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.