline{\chi_2}(-1) = (-1)^k$. This finishes the proof of Lemma 7. □

Proof of Proposition 4. According to Lemma 7, it remains to deal with the case where $\mathfrak{c}_2 \mid v'$. In that case, by reducing the equality $u\delta - v\beta = 1$ modulo $\mathfrak{c}_2$, we get $u\delta \equiv 1 \pmod{\mathfrak{c}_2}$. Furthermore, we have $\gcd(M', \mathfrak{c}_2) \mid v'$ and hence $\gcd(M', \mathfrak{c}_2) = 1$. Therefore if we assume that $\gcd(v'/\mathfrak{c}_2, \mathfrak{c}_1) = 1$, it follows that

$$-\chi_1(-v'/\mathfrak{c}_2)\overline{\chi_2}(M'u) = -\chi_1(-v'/\mathfrak{c}_2)\chi_2(\delta)\overline{\chi_2}(M') = \xi$$

is a root of unity.

Furthermore, by [Miy06, (3.3.14)], we have

$$L(k, \chi_1\overline{\chi_2}) = L(k, (\chi_1\overline{\chi_2})_0) \prod_{p|N} \left(1 - \frac{(\chi_1\overline{\chi_2})_0(p)}{p^k}\right),$$

where $(\chi_1\overline{\chi_2})_0$ denotes the primitive character associated with $\chi_1\overline{\chi_2}$. Moreover, it follows from the Euler product for $L(k, (\chi_1\overline{\chi_2})_0)$ that $L(k, \chi_1\overline{\chi_2}) \neq 0$.

Now using the assumption $(\chi_1\overline{\chi_2})_0(-1) = (-1)^k$ and [Miy06, Thm. 3.3.4], we get that

$$L(k, (\chi_1\overline{\chi_2})_0) = -W((\chi_1\overline{\chi_2})_0) \cdot \frac{C_k}{\mathfrak{c}_0^k} \cdot \frac{B_{k,(\overline{\chi_1}\chi_2)_0}}{2k}.$$

Combining these facts together with Lemma 7 concludes the proof of Proposition 4. □

1.5. **The case of weight 2.** The goal of this subsection is to prove Lemma 6 in the case $k = 2$. This is achieved in Lemma 10. For $\varepsilon \geq 0$, we use the notation

$$w^{2,\varepsilon} = w^2|w|^{2\varepsilon}, \quad w \in \mathbf{C}.$$

Let $y_0 > 0$ be a positive real number. The notation $g_1 \ll_{y_0} g_2$ means that there exists a positive constant C, depending only on y_0, such that $|g_1(r)| \leq C|g_2(r)|$ for all r in the common domain of g_1, g_2.

Let

$$S_\varepsilon(z) = \sum_{n\in\mathbf{Z}} \frac{1}{(z+n)^{2,\varepsilon}}, \quad z \in \mathbf{C} \setminus \mathbf{R}.$$

For $z \in \mathfrak{H}$, the function $S_\varepsilon(z)$ corresponds to the function $S(z; 2+\varepsilon, \varepsilon)$ in the notation of [Miy06, (7.2.7)].

Lemma 8. *Fix $y_0 > 0$. Then, we have that*

$$S_\varepsilon(z) \ll_{y_0} \frac{1}{\Gamma(\varepsilon)|y|^{1+2\varepsilon}} + e^{-2\pi|y|}, \quad y = \mathrm{Im}(z), \quad |y| \geq y_0, \quad 0 < \varepsilon \leq 1,$$

where for any real number $s > 0$, $\Gamma(s) = \int_0^\infty e^{-t}t^{s-1}dt$.

Proof. Since we have $S_\varepsilon(x - iy) = S_\varepsilon(-x + iy)$, we can assume that $y \geq y_0$. For $m \in \mathbf{Z}$, let us denote by $\xi_\varepsilon(y; m)$ the function $\xi(y; 2+\varepsilon, \varepsilon; m)$ of [Miy06, (7.2.11)]. According to Theorem 7.2.8 of loc. cit., we then have

$$S_\varepsilon(z) = \xi_\varepsilon(y; 0) + \sum_{\substack{m\in\mathbf{Z}\\ m\neq 0}} e^{2\pi imx}\xi_\varepsilon(y; m), \quad z = x + iy, \tag{8}$$

where the series converges absolutely. Furthermore, for $m \in \mathbf{Z}$, we have by loc. cit., Theorem 7.2.5, that

$$\xi_\varepsilon(y; m) = \begin{cases} -\frac{(2\pi)^{2+\varepsilon}}{\Gamma(2+\varepsilon)} \frac{1}{(2y)^\varepsilon} m^{1+\varepsilon} e^{-2\pi ym} \omega(4\pi ym; 2+\varepsilon, \varepsilon) & \text{if } m > 0, \\ -\frac{(2\pi)^{2+2\varepsilon}\Gamma(1+2\varepsilon)}{\Gamma(2+\varepsilon)\Gamma(\varepsilon)} \frac{1}{(4\pi y)^{1+2\varepsilon}} & \text{if } m = 0, \\ -\frac{(2\pi)^\varepsilon}{\Gamma(\varepsilon)} \frac{1}{(2y)^{2+\varepsilon}} \frac{1}{|m|^{1-\varepsilon}} e^{-2\pi y|m|} \omega(4\pi y|m|; \varepsilon, 2+\varepsilon) & \text{if } m < 0. \end{cases}$$

The definition of the function ω is stated in loc. cit., (7.2.31). It follows from Theorem 7.2.7 in loc. cit. that for all $m \in \mathbf{Z} \setminus \{0\}$, $y \geq y_0$ and $0 < \varepsilon \leq 1$, we have

$$\omega(4\pi y|m|; 2+\varepsilon, \varepsilon) \ll_{y_0} 1 \quad \text{and} \quad \omega(4\pi y|m|; \varepsilon, 2+\varepsilon) \ll_{y_0} 1.$$

Therefore, for all $y \geq y_0$ and $0 < \varepsilon \leq 1$ we have

$$\xi_\varepsilon(y; m) \ll_{y_0} \begin{cases} m^2 e^{-2\pi ym} & \text{if } m > 0, \\ \frac{1}{\Gamma(\varepsilon)y^{1+2\varepsilon}} & \text{if } m = 0, \\ e^{-2\pi y|m|} & \text{if } m < 0, \end{cases}$$

and (8) implies

$$S_\varepsilon(z) \ll_{y_0} \frac{1}{\Gamma(\varepsilon) y^{1+2\varepsilon}} + \sum_{m\geq 1} m^2 e^{-2\pi y m} + \sum_{m\geq 1} e^{-2\pi y m}.$$

On the other hand, for all $y \geq y_0$, we have

$$\sum_{m\geq 1} (m^2+1) e^{-2\pi y m} = \frac{e^{-2\pi y}(e^{-4\pi y} - e^{-2\pi y} + 2)}{(1-e^{-2\pi y})^3} \ll_{y_0} e^{-2\pi y},$$

hence the result follows. □

Lemma 9. *For any $a_1, a_2, D \in \mathbf{Z}$ with $D \neq 0$, set*

$$\sigma_\varepsilon(z; a_1, a_2, D) = \sum_{\substack{(m,n)\in\mathbf{Z}^2 \\ a_1+Dm\neq 0}} \frac{1}{(z(a_1+Dm)+a_2+Dn)^{2,\varepsilon}}.$$

Then, we have that

$$\lim_{\mathrm{Im}(z)\to\infty} \lim_{\varepsilon\to 0^+} \sigma_\varepsilon(z; a_1, a_2, D) = 0.$$

Proof. Assume $y = \mathrm{Im}(z) \geq 1$. We have that

$$\begin{aligned}\sigma_\varepsilon(z; a_1, a_2, D) &= \frac{1}{D^{2,\varepsilon}} \sum_{\substack{m\in\mathbf{Z} \\ a_1+Dm\neq 0}} \sum_{n\in\mathbf{Z}} \frac{1}{\left(z(\frac{a_1}{D}+m)+\frac{a_2}{D}+n\right)^{2,\varepsilon}} \\ &= \frac{1}{D^{2,\varepsilon}} \sum_{\substack{m\in\mathbf{Z} \\ a_1+Dm\neq 0}} S_\varepsilon\left(z\left(\frac{a_1}{D}+m\right)+\frac{a_2}{D}\right).\end{aligned}$$

Define

$$y_0 = \min\left\{\left|\mathrm{Im}\left(z\left(\frac{a_1}{D}+m\right)\right)\right| ; \mathrm{Im}(z)\geq 1, m\in\mathbf{Z} : a_1+Dm\neq 0\right\}.$$

Since $\mathbf{Z}$ is discrete, we have $y_0 > 0$. Using Lemma 8 with this choice of y_0, we find that for $\varepsilon \leq 1 \leq y$ and $m \in \mathbf{Z}$ such that $a_1 + Dm \neq 0$, we have

$$S_\varepsilon\left(z\left(\frac{a_1}{D}+m\right)+\frac{a_2}{D}\right) \ll_{y_0} \frac{1}{\Gamma(\varepsilon) y^{1+2\varepsilon}} \cdot \frac{1}{\left|\frac{a_1}{D}+m\right|^{1+2\varepsilon}} + e^{-2\pi y\left|\frac{a_1}{D}+m\right|}.$$

Therefore, we have

$$\sigma_\varepsilon(z; a_1, a_2, D) \ll_{y_0} \frac{1}{|D|^{2(1+\varepsilon)}} \left(\frac{1}{y^{1+2\varepsilon}} \cdot \frac{1}{\Gamma(\varepsilon)} \cdot \zeta(1+2\varepsilon) + \sum_{n\geq 1} e^{-\frac{2\pi y n}{|D|}}\right).$$

Since $\sum_{n\geq 1} e^{-\frac{2\pi y n}{|D|}} \ll_{y_0} e^{-\frac{2\pi y}{|D|}}$, we have that

$$\limsup_{\varepsilon\to 0^+} |\sigma_\varepsilon(z; a_1, a_2, D)| \ll_{y_0} \frac{1}{D^2}\left(\frac{1}{y} + e^{-\frac{2\pi y}{|D|}}\right).$$

This estimate justifies the claim. □

Lemma 10. *Lemma 6 is true for $k = 2$.*

Proof. Using (6), we have in particular that

$$\Upsilon_2^{\chi_1,\chi_2}(\gamma, M) = \frac{\mathfrak{c}_2^2}{2C_2 W(\overline{\chi_2})} \lim_{\mathrm{Im}(z)\to\infty} \lim_{\varepsilon\to 0^+} \left(\left(\alpha_{M\mathfrak{c}_2} G_{2,\varepsilon}^{\chi_1,\chi_2}\right) |_2\gamma \right)(z). \tag{9}$$

For $\varepsilon > 0$, let

$$T_\varepsilon(z) = \sum_{(m,n)\in C} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mM\mathfrak{c}_2\beta + n\delta)^{2,\varepsilon}} \tag{10}$$

and

$$R_\varepsilon(z) = \sum_{\substack{(m,n)\notin C \\ (m,n)\neq(0,0)}} \frac{\chi_1(m)\overline{\chi_2}(n)}{(z(mM\mathfrak{c}_2 u + nv) + mM\mathfrak{c}_2\beta + n\delta)^{2,\varepsilon}},$$

where, as in Lemma 6,

$$C = \left\{(m,n) \in \mathbf{Z}^2 \backslash \{(0,0)\} : mM\mathfrak{c}_2 u + nv = 0\right\}.$$

Then, we have

$$\left(\alpha_{M\mathfrak{c}_2} G_{2,\varepsilon}^{\chi_1,\chi_2}\right) |_2\gamma(z) = |vz+\delta|^\varepsilon \sum_{\substack{(m,n)\in\mathbf{Z}^2 \\ (m,n)\neq(0,0)}} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mM\mathfrak{c}_2(uz+\beta) + n(vz+\delta))^{2,\varepsilon}}$$

and therefore

$$\lim_{\varepsilon\to 0^+} \left(\alpha_{M\mathfrak{c}_2} G_{2,\varepsilon}^{\chi_1,\chi_2}\right) |_2\gamma(z) = \lim_{\varepsilon\to 0^+} \left(T_\varepsilon(z) + R_\varepsilon(z)\right).$$

Since the parameters appearing in the sum defining T_ε are linked by a linear relation, the series obtained by setting $\varepsilon = 0$ in (10) is absolutely convergent. Hence, we have that

$$\lim_{\varepsilon\to 0^+} T_\varepsilon(z) = \sum_{(m,n)\in C} \frac{\chi_1(m)\overline{\chi_2}(n)}{(mM\mathfrak{c}_2\beta + n\delta)^2}.$$

In particular, this limit is independent of z. Hence, in light of (9), in order to finish the proof we need to show that

$$\lim_{y\to\infty} \lim_{\varepsilon\to 0^+} R_\varepsilon(z) = 0. \tag{11}$$

We have that

$$R_\varepsilon(z) = \sum_{a=0}^{\mathfrak{c}_1-1} \sum_{b=0}^{\mathfrak{c}_2-1} \chi_1(a)\overline{\chi_2}(b) \sum_{\substack{(c,d)\in C_{a,b} \\ c\neq 0}} \frac{1}{(cz+d)^{2,\varepsilon}}, \tag{12}$$

where

$$C_{a,b} = \{(mM\mathfrak{c}_2 u + nv, mM\mathfrak{c}_2\beta + n\delta) : m \equiv a \mod \mathfrak{c}_1, n \equiv b \mod \mathfrak{c}_2\}.$$

Now we proceed to split each of the sums in (12) indexed by $C_{a,b}$ in a finite number of sums of the type handled by Lemma 9. Let

$$\mathbb{M} = \begin{pmatrix} M\mathfrak{c}_1\mathfrak{c}_2 u & M\mathfrak{c}_1\mathfrak{c}_2\beta \\ \mathfrak{c}_2 v & \mathfrak{c}_2\delta \end{pmatrix}, \quad \theta^{a,b} = (aM\mathfrak{c}_2 u + bv, aM\mathfrak{c}_2\beta + b\delta).$$

Then, $C_{a,b} = \theta^{a,b} + \mathbf{Z}^2 \cdot \mathbb{M}$ (here, we represent the elements of $\mathbf{Z}^2$ as row vectors). Let $D := \det \mathbb{M} = M\mathfrak{c}_1\mathfrak{c}_2^2$. By the elementary divisors theorem, we have that

$D\mathbf{Z} \times D\mathbf{Z} \subset \mathbf{Z}^2 \cdot \mathbb{M}$ is a subgroup of index D. Let $\{r_1, r_2, \dots, r_D\}$ be a system of representatives of the quotient $\mathbf{Z}^2 \cdot \mathbb{M}/D\mathbf{Z} \times D\mathbf{Z}$. Then, in the notation of Lemma 9, we have that

$$R_\varepsilon(z) = \sum_{a=0}^{\mathfrak{c}_1-1} \sum_{b=0}^{\mathfrak{c}_2-1} \chi_1(a)\overline{\chi_2}(b) \sum_{i=1}^{D} \sigma_\varepsilon\left(z; \theta_1^{a,b} + r_{i,1}, \theta_2^{a,b} + r_{i,2}, D\right),$$

where, for any vector $w \in \mathbf{R}^2$ we write $w = (w_1, w_2)$. Then, using Lemma 9, we deduce the truth of (11). □

2. Adelization of modular forms and Hecke operators

In this short section we briefly introduce some useful notation and make explicit our normalizations for modular forms and Hecke operators in the adelic setting.

For simplicity, we set, in this section, $\mathrm{G} = \mathrm{GL}_2$ considered as an algebraic group over $\mathbf{Q}$. We denote by $\mathbf{A}$ the ring of adèles of $\mathbf{Q}$. Let

$$\mathrm{G}(\mathbf{R})^+ = \{\gamma \in \mathrm{G}(\mathbf{R}) \colon \det \gamma > 0\}.$$

For each prime number p, we denote by $\iota_p \colon \mathrm{G}(\mathbf{Q}) \to \mathrm{G}(\mathbf{A})$ the map induced by the ring homomorphism $\mathbf{Q} \hookrightarrow \mathbf{Q}_p \to \mathbf{A}$. We define similarly $\iota_\infty \colon \mathrm{G}(\mathbf{R}) \to \mathrm{G}(\mathbf{A})$ using the inclusion $\mathbf{R} \hookrightarrow \mathbf{A}$. We then embed $\mathrm{G}(\mathbf{Q})$ in $\mathrm{G}(\mathbf{A})$ diagonally (that is, using $\prod_p \iota_p \times \iota_\infty$) and we embed $\mathrm{G}(\mathbf{R})^+$ at infinity (that is, using ι_∞).

Let $N \geq 1$ be a positive integer. For every prime number p set

$$K_p(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G}(\mathbf{Z}_p) \colon c \equiv 0 \pmod{N\mathbf{Z}_p} \right\}$$

and define $K_0(N) = \prod_p K_p(N)$ as a subgroup of $\mathrm{G}(\mathbf{A}_\mathrm{f})$ where $\mathbf{A}_\mathrm{f}$ denotes the finite adèles of $\mathbf{Q}$. The strong approximation theorem ([Bum97, Thm. 3.3.1] for G then implies that

$$\mathrm{G}(\mathbf{A}) = \mathrm{G}(\mathbf{Q})\mathrm{G}(\mathbf{R})^+ K_0(N). \tag{13}$$

We denote by ω the adelization (loc. cit., Prop. 3.1.2) of a given Dirichlet character χ of modulus N, and define the group homomorphism

$$\begin{array}{rccc} \lambda\colon & K_0(N) & \longrightarrow & \mathbf{C}^\times \\ & \left(\begin{pmatrix} a_p & b_p \\ c_p & d_p \end{pmatrix}\right)_p & \longmapsto & \displaystyle\prod_{p \mid N} \omega_p(d_p) \end{array}.$$

Let p be a prime divisor of N. For every integer $n \in \{0, \dots, p-1\}$, define

$$\xi_n = \begin{pmatrix} p & n \\ 0 & 1 \end{pmatrix}.$$

Let $k_0 \in K_0(N)$. Denote by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in K_p(N)$ the p-th component of k_0. Let $n \in \{0, \dots, p-1\}$ be an integer. Since $p \mid N$, we have that $cn + d \in \mathbf{Z}_p^\times$ and we define m to be the unique integer in $\{0, \dots, p-1\}$ such that

$$(cn + d)m \equiv an + b \pmod{p\mathbf{Z}_p}.$$

Let $k_0' = \iota_p(\xi_m)^{-1} k_0 \iota_p(\xi_n)$. It follows from the matrix identity in $\mathrm{G}(\mathbf{Q}_p)$,

$$\xi_m^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \xi_n = \begin{pmatrix} a - mc & \frac{an+b-m(cn+d)}{p} \\ cp & cn + d \end{pmatrix},$$

that

$$k_0' \in K_0(N) \quad \text{and} \quad \lambda(k_0') = \lambda(k_0). \tag{14}$$

Let $g \in \mathrm{G}(\mathbf{A})$, that we decompose as

$$g = \gamma g_\infty k_0, \quad \gamma \in \mathrm{G}(\mathbf{Q}), \quad g_\infty \in \mathrm{G}(\mathbf{R})^+, \quad k_0 \in K_0(N)$$

using (13). We then check place-by-place that the following equality holds (see loc. cit., p. 345):

$$g\iota_p(\xi_n) = (\gamma\xi_m)\left(\xi_{m,\infty}^{-1} g_\infty\right)\left(\xi_{m,\mathrm{f}}^{-1}\iota_p(\xi_m)k_0'\right) \in \mathrm{G}(\mathbf{Q})\mathrm{G}(\mathbf{R})^+ K_0(N), \tag{15}$$

where $n \in \{0, \dots, p-1\}$ and $m \in \{0, \dots, p-1\}$, $k_0' \in K_0(N)$ are defined above. Here, $\xi_{m,\mathrm{f}}$ and $\xi_{m,\infty}$ denote the finite and the infinite components of $\xi_m \in \mathrm{G}(\mathbf{A})$, respectively.

Let $k \geq 2$ be an integer. Denote by $S_k(N, \chi)$ the space of cuspidal modular forms of weight k, level N and Nebentypus character χ. To a modular form $F \in S_k(N, \chi)$, we attach

$$\phi_F \colon \mathrm{G}(\mathbf{A}) \to \mathbf{C}, \quad \phi_F(g) = F(g_\infty \cdot i) j(g_\infty, i)^{-k} \lambda(k_0), \quad g = \gamma g_\infty k_0.$$

Here, for $g_\infty = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{G}(\mathbf{R})^+$, we have $j(g_\infty, z) = (cz + d) \det g_\infty^{-1/2}$. Since

$$\mathrm{G}(\mathbf{Q}) \cap \mathrm{G}(\mathbf{R})^+ K_0(N) = \Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbf{Z}) \colon c \equiv 0 \pmod{N} \right\}$$

and for every $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, we have $\lambda(\gamma) = \chi(d)^{-1}$ (as ω is trivial on $\mathbf{Q}^\times$), the function ϕ_F is a well-defined automorphic form (loc. cit., §3.6). Define π_F to be the linear span of right translates of ϕ_F under $\mathrm{G}(\mathbf{A})$ and assume that F is an eigenfunction for the Hecke operators away from N. Then π_F decomposes as a restricted tensor product $\bigotimes' \pi_{F,v}$, where v runs over the places of $\mathbf{Q}$ and $\pi_{F,v}$ is an admissible irreducible representation of $\mathrm{G}(\mathbf{Q}_v)$ (loc. cit., §3.3). We now define the p-th Hecke operator in this adelic setting as follows (note the factor $1/\sqrt{p}$):

$$\widetilde{U_p} = \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \pi_{F,p}(\xi_n). \tag{16}$$

The following result will be used in the proofs of Theorems 1 and 2.

Lemma 11. *Let U_p denote the p-th Hecke operator acting on $S_k(N, \chi)$. Then, we have*

$$p^{\frac{k-1}{2}} \widetilde{U_p} \phi_F = \phi_{U_p F}.$$

Proof. Let $g = \gamma g_\infty k_0 \in \mathrm{G}(\mathbf{A})$. Then, in the notation of (15), we have (using the fact that the map $n \mapsto m$ is a bijection of $\{0, \dots, p-1\}$):

$$\begin{aligned}\widetilde{U_p}\phi_F(g) &= \frac{1}{\sqrt{p}} \sum_{n=0}^{p-1} \phi_F\left(g\iota_p(\xi_n)\right) \\ &= \frac{1}{\sqrt{p}} \sum_{m=0}^{p-1} \phi_F\left((\gamma\xi_m)\left(\xi_{m,\infty}^{-1} g_\infty\right)\left(\xi_{m,\mathrm{f}}^{-1}\iota_p(\xi_m)k_0'\right)\right) \\ &= \frac{1}{\sqrt{p}} \sum_{m=0}^{p-1} F\left(\left(\xi_{m,\infty}^{-1} g_\infty\right)\cdot i\right) j\left(\xi_{m,\infty}^{-1} g_\infty, i\right)^{-k} \lambda\left(\xi_{m,\mathrm{f}}^{-1}\iota_p(\xi_m)k_0'\right).\end{aligned}$$

Furthermore, from the definition of ξ_m and (14), we have

$$\lambda\left(\xi_{m,\mathrm{f}}^{-1}\iota_p(\xi_m)k_0'\right) = \lambda(k_0') = \lambda(k_0),$$

and from the automorphy relation for F, we have

$$F\left(\left(\xi_{m,\infty}^{-1} g_\infty\right)\cdot i\right) j\left(\xi_{m,\infty}^{-1} g_\infty, i\right)^{-k} = p^{-k/2} F\left(\frac{g_\infty \cdot i - m}{p}\right) j(g_\infty, i)^{-k}.$$

We conclude that

$$\widetilde{U_p}\phi_F(g) = \frac{1}{p^{(k+1)/2}} \sum_{m=0}^{p-1} F\left(\frac{g_\infty \cdot i - m}{p}\right) j(g_\infty, i)^{-k} \lambda(k_0).$$

Hence, the desired identity follows from the formula

$$U_p F(z) = \frac{1}{p}\sum_{m=0}^{p-1} F\left(\frac{z+m}{p}\right) = \frac{1}{p}\sum_{m=0}^{p-1} F\left(\frac{z-m}{p}\right), \quad z \in \mathfrak{H}. \qquad \square$$

3. Proofs of the main results

3.1. **Proof of Theorem 1.** Let $\nu_1, \nu_2 \colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{F}}_l^\times$ be characters such that $\rho = \nu_1 \oplus \nu_2$ defines an odd (semi-simple) Galois representation of Serre type (N, k, ε). Assume throughout that $l > k+1$. Each of the characters ν_i $(i = 1, 2)$ can be decomposed as $\nu_i = \varepsilon_i \chi_l^{a_i}$, where ε_i is unramified at l, a_i is a non-negative integer and χ_l denotes the mod l cyclotomic character. Without loss of generality, we may further assume that $0 \le a_1 \le a_2 \le l-2$. According to Serre's definition of the weight k (see [Ser87, (2.3.2)]), we then have:

$$k = \begin{cases} 1 + la_1 + a_2 & \text{if } (a_1, a_2) \neq (0,0), \\ l & \text{if } (a_1, a_2) = (0,0). \end{cases}$$

Since we have assumed $l > k+1$, it follows that $(a_1, a_2) = (0, k-1)$. This proves the first part of Theorem 1.

Let us then prove the equivalence. Denote by $\mathfrak{c}_1$ and $\mathfrak{c}_2$ the conductors of ε_1 and ε_2, respectively. We have the Serre parameters $\varepsilon = \varepsilon_1\varepsilon_2$ and $N = \mathfrak{c}_1\mathfrak{c}_2$. If $(N, k) = (1, 2)$, then both ε_1 and ε_2 are trivial and therefore, in the notation of the theorem, we have

$$B_{2,\eta} = B_2 \pmod{l} \quad \text{and} \quad B_2 = \frac{1}{6} \not\equiv 0 \pmod{l}.$$

On the other hand, there is no non-zero cuspidal eigenform of weight 2 and level 1 over $\overline{\mathbf{F}}_l$ for $l \geq 5$. Hence, the desired equivalence is established in this case.

From now on, let us then assume that either $N > 1$ or $k > 2$. Fix a place w of $\overline{\mathbf{Q}}$ above l and denote by χ_1 and χ_2 the multiplicative lifts with respect to w (in the sense of subsection 1.2) of ε_1 and ε_2, respectively. We view $\chi = \chi_1\chi_2$ as a Dirichlet character modulo N. The Eisenstein series $E_k^{\chi_1,\chi_2}$ introduced in subsection 1.3 (which is well-defined as we have $(N,k) \neq (1,2)$) has weight k, level N and Nebentypus character χ. Moreover, it is a normalized eigenform for the full Hecke algebra at level N. In particular, if we write

$$E_k^{\chi_1,\chi_2}(z) = \sum_{n\geq 0} a_n\left(E_k^{\chi_1,\chi_2}\right) e^{2i\pi zn} \quad (z \in \mathfrak{H}),$$

then its eigenvalue for the action of the Hecke operator at an arbitrary prime p is given by

$$a_p\left(E_k^{\chi_1,\chi_2}\right) = \chi_1(p) + \chi_2(p)p^{k-1}.$$

By assumption, there exists an eigenform f of type (N,k,ε) over $\overline{\mathbf{F}}_l$ such that, in the notation of the Introduction, we have $\rho_f \simeq \rho$. Let us write $f = \sum_{n\geq 1} a_n q^n$ as in [Ser87, Déf. p. 193]. In other words, there exists $F = \sum_{n\geq 1} A_n q^n$ a weight-k cuspidal form of level N and Nebentypus character χ such that $A_n \in \overline{\mathbf{Z}}_w$ and

$$\nu_w(A_n) = a_n, \quad \text{for any integer } n \geq 1, \tag{17}$$

in the notation of subsection 1.2. By the Deligne-Serre lifting lemma ([DS74, Lem. 6.11]), one may further assume that F is a normalized eigenform for all the Hecke operators at level N. Denote by E the number field generated by the Hecke eigenvalues of F and by λ the prime ideal above l in E induced by w. Let E_λ be the completion of E at λ. Thanks to the isomorphism $\rho \simeq \rho_f$ and (17), the semi-simplification of the reduction modulo λ of the λ-adic representation of F,

$$\rho_{F,\lambda}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}_2(E_\lambda),$$

is isomorphic to ρ. Since F has level N and ρ conductor N away from l, the form F is actually a newform. For every prime $p \nmid Nl$, we have

$$\nu_w(A_p) = \varepsilon_1(p) + \varepsilon_2(p)p^{k-1},$$

where, $\varepsilon_i(p) = \varepsilon_i(\mathrm{Frob}_p)$ if ε_i is unramified at p and $\varepsilon_i(p) = 0$; otherwise, for $i = 1, 2$. The next step is to extend these congruences to arbitrary primes $p \neq l$, as stated in the following key result. (Note that only the case $N > 1$ requires a proof.)

Proposition 12. *In this notation, we have*

$$\nu_w(A_p) = \varepsilon_1(p) + \varepsilon_2(p)p^{k-1}, \quad \textit{for every prime } p \neq l.$$

Proof. We have seen that the equality holds for primes not dividing Nl. Let p be a prime dividing N (note that, by definition, N is coprime to l and hence $p \neq l$). We denote by $\mathfrak{c}$ the conductor of χ. We shall split the proof into three cases:

(1) $\mathrm{ord}_p(N) = 1$ and $\mathrm{ord}_p(\mathfrak{c}) = 0$;
(2) $\mathrm{ord}_p(N) \geq 2$ and $\mathrm{ord}_p(\mathfrak{c}) < \mathrm{ord}_p(N)$;
(3) $\mathrm{ord}_p(N) = \mathrm{ord}_p(\mathfrak{c})$.

To deal with the first two cases, we first observe that if $\mathrm{ord}_p(\mathfrak{c}) < \mathrm{ord}_p(N)$, then both characters χ_1 and χ_2 are ramified at p. Indeed, since $\mathrm{ord}_p(N) > 0$ and $N = \mathfrak{c}_1\mathfrak{c}_2$, at least one of the two characters χ_1 and χ_2 is ramified at p. On the other hand, if the other one is unramified at p then, we have

$$\mathrm{ord}_p(\mathfrak{c}) = \mathrm{ord}_p(\mathfrak{c}_1) + \mathrm{ord}_p(\mathfrak{c}_2) = \mathrm{ord}_p(N),$$

obtaining a contradiction.

In the first case, using this observation, we obtain

$$1 = \mathrm{ord}_p(N) = \mathrm{ord}_p(\mathfrak{c}_1) + \mathrm{ord}_p(\mathfrak{c}_2) \geq 2$$

and a contradiction. Case (1) therefore does not occur.

In the second case, we have that $A_p = 0$ ([Miy06, Thm. 4.6.17]) and by the above observation, both χ_1, χ_2 (and hence ε_1 and ε_2) are ramified at p. We therefore have the desired equality as both sides are zero.

It therefore remains to deal with the last case. Let ϕ_F be the adelization of F as defined in Section 2. Denote by π_F the corresponding automorphic representation. Since F is p-new, then ϕ_F is a so-called new-vector for $\pi_{F,p}$ (in the sense of [LW12, Thm. 2.2]). The endomorphism $\widetilde{U_p}$ defined in (16) acts on the (one-dimensional) vector space of new-vectors of $\pi_{F,p}$ by multiplication by an eigenvalue that we denote by $\lambda(\pi_{F,p})$. It then follows from Lemma 11 that we have

$$\lambda(\pi_{F,p}) = A_p/p^{(k-1)/2}.$$

Using the assumption $\mathrm{ord}_p(N) = \mathrm{ord}_p(\mathfrak{c})$, we have that $\lambda(\pi_{F,p})$ has absolute value 1 and therefore is $\neq 0$ ([Miy06, Thm. 4.6.17]). On the other hand, we see from the classification of irreducible admissible infinite-dimensional smooth representations of $\mathrm{GL}_2(\mathbf{Q}_p)$ (as recalled in Table 1 of [LW12] for instance) that in this case $\pi_{F,p}$ necessarily is a principal series $\pi(\mu_1, \mu_2)$ associated with some characters μ_1, μ_2 of $\mathbf{Q}_p^\times$. Equating the Hecke eigenvalues we find that

$$p^{(k-1)/2}(\mu_1^*(p) + \mu_2^*(p)) = A_p, \tag{18}$$

where

$$\mu_i^*(p) = \begin{cases} \mu_i(p) & \text{if } \mu_i \text{ is unramified at } p, \\ 0 & \text{otherwise,} \end{cases} \qquad \text{for } i = 1, 2.$$

Let $\sigma^\lambda(\pi_{F,p})$ be the representation of the local Weil group $W(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ attached to $\pi_{F,p}$ by the local Langlands correspondence. By a theorem of Carayol ([Car86, Thm. (A)]), it agrees with (the restriction to the Weil group of) the local representation $\rho_{F,\lambda}|_{\mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)}$.

Let us denote by $\overline{\mu_1}$ and $\overline{\mu_2}$ the reductions modulo w of μ_1 and μ_2, respectively. According to §0.5 in loc. cit., we therefore have the following equality of characters of $\mathbf{Q}_p^\times$ with values in $\overline{\mathbf{F}}_l^\times$:

$$\left\{\overline{\mu_1}\chi_l^{(k-1)/2}, \overline{\mu_2}\chi_l^{(k-1)/2}\right\} = \left\{\varepsilon_1, \varepsilon_2\chi_l^{k-1}\right\}.$$

The result now follows from (18). □

Let us now consider the Eisenstein series $E_k^{\chi_1,\chi_2}$. Since both F and $E_k^{\chi_1,\chi_2}$ are eigenfunctions for the full Hecke algebra at level N, it follows from the previous proposition and the multiplicativity of the Fourier coefficients that

$$\nu_w(A_n) = \nu_w\left(a_n\left(E_k^{\chi_1,\chi_2}\right)\right), \quad \text{for all prime-to-}l \text{ integers } n.$$

Note that by Lemma 3 and (4), the q-expansion of the Eisenstein series $E_k^{\chi_1,\chi_2}$ lies in $\overline{\mathbf{Z}}_w[[q]]$. Let us denote by $\overline{E}$ its reduction modulo w. Then, both f and $\overline{E}$ have the same image under the Θ-operator whose action on the q-expansions is $q\frac{d}{dq}$ (see [Kat77, Ch. II]).

We remark that, since we are assuming that $k \geq 2$ and $l \nmid N$, the space of modular forms for $\Gamma_1(N)$ over $\overline{\mathbf{F}}_l$ in the sense of Katz and in the sense of Serre are naturally isomorphic [DI95, Theorem 12.3.7]. Then, since $l > k+1$, we can use [Kat77, Cor. 3] to assert that the Θ-operator is injective. Hence, $\overline{E}$ is a cuspidal form over $\overline{\mathbf{F}}_l$. This implies that w divides the constant term of $E_k^{\chi_1,\chi_2}$ at each of the cusps.

In particular, it divides the constant term of the Fourier expansion at ∞ of $E_k^{\chi_1,\chi_2}|_k\gamma$, where $\gamma = \left(\begin{smallmatrix} 1 & 0 \\ \mathfrak{c}_2 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. According to Proposition 4 (applied to $M = 1$ in its notation), w divides

$$\left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0}\right)^k \frac{W\left((\chi_1\overline{\chi_2})_0\right)}{W\left(\overline{\chi_2}\right)} \frac{B_{k,(\overline{\chi_1}\chi_2)_0}}{2k} \prod_{p|N} \left(1 - (\chi_1\overline{\chi_2})_0(p)p^{-k}\right).$$

However, $\mathfrak{c}_0$, $\mathfrak{c}_2$, $W\left((\chi_1\overline{\chi_2})_0\right)$, $2k$ and $W\left(\overline{\chi_2}\right)$ are all coprime to l. Moreover, $(\overline{\chi_1}\chi_2)_0$ is nothing but the multiplicative lift of $\eta = \varepsilon_1^{-1}\varepsilon_2$ with respect to w. Hence, either $B_{k,\eta} = 0$, or there exists a prime $p \mid N$ such that $\eta(p)p^k = 1$. This proves the direct implication in Theorem 1.

Conversely, assume that either condition of the theorem is satisfied. Then, by definition of the characters χ_1 and χ_2 and of the Bernoulli number $B_{k,\eta}$, the place w divides (the numerator of)

$$B_{k,(\overline{\chi_1}\chi_2)_0} \cdot \prod_{p|N} \left((\overline{\chi_1}\chi_2)_0(p)p^k - 1\right).$$

Then, according to Proposition 4 (with $M = 1$), the constant term of the Eisenstein series $E_k^{\chi_1,\chi_2}$ vanishes at each of the cusp of the modular curve $X_1(N)$. Let f be its reduction modulo w, which is an eigenform with coefficients in $\overline{\mathbf{F}}_l$. As we argued before, f can be seen both as a Katz or Serre modular form. Then, the q-expansion principle allows us to ensure that f is a cuspidal eigenform (cf. [DI95, Remark 12.3.5]).

On the other hand, for every prime $q \nmid Nl$, we have

$$\mathrm{trace}\left(\rho_f(\mathrm{Frob}_q)\right) = \nu_w\left(a_q(E_k^{\chi_1,\chi_2})\right) = \varepsilon_1(q) + \varepsilon_2(q)q^{k-1} = \mathrm{trace}\left(\rho(\mathrm{Frob}_q)\right).$$

Since $\det\rho_f = \varepsilon\chi_l^{k-1} = \det\rho$, the Chebotarev density and Brauer-Nesbitt theorems, as explained in [DS74, Lem. 3.2], imply that $\rho_f \simeq \rho$. Then, f is the desired eigenform. This finishes the proof of Theorem 1.

3.2. **Proof of Theorem 2.** In the case $(N,k) = (1,2)$ (where we necessarily have $\rho \simeq \mathbf{1} \oplus \chi_l$ and hence ρ is not strongly modular), the result is due to Mazur ([Maz77, Prop. 5.12]).

We therefore assume throughout that $(N,k) \neq (1,2)$ and start by proving the direct implication.

Using the assumption that the representation ρ arises from a modular form f of type (NM,k,ε) over $\overline{\mathbf{F}}_l$, we show as before that there exists $F = \sum_{n\geq 1} A_n q^n$, a weight-$k$ normalized cuspidal eigenform of level NM and Nebentypus character χ with the following property. Let λ be the prime ideal of the coefficient field of F

induced by w. The semi-simplification of the reduction modulo λ of the λ-adic representation attached to F is isomorphic to ρ. Let F_0 denote the newform associated with F. The λ-adic representations attached to F_0 and F are isomorphic. In particular, after reduction modulo λ and semi-simplification, they both give rise to ρ. Since ρ has conductor N, it follows from [Car86, Thm. (A)] and the considerations in [Car89, **1.-2.**], that the level of F_0 is divisible by N. Moreover, we have assumed that ρ is not strongly modular, and thus the level of F_0 is strictly greater than N. Since it is a divisor of NM, it has to be equal to NM and $F = F_0$ necessarily is a newform. Therefore, considering its associated automorphic representation, we prove the following result using the same arguments as in Proposition 12.

Proposition 13. *In this notation, we have*

$$\nu_w(A_p) = \varepsilon_1(p) + \varepsilon_2(p)p^{k-1}, \quad \textit{for every prime } p \neq l, M.$$

We now turn our attention to the local situation at M and prove the following statement.

Proposition 14. *We have*

(1) *either* $\eta(M)M^k = 1$;
(2) *or,* $\eta(M)M^{k-2} = 1$ *and* $\nu_w(A_M) = \varepsilon_1(M)$.

Proof. According to [Miy06, Thm. 4.6.17(2)], we have $A_M \neq 0$. In particular, the form F is M-primitive in the sense of [AL78, Def. p. 236] (see the remark right after the definition). Therefore, according to Proposition 2.8 of [LW12], the local component at M of the automorphic represention of F corresponds to a Steinberg representation. Moreover, we have the following equality between sets of characters of a decomposition group at M in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ with values in $\overline{\mathbf{F}}_l^{\times}$:

$$\left\{\varepsilon_1, \varepsilon_2\chi_l^{k-1}\right\} = \left\{\mu\chi_l^{k/2}, \mu\chi_l^{k/2-1}\right\},$$

where μ is the unramified character that sends a Frobenius element at M to $\mu(M) = \nu_w\left(A_M/M^{k/2-1}\right)$. We therefore have two cases to consider:

- Assume that, locally at M, we have $\varepsilon_1 = \mu\chi_l^{k/2}$. Then, in particular, we have $\varepsilon_1(M)^2 = \mu(M)^2M^k$. On the other hand, according to [Miy06, Thm. 4.6.17], we have $\mu(M)^2 = (\varepsilon_1\varepsilon_2)(M)$. Therefore, we get $\eta(M)M^k = 1$. (Note that the other equality, namely $\varepsilon_2\chi_l^{k-1} = \mu\chi_l^{k/2-1}$, does not provide any additional information.)
- Assume instead that, locally at M, we have $\varepsilon_1 = \mu\chi_l^{k/2-1}$. Then, on the one hand, we have that $\varepsilon_1(M) = \mu(M)M^{k/2-1}$ and hence $\nu_w(A_M) = \varepsilon_1(M)$. On the other hand, we have (using loc. cit.) $M^{2k-2}\varepsilon_2(M)^2 = \mu(M)^2M^k$. Therefore, we get $\eta(M)M^{k-2} = 1$. Hence the result follows. (Once again, the other equality, namely $\varepsilon_2\chi_l^{k-1} = \mu\chi_l^{k/2}$, does not give any other information.) □

In order to finish the proof of Theorem 2, it therefore remains to show that, under the assumption that ρ is not strongly modular, condition (14) in Proposition 14 implies condition (14). For that purpose, let us assume that condition (14) is satisfied and consider the following Eisenstein series:

$$F_1 = E_k^{\chi_1,\chi_2} - \chi_2(M)M^{k-1}\alpha_M E_k^{\chi_1,\chi_2}.$$

It is a well-known fact that F_1 is an eigenform for the full Hecke algebra at level NM with eigenvalues

$$a_p(F_1) = \chi_1(p) + \chi_2(p)p^{k-1}, \quad \text{for primes } p \neq M,$$

and $a_M(F_1) = \chi_1(M)$. In particular, as a consequence of Proposition 13 and our assumption, we have

$$\nu_w\left(a_n(F_1)\right) = \nu_w(A_n), \quad \text{for every integer } n \text{ coprime to } l, \tag{19}$$

where $\{a_n(F_1)\}_{n\geq 1}$ denote the coefficients of the Fourier expansion of F_1 at ∞. By definition of F_1, Lemma 3 and (4), this q-expansion lies in $\overline{\mathbf{Z}}_w[[q]]$. Let us thus denote by $\overline{F_1}$ the reduction of F_1 modulo w. According to (19), $\overline{F_1}$ and the reduction of F modulo w have the same image under the Θ-operator. Since $l > k+1$, the injectivity of Θ ([Kat77, Cor. 3]) implies that $\overline{F_1}$ is cuspidal. Therefore, we have that w divides the numerator of the constant of the term of the Fourier expansion of F_1 at each cusp of the modular curve at level NM. According to Corollary 5, such a constant term at the cusp $1/(M\mathfrak{c}_2)$ is given (up to roots of unity) by

$$\Upsilon_k^{\chi_1,\chi_2}(\gamma,1)\left(1-\overline{\chi_1}(M)\chi_2(M)M^{k-1}\right),$$

where $\gamma \in \mathrm{SL}_2(\mathbf{Z})$ is such that $\gamma\cdot\infty = 1/(M\mathfrak{c}_2)$. On the other hand, for such a γ, thanks to Theorem 1 and Proposition 4, the assumption that ρ is not strongly modular guarantees that $\Upsilon_k^{\chi_1,\chi_2}(\gamma,1)$ is (non-zero and) not divisible by w. Therefore, it follows that $\eta(M)M^{k-1} = 1$ and hence $M \equiv 1 \pmod{l}$ (as we have assumed $\eta(M)M^{k-2} = 1$). This implies the desired equality $\eta(M)M^k = 1$ and concludes the proof of the direct implication.

In the other direction, assuming that $\eta(M)M^k = 1$, we now consider the Eisenstein series defined by

$$F_2 = E_k^{\chi_1,\chi_2} - \chi_1(M)\alpha_M E_k^{\chi_1,\chi_2}.$$

For any $\gamma \in \mathrm{SL}_2(\mathbf{Z})$, let us denote by $a_0\left(F_2|_k\gamma\right)$ the constant term of the Fourier expansion at ∞ of $F_2|_k\gamma$. According to Corollary 5, using its notation, we have that

$$a_0\left(F_2|_k\gamma\right) = \Upsilon_k^{\chi_1,\chi_2}(\gamma,1)\left(1-\left(\frac{r}{M}\right)^k(\chi_1\overline{\chi_2})(M/r)\right),$$

where $r = 1$ or M. In both cases, using the assumption $\eta(M)M^k = 1$, we have that $\nu_w\left(a_0\left(F_2|_k\gamma\right)\right) = 0$. We denote by f the reduction of F_2 modulo w. It is a well-defined cuspidal form of type (NM,k,ε) over $\overline{\mathbf{F}}_l$ which is an eigenform for the full Hecke algebra at level NM with eigenvalue for the Hecke operator at p given by

$$\varepsilon_1(p) + \varepsilon_2(p)p^{k-1}, \quad \text{for all primes } p \neq M.$$

Then, the Chebotarev density and Brauer-Nesbitt theorems, as explained in [DS74, Lem. 3.2], imply that ρ arises from a form of type (NM,k,ε) as desired.

Acknowledgments

The authors wish to thank Vinayak Vatsal for inspiring discussions and the Pacific Institute for the Mathematical Sciences in Vancouver for providing ideal conditions to carry out part of this project. We also thank the anonymous referee for precise comments that have improved the exposition.

References

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), no. 3, 221–243, DOI 10.1007/BF01390245. MR508986

[BD14] Nicolas Billerey and Luis V. Dieulefait, *Explicit large image theorems for modular forms*, J. Lond. Math. Soc. (2) **89** (2014), no. 2, 499–523, DOI 10.1112/jlms/jdt072. MR3188630

[BM15] Nicolas Billerey and Ricardo Menares, *On the modularity of reducible* mod l *Galois representations*, Math. Res. Lett. **23** (2016), no. 1, 15–41, DOI 10.4310/MRL.2016.v23.n1.a2. MR3512875

[Bum97] Daniel Bump, *Automorphic forms and representations*, Cambridge Studies in Advanced Mathematics, vol. 55, Cambridge University Press, Cambridge, 1997. MR1431508

[Car59a] Leonard Carlitz, *Arithmetic properties of generalized Bernoulli numbers*, J. Reine Angew. Math. **202** (1959), 174–182, DOI 10.1515/crll.1959.202.174. MR0109132

[Car59b] Leonard Carlitz, *Some arithmetic properties of generalized Bernoulli numbers*, Bull. Amer. Math. Soc. **65** (1959), 68–69, DOI 10.1090/S0002-9904-1959-10278-0. MR0104630

[Car86] Henri Carayol, *Sur les représentations l-adiques associées aux formes modulaires de Hilbert*, Ann. Sci. École Norm. Sup. (4) **19** (1986), no. 3, 409–468. MR870690

[Car89] Henri Carayol, *Sur les représentations galoisiennes modulo l attachées aux formes modulaires*, Duke Math. J. **59** (1989), no. 3, 785–801, DOI 10.1215/S0012-7094-89-05937-1. MR1046750

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem (Toronto, ON, 1993), CMS Conf. Proc., vol. 17, Amer. Math. Soc., Providence, RI, 1995, pp. 39–133. MR1357209

[DS74] Pierre Deligne and Jean-Pierre Serre, *Formes modulaires de poids* 1, Ann. Sci. École Norm. Sup. (4) **7** (1974), 507–530 (1975). MR0379379

[Kat77] Nicholas M. Katz, *A result on modular forms in characteristic p*, Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976), Lecture Notes in Math., Vol. 601, Springer, Berlin, 1977, pp. 53–61. MR0463169

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504, DOI 10.1007/s00222-009-0205-7. MR2551763

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586, DOI 10.1007/s00222-009-0206-6. MR2551764

[LW12] David Loeffler and Jared Weinstein, *On the computation of local components of a newform*, Math. Comp. **81** (2012), no. 278, 1179–1200, DOI 10.1090/S0025-5718-2011-02530-5. MR2869056

[Maz77] Barry Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. **47** (1977), 33–186 (1978). MR488287

[Miy06] Toshitsune Miyake, *Modular forms*, Reprint of the first 1989 English edition, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006. Translated from the 1976 Japanese original by Yoshitaka Maeda. MR2194815

[Rib75] Kenneth A. Ribet, *On l-adic representations attached to modular forms*, Invent. Math. **28** (1975), 245–275, DOI 10.1007/BF01425561. MR0419358

[Ser87] Jean-Pierre Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230, DOI 10.1215/S0012-7094-87-05413-5. MR885783

Université Clermont Auvergne, Université Blaise Pascal, Laboratoire de Mathématiques, BP 10448, F-63000 Clermont-Ferrand, France – and – CNRS, UMR 6620, LM, F-63171 Aubière, France

E-mail address: Nicolas.Billerey@uca.fr

Pontificia Universidad Católica de Valparaíso, Instituto de Matemáticas, Blanco Viel 596, Cerro Barón, Valparaíso, Chile

E-mail address: ricardo.menares@pucv.cl

PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 145, Number 10, October 2017, Pages 4111–4117
http://dx.doi.org/10.1090/proc/13475
Article electronically published on June 16, 2017

A RESULT ON THE EQUATION $x^p + y^p = z^r$ USING FREY ABELIAN VARIETIES

NICOLAS BILLEREY, IMIN CHEN, LUIS DIEULEFAIT, AND NUNO FREITAS

(Communicated by Romyar T. Sharifi)

Abstract. We prove a Diophantine result on generalized Fermat equations of the form $x^p + y^p = z^r$ which for the first time requires the use of Frey abelian varieties of dimension ≥ 2 in Darmon's program. More precisely, for $r \geq 5$ a regular prime we prove that there exists a constant $C(r)$ such that for every prime number $p > C(r)$ the equation $x^p + y^p = z^r$ has no non-trivial primitive integer solutions (a, b, c) satisfying $r \mid ab$ and $2 \nmid ab$.

For the proof, we complement Darmon's ideas in a particular case by providing an irreducibility criterion for the mod $\mathfrak{p}$ representations attached to certain families of abelian varieties of GL_2-type over totally real fields.

1. Introduction

Darmon [2] has initiated a remarkable program to study the generalized Fermat equation

(1.1)
$$x^p + y^q = z^r, \qquad 1/p + 1/q + 1/r < 1, \qquad x, y, z \in \mathbb{Z}, \qquad xyz \neq 0, \qquad \gcd(x, y, z) = 1,$$

where the exponents $p, q, r \geq 2$ are prime numbers. He divides the analysis of this equation into the three one-parameter families (r, r, p), (p, p, r) and (r, q, p) where in each case the parameter p is allowed to vary and the other exponents are fixed. A notable feature of his program is that it uses higher dimensional abelian varieties and their (still mostly conjectural) modularity instead of just elliptic curves. However, very little is understood about the relevant abelian varieties and Darmon's program has not yet produced any Diophantine result, apart from a few cases where the abelian varieties involved are of dimension one, i.e., elliptic curves.

Darmon's program follows the strategy of the 'modular method': the Frey abelian variety $A(x, y, z)$ attached to a non-trivial (i.e. $xyz \neq 0$) putative solution (x, y, z) of (1.1) can be distinguished from the abelian varieties attached to the known trivial solutions (i.e. $xyz = 0$) through their Galois representations. Indeed, the p-torsion representation attached to $A(x, y, z)$ should be large in general, while if (x, y, z) is a trivial solution, then this image is usually reducible or contained in

Received by the editors May 7, 2016 and, in revised form, August 19, 2016.
2010 *Mathematics Subject Classification.* Primary 11D41.
Key words and phrases. Fermat equations, Frey abelian varieties, irreducibility.
The first author acknowledges the financial support of CNRS and ANR-14-CE-25-0015 Gardio, the second author acknowledges the financial support of an NSERC Discovery Grant, the third author acknowledges the financial support of the MEC project MTM2015-66716-P and the fourth author acknowledges financial support from from the grant *Proyecto RSME-FBBVA* 2015 *José Luis Rubio de Francia*.

the normalizer of a Cartan subgroup. Modularity of the abelian varieties $A(x,y,z)$ and level lowering results imply a congruence mod p between eigenforms, which bounds p under the set-up described above. Another interesting feature of Darmon's program is the use of classical cyclotomic criteria to eliminate the possibility of a congruence to an $\mathfrak{r}$-Eisenstein $\mathbb{Q}$-form at the lower levels [2, Proposition 3.20].

The objective of this work is twofold. We first develop an irreducibility criterion for the p-torsion representations attached to certain families of abelian varieties. Secondly, by following the idea in the previous paragraph and results from [2], we will show how the criterion can be used to unconditionally establish a Diophantine statement via Darmon's program that for the first time requires Frey abelian varieties of dimension ≥ 2.

We recall that an odd prime number r is called *regular* if it does not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta_r)$. It is an open conjecture due to Siegel that there are infinitely many regular primes. We will prove the following theorem.

Theorem 1. *Let $r \geq 5$ be a regular prime. There exists a constant $C(r)$ such that for every prime number $p > C(r)$ the equation*

$$x^p + y^p = z^r \tag{1.2}$$

has no non-trivial (i.e. $abc \neq 0$) primitive (i.e. $\gcd(a,b,c) = 1$) solutions $(a,b,c) \in \mathbb{Z}^3$ satisfying $r \mid ab$ and $2 \nmid ab$.

2. An irreducibility criterion

The following terminology has been introduced by Ribet.

Definition 2.1. An abelian variety A over a number field K is said to be of GL_2-type if its endomorphism algebra $\mathrm{End}_K(A) \otimes \mathbb{Q} = F$ is a number field satisfying $[F : \mathbb{Q}] = \dim A$.

Let A/K be an abelian variety of GL_2-type. Set $F = \mathrm{End}_K(A) \otimes \mathbb{Q}$ and let p be a prime number. Denote by $T_p(A)$ the Tate module of A and write $V_p(A) = T_p(A) \otimes \mathbb{Q}_p$. Then, for each prime ideal $\mathfrak{p}$ of F over p, the absolute Galois group G_K of K acts $F_\mathfrak{p}$-linearly on $V_\mathfrak{p}(A) = V_p(A) \otimes_{F_p} F_\mathfrak{p}$ where $F_\mathfrak{p}$ denotes the completion of F at $\mathfrak{p}$ and $F_p = F \otimes \mathbb{Q}_p = \prod_{\mathfrak{p}|p} F_\mathfrak{p}$. This gives rise to a strictly compatible system of 2-dimensional p-adic Galois representations

$$\widetilde{\rho}_{A,\mathfrak{p}} : G_K \longrightarrow \mathrm{GL}_2(F_\mathfrak{p}).$$

The representation $\widetilde{\rho}_{A,\mathfrak{p}}$ can be conjugated to take values in $\mathrm{GL}_2(\mathcal{O}_\mathfrak{p})$ where $\mathcal{O}_\mathfrak{p}$ stands for the ring of integers in $F_\mathfrak{p}$. By reduction modulo the maximal ideal, we then get a representation

$$\rho_{A,\mathfrak{p}} : G_K \longrightarrow \mathrm{GL}_2(\mathbb{F}_\mathfrak{p}),$$

with values in the residue field $\mathbb{F}_\mathfrak{p}$ of $F_\mathfrak{p}$ which is unique up to semi-simplification and isomorphism.

The aim of this section is to provide a uniform bound on the residual characteristic of prime ideals $\mathfrak{p}$ for which the corresponding representations $\rho_{A,\mathfrak{p}}$ is reducible when A runs through certain families of abelian varieties of GL_2-type. For elliptic curves over totally real fields, such irreducibility criteria were previously known and different variants (for various families of curves) can be found in the work of Serre [11], Kraus [7,8], Billerey [1], David [3], Dieulefait-Freitas [4] and Freitas-Siksek [5].

Recently, Larson and Vaintrob [9] have proven general results which classify the so-called associated mod p characters of abelian varieties A over a number field K for p sufficiently large. Their results have consequences to proving irreducibility criteria for the representations $\rho_{A,\mathfrak{p}}$ which we discuss here with a view towards applications to Frey abelian varieties.

For that purpose, we introduce some useful definitions.

Definition 2.2. Let A/K be an abelian variety with potentially good reduction at a prime $\mathfrak{q}$ of a number field K. We say that A *has residual degree* f *at* $\mathfrak{q}$ if f is minimal among the degrees of the residual extensions corresponding to all extensions $L/K_{\mathfrak{q}}$ such that A/L has good reduction.

The following definition is motivated by [9, Lemma 4.6].

Definition 2.3. We say that an abelian variety A/K *has inertial exponent* $c \in \mathbb{N}$ if for every finite prime v of the number field K, there exists a finite Galois extension M/K such that A/M is semistable at all primes of M lying over v, and the exponent of the inertia subgroup at v of $\mathrm{Gal}(M/K)$ divides c.

We write $\overline{\mathbb{Z}}$ for the ring of integers of $\overline{\mathbb{Q}}$. Given an ideal $\mathfrak{q}$ of the ring of integers of a number field K, we write $N(\mathfrak{q})$ for its norm.

Theorem 2. *Let K be a totally real number field and fix a prime $\mathfrak{q}$ of K. Let $c, f \geq 1$ be integers with c even. Consider a finite set $S_f(\mathfrak{q})$ of elements of the form $\alpha_1 + \alpha_2$ where $\alpha_i \in \overline{\mathbb{Z}}$ are (for every embedding $\overline{\mathbb{Z}} \hookrightarrow \mathbb{C}$) of complex absolute value $N(\mathfrak{q})^{f/2}$ and $\alpha_1\alpha_2 = N(\mathfrak{q})^f$.*

Then there exists a constant $c_1 = c_1(K, c, f, S_f(\mathfrak{q}))$ such that the following holds. Suppose that $p > c_1$ and A/K is an abelian variety satisfying

- *(i) A is semistable at the primes of K above p,*
- *(ii) A is of GL_2-type with multiplications by some totally real field F,*
- *(iii) all endomorphisms of A are defined over K, that is, $\mathrm{End}_K(A) = \mathrm{End}_{\overline{K}}(A)$,*
- *(iv) A over K has inertial exponent c,*
- *(v) A has potentially good reduction at $\mathfrak{q}$ with residual degree f,*
- *(vi) the trace of $\mathrm{Frob}_{\mathfrak{q}}^f$ acting on $V_{\mathfrak{p}}(A)$ lies in $S_f(\mathfrak{q})$, where $\mathfrak{p}$ is a prime of F above p.*

Then the representation $\rho_{A,\mathfrak{p}}$ is irreducible.

Remark 2.4. Let $L/K_{\mathfrak{q}}$ be an extension with residual degree f such that A over L has good reduction. Let $\mathfrak{q}'$ be the maximal ideal of L. Then $\mathrm{Frob}_{\mathfrak{q}'} = \mathrm{Frob}_{\mathfrak{q}}^f$ and hence the characteristic polynomial of $\rho_{A,\mathfrak{p}}(\mathrm{Frob}_{\mathfrak{q}}^f)$ is well defined.

Remark 2.5. In the application to the generalized Fermat equation, we will take $S_f(\mathfrak{q})$ to be the set of possible traces of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$, where $A(x,y,z)$ is a Frey abelian variety defined over K attached to a primitive solution $(x,y,z) \in \mathbb{Z}^3$ of $x^p + y^p = z^r$, $A(x,y,z)$ satisfies (i)-(iv), and we impose a collection of q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ so that $A(x,y,z)$ satifies (v).

To make this more concrete, let us suppose, for simplicity, there is a fixed finite extension $L/K_{\mathfrak{q}}$ with inertia degree f and ring of integers $\mathcal{O}_L$, and some q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ allow one to give a model over $\mathcal{O}_L$ for $A(x,y,z)$ with good reduction at the prime $\mathfrak{q}'$ of L above $\mathfrak{q}$ such that the reduction modulo $\mathfrak{q}'$ is the same for any $(x,y,z) \in \mathbb{Z}^3$ satisfying the q-adic conditions. In particular, the trace

of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$ is a single well-defined value for $(x,y,z) \in \mathbb{Z}^3$ satisfying these q-adic conditions.

Let $S_f(\mathfrak{q})$ be the set of traces of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $V_{\mathfrak{p}}(A(x,y,z))$ for a collection of q-adic conditions on $(x,y,z) \in \mathbb{Z}^3$ as above. Applying Theorem 2, we deduce the irreducibility of $\rho_{A(x,y,z),\mathfrak{p}}$ for $(x,y,z) \in \mathbb{Z}^3$ a primitive solution of $x^p + y^p = z^r$ satisfying the collection of q-adic conditions.

Proof of Theorem 2. Let A be an abelian variety satisfying conditions (i)-(v) in the statement. Suppose that $\rho_{A,\mathfrak{p}}$ is reducible. Let $\psi_i : G_K \to \mathbb{F}_{\mathfrak{p}}^\times$, for $i = 1, 2$, denote the two diagonal characters of $\rho_{A,\mathfrak{p}}$. Then each ψ_i is an associated mod p character of A of degree 1 in the sense of [9, p. 518]. Since A has inertial exponent c, then ψ_i^c is unramified at all primes $v \nmid p$ of K by [6, Proposition 3.5 (iv)]. Moreover, since by assumption c is even, ψ_i^c is unramified at infinity.

We note that in [9] a quantity $c = c(g)$ is used, however, the proofs of the results there are still valid as long as the A in question has inertial exponent c which is even.

We identify ψ_i with a character of the idéles using the reciprocity map of global class field theory. Let θ^S be defined as in [9, Definition 2.6] (with $L = \overline{\mathbb{Q}}$ in their notation), where $S \in \mathbb{Z}[\Gamma_K]$ and Γ_K is the set of embeddings of K into $\overline{\mathbb{Q}}$.

By [9, Lemma 5.4] and the semistability assumption (i), there exists $S_i \in \mathbb{Z}[\Gamma_K]$ such that $\psi_i(x_{\hat{p}})^c \equiv \theta^{S_i}(x)^c \pmod{\mathfrak{p}}$ for all $x \in K^\times$ relatively prime to p, where $x_{\hat{p}}$ is the prime to p-part of x regarded as an idèle of K.

We note that the invocation of [9, Lemma 5.4] requires $p \nmid \Delta_K$, where Δ_K is the absolute discriminant of K, because the proof of this lemma uses [9, Lemma 4.10]. However, the condition $p \nmid c$ is not necessary as we assume semistability at p by (i), and hence there is no need to use [9, Lemma 4.8].

Let $B_{\mathrm{char}}(K,c)$ be as given in [9, §7.2, p. 548]. For $p \nmid B_{\mathrm{char}}(K,c)$, θ^{S_i} is balanced by [9, Lemma 2.15, Lemma 5.6 and §7.2]. As K is totally real, a balanced character for K means being a power of the norm character [9, Definition 2.13]. Thus, θ^{S_i} is a non-negative power of the norm character.

From (ii) F is totally real, and from (iii) A has all of its endomorphisms defined over K. Hence [10, Lemma 4.5.1] says that we have

$$\det \rho_{A,\mathfrak{p}} = \psi_1 \psi_2 = \mathrm{cyc}_p, \tag{2.6}$$

where cyc_p denotes the mod p cyclotomic character. Thus, θ^{S_i} is either trivial or the norm character and $\theta^{S_1}\theta^{S_2}$ is the norm character. Hence, by relabelling ψ_1 and ψ_2 if necessary, we may assume ψ_1^c, is unramified at all primes of K.

Let $\iota : \mathbb{F}_{\mathfrak{p}}^\times \to \mathbb{C}^\times$ be an injective homomorphism. Then $\iota \circ \psi_1$ is unramified at a prime v of K if and only if ψ_1 is unramified at v. The group of continuous characters of G_K with values in $\mathbb{C}^\times$ which are unramified at all primes of K are dual to the class group of K. Hence, we have that $(\iota \circ \psi_1^c)^{h'_K} = 1$ where h'_K is the exponent of the class group of K. Thus, $\psi_1^{ch'_K} = 1$. By (v), (vi), and Remark 2.4, we obtain that

$$p \mid \prod_{a \in S_f(\mathfrak{q})} \mathrm{Res}(X^{ch'_K} - 1, X^2 - aX + N(\mathfrak{q})^f),$$

where Res denotes the resultant. Since the polynomials in the resultant have no common roots (because the absolute value of the roots of $X^2 - aX + N(\mathfrak{q})^f$ is different from 1) we conclude that the resultant is non-zero. Therefore, letting c_1

denote a constant larger than any prime dividing $B_{\mathrm{char}}(K, c)$, Δ_K, and the above resultant, gives the desired bound. □

Corollary 1. *Let K be a totally real field, $\mathfrak{q}$ a prime of K and g a positive integer. There is a constant $C(K, g, \mathfrak{q})$ such that the following holds: Suppose $p > C(K, g, \mathfrak{q})$ is a prime. Then for all g-dimensional abelian varieties A/K with potentially good reduction at $\mathfrak{q}$ satisfying conditions (i)-(iii) in Theorem 2 the representation $\rho_{A,\mathfrak{p}}$ is irreducible.*

Proof. Since A achieves semistable reduction over $K(A[12])$ by [6, Proposition 4.7], and the degree of the Galois extension $K(A[12])/K$ is bounded in terms of g, this bounds the possible residual degrees of A at $\mathfrak{q}$ and inertial exponents of A in terms of g.

Let $c_{K,g}$ be the product of all the possible inertial exponents from the above paragraph.

If A has residual degree f at the prime $\mathfrak{q}$ of K, then the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_{\mathfrak{p}}(A)$ divides the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_p(A)$. If the dimension of A is fixed, then by [9, Lemma 7.6] there are only finitely many possibilities for the latter. Hence, for each possible f from the first paragraph, take $S_f(\mathfrak{q})$ to be the set of traces of the finitely many possibilities for the characteristic polynomial of $\mathrm{Frob}_{\mathfrak{q}}^f$ on $T_{\mathfrak{p}}(A)$.

For each f apply Theorem 2 with $S_f(\mathfrak{q})$ and $c = c_{K,g}$ to get a bound $c_f = c(K, c_{K,g}, f, S_f(\mathfrak{q}))$. The corollary follows by letting $C(K, g, \mathfrak{q})$ be the maximum of the c_f. □

Remark 2.7. There is an alternate method to deduce irreducibility which follows more directly from [9, Corollary 5.19]. We instead picked the proof above for two reasons. On the one hand, it is more natural as an extension of the proofs known for the case of elliptic curves and, on the other hand, since it uses properties that are normally satisfied by Frey abelian varieties, it should be better suited to giving simpler bounds in concrete Diophantine applications.

3. Application to $x^p + y^p = z^r$

In this section we use the irreducibility criterion from the previous section to establish an unconditional Diophantine statement as an application of Darmon's program [2] which requires Frey abelian varieties of dimension ≥ 2.

For an odd prime r, let ζ_r be a primitive r-th root of unity and denote by K the maximal totally real subfield of $\mathbb{Q}(\zeta_r)$. Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution of (1.2). Put $t = a^p/c^r$ and consider the abelian variety $J_r^+(t)$ defined in Section 1.3 of [2]. According to Eq. (5) in loc. cit., one has

$$\mathrm{End}_{\overline{K}}(J_r^+(t)) = \mathcal{O}_K.$$

In particular, $J_r^+(t)$ becomes of GL_2-type over K with real multiplication by K (see also [12]). Let $J_r^+(a, b, c)$ be the $\mathbb{Q}$-model of $J_r^+(a^p/c^r)$ defined in [2, p.425].

The following two results follow from (the proof of) Proposition 1.15, Theorem 3.22 and Definition 3.6 of [2].

Lemma 1. *Let $(a, b, c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to $x^p + y^p = z^r$. Suppose $r \mid ab$. Then the abelian variety $J_r^+(a, b, c)/K$ is semistable. Moreover, if $2 \nmid ab$ it has good reduction at all primes $\mathfrak{q}$ above 2 and its reduction mod $\mathfrak{q}$ is well defined on the congruence class of $(a, b, c) \pmod 2$.*

Theorem 3. *Let r be a regular prime. Then there exists a constant $c_2(r)$ such that, for all $p > c_2(r)$, and non-trivial primitive solutions $(a,b,c) \in \mathbb{Z}^3$ to (1.2) with $r \mid ab$, the* mod $\mathfrak{p}$ *representation $\rho^+_{r,\mathfrak{p}}$ associated to $J^+_r(a,b,c)$ is reducible.*

As a consequence of these results and our irreducibility criterion in Theorem 2 we can now prove our main Diophantine application.

Proof of Theorem 1. Let $(a,b,c) \in \mathbb{Z}^3$ be a non-trivial primitive solution to $x^p + y^p = z^r$ satisfying $r \mid ab$ and $2 \nmid ab$. Write $J = J^+_r(a,b,c)/K$. From Lemma 1, we have that J is semistable with good reduction at all $\mathfrak{q} \mid 2$ and where the reduction mod $\mathfrak{q}$ is well defined on the congruence class of $(a,b,c) \pmod 2$. In particular, for J we have even inertial exponent $c = 2$ and residual degree $f = 1$ at all $\mathfrak{q} \mid 2$. Recalling Remark 2.5 with the 2-adic condition $2 \nmid ab$, we take $S_f(\mathfrak{q})$ to be the singleton set consisting of the trace of $\mathrm{Frob}_{\mathfrak{q}}$ acting on the $\mathfrak{p}$-torsion of $J^+_r(1,-1,0)$.

From Theorem 2 we obtain a constant $c_1(r)$ such that if $p > c_1(r)$ and $\mathfrak{p} \mid p$ in K, then the mod $\mathfrak{p}$ representation $\rho^+_{r,\mathfrak{p}}$ is irreducible.

From Theorem 3 we obtain a constant $c_2(r)$ such that if $p > c_2(r)$ and $\mathfrak{p} \mid p$ in K, then $\rho^+_{r,\mathfrak{p}}$ is reducible.

Letting $C(r)$ be the maximum of $c_1(r)$ and $c_2(r)$, we obtain a contradiction for all exponents $p > C(r)$. □

Acknowledgment

The third author would like to thank Eknath Ghate for several useful conversations during an early phase of this project.

References

[1] Nicolas Billerey, *Critères d'irréductibilité pour les représentations des courbes elliptiques* (French, with English and French summaries), Int. J. Number Theory **7** (2011), no. 4, 1001–1032, DOI 10.1142/S1793042111004538. MR2812649

[2] Henri Darmon, *Rigid local systems, Hilbert modular forms, and Fermat's last theorem*, Duke Math. J. **102** (2000), no. 3, 413–449, DOI 10.1215/S0012-7094-00-10233-5. MR1756104

[3] Agnès David, *Caractère d'isogénie et critéres d'irréductibilité*, arXiv:1103.3892 (2012).

[4] Luis Dieulefait and Nuno Freitas, *Fermat-type equations of signature $(13,13,p)$ via Hilbert cuspforms*, Math. Ann. **357** (2013), no. 3, 987–1004, DOI 10.1007/s00208-013-0920-7. MR3118622

[5] Nuno Freitas and Samir Siksek, *Criteria for irreducibility of* mod p *representations of Frey curves* (English, with English and French summaries), J. Théor. Nombres Bordeaux **27** (2015), no. 1, 67–76. MR3346965

[6] Alexander Grothendieck, *Modèles de Néron et monodromie.*, In *Séminaire de Géométrie Algébrique* **7, Exposé 9** (1967–1969).

[7] Alain Kraus, *Courbes elliptiques semi-stables et corps quadratiques* (French, with French summary), J. Number Theory **60** (1996), no. 2, 245–253, DOI 10.1006/jnth.1996.0122. MR1412962

[8] Alain Kraus, *Courbes elliptiques semi-stables sur les corps de nombres* (French, with English summary), Int. J. Number Theory **3** (2007), no. 4, 611–633, DOI 10.1142/S1793042107001127. MR2371778

[9] Eric Larson and Dmitry Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, J. Inst. Math. Jussieu **13** (2014), no. 3, 517–559, DOI 10.1017/S1474748013000182. With an appendix by Brian Conrad. MR3211798

[10] Kenneth A. Ribet, *Galois action on division points of Abelian varieties with real multiplications*, Amer. J. Math. **98** (1976), no. 3, 751–804, DOI 10.2307/2373815. MR0457455

[11] Jean-Pierre Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques* (French), Invent. Math. **15** (1972), no. 4, 259–331, DOI 10.1007/BF01405086. MR0387283

[12] Walter Tautz, Jaap Top, and Alain Verberkmoes, *Explicit hyperelliptic curves with real multiplication and permutation polynomials*, Canad. J. Math. **43** (1991), no. 5, 1055–1064, DOI 10.4153/CJM-1991-061-x. MR1138583

Laboratoire de Mathématiques, Université Clermont Auvergne, Université Blaise Pascal, BP 10448, F-63000 Clermont-Ferrand, France – and – CNRS, UMR 6620, LM, F-63171 Aubière, France

E-mail address: Nicolas.Billerey@math.univ-bpclermont.fr

Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, Canada V5A 1S6

E-mail address: ichen@sfu.ca

Departament d'Algebra i Geometria, Universitat de Barcelona, G.V. de les Corts Catalanes 585, 08007 Barcelona, Spain

E-mail address: ldieulefait@ub.edu

Department of Mathematics, University of British Columbia, Vancouver, British Columbia, Canada V6T 1Z2

E-mail address: nunobfreitas@gmail.com

JOURNAL de Théorie des Nombres de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nicolas BILLEREY et Filippo A. E. NUCCIO MORTARINO MAJNO DI CAPRIGLIO

Représentations galoisiennes diédrales et formes à multiplication complexe

Tome 30, n° 2 (2018), p. 651-670.

<http://jtnb.cedram.org/item?id=JTNB_2018__30_2_651_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 651–670

Représentations galoisiennes diédrales et formes à multiplication complexe

par Nicolas BILLEREY et Filippo A. E. NUCCIO MORTARINO MAJNO DI CAPRIGLIO

Résumé. Pour une représentation galoisienne diédrale en caractéristique ℓ on établit (sous certaines hypothèses) l'existence d'une newform à multiplication complexe, dont on contrôle le poids, le niveau et le caractère, telle que la représentation ℓ-adique associée est congrue modulo ℓ à celle de départ.

Abstract. Given a dihedral Galois representation in characteristic ℓ, we establish (under some assumption) the existence of a CM newform, whose weight, level and Nebentypus we pin down, such that its ℓ-adic representation is congruent modulo ℓ to the one we started with.

1. Introduction

Soit $\overline{\mathbf{Q}}$ une clôture algébrique de $\mathbf{Q}$, ℓ un nombre premier et $\overline{\mathbf{F}}_\ell$ une clôture algébrique du corps $\mathbf{F}_\ell$ à ℓ éléments. Par représentation galoisienne, on entend ici une représentation irréductible et continue $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ où $\mathrm{G}_{\mathbf{Q}} = \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. On dit qu'une telle représentation galoisienne est modulaire si elle est isomorphe à la réduction d'une représentation ℓ-adique associée à une forme parabolique propre f de poids ≥ 2. Dans ce cas, on dit alors aussi que ρ provient de la forme f.

On dit qu'une représentation galoisienne ρ est diédrale si son image projective dans $\mathrm{PGL}_2(\overline{\mathbf{F}}_\ell)$, est isomorphe au groupe diédral D_n d'ordre $2n$ avec $n \geq 3$. Soit C_n l'unique sous-groupe cyclique d'ordre n de D_n. On note alors K le sous-corps quadratique de $\overline{\mathbf{Q}}$ laissé fixe par le noyau du caractère

$$\mathrm{G}_{\mathbf{Q}} \xrightarrow{\mathbf{P}\rho} D_n \longrightarrow D_n/C_n \simeq \{\pm 1\}$$

où $\mathbf{P}\rho$ est la composée de ρ avec la projection $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell) \to \mathrm{PGL}_2(\overline{\mathbf{F}}_\ell)$.

Manuscrit reçu le 5 décembre 2016, révisé le 16 mai 2017, accepté le 16 juin 2017.
Classification Mathématique (2010). 11F80, 11R37.
Mots-clefs. Représentations galoisiennes, théorie du corps de classes, formes modulaires à multiplication complexe.
N.B. remercie le projet ANR-14-CE25-0015 Gardio de l'Agence Nationale de la Recherche et la Fédération de Recherche en Mathématiques Rhône-Alpes-Auvergne (CNRS FR 3490) pour leur soutien financier.
Lors de la rédaction de ce travail, F.N. a bénéficié d'une décharge de service de l'Université Jean Monnet de Saint-Étienne, et tient à remercier les collègues qui l'ont rendue possible.

On rappelle qu'une newform $g = \sum_{n\geq 1} c_n q^n$ est dite à multiplication complexe s'il existe un caractère de Dirichlet non trivial ν tel que pour tout p dans un ensemble de nombres premiers de densité 1, on a $c_p = \nu(p)c_p$. On montre alors que le corps F correspondant au noyau de ν est quadratique imaginaire et on dit aussi que g a multiplication complexe par F.

Il est bien connu que les représentations galoisiennes attachées aux formes à multiplication complexe sont, en général, diédrales. Par ailleurs, c'est un cas particulier de la célèbre conjecture de modularité de Serre (qui était connu longtemps avant la démonstration générale de Khare–Wintenberger) qu'une représentation diédrale impaire provient d'une forme modulaire de poids ≥ 2. On trouve une preuve moderne de ce résultat dans [28], optimale par rapport au poids et au niveau, mais qui ne fournit pas de renseignement sur la nature de la forme modulaire correspondante. La construction d'une telle forme de poids ≥ 2 est aussi esquissée dans [6], en combinant l'exemple p. 517 avec les §6.9 et 6.10 ; là encore, rien ne justifie qu'elle soit à multiplication complexe.

Dans ce travail, on s'intéresse à la question plus précise de déterminer si une représentation galoisienne diédrale ρ donnée provient d'une forme modulaire *à multiplication complexe de poids* $k(\rho)$, où $k(\rho) \geq 2$ désigne le poids de Serre de la représentation ρ (défini dans [18, §2]). Dans ce cas, on souhaite également déterminer le niveau minimal de la forme correspondante.

Le résultat que l'on obtient dans cette direction est le suivant où l'on a noté $N(\rho)$ la partie première à ℓ du conducteur d'Artin de ρ (*loc. cit.*, n° 1.2) et $\varepsilon(\rho)$ le caractère associé à ρ par Serre (*loc. cit.*, n° 1.3).

Théorème 1.1. *Soit ρ une représentation galoisienne diédrale. Avec les notations précédentes, on suppose :*

(i) *K est quadratique imaginaire ;*
(ii) *$2 \leq k(\rho) \leq \ell - 1$ et $\ell \geq 5$.*

Alors, ρ est modulaire et provient d'une newform à multiplication complexe par le corps K, de poids $k(\rho)$ et de niveau

$$N' = \begin{cases} N(\rho) & \text{si } \ell \text{ est non ramifié dans } K ; \\ \ell^2 N(\rho) & \text{si } \ell \text{ est ramifié dans } K. \end{cases}$$

De plus, on a les propriétés suivantes :

(1) *si ℓ est ramifié dans K, alors $\ell \in \{2k(\rho) - 1,\ 2k(\rho) - 3\}$;*
(2) *si $\varepsilon(\rho)$ est trivial, alors la forme à multiplication complexe peut être choisie de caractère trivial et de niveau divisant N'.*

Remarques 1.2.

(1) Dans le cas $\varepsilon(\rho) = 1$ et $k(\rho) = 2$, le théorème 1.1 est démontré dans [10].

(2) Le résultat est optimal au sens suivant. D'une part, si ρ provient d'une newform (à multiplication complexe ou non), alors celle-ci est de niveau divisible par $N(\rho)$: cela résulte d'un théorème de Carayol (voir [3, théorème (A)] et [4, §1–2]). D'autre part, l'exemple 4.1 de la section 4 montre que le niveau proposé ne peut, en général, être abaissé dans le cas où ℓ est ramifié dans K.

(3) L'hypothèse que K soit imaginaire entraîne en particulier que ρ est impaire, dans le sens que le déterminant de $\rho(c)$ vaut -1 pour toute conjugaison complexe $c \in \mathrm{G}_{\mathbf{Q}}$.

Soit $A/\mathbf{Q}$ une variété abélienne simple. On note $\mathrm{End}_{\mathbf{Q}}(A)$ l'anneau de ses endomorphismes définis sur $\mathbf{Q}$. Suivant une terminologie de Ribet, on dit que A est de type GL_2 si $E = \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ est un corps de nombres de degré $\dim(A)$. Pour toute place finie λ de E au-dessus de ℓ de corps résiduel $\mathbf{F}_\lambda$, on note alors

$$\rho_{A,\lambda} : \mathrm{G}_{\mathbf{Q}} \longrightarrow \mathrm{GL}_2(\mathbf{F}_\lambda)$$

la représentation donnant l'action de $\mathrm{G}_{\mathbf{Q}}$ sur $A[\lambda]$ (voir [13, p. 7]). Le corollaire suivant au théorème 1.1 ci-dessus généralise [5, Theorem 1.6] et justifie [7, Remark 4.4] ; c'est essentiellement une conséquence de [10, Theorem 1]. Pour les définitions et propriétés des sous-groupes de Cartan, voir [16, §2] ou [9, Chapter XI, §2].

Corollaire 1.3. *Soit $A/\mathbf{Q}$ une variété abélienne de type GL_2 de conducteur N_A et λ une place finie de $E = \mathrm{End}_{\mathbf{Q}}(A) \otimes \mathbf{Q}$ au-dessus de ℓ. On suppose $\ell \geq 5$, $\ell \nmid N_A$ et l'image de $\rho_{A,\lambda}$ contenue dans le normalisateur d'un sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_\lambda)$. Alors, $\rho_{A,\lambda}$ provient d'une newform à multiplication complexe de poids 2 et de niveau $N(\rho_{A,\lambda})$ (divisant N_A) qui, de plus, est de caractère trivial lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$.*

Démonstration. D'après [13, Lemma 3.1], on a $\det(\rho_{A,\lambda}) = \epsilon\chi$, où χ désigne le caractère cyclotomique mod ℓ et ϵ est un caractère non ramifié hors de N_A et même trivial lorsque E est totalement réel et A a tous ses endomorphismes définis sur $\mathbf{Q}$ [12, Lemma 4.5.1]. Soit G_ℓ un groupe de décomposition en ℓ de $\mathrm{G}_{\mathbf{Q}}$ et I_ℓ son sous-groupe d'inertie. On sait que la semi-simplifiée de $\rho_{A,\lambda}|_{I_\ell}$ se factorise par l'inertie modérée et qu'elle est donc diagonalisable ([16, proposition 4 et s.]). On note ϕ et ϕ' les deux caractères correspondant. D'après [11, corollaire 3.4.4], on peut écrire $\phi = \psi_2^a \psi_2'^b$ et $\phi' = \psi_2^n \psi_2'^m$ où ψ_2 et ψ_2' sont les deux caractères fondamentaux de niveau 2 ([16, n° 1.7]) et où a, b, n et m sont des entiers égaux à 0 ou 1. Comme

$\phi\phi' = \chi = \psi_2\psi_2'$, il vient :

$$\{\phi, \phi'\} = \{\psi_2, \psi_2'\} \quad \text{ou} \quad \{\phi, \phi'\} = \{1, \chi\}.$$

Le premier cas donne $k(\rho_{A,\lambda}) = 2$ d'après (2.8.1) de [18, proposition 3]. En particulier, on a $\varepsilon(\rho_{A,\lambda}) = \epsilon$. Par ailleurs, l'image de $\rho_{A,\lambda}$ ne contient pas d'élément d'ordre ℓ. Dans le second cas, on a donc

$$\rho_{A,\lambda}|_{I_\ell} \simeq \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix}$$

et on conclut à $k(\rho_{A,\lambda}) = 2$ d'après (2.8.2) de *loc. cit.* Or, la représentation $\rho_{A,\lambda}$ est impaire d'après [13, Lemma 3.2]. Pour toute conjugaison complexe $c \in \mathrm{G}_{\mathbf{Q}}$, l'élément $\rho_{A,\lambda}(c)$ est donc conjugué à la matrice diagonale de valeurs propres $\{-1, +1\}$. Comme celles-ci ne sont pas conjuguées sur $\mathbf{F}_\lambda$, l'élément $\rho_{A,\lambda}(c)$ n'est contenu dans aucun sous-groupe de Cartan non déployé de $\mathrm{GL}_2(\mathbf{F}_\lambda)$ ([9, p. 181]). En particulier, la représentation $\rho_{A,\lambda}$ est diédrale et le corps quadratique K correspondant est imaginaire. Comme $\ell \geq 5$ et $k(\rho_{A,\lambda}) = 2$, on déduit du théorème 1.1 le résultat voulu. □

L'article est organisé de la façon suivante. La section 2 contient des rappels sur les Größencharaktere et un résultat (proposition 2.1) essentiel à la démonstration du théorème principal (théorème 1.1) qui, elle, occupe la section 3. La dernière section est consacrée à deux exemples numériques.

Remerciements. Les auteurs remercient Gebhard Böckle pour une question ayant mené à ce travail. N.B. est également reconnaissant envers Imin Chen, Luis Dieulefait, Pierre Lezowski et Joan Nualart pour d'intéressantes discussions.

2. Une proposition de la théorie du corps de classes

Dans cette section, on rappelle quelques notions sur les Größencharaktere puis on démontre une proposition (proposition 2.1) de la théorie du corps de classes qui nous sera utile au paragraphe 3.4. Dans toute la suite, K désigne un corps quadratique imaginaire contenu dans $\overline{\mathbf{Q}}$. On identifie $\overline{\mathbf{Q}}$ à un sous-corps de $\mathbf{C}$ et on fixe, une fois pour toutes, un plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$ où $\overline{\mathbf{Q}}_\ell$ désigne une clôture algébrique de $\mathbf{Q}_\ell$ de corps résiduel $\overline{\mathbf{F}}_\ell$. Cela induit une place de $\overline{\mathbf{Q}}$ au-dessus de ℓ notée v.

On adopte par ailleurs les notations suivantes :

- $\mathcal{O}_K$ est l'anneau des entiers de K, $\mathcal{O}_K^\times$ son groupe des unités et $-D_K$ son discriminant ;
- Σ_K est l'ensemble des places ultramétriques de K ;
- K_w est le complété de K en w $(w \in \Sigma_K)$;
- $\mathcal{O}_w^\times$, π_w, p_w sont respectivement le groupe des unités, une uniformisante et la caractéristique résiduelle du corps local K_w $(w \in \Sigma_K)$;

- $\mathcal{O}_w^{(m)}$ est l'ensemble des unités $u \in \mathcal{O}_w^\times$ congrues à 1 modulo π_w^m avec $m \geq 1$ entier $(w \in \Sigma_K)$;
- $\mathfrak{p}_w$ est l'idéal premier de $\mathcal{O}_K$ induit par w $(w \in \Sigma_K)$;
- $\mathbf{A}_K^\times$ est le groupe des idèles de K ; si $a \in \mathbf{A}_K^\times$ et $w \in \Sigma_K$, on note a_w la composante de a en w ;
- $C_K = \mathbf{A}_K^\times / K^\times$ est le groupe des classes d'idèles de K ;
- $\mathbf{A}_{K,\mathrm{f}}^\times$ (resp. $\mathbf{A}_{K,\infty}^\times$) est l'ensemble des idèles finis (resp. infinis) de K.
- Étant donnés une place $w \in \Sigma_K$ et un idéal fractionnaire $\mathfrak{m}$ de K, on note $\mathrm{ord}_w(\mathfrak{m})$ la valuation de $\mathfrak{m}$ en l'idéal premier $\mathfrak{p}_w$. On définit
$$U_\mathfrak{m} = \left\{ a \in \mathbf{A}_K^\times \,\middle|\, w(a_w - 1) \geq \mathrm{ord}_w(\mathfrak{m}),\ \forall\, w \in \Sigma_K \right\}$$
et $E_\mathfrak{m} = U_\mathfrak{m} \cap \mathcal{O}_K^\times$.
- Enfin, si $\mathfrak{p}$ est un idéal premier de $\mathcal{O}_K$, on note $\pi_\mathfrak{p}$ une uniformisante locale en la place de K induite par $\mathfrak{p}$.

2.1. Par Größencharakter χ de K on entend ici un homomorphisme de groupes continu
$$\chi : \mathbf{A}_K^\times \longrightarrow \mathbf{C}^\times$$
tel que $\chi(K^\times) = 1$. Si $w \in \Sigma_K$, on note χ_w la composante en w de χ et on désigne par χ_f (resp. χ_∞) la partie finie (resp. infinie) de χ. On dit que χ est ramifié en $w \in \Sigma_K$ s'il existe une unité $u \in \mathcal{O}_w^\times$ telle que $\chi_w(u) \neq 1$. Dans le cas contraire, on dit que χ est non ramifié en w. Par continuité, χ est non ramifié en toutes les places de K sauf un nombre fini. Si χ est ramifié en $w \in \Sigma_K$, il existe un entier $m_w \geq 1$ minimal tel que $\chi_w(\mathcal{O}_w^{(m_w)}) = 1$. Le conducteur de χ est alors, par définition, l'idéal de $\mathcal{O}_K$
$$\mathfrak{f}_\chi = \prod_w \mathfrak{p}_w^{m_w}$$
où $w \in \Sigma_K$ parcourt l'ensemble des places où χ est ramifié.

On dit enfin qu'un Größencharakter χ est de type à l'infini (m, n) avec $m, n \in \mathbf{Z}$ lorsque
$$\chi_\infty(z) = \frac{1}{z^m (z^c)^n}, \quad \text{pour tout } z \in \mathbf{A}_{K,\infty}^\times \simeq \mathbf{C}^\times,$$
où z^c désigne le conjugué complexe de z. Un tel Größencharakter est de type (A_0) dans la terminologie de Weil ([27, p. 4]).

2.2. On note $z \mapsto \overline{z}$ l'homomorphisme de réduction $\overline{\mathbf{Z}}_\ell \to \overline{\mathbf{F}}_\ell$ où $\overline{\mathbf{Z}}_\ell$ désigne l'anneau des entiers de $\overline{\mathbf{Q}}_\ell$.

Soit $\overline{\mathbf{Z}}$ l'anneau des entiers de $\overline{\mathbf{Q}}$. Il existe alors ([26, Chapter 2]) un unique homomorphisme de groupes $\overline{\mathbf{F}}_\ell^\times \to \overline{\mathbf{Z}}^\times$ noté $x \mapsto \widetilde{x}$ à valeurs dans les racines de l'unité d'ordre premier à ℓ tel que
$$x = \overline{\widetilde{x}}, \quad \text{pour tout } x \in \overline{\mathbf{F}}_\ell^\times.$$

Par ailleurs, si ζ est une racine de l'unité d'ordre premier à ℓ, on a $\zeta = \widetilde{\overline{\zeta}}$.

Étant donné un groupe G et un caractère $\varphi : G \to \overline{\mathbf{F}}_\ell^\times$, on définit le relèvement de Teichmüller (ou multiplicatif)

$$\widetilde{\varphi} : G \longrightarrow \overline{\mathbf{Q}}^\times$$

de φ comme le composé de φ avec le morphisme $x \mapsto \widetilde{x}$ ci-dessus. C'est le seul caractère à valeurs dans les racines de l'unité d'ordre premier à ℓ de $\overline{\mathbf{Q}}$ vérifiant

$$\overline{\widetilde{\varphi}(x)} = \varphi(x), \quad \text{pour tout } x \in G.$$

2.3. Étant donné un Größencharakter χ de K de type à l'infini (m, n) avec $m, n \geq 0$, on vérifie que pour toute place $w \in \Sigma_K$, on a $\chi(\pi_w) \in \overline{\mathbf{Z}}$, où l'on note encore $\pi_w \in \mathbf{A}_{K,\mathrm{f}}^\times$ l'idèle ayant composantes triviales en dehors de w et qui coïncide avec l'uniformisante π_w choisie en w. En effet, si h désigne le nombre de classes de K, l'idéal $\mathfrak{p}_w^h$ est principal et engendré par, disons, $a \in \mathcal{O}_K$. Soit x l'idèle $\pi_w^h a^{-1}$. Alors x est une unité en toute place finie de K et on a

$$\chi(\pi_w)^h = \chi\left(\pi_w^h\right)\chi\left(a^{-1}\right) = \chi(x) = \chi_{\mathrm{f}}(x)a^m(a^c)^n \in \overline{\mathbf{Z}}.$$

La proposition suivante est le résultat principal de cette section ; elle généralise notamment [5, Proposition 3.1].

Proposition 2.1. *Supposons $\ell \geq 5$. Soit α un Größencharakter de K d'image finie et de conducteur $\mathfrak{f}_\alpha$, et soit k un entier ≥ 2. Alors, il existe un Größencharakter δ de K de type à l'infini $(k-1, 0)$ et conducteur $\mathfrak{f}_\delta$ vérifiant*

$$\mathrm{ord}_w(\mathfrak{f}_\delta) = \mathrm{ord}_w(\mathfrak{f}_\alpha) \quad \textit{pour toute place } w \in \Sigma_K \setminus \{v\} \tag{2.1}$$

et tel quel pour toute place $w \in \Sigma_K \setminus \{v\}$ première à $\mathfrak{f}_\alpha$, on a

$$\overline{\delta(\pi_w)} = \overline{\alpha(\pi_w)}. \tag{2.2}$$

De plus, on a

(1) *si* $\mathrm{ord}_v(\mathfrak{f}_\alpha) \geq 2$, *alors* $\mathrm{ord}_v(\mathfrak{f}_\delta) = \mathrm{ord}_v(\mathfrak{f}_\alpha)$;
(2) *si* $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$, *alors*

$$\mathrm{ord}_v(\mathfrak{f}_\delta) = \begin{cases} 0 & \textit{si pour toute unité } u \in \mathcal{O}_v^\times \textit{ on a } \alpha_v(u) = \widetilde{\overline{u}}^{1-k} \\ 1 & \textit{sinon ;} \end{cases}$$

(3) *si* $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 0$, *alors*

$$\mathrm{ord}_v(\mathfrak{f}_\delta) = \begin{cases} 0 & \textit{si } \ell^f - 1 \mid k-1 \\ 1 & \textit{sinon,} \end{cases}$$

où f est le degré résiduel de K en ℓ.

Démonstration. Comme on a supposé K quadratique imaginaire et $\ell \geq 5$, on a, avec les notations précédentes, $E_{\mathfrak{p}_v} = U_{\mathfrak{p}_v} \cap \mathcal{O}_K^\times = \{1\}$. D'après [16, p. 286], il existe alors $f \in \mathrm{Hom}(\mathbf{A}_K^\times, \mathbf{C}^\times)$ tel que

(I) $f(x) = 1$ pour tout $x \in U_{\mathfrak{p}_v}$,
(II) $f(x) = x^{k-1}$ pour tout $x \in K^\times$.

Posons alors

$$\beta(x) = f(x)x_\infty^{1-k}, \quad \text{pour tout } x \in \mathbf{A}_K^\times,$$

où $x_\infty \in \mathbf{A}_{K,\infty}^\times$ désigne la composante à l'infini de l'idèle x. Comme $U_{\mathfrak{p}_v}$ est ouvert dans $\mathbf{A}_K^\times$ et contenu dans le noyau de f, il s'en suit que f, puis l'homomorphisme β, sont continus. Par ailleurs, si $x \in K^\times$, on a d'après la propriété (II) ci-dessus

$$\beta(x) = f(x)x^{1-k} = 1.$$

Autrement dit, β est un Größencharakter de K. De plus, si $w \in \Sigma_K$ et $x \in \mathcal{O}_w^\times \cap U_{\mathfrak{p}_v}$, on a $\beta_w(x) = 1$. En particulier, β est de conducteur divisant $\mathfrak{p}_v$. Enfin, si $x \in \mathbf{A}_{K,\infty}^\times$, on a $x \in U_{\mathfrak{p}_v}$, puis $\beta_\infty(x) = x^{1-k}$. Le Größencharakter β est donc de type à l'infini $(k-1, 0)$.

Comme l'a montré Weil dans [27, p. 5], il existe une extension finie L de $\mathbf{Q}$, qu'on regarde plongée dans $\overline{\mathbf{Q}}$, qui contient les valeurs de β_w pour toute place w. Quitte à l'élargir, on peut de plus supposer qu'elle contient K. On note L_v le complété de L en la place de L induite par la place v de $\overline{\mathbf{Q}}$ et on commence par définir un caractère $\gamma_0 : \mathbf{A}_K^\times \to L_v^\times$ par la règle

$$\begin{cases} (\gamma_0)_w = \beta_w^{-1} & (w \in \Sigma_K \setminus \{v\}) \\ (\gamma_0)_v = \beta_v^{-1} \cdot (-)^{k-1} & \\ (\gamma_0)_\infty = 1 & \end{cases}$$

où $(-)^{k-1}$ désigne l'élévation à la puissance $k-1$. En tant que produit de caractères continus, γ_0 est continu. Soit $a \in K^\times$. On a alors

$$\begin{aligned} \gamma_0(a) &= \left(\prod_{w \in \Sigma_K \setminus \{v\}} \beta_w(a)^{-1} \right) \cdot \beta_v(a)^{-1} \cdot a^{k-1} \\ &= \beta_{\mathrm{f}}(a)^{-1} \cdot a^{k-1} = \beta_\infty(a) \cdot a^{k-1} = 1 \end{aligned}$$

car β est trivial sur les idèles principaux et de type à l'infini $(k-1, 0)$. Il s'en suit que l'on peut regarder γ_0 en tant que caractère continu de C_K et aussi du quotient $C_K/\mathbf{A}_{K,\infty}^\times$. Comme K est totalement imaginaire, l'isomorphisme de réciprocité de la théorie du corps de classes globale identifie ce quotient avec l'abélianisé $\mathrm{G}_K^{\mathrm{ab}}$ de G_K, et montre en particulier qu'il s'agit d'un groupe compact. L'image de l'homomorphisme continu γ_0 est

donc contenue dans le groupe $\mathcal{O}_{L_v}^\times$ des unités de L_v. On note

$$\overline{\gamma_0} : \mathbf{A}_K^\times \longrightarrow \overline{\mathbf{F}}_\ell^\times$$

la composée de γ_0 avec l'homomorphisme de réduction $\overline{\mathbf{Z}}_\ell \to \overline{\mathbf{F}}_\ell$. C'est un caractère d'image finie. On définit alors

$$\gamma = \widetilde{\overline{\gamma_0}} : \mathbf{A}_K^\times \longrightarrow \overline{\mathbf{Z}}^\times \subset \mathbf{C}^\times$$

comme étant le relèvement de Teichmüller de $\overline{\gamma_0}$ détaillé au paragraphe 2.2. Il s'agit donc d'un Größencharakter de type à l'infini $(0,0)$, type dit « trivial ».

Pour compléter la preuve de la proposition, posons $\delta = \alpha\beta\gamma$: il s'agit bien d'un Größencharakter de type à l'infini égal au type à l'infini de β, à savoir $(k-1,0)$, puisque tant α que γ ont un type à l'infini trivial. Il reste à présent à déterminer $\mathfrak{f}_\delta$ et à démontrer les congruences (2.2).

Montrons tout d'abord les congruences (2.2). Soit $w \in \Sigma_K \setminus \{v\}$ une place ultramétrique de K en laquelle α est non ramifié. D'après ce qui précède, on a $\gamma_0(\pi_w) = \beta(\pi_w)^{-1} \in \overline{\mathbf{Z}}_\ell^\times$ et, par ailleurs, $\alpha(\pi_w) \in \overline{\mathbf{Z}}_\ell$. Par réduction, il vient donc

$$\overline{\delta(\pi_w)} = \overline{\alpha(\pi_w)}\,\overline{\beta(\pi_w)}\,\overline{\beta(\pi_w)^{-1}} = \overline{\alpha(\pi_w)}$$

et le résultat souhaité.

Étudions à présent le conducteur $\mathfrak{f}_\delta$. Soit w une place finie de K distincte de v et $u \in \mathcal{O}_w^\times$. Comme β est non ramifié en w, on a $\beta_w(u) = 1 = \gamma_w(u)$ et donc $\delta_w(u) = \alpha_w(u)$, ce qui entraîne (2.1).

Passons maintenant à la démonstration des points (1)–(3). Soit $u \in \mathcal{O}_v^\times$. Comme $\mathfrak{f}_\beta \mid \mathfrak{p}_v$, le caractère β_v est trivial sur $\mathcal{O}_v^{(1)}$ et $\beta_v(u)$ est une racine de l'unité d'ordre premier à ℓ. On a donc $\gamma_v(u) = \beta_v(u)^{-1}\widetilde{\overline{u}}^{k-1}$, puis

$$\delta_v(u) = \alpha_v(u)\widetilde{\overline{u}}^{k-1}. \tag{2.3}$$

En particulier, on a $\delta_v(u) = \alpha_v(u)$, pour toute unité $u \in \mathcal{O}_v^{(1)}$.

(1) Supposons $\mathrm{ord}_v(\mathfrak{f}_\alpha) \geq 2$. Alors, il existe une unité $u \in \mathcal{O}_v^{(1)}$ telle que $\delta_v(u) = \alpha_v(u) \neq 1$. D'où $\mathrm{ord}_v(\mathfrak{f}_\delta) \geq 2$ et $\mathrm{ord}_v(\mathfrak{f}_\delta) = \mathrm{ord}_v(\mathfrak{f}_\alpha)$ car les restrictions de δ_v et α_v à $\mathcal{O}_v^{(1)}$ coïncident.

(2) Supposons $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$. Pour toute unité $u \in \mathcal{O}_v^{(1)}$, on a alors $\delta_v(u) = 1$, d'où $\mathrm{ord}_v(\mathfrak{f}_\delta) \leq 1$. Par ailleurs, d'après (2.3), on a $\mathrm{ord}_v(\mathfrak{f}_\delta) = 1$ si, et seulement si, il existe une unité $u \in \mathcal{O}_v^\times$ telle que $\alpha_v(u) \neq \widetilde{\overline{u}}^{1-k}$.

(3) Supposons $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 0$. Alors pour toute unité $u \in \mathcal{O}_v^\times$, on a $\delta_v(u) = \widetilde{\overline{u}}^{k-1}$ et donc le caractère δ_v est trivial sur $\mathcal{O}_v^{(1)}$, c'est-à-dire $\mathrm{ord}_v(\mathfrak{f}_\delta) \leq 1$. Par ailleurs, le quotient $\mathcal{O}_v^\times/\mathcal{O}_v^{(1)}$ s'identifie

à $(\mathcal{O}_K/\mathfrak{p}_v)^\times$. En particulier, on a $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$ si, et seulement si, $\ell^f - 1$ divise $k-1$.

Cela termine la démonstration de la proposition 2.1. □

3. Démonstration du théorème principal

3.1. Étude locale. On commence par rappeler la définition centrale suivante.

Définition 3.1. Une représentation irréductible continue $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ est dite diédrale si son image projective dans $\mathrm{PGL}_2(\overline{\mathbf{F}}_\ell)$, est isomorphe au groupe diédral D_n d'ordre $2n$ avec $n \geq 3$.

Soit $\rho : \mathrm{G}_{\mathbf{Q}} \to \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ une représentation galoisienne satisfaisant aux hypothèses du théorème 1.1. On vérifie à l'aide de la classification des sous-groupes finis de $\mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ (voir par exemple [2, Theorem 3.4]) que l'ordre de l'image de ρ est nécessairement premier à ℓ. Avec les notations de l'Introduction, on a donc en particulier $\mathrm{pgcd}(n, \ell) = 1$. Par construction, $\mathbf{P}\rho(\mathrm{G}_K) = C_n$ est cyclique, avec $\mathrm{G}_K = \mathrm{Gal}(\overline{\mathbf{Q}}/K)$. Comme $\mathbf{P}\rho(\mathrm{G}_K)$ s'obtient à partir de $\rho(\mathrm{G}_K)$ après passage au quotient par des éléments de son centre, on en déduit que $\rho(\mathrm{G}_K)$ est abélienne. Ainsi, il existe deux caractères

$$\varphi, \varphi' : \mathrm{G}_K \longrightarrow \overline{\mathbf{F}}_\ell^\times$$

tels que $\varphi \neq \varphi'$ et $\rho|_{\mathrm{G}_K} \simeq \varphi \oplus \varphi'$. Soit $\sigma \in \mathrm{G}_{\mathbf{Q}} \setminus \mathrm{G}_K$. On définit $\widehat{\varphi} : \mathrm{G}_K \to \overline{\mathbf{F}}_\ell^\times$ par $\widehat{\varphi}(\tau) = \varphi(\sigma^{-1}\tau\sigma)$ pour tout $\tau \in \mathrm{G}_K$: cette définition est indépendante de σ car l'image de φ est abélienne. Soit v un vecteur propre pour $\rho|_{\mathrm{G}_K}$ de valeur propre $\varphi(\tau)$ pour tout $\tau \in \mathrm{G}_K$. On a alors, pour tout $\tau \in \mathrm{G}_K$,

$$\rho(\tau)\rho(\sigma)v = \rho(\sigma\sigma^{-1}\tau\sigma)v = \rho(\sigma)\rho(\sigma^{-1}\tau\sigma)v = \widehat{\varphi}(\tau)\rho(\sigma)v$$

d'où l'on déduit $\varphi' = \widehat{\varphi}$. On a donc $\rho \simeq \mathrm{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbf{Q}}}(\varphi) \simeq \mathrm{Ind}_{\mathrm{G}_K}^{\mathrm{G}_{\mathbf{Q}}}(\widehat{\varphi})$. Dans la base $\{v, \rho(\sigma)v\}$, la matrice de $\rho(\sigma)$ s'écrit

$$\begin{pmatrix} 0 & \varphi(\sigma^2) \\ 1 & 0 \end{pmatrix}. \tag{3.1}$$

L'objectif de ce paragraphe est d'étudier la ramification de φ et de K en ℓ. Soit G_ℓ le groupe de décomposition de $\mathrm{G}_{\mathbf{Q}}$ relatif au plongement fixé $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$ et I_ℓ son sous-groupe d'inertie. On note pour simplifier $k = k(\rho)$, avec $k(\rho)$ comme dans [18, §2]. On rappelle que l'on a supposé $2 \leq k \leq \ell - 1$ et $\ell \geq 5$.

L'image de ρ est d'ordre premier à ℓ. En particulier, $\rho|_{I_\ell}$ se factorise par l'inertie modérée et est diagonalisable ([16, proposition 4 et s.]). On note ϕ et ϕ' les deux caractères correspondants. Ils sont de niveau 1 ou 2 et lorsqu'ils sont de niveau 2, on a $\phi' = \phi^\ell$ ([18, proposition 1]). On rappelle

que $\mathfrak{p}_v$ désigne l'idéal premier de K au-dessus de ℓ induit par la place v (c'est-à-dire par le plongement $\overline{\mathbf{Q}} \hookrightarrow \overline{\mathbf{Q}}_\ell$). On considère alors les groupes de décomposition $\mathrm{G}_{\mathfrak{p}_v} \leq \mathrm{G}_\ell$ et d'inertie $I_{\mathfrak{p}_v} \leq I_\ell$.

(1) On suppose que ϕ et ϕ' sont de niveau 1. Comme l'image de ρ ne contient pas d'élément d'ordre ℓ, l'image par ρ de l'inertie sauvage est triviale. Comme on a supposé $2 \leq k \leq \ell - 1$, on a, d'après [18, (2.3.2)],

$$\rho|_{I_\ell} = \begin{pmatrix} 1 & 0 \\ 0 & \chi^{k-1} \end{pmatrix}$$

où χ désigne le caractère cyclotomique mod ℓ.

(a) Supposons ℓ non ramifié dans K. Alors, $I_{\mathfrak{p}_v}$ s'identifie à I_ℓ et, comme $\ell > k$, le caractère χ^{k-1} est non trivial. On en déduit que soit φ est non ramifié en $\sigma(\mathfrak{p}_v)$ et que sa restriction au sous-groupe d'inertie en $\mathfrak{p}_v$ est donnée par la puissance $(k-1)$-ième du caractère cyclotomique, ou qu'il en est ainsi pour φ'. Si $\sigma(\mathfrak{p}_v) = \mathfrak{p}_v$, c'est une contradiction dans les deux cas. On a donc montré que ℓ est décomposé dans K. Par ailleurs, quitte à remplacer v par σv, on peut supposer φ non ramifié en $\sigma(\mathfrak{p}_v)$ et modérément ramifié en $\mathfrak{p}_v$ avec, pour tout $\tau \in I_{\mathfrak{p}_v}$, $\varphi(\tau) = \chi^{k-1}(\tau)$.

(b) Supposons ℓ ramifié dans K. Alors, d'après la définition (donnée en Introduction) du corps K, on a $\mathbf{P}\rho(I_\ell) \not\subset C_n$. Or, l'image du caractère χ^{k-1} est d'ordre $(\ell-1)/\operatorname{pgcd}(\ell-1, k-1)$ et, en vue de la description de $\rho|_{I_\ell}$, elle coïncide avec l'image de $\mathbf{P}\rho(I_\ell)$, qui est donc cyclique et par suite d'ordre 2. On en tire $\ell - 1 = 2 \cdot \operatorname{pgcd}(\ell-1, k-1)$, d'où $\ell = 2k-1$ car $\ell > k$. En outre, le fait que $\mathbf{P}\rho(I_\ell)$ soit d'ordre 2 montre que l'indice de ramification de ℓ dans l'extension $\overline{\mathbf{Q}}^{\mathrm{Ker}(\mathbf{P}\rho)}/\mathbf{Q}$ est égal à 2 et par suite $\mathbf{P}\rho(I_{\mathfrak{p}_v}) = 1$. Il vient donc que φ est non ramifié en $\mathfrak{p}_v$.

(2) On suppose que ϕ et ϕ' sont de niveau 2. Alors, d'après [18, n° 2.2], $\rho|_{I_\ell}$ est irréductible. En particulier, cela exclut d'avoir $\mathrm{G}_\ell \subset \mathrm{G}_K$, i.e. ℓ décomposé dans K. Autrement dit, ℓ est inerte ou ramifié dans K et comme on a supposé $2 \leq k \leq \ell - 1$, on a d'après [18, (2.2.4)]

$$\rho|_{I_\ell} = \begin{pmatrix} \psi_2^{k-1} & 0 \\ 0 & \psi_2^{\ell(k-1)} \end{pmatrix},$$

où ψ_2 est un caractère fondamental de niveau 2 (pour sa définition, voir [16, n° 1.7]). On trouve que le caractère ψ_2^{k-1} est d'ordre

$$\frac{\ell^2 - 1}{\operatorname{pgcd}(\ell^2 - 1, k-1)} > 2$$

et n'est donc trivial sur aucun sous-groupe de I_ℓ d'indice ≤ 2. Par conséquent, tant φ que φ' sont ramifiés en $\mathfrak{p}_v$ et, quitte à remplacer φ avec φ', on a que $\varphi(\tau) = \psi_2^{k-1}(\tau)$ pour tout $\tau \in I_{\mathfrak{p}_v}$.

Supposons enfin ℓ ramifié dans K. Comme précédemment, l'image projective $\mathbf{P}\rho(I_\ell)$ n'est pas contenue dans C_n. Or, $\mathbf{P}\rho(I_\ell)$ est cyclique et s'identifie à l'image de $\psi_2^{(\ell-1)(k-1)}$. On en déduit que $\mathbf{P}\rho(I_\ell)$ est d'ordre 2, puis que $2 \cdot \operatorname{pgcd}(\ell^2-1, (\ell-1)(k-1)) = \ell^2 - 1$, et finalement $\ell = 2k-3$.

On résume les résultats ci-dessus dans la proposition suivante.

Proposition 3.2. *Avec les hypothèses et notations de ce paragraphe, on peut supposer que l'on est dans l'une des situations suivantes.*

(1) *Supposons ϕ et ϕ' de niveau 1. Alors,*
   (a) *soit ℓ est décomposé dans K et dans ce cas φ est non ramifié en $\sigma(\mathfrak{p}_v)$, modérément ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \chi^{k-1}(\tau)$, où χ désigne le caractère cyclotomique mod ℓ.*
   (b) *soit ℓ est ramifié dans K et dans ce cas on a $\ell = 2k-1$ et φ est non ramifié en $\mathfrak{p}_v$.*

(2) *Supposons ϕ et ϕ' de niveau 2. Alors,*
   (a) *soit ℓ est inerte dans K ;*
   (b) *soit ℓ est ramifié dans K et $\ell = 2k-3$.*

   Dans les deux cas, φ est ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \psi_2^{k-1}(\tau)$, avec ψ_2 caractère fondamental de niveau 2.

3.2. On étudie ici la variation du conducteur d'Artin par rapport à l'opération d'induction. On rappelle que l'on a $\rho = \operatorname{Ind}_{G_K}^{G_\mathbf{Q}}(\varphi)$. On désigne par $\mathfrak{N}(\rho)$ (resp. $\mathfrak{N}(\varphi)$) le conducteur d'Artin de ρ (resp. de φ) défini dans [14, chapitre VI, §3]. Ce sont, par définition, des idéaux de $\mathbf{Z}$ et de $\mathcal{O}_K$, respectivement. On rappelle que, suivant la notation de Serre [18, n° 1.2], $N(\rho)$ désigne le générateur positif de la partie première à ℓ de $\mathfrak{N}(\rho)$.

Pour un entier naturel n, on note $n^{(\ell)}$ sa partie première à ℓ. Le résultat suivant résulte de [23, Corollary 1].

Lemme 3.3 (Taguchi)**.** *Avec les notations et hypothèses précédentes, on a*

$$N(\rho) = D_K^{(\ell)} \operatorname{Norm}_{K/\mathbf{Q}}(\mathfrak{N}(\varphi))^{(\ell)}.$$

Remarque 3.4. Dans [23] aucune preuve du Corollary 1 n'est offerte et l'auteur fait référence à [14, Chapter VI, §3], où le procédé de « globalisation » est traité dans le cas de représentations à coefficients complexes, et cela en utilisant la théorie des caractères. Il est bien connu (voir, par exemple, [17, §15.5]) que cette théorie s'étend aux représentations en caractéristique ℓ d'un groupe d'ordre premier à ℓ, ce qui est le contexte dans lequel nous travaillons à présent. Les arguments de [14, chapitre VI, §3] s'adaptent alors pour prouver la validité du résultat cité de Taguchi.

3.3. Dans ce paragraphe, on fixe une extension finie $L/\mathbf{Q}_\ell$. On note k_L son corps résiduel de sorte que l'on a $k_L = \mathbf{F}_q$ où $q = |k_L|$ désigne le cardinal de k_L. On note L^{ab} (resp. L^{nr}) l'extension abélienne (resp. non ramifiée) maximale de L contenue dans $\overline{\mathbf{Q}}_\ell$. Le morphisme $\theta_{q-1} : \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/L^{\mathrm{nr}}) \to k_L^\times$ construit par Serre dans [16, §1.3] (et dont les conjugués sur k_L forment l'ensemble des caractères fondamentaux de niveau r de $\overline{\mathbf{Q}}_\ell/L$, où $q = \ell^r$) se factorise par le groupe $I_t(L^{\mathrm{ab}}/L)$ d'inertie modérée de l'extension L^{ab}/L et on note encore

$$\theta_{q-1} : I_t(L^{\mathrm{ab}}/L) \longrightarrow k_L^\times$$

le morphisme passé au quotient. Par ailleurs, l'application de réciprocité de la théorie du corps de classes locale fournit un homomorphisme surjectif

$$\omega : k_L^\times \longrightarrow I_t(L^{\mathrm{ab}}/L).$$

Un calcul, détaillé dans [16, proposition 3], montre alors que l'on a

$$\theta_{q-1}(\omega(x)) = x^{-1}, \tag{3.2}$$

pour tout $x \in k_L^\times$. Ce résultat nous sera utile dans la démonstration qui suit.

3.4. Démonstration du théorème principal. On reprend les notations et hypothèses du paragraphe 3.1. Soit $\widetilde{\varphi} : \mathrm{G}_K \to \overline{\mathbf{Z}}^\times \subset \mathbf{C}^\times$ le relèvement multiplicatif de φ défini au paragraphe 2.2. Il se factorise par l'abélianisé $\mathrm{G}_K^{\mathrm{ab}}$ de G_K. On note

$$\mathrm{rec}_K : \mathbf{A}_K^\times \longrightarrow \mathrm{G}_K^{\mathrm{ab}}$$

l'application de réciprocité de la théorie du corps de classes globale et on pose

$$\alpha = \widetilde{\varphi} \circ \mathrm{rec}_K : \mathbf{A}_K^\times \longrightarrow \mathbf{C}^\times.$$

C'est un Größencharakter de K d'image finie, de conducteur $\mathfrak{f}_\alpha$ égal au conducteur d'Artin de φ (voir [14, chapitre VI, notamment p. 110]). D'après le lemme 3.3 et la construction de α, on a

$$N(\rho) = D_K^{(\ell)} \,\mathrm{Norm}_{K/\mathbf{Q}}\big(\mathfrak{N}(\varphi)\big)^{(\ell)} = D_K^{(\ell)} \,\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\alpha)^{(\ell)}. \tag{3.3}$$

Soit δ le Größencharakter de K fourni par la proposition 2.1 appliquée au Größencharakter α ci-dessus et à l'entier $k = k(\rho)$. On définit un caractère, noté δ_{H}, du groupe des idéaux fractionnaires de K premiers à $\mathfrak{f}_\delta$ de la façon suivante :

$$\delta_{\mathrm{H}}(\mathfrak{p}) = \delta(\pi_\mathfrak{p}) \quad \text{pour tout premier } \mathfrak{p} \nmid \mathfrak{f}_\delta \text{ de } \mathcal{O}_K,$$

où l'on note encore $\pi_\mathfrak{p} \in \mathbf{A}_{K,\mathrm{f}}^\times$ l'idèle ayant composantes triviales en dehors de la place induite par $\mathfrak{p}$ et qui coïncide avec l'uniformisante $\pi_\mathfrak{p}$ choisie en

cette place. Soit η la fonction définie pour $m \in \mathbf{Z}$ par

$$\eta(m) = \frac{\delta_{\mathrm{H}}(m\mathcal{O}_K)}{m^{k(\rho)-1}},$$

où l'on convient que $\delta_{\mathrm{H}}(m\mathcal{O}_K) = 0$ lorsque $m\mathcal{O}_K$ et $\mathfrak{f}_\delta$ ne sont pas premiers entre eux. Une vérification rapide montre que η induit un caractère de Dirichlet modulo $M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)$ (voir le lemme 3.7 pour un résultat plus précis).

Soit enfin $\left(\frac{-D_K}{\cdot}\right)$ le symbole de Kronecker correspondant au corps K vu comme caractère de Dirichlet modulo D_K et posons $\varepsilon = \left(\frac{-D_K}{\cdot}\right)\eta$, vu comme caractère de Dirichlet modulo MD_K. Pour $z \in \mathbf{C}$, de partie imaginaire $\Im(z) > 0$, on pose alors

$$g_\delta(z) = \sum_{\substack{(\mathfrak{a},\mathfrak{f}_\delta)=1 \\ \mathfrak{a} \text{ entier}}} \delta_{\mathrm{H}}(\mathfrak{a}) q^{\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{a})} = \sum_{n\geq 1} c_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

Le résultat suivant est dû à Hecke et Shimura (voir [8, p. 717] ainsi que [20, Lemma 3] et [21, p. 138]).

Théorème 3.5 (Hecke, Shimura)**.** *La série g_δ est le développement de Fourier d'une newform de poids $k(\rho)$, niveau MD_K et caractère ε à multiplication complexe par le corps K.*

Dans la démonstration du théorème 1.1 ci-dessous, on note pour simplifier k à la place de $k(\rho)$. D'après la proposition 2.1, $\mathfrak{f}_\alpha$ et $\mathfrak{f}_\delta$ coïncident hors de v. En particulier, on a

$$N(\rho) = D_K^{(\ell)} \,\mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)^{(\ell)} = (MD_K)^{(\ell)}. \tag{3.4}$$

On calcule à présent la valuation de MD_K en ℓ afin de déterminer l'entier MD_K lui-même. On procède suivant les différents cas de la proposition 3.2 dont on reprend la terminologie et la notation.

(1) On distingue deux cas :

(a) Supposons ℓ décomposé dans K. D'après la proposition 3.2, φ est modérément ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \chi^{k-1}(\tau)$. Il suit que $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$ car il en est ainsi pour $\widetilde{\chi} \circ \mathrm{rec}_K$. Par ailleurs, le complété K_v de K en v s'identifie à $\mathbf{Q}_\ell$ et d'après [16, proposition 8] le caractère fondamental $\theta_{\ell-1}$ de niveau 1 est le caractère cyclotomique χ. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_\ell^\times$. Avec les notations des paragraphes 2.2 et 3.3, il découle de l'égalité (3.2) et de la compatibilité entre les théories du corps de classes locale et globale que l'on a

$$\alpha_v(u) = \widetilde{\varphi(\omega(x))} = \widetilde{\theta_{\ell-1}(\omega(x))}^{\,k-1} = \widetilde{x}^{1-k} = \widetilde{\overline{u}}^{1-k}.$$

D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$. D'où il vient $\mathrm{ord}_\ell(MD_K) = 0$ et $MD_K = N(\rho)$ d'après (3.4).

(b) Supposons ℓ ramifié dans K, donc $\ell \mid D_K$. D'après la proposition 3.2, φ est non ramifié en $\mathfrak{p}_v$ et $\ell = 2k-1$. On a $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 0$ et $\ell(= 2k-1) > k$. En particulier, on déduit du point 3 de la proposition 2.1 que l'on a $\mathrm{ord}_v(\mathfrak{f}_\delta) = 1$, puis $\mathrm{ord}_\ell(MD_K) = 2$ et $MD_K = \ell^2 N(\rho)$.

(2) D'après la proposition 3.2, ℓ est inerte ou ramifié dans K, φ est ramifié en $\mathfrak{p}_v$ et pour tout $\tau \in I_{\mathfrak{p}_v}$, on a $\varphi(\tau) = \psi_2^{k-1}(\tau)$, avec ψ_2 caractère fondamental de niveau 2. Par suite, φ est modérément ramifié et $\mathrm{ord}_v(\mathfrak{f}_\alpha) = 1$. Quitte à remplacer φ par φ', on peut de plus supposer que l'on a l'égalité $\varphi = \theta_{\ell^2-1}^{k-1}$ entre caractères de $I_{\mathfrak{p}_v}$.

(a) Supposons ℓ inerte dans K. Dans ce cas, l'extension $K_v/\mathbf{Q}_\ell$ est quadratique non ramifiée. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_{\ell^2}^\times$. D'après l'égalité (3.2), on a comme précédemment,

$$\alpha_v(u) = \widetilde{\varphi(\omega(x))} = \widetilde{\theta_{\ell^2-1}(\omega(x))}^{k-1} = \widetilde{x}^{1-k} = \widetilde{\overline{u}}^{1-k}.$$

D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 0$. D'où il vient $MD_K = N(\rho)$.

(b) Supposons enfin ℓ ramifié dans K. Dans ce cas, l'extension $K_v/\mathbf{Q}_\ell$ est quadratique ramifiée. Soit $u \in \mathcal{O}_v^\times$. On pose $x = \overline{u} \in \mathbf{F}_\ell^\times$. Comme le produit des caractères fondamentaux de niveau 2 est le caractère fondamental de niveau 1, on déduit comme ci-dessus des égalités $\ell = 2k-3$ et (3.2) que l'on a

$$\begin{aligned}\alpha_v(u)^2 = \widetilde{\varphi(\omega(x))}^2 = \widetilde{\theta_{\ell^2-1}^{2(k-1)}(\omega(x))} = \widetilde{\theta_{\ell^2-1}^{\ell+1}(\omega(x))} \\ = \widetilde{\theta_{\ell-1}(\omega(x))} = \widetilde{x}^{-1} = \widetilde{\overline{u}}^{-1}.\end{aligned}$$

Or, on a $\widetilde{\overline{u}}^{2(1-k)} = \widetilde{x}^{-(\ell+1)} = \widetilde{x}^{-2} = \widetilde{\overline{u}}^{-2}$, qui n'est pas égal à $\widetilde{\overline{u}}^{-1}$ dès lors que $\overline{u} \neq 1$: en particulier $\alpha_v(u) \neq \widetilde{\overline{u}}^{1-k}$ dès lors que $u \in \mathcal{O}_v^\times \setminus \mathcal{O}_v^{(1)}$. D'après le point (2) de la proposition 2.1, on a donc $\mathrm{ord}_v(\mathfrak{f}_\delta) = 1$. D'où il vient $\mathrm{ord}_\ell(MD_K) = 2$, puis $MD_K = \ell^2 N(\rho)$.

On a donc montré que l'on a

$$MD_K = \begin{cases} N(\rho) & \text{si } \ell \text{ est non ramifié dans } K\,; \\ \ell^2 N(\rho) & \text{si } \ell \text{ est ramifié dans } K. \end{cases} \tag{3.5}$$

Prouvons à présent que ρ provient bien de g_δ (par réduction modulo v) : pour ce faire, nous allons vérifier que pour tout nombre premier $q \nmid N(\rho)\ell$, le polynôme caractéristique de $\rho(\mathrm{Frob}_q)$ est la réduction (modulo v) de

$$X^2 - c_q X + \varepsilon(q) q^{k-1},$$

où Frob_q est un représentant de Frobenius en q dans $\mathrm{G}_{\mathbf{Q}}$.

Cas inerte: On suppose q inerte dans K, de sorte qu'on peut choisir $\sigma = \mathrm{Frob}_q \in \mathrm{G}_{\mathbf{Q}} \setminus \mathrm{G}_K$ au début du paragraphe 3.1. On pose $\mathfrak{q} = q\mathcal{O}_K$. On a d'une part les égalités $c_q = 0$ et $\varepsilon(q)q^{k-1} = -\delta_{\mathrm{H}}(\mathfrak{q})$. D'autre part, l'écriture (3.1) entraîne $\operatorname{tr}\rho(\mathrm{Frob}_q) = 0$ ainsi que $\det\rho(\mathrm{Frob}_q) = -\varphi(\mathrm{Frob}_q^2)$. La théorie du corps de classes locale et la proposition 2.1 donnent alors

$$\varphi\left(\mathrm{Frob}_q^2\right) = \overline{\alpha(\pi_{\mathfrak{q}})} = \overline{\delta(\pi_{\mathfrak{q}})} = \overline{\delta_{\mathrm{H}}(\mathfrak{q})}.$$

Cas décomposé: On suppose q décomposé dans K et on note $\mathfrak{q}, \mathfrak{q}'$ les idéaux premiers de $\mathcal{O}_K$ au-dessus de q. Alors $\mathrm{Frob}_q \in \mathrm{G}_K$ est une substitution de Frobenius en $\mathfrak{q}$ et en $\mathfrak{q}'$. On a, d'une part, $c_q = \delta_{\mathrm{H}}(\mathfrak{q}) + \delta_{\mathrm{H}}(\mathfrak{q}')$ et $\varepsilon(q)q^{k-1} = \delta_{\mathrm{H}}(\mathfrak{q}\mathfrak{q}')$. D'autre part, on a comme précedemment,

$$\begin{aligned}\operatorname{tr}\rho(\mathrm{Frob}_q) &= \varphi(\mathrm{Frob}_q) + \widehat{\varphi}(\mathrm{Frob}_q) = \overline{\alpha(\pi_{\mathfrak{q}})} + \overline{\alpha(\pi_{\mathfrak{q}'})} \\ &= \overline{\delta(\pi_{\mathfrak{q}})} + \overline{\delta(\pi_{\mathfrak{q}'})} = \overline{c_q}\end{aligned}$$

et

$$\begin{aligned}\det\rho(\mathrm{Frob}_q) &= \varphi(\mathrm{Frob}_q)\widehat{\varphi}(\mathrm{Frob}_q) = \overline{\alpha(\pi_{\mathfrak{q}})}\,\overline{\alpha(\pi_{\mathfrak{q}'})} \\ &= \overline{\delta(\pi_{\mathfrak{q}})}\,\overline{\delta(\pi_{\mathfrak{q}'})} = \overline{\delta_{\mathrm{H}}(\mathfrak{q}\mathfrak{q}')}.\end{aligned}$$

On en déduit le résultat voulu avec [6, lemme 3.2].

Pour terminer la démonstration du théorème 1.1, il reste à vérifier l'affirmation sur le caractère. Soit $\varepsilon(\rho)$ le caractère associé à ρ par Serre comme dans [18, n° 1.3] : par construction, il est égal à la réduction (modulo v) de ε. On fait l'hypothèse que $\varepsilon(\rho)$ est trivial, i.e. $\det\rho = \chi^{k-1}$ avec χ le caractère cyclotomique mod ℓ. On doit alors montrer qu'il existe une forme à multiplication complexe vérifiant les conditions du théorème et dont le caractère est trivial. Pour cela, on va considérer une tordue de g_δ par un caractère de Dirichlet particulier. On a la décomposition suivante de l'entier M :

$$M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta) = \prod_{\mathfrak{p}} \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)} = \prod_p p^{\sum_{\mathfrak{p}|p} f_{\mathfrak{p}/p}\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)},$$

où $f_{\mathfrak{p}/p}$ désigne le degré résiduel de l'idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$ au-dessus du premier p.

Lemme 3.6. *Lorsque* $\det\rho = \chi^{k-1}$ *la valuation* $\mathrm{ord}_p(M)$ *de* M *en tout nombre premier* p *ne divisant pas* D_K *est paire, égale à* $2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$ *où* $\mathfrak{p}$ *est un premier de* $\mathcal{O}_K$ *au-dessus de* p.

Démonstration. Soit p ne divisant pas D_K tel que $\mathrm{ord}_p(M) > 0$. Lorsque p est inerte dans K, avec $p\mathcal{O}_K = \mathfrak{p}$, le résultat est immédiat car alors $\mathrm{ord}_p(M) = 2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$. On suppose donc à présent p décomposé dans K, disons $p\mathcal{O}_K = \mathfrak{p}\bar{\mathfrak{p}}$. On note que p est nécessairement différent de ℓ car

lorsque ℓ est décomposé dans K, alors, grâce à (3.5), on a $MD_K = N(\rho)$ qui est premier à ℓ. D'après (3.3) et la proposition 2.1 on a $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}(\varphi))$, et de même pour $\bar{\mathfrak{p}}$. Soit $I_{\mathfrak{p}}$ un groupe d'inertie en $\mathfrak{p}$ dans G_K. D'après l'hypothèse $\det\rho = \chi^{k-1}$ et avec les notations du paragraphe 3.1, on a $\varphi_{|I_{\mathfrak{p}}} = \widehat{\varphi}^{-1}_{|I_{\mathfrak{p}}}$ parce que $\chi_{|I_{\mathfrak{p}}} = 1$. D'où il vient

$$\mathrm{ord}_{\mathfrak{p}}(\mathfrak{N}(\varphi)) = \mathrm{ord}_{\mathfrak{p}}\left(\mathfrak{N}\left(\widehat{\varphi}^{-1}\right)\right) = \mathrm{ord}_{\mathfrak{p}}\left(\mathfrak{N}\left(\widehat{\varphi}\right)\right) = \mathrm{ord}_{\bar{\mathfrak{p}}}\left(\mathfrak{N}\left(\varphi\right)\right)$$

puis $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) = \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{f}_\delta)$ et $\mathrm{ord}_p(M) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta) + \mathrm{ord}_{\bar{\mathfrak{p}}}(\mathfrak{f}_\delta) = 2\,\mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$. □

On pose alors

$$M' = \prod_{p \nmid D_K} p^{\mathrm{ord}_p(M)/2} \times \prod_{p \mid D_K} p^{x_p},$$

où pour tout nombre premier p divisant D_K, on définit

$$x_p = \begin{cases} \mathrm{ord}_p(M)/2 & \text{si } \mathrm{ord}_p(M) \text{ est pair;} \\ (\mathrm{ord}_p(M)+1)/2 & \text{si } \mathrm{ord}_p(M) \text{ est impair.} \end{cases}$$

D'après le lemme précédent, M' est un entier naturel divisant M qui vérifie $\mathrm{ord}_{\mathfrak{p}}(M') \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$ pour tout $\mathfrak{p} \mid \mathfrak{f}_\delta$: cela suit du lemme 3.6 pour les $\mathfrak{p}$ premiers à D_K, et pour ceux qui divisent D_K du calcul $\mathrm{ord}_{\mathfrak{p}}(M') = 2\,\mathrm{ord}_p(M') \geq \mathrm{ord}_p(M) = \mathrm{ord}_{\mathfrak{p}}(\mathfrak{f}_\delta)$, où on a noté $p = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{p})$.

Lemme 3.7. *Le caractère ε se factorise modulo M'.*

Démonstration. On reprend les notations du début de ce paragraphe et on commence par comparer $m^{k-1}\eta(m)$ avec $\delta_{\mathrm{f}}(m) = m^{k-1}$ pour un entier $m \equiv 1 \pmod{M'}$. Comme M' et M ont les mêmes diviseurs premiers, on a en particulier $\mathrm{pgcd}(m, M) = 1$. On remarque tout d'abord que la formule

$$\delta_{\mathrm{H}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} = \delta(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)}$$

est valable pour tout idéal premier $\mathfrak{p}$ de $\mathcal{O}_K$. En effet, lorsque $\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K) = 0$, elle est triviale et lorsque $\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K) > 0$, cela résulte du fait que cela entraîne $\mathfrak{p} \nmid M = \mathrm{Norm}_{K/\mathbf{Q}}(\mathfrak{f}_\delta)$ et par suite la formule n'est autre chose que la définition de δ_{H}. Ainsi, on a

$$m^{k-1}\eta(m) = \delta_{\mathrm{H}}(m\mathcal{O}_K) = \prod_{\mathfrak{p}} \delta_{\mathrm{H}}(\mathfrak{p})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} = \prod_{\mathfrak{p}} \delta(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)}$$

et grâce à $m^{k-1} = \delta_{\mathrm{f}}(m) = \prod_{\mathfrak{p}\mid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m)$

$$\begin{aligned} m^{k-1} &= \prod_{\mathfrak{p}\mid m\mathcal{O}_K} \delta_{\mathfrak{p}}(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) \\ &= \prod_{\mathfrak{p}} \delta_{\mathfrak{p}}(\pi_{\mathfrak{p}})^{\mathrm{ord}_{\mathfrak{p}}(m\mathcal{O}_K)} \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) = m^{k-1}\eta(m) \times \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m). \end{aligned}$$

Notons $P(m) = \prod_{\mathfrak{p}\nmid m\mathcal{O}_K} \delta_{\mathfrak{p}}(m) = \eta(m)^{-1}$ le produit apparaissant à la dernière ligne de la formule ci-dessus. Tout d'abord, on remarque que l'on a

$P(m) = \prod_{\mathfrak{p}|\mathfrak{f}_\delta} \delta_\mathfrak{p}(m)$ car d'une part $\mathrm{pgcd}(\mathfrak{f}_\delta, m\mathcal{O}_K) = 1$ et d'autre part, si $\mathfrak{p} \nmid m\mathcal{O}_K$ et $\mathfrak{p} \nmid \mathfrak{f}_\delta$, alors $m \in \mathcal{O}_\mathfrak{p}^\times$, puis $\delta_\mathfrak{p}(m) = 1$. Comme pour tout $\mathfrak{p} \mid \mathfrak{f}_\delta$ on a $\mathrm{ord}_\mathfrak{p}(m-1) \geq \mathrm{ord}_\mathfrak{p}(M') \geq \mathrm{ord}_\mathfrak{p}(\mathfrak{f}_\delta)$, par définition du conducteur d'un Größencharakter, on en déduit $P(m) = 1$, puis $\eta(m) = 1$. Maintenant on remarque que l'on a

$$\varepsilon(m) = \eta(m) \left(\frac{-D_K}{m}\right) = \left(\frac{-D_K}{m}\right) = \pm 1$$

car η se factorise modulo M'. Or, $\varepsilon(m)$ se réduit sur 1 modulo ℓ par hypothèse. On a donc $\varepsilon(m) = 1$ et le résultat voulu. □

Le caractère ε, se réduisant sur le caractère trivial, est nécessairement d'ordre une puissance de ℓ, disons ℓ^h. On pose alors $\mu = \varepsilon^{(\ell^h-1)/2}$. C'est un caractère de même ordre et de même conducteur que ε vérifiant $\mu^2 = \varepsilon^{-1}$. Pour $z \in \mathbf{C}$, de partie imaginaire $\Im(z) > 0$, on pose alors

$$g^\dagger(z) = (g_\delta \otimes \mu)(z) = \sum_{n\geq 1} \mu(n) c_n q^n, \quad \text{avec } q = e^{2i\pi z}.$$

D'après [19, Proposition 3.64], $g^\dagger$ est le développement de Fourier d'une forme propre de poids k, de caractère $\varepsilon\mu^2 = 1$ et de niveau $\mathrm{ppcm}(MD_K, r^2)$ où r est le conducteur de ε (ou de μ). Or, on vérifie que M'^2 divise le produit MD_K. Ainsi, $\mathrm{ppcm}(MD_K, r^2) = MD_K$ d'après le lemme 3.7. Soit g la newform associée à $g^\dagger$. Alors, g est de niveau divisant MD_K et à multiplication complexe par K. Comme μ se réduit sur le caractère trivial, la réduction de la représentation v-adique associée à g est isomorphe à celle de g_δ, puis à ρ. Ceci achève la démonstration du théorème 1.1.

4. Exemples numériques

Pour l'exemple ci-dessous nous avons utilisé le logiciel PARI/GP ([25]).

4.1. Soit $\Delta = \sum_{n\geq 1} \tau(n) q^n = q - 24q^2 + 252q^3 - 1472q^4 + 4830q^5 + \cdots$ l'unique forme parabolique normalisée de poids 12 et de niveau 1. On note

$$\rho_{\Delta,23} : \mathrm{G}_\mathbf{Q} \longrightarrow \mathrm{GL}_2(\mathbf{F}_{23})$$

l'unique représentation semi-simple non ramifiée hors de 23 telle que

$$\det \rho_{\Delta,23}(\mathrm{Frob}_p) = \tau(p) \pmod{23} \quad \text{et} \quad \mathrm{tr}\, \rho_{\Delta,23}(\mathrm{Frob}_p) = p^{11} \pmod{23}$$

pour tout nombre premier $p \neq 23$. Elle est de poids $k(\rho_{\Delta,23}) = 12$ et de conducteur $N(\rho_{\Delta,23}) = 1$.

Il résulte des congruences de Wilton ([29, p. 2]) que la représentation $\rho_{\Delta,23}$ est diédrale. Soit, plus explicitement, H le corps de classes de Hilbert de $K = \mathbf{Q}(\sqrt{-23})$. C'est une extension de degré 6 de $\mathbf{Q}$ de groupe de Galois D_3. Alors, $\rho_{\Delta,23}$ est isomorphe à la représentation

$$\mathrm{G}_\mathbf{Q} \longrightarrow \mathrm{Gal}(H/\mathbf{Q}) \simeq D_3 \xrightarrow{\sigma} \mathrm{GL}_2(\mathbf{Z}) \longrightarrow \mathrm{GL}_2(\mathbf{F}_{23}),$$

où $\sigma : D_3 \to \mathrm{GL}_2(\mathbf{Z})$ est l'unique représentation irréductible de degré 2 du groupe D_3 (voir [15, §3.4]) et où la dernière flèche est l'application de réduction modulo 23.

On explicite à présent la forme à multiplication complexe dont l'existence est garantie par le théorème 1.1. Soit δ un Größencharakter de K de type à l'infini $(11, 0)$ et conducteur $\sqrt{-23}\mathcal{O}_K$ tel que, avec les notations du paragraphe 3.4, $\eta = (\frac{-23}{\cdot})$. La newform g_δ associée à δ est alors de poids 12, niveau 23^2, caractère trivial et de corps des coefficients l'extension totalement réelle L de degré 3 de $\mathbf{Q}$ engendrée par une racine α du polynôme $X^3 - 6X - 3$ (pour les détails, voir le fichier `DeltaMod23.gp`, disponible sur le site de la revue [1]). On a

$$g_\delta = \sum_{n\geq 1} c_n q^n = q + (-21\alpha^2 - 4\alpha + 84)q^2 + (53\alpha^2 + 251\alpha - 212)q^3 + \cdots$$

On pose

$$\Delta^\dagger = \sum_{\substack{n\geq 1\\ 23\nmid n}} \tau(n)q^n = \sum_{n\geq 1} \tau'(n)q^n$$

de sorte que $\Delta^\dagger(z) = \Delta(z) - U_{23}(\Delta)(23z)$ où U_{23} est l'opérateur de Hecke en 23 agissant sur les formes de poids 12 et de niveau divisible par 23. Ainsi, $\Delta^\dagger$ et g_δ sont des formes normalisées de poids 12, niveau 23^2 et caractère trivial qui sont propres pour l'algèbre de Hecke engendrée par les opérateurs $\{T_p,\ p \text{ premier},\ p \neq 23\}$.

Soit $\lambda_{23} = (\alpha - 5)\mathcal{O}_L$ l'unique idéal premier de l'anneau $\mathcal{O}_L$ des entiers de L ramifié au-dessus de 23. Vérifions que l'on a

$$\tau'(n) \equiv c_n \pmod{\lambda_{23}}, \quad \text{pour tout entier } n \leq m,$$

où $m = \left[\mathrm{SL}_2(\mathbf{Z}) : \Gamma_0\left(23^2\right)\right] = 552$. Pour les entiers n divisibles par 23, cela résulte immédiatement des égalités $\tau'(n) = 0$ et $c_n = 0$. Lorsque $23 \nmid n$, on se ramène par multiplicativité des coefficients de Fourier au cas où n est premier et on utilise la commande `CoefficientFormeCM` du fichier `DeltaMod23.gp` (l'ensemble des calculs prend quelques secondes sur un ordinateur de bureau). D'après [22, Theorem 1], il vient donc $\tau'(n) \equiv c_n \pmod{\lambda_{23}}$, pour tout entier $n \geq 1$, puis

$$\tau(p) \equiv c_p \pmod{\lambda_{23}}, \quad \text{pour tout nombre premier } p \neq 23.$$

On conclut avec [6, lemme 3.2] que $\rho_{\Delta,23}$ est isomorphe à la réduction modulo λ_{23} de la représentation galoisienne 23-adique associée à g_δ. En particulier, comme l'affirme le théorème 1.1, $\rho_{\Delta,23}$ provient bien d'une forme à multiplication complexe de poids $k(\rho_{\Delta,23}) = 12$ et de niveau $N' = 23^2 N(\rho_{\Delta,23}) = 23^2$.

Remarque 4.1. On constate ici que le niveau 23^2 est optimal. En effet, il n'existe pas de forme à multiplication complexe de poids 12 et de niveau 1 ou 23 congrue à Δ modulo 23.

4.2. Le corollaire 1.3 s'applique également à la représentation modulo 7 attachée à la courbe elliptique d'équation

$$Y^2 + Y = X^3 - X^2 - 18507X - 989382$$

notée 65533.a1 dans LMFDB ([24]). La détermination de la forme à multiplication complexe (de niveau 71^2) dont l'existence est garantie par le corollaire 1.3 s'effectue par une méthode analogue à celle utilisée précédemment. Les détails sont accessibles dans le fichier `EMod7.gp` (disponible sur le site de la revue [1]).

Bibliographie

[1] N. Billerey & F. A. E. Nuccio, « Représentations galoisiennes diédrales et formes à multiplication complexe », *J. Théor. Nombres Bordx* **30** (2018), n° 2, p. 651-670, http://jtnb.cedram.org/jtnb-bin/fitem?id=JTNB_2018__30_2_651_0.

[2] D. M. Bloom, « The subgroups of PSL(3, q) for odd q », *Trans. Am. Math. Soc.* **127** (1967), p. 150-178.

[3] H. Carayol, « Sur les représentations l-adiques associées aux formes modulaires de Hilbert », *Ann. Sci. Éc. Norm. Supér.* **19** (1986), n° 3, p. 409-468.

[4] ———, « Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires », *Duke Math. J.* **59** (1989), n° 3, p. 785-801.

[5] I. Chen, « Surjectivity of mod ℓ representations attached to elliptic curves and congruence primes », *Can. Math. Bull.* **45** (2002), n° 3, p. 337-348.

[6] P. Deligne & J.-P. Serre, « Formes modulaires de poids 1 », *Ann. Sci. Éc. Norm. Supér.* **7** (1974), p. 507-530.

[7] E. Ghate & P. Parent, « On uniform large Galois images for modular abelian varieties », *Bull. Lond. Math. Soc.* **44** (2012), n° 6, p. 1169-1181.

[8] E. Hecke, *Mathematische Werke*, Herausgegeben im Auftrage der Akademie der Wissenschaften zu Göttingen, Vandenhoeck & Ruprecht, 1959, 955 pages.

[9] S. Lang, *Introduction to modular forms*, Grundlehren der Mathematischen Wissenschaften, vol. 222, Springer, 1976, ix+261 pages.

[10] J. Nualart, « Minimal lifts of dihedral 2-dimensional Galois representations », *Bull. Braz. Math. Soc. (N.S.)* **42** (2011), n° 3, p. 359-371.

[11] M. Raynaud, « Schémas en groupes de type $(p, \ldots, p)$ », *Bull. Soc. Math. Fr.* **102** (1974), p. 241-280.

[12] K. A. Ribet, « Galois action on division points of Abelian varieties with real multiplications », *Am. J. Math.* **98** (1976), n° 3, p. 751-804.

[13] ———, « Abelian varieties over **Q** and modular forms », in *Algebra and topology 1992 (Taejŏn)*, Korea Advanced Institute of Science and Technology, Mathematics Research Center, 1992, p. 53-79.

[14] J.-P. Serre, *Corps locaux*, 2ème éd., Publications de l'Institut de Mathématique de l'Université de Nancago, vol. 8, Hermann, 1968, 243 pages.

[15] ———, « Une interprétation des congruences relatives à la fonction τ de Ramanujan », in *Séminaire Delange-Pisot-Poitou : 1967/68*, Théorie des Nombres, vol. 1, Faculté des Sciences de Paris. Secrétariat Mathématique, 1969, Exp. 14, 17 p.

[16] ———, « Propriétés galoisiennes des points d'ordre fini des courbes elliptiques », *Invent. Math.* **15** (1972), n° 4, p. 259-331.

[17] ———, *Représentations linéaires des groupes finis*, Hermann, 1978, 184 pages.

[18] ———, « Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ », *Duke Math. J.* **54** (1987), n° 1, p. 179-230.
[19] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Iwanami Shoten ; Princeton University Press, 1971, xiii+267 pages.
[20] ———, « On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields », *Nagoya Math. J.* **43** (1971), p. 199-208.
[21] ———, « Class fields over real quadratic fields and Hecke operators », *Ann. Math.* **95** (1972), p. 130-190.
[22] J. Sturm, « On the congruence of modular forms », in *Number theory (New York, 1984-85)*, Lecture Notes in Mathematics, vol. 1240, Springer, 1984, p. 1984-1985.
[23] Y. Taguchi, « Induction formula for the Artin conductors of mod ℓ Galois representations », *Proc. Am. Math. Soc.* **130** (2002), n° 10, p. 2865-2869.
[24] The LMFDB Collaboration, « The L-functions and Modular Forms Database », 2013, http://www.lmfdb.org.
[25] The PARI Group, « PARI/GP version `2.9.2` », 2014, available from http://pari.math.u-bordeaux.fr/.
[26] L. C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Mathematics, vol. 83, Springer, 1997, xiv+487 pages.
[27] A. Weil, « On a certain type of characters of the idèle-class group of an algebraic number-field », in *Proceedings of the international symposium on algebraic number theory (Tokyo & Nikko, 1955)*, Science Council of Japan, 1956, p. 1-7.
[28] G. Wiese, « Dihedral Galois representations and Katz modular forms », *Doc. Math.* **9** (2004), p. 123-133.
[29] J. R. Wilton, « Congruence Properties of Ramanujan's Function tau(n) », *Proc. Lond. Math. Soc.* **31** (1930), n° 1, p. 1-10.

Nicolas Billerey
Université Clermont Auvergne
LMBP UMR 6620 – CNRS
Campus des Cézeaux
3, place Vasarely
F-63178 Aubière, France
E-mail: nicolas.billerey@uca.fr
URL: http://math.univ-bpclermont.fr/~billerey/

Filippo A. E. Nuccio Mortarino Majno di Capriglio
Université de Lyon
Institut Camille Jordan
UMR 5208 – CNRS
Université Jean Monnet
23, rue du Docteur Paul Michelon
F-42023 Saint-Étienne, France
E-mail: filippo.nuccio@univ-st-etienne.fr
URL: http://perso.univ-st-etienne.fr/nf51454h/