Courbes elliptiques et cryptographie

Hägler Michael

Assistante responsable : Marusia Rebolledo
Professeur responsable : Eva Bayer Fluckiger
Date : 19 février 2006

Table des matières

Introduction

Nous allons présenter, dans cet article, deux systèmes de chiffrement à clé publique basés sur les courbes elliptiques. Un système à clé publique est un cryptosysème où aucun secret n'est partagé entre l'émetteur et le récepteur : seule l'opération de déchiffrement doit être contrôlée par une clé gardée secrète ; le chiffrement peut, quant à lui, être exécuté à l'aide d'une clé connue publiquement, à condition qu'il soit impossible d'en déduire la clé secrète. On parle alors de cryptage asymétrique par opposition au cryptage symétrique. Nous parlerons également de plusieurs problème liés à la cryptographie et utilisant les courbes elliptiques. Plus précisément, nous parlerons du problème du logarithme discret, nous verrons qu'il existe des tests de primalité et des algorithmes de factorisations utilisant les courbes elliptiques et finalement nous verrons comment compter les points sur certaines courbes elliptiques. Ces derniers aspects sont indissociables de ce genre de systèmes de cryptage.

Chapitre 1

Eléments théoriques

1.1 Propriétés générales des courbes elliptiques

Définition 1.1. *Soit K un corps, on appelle* équation de Weierstrass *sur K une équation du type*

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

avec $a_i \in K$. Une courbe donnée par une telle équation est dite lisse *si le système suivant n'admet pas de solution*

$$\begin{cases} a_1y = 3x^2 + 2a_2x + a_4 \\ 2y + a_1x + a_3 = 0 \end{cases}$$

autrement dit si les dérivées partielles en x et en y de

$$f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

ne s'annulent pas en même temps.

Une courbe elliptique E définie sur K est une courbe lisse donnée par une équation de Weierstrass définie sur K à laquelle on a rajouté un point "à l'infini", noté O ;

$$E = \big\{(x, y) \in \overline{K}^2 \big| y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\big\} \cup \big\{O\big\}.$$

Si la caractéristique de K ($\mathrm{char}(K)$) n'est pas 2 ni 3, alors en faisant les deux changements de variables successifs $y \to 1/2(y - a_1x - a_3)$ et ensuite $(x, y) \to ((x - 3b_2)/36, y/216)$ dans E, où $b_2 = a_1^2 + 4a_2$, nous obtenons

$$E : y^2 = x^3 - 27c_4x - 54c_6,$$

avec $b_4 = 2a_4 + a_1a_3, b_6 = a_3^2 + 4a_6, c_4 = b_2^2 - 24b_4, c_6 = -b_2^3 + 36b_2b_4 - 216b_6$. Ainsi si $\mathrm{char}(K) \neq 2, 3$, nous pouvons toujours travailler avec des courbes elliptiques de la forme

$$E : y^2 = x^3 + Ax + B.$$

Dans ce cas la courbe est lisse si

$$4A^3 + 27B^2 \neq 0.$$

Proposition 1.2. *Soient E une courbe elliptique définie sur un corps K, et deux points $P, Q \in E(K)$, L la droite reliant P à Q (la tangente à E si $P = Q$) et R le troisième point d'intersection de L avec E. Soit L' la droite verticale passant par R. On définit $P + Q \in E(K)$ comme étant le deuxième point d'intersection de L' avec E. Muni de cette loi de composition $(E(K), +)$ est un groupe abélien dont l'élément neutre est le point à l'infini (O).*

La preuve n'est pas donnée ici ([6]).

Regardons géométriquement ce qui se passe lorsque nous additionnons deux points sur une courbe elliptique sur $\mathbb{R}$.

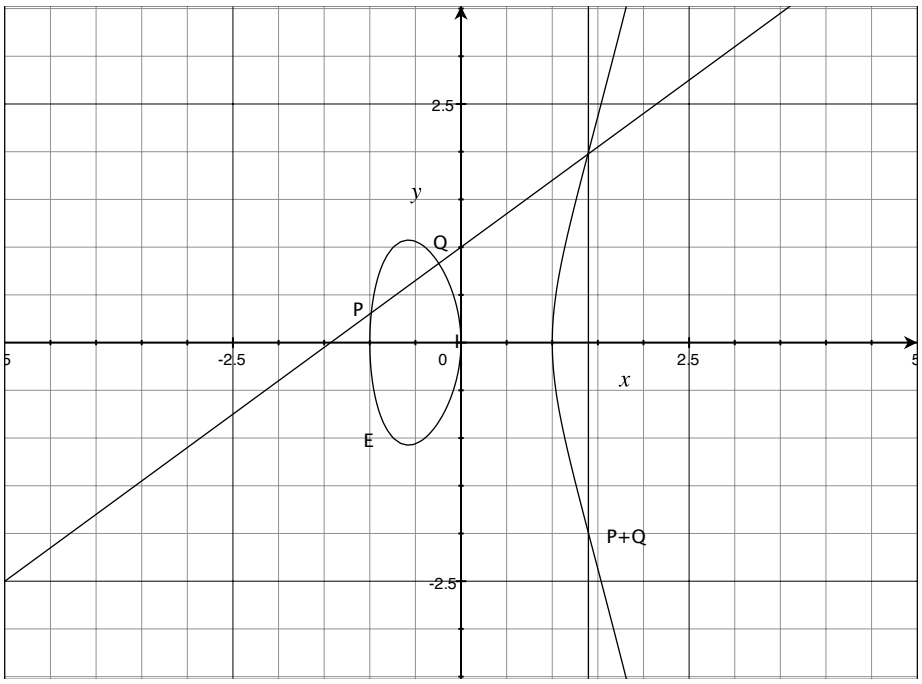

FIG. 1.1 – Courbe elliptique d'équation $y^2 = 3x^3 - 3x$.

Remarque. Nous allons dans tout ce qui suit, sauf mention contraire, uniquement considérer des corps ayant une caractéristique différente de 2 et 3, pour pouvoir écrire une courbe elliptique sous la forme de Weierstrass simplifiée.

Loi de groupe 1.3. *Nous allons donner une manière explicite de calculer la somme de deux points d'une courbe elliptique.*

Soient $E : y^2 = x^3 + Ax + B$ une courbe elliptique et $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ des points de E, avec $P_1, P_2 \neq O$. On a $P_1 + P_2 = P_3 = (x_3, y_3)$ avec :

1. *Si $x_1 \neq x_2$, alors*

$$x_3 = m^2 - x_1 - x_2, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{où } m = \frac{y_2 - y_1}{x_2 - x_1}.$$

2. *Si* $x_1 = x_2$ *mais* $y_1 \neq y_2$, *alors* $P_3 = O$.

3. *Si* $P_1 = P_2$ *et* $y_1 \neq 0$, *alors*

$$x_3 = m^2 - 2x_1, \quad y_3 = m(x_1 - x_3) - y_1, \quad \text{où } m = \frac{3x_1^2 + A}{2y_1}.$$

4. *Si* $P_1 = P_2$ *et* $y_1 = 0$, *alors* $P_3 = O$.

De plus, on a

$$P + O = P$$

pour tout P *sur* E.

Il est intéressant de noter, que dans ces formules, nous n'avons jamais utiliser B pour calculer les coordonnées de P_3.

Nous allons donner quelques propriétés sur les points de torsion d'une courbe elliptique E définie sur un corps quelconque K.

Définition 1.4. *Soit* E *une courbe elliptique définie sur un corps* K. *Soit* n *un nombre entier positif. On pose :*

$$E[n] := \big\{P \in E(\overline{K}) \big| nP = O\big\},$$

où $\overline{K}$ *est une clôture algébrique de* K.

Théorème 1.5 ([3] p.75)**.** *Si la caractéristique de* K *est nulle ou ne divise pas* n, *alors*

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}.$$

Si la caractéristique de K *est* $p > 0$ *et* $p|n$, *écrivons* $n = p^r n'$ *avec* $p \nmid n'$. *Alors*

$$E[n] \cong \mathbb{Z}/n'\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z} \text{ ou } E[n] \cong \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n'\mathbb{Z}.$$

En particulier, $E[p] \cong \mathbb{Z}/p\mathbb{Z}$ *ou* $E[p] = \big\{O\big\}$.

Définition 1.6. *Soit une courbe elliptique* E *définie sur un corps* K *de caractéristique* p. *On dit que* E *est une courbe elliptique* supersingulière *si*

$$E[p] = \big\{O\big\}.$$

L'accouplement de Weil

Définition 1.7. *Soit un corps* K *et soit* n *un nombre entier qui n'est pas divisible par la caractéristique de* K. *On pose :*

$$\mu_n(\overline{K}) := \big\{x \in \overline{K} \big| x^n = 1\big\},$$

le groupe des racines $n^{ème}$ *de l'unité dans* $\overline{K}$. *Puisque la caractéristique de* K *ne divise pas* n, *l'équation* $x^n = 1$ *n'a pas de racines multiples. Ainsi* μ_n *est cyclique d'ordre* n.

Un générateur ζ *de* μ_n *est appelé une racine primitive* $n^{ème}$ *de l'unité.*

Théorème 1.8 ([3] p.83)**.** *Soit E une courbe elliptique définie sur un corps K et soit n un entier positif tel que la caractéristique de K ne divise pas n. Alors il existe une application*

$$e_n : E[n] \times E[n] \to \mu_n,$$

appelé l'accouplement de Weil, qui satisfait les propriétés suivantes :

1. *e_n est bilinéaire, c'est-à-dire*

$$e_n(S_1 + S_2, T) = e_n(S_1, T)e_n(S_2, T)$$

et

$$e_n(S, T_1 + T_2) = e_n(S, T_1)e_n(S, T_2)$$

pour tous $S, S_1, S_2, T, T_1, T_2 \in E[n]$.

2. *$e_n(T, T) = 1$ pour tout $T \in E[n]$.*
3. *$e_n(S, T) = e_n(T, S)^{-1}$ pour tout $S, T \in E[n]$, i.e e_n est antisymétrique.*
4. *e_n est non dégénéré, c'est-à-dire que si $e_n(S, T) = 1$ pour tout $T \in E[n]$ alors $S = O$ et si $e_n(S, T) = 1$ pour tout $S \in E[n]$ alors $T = O$.*

Corollaire 1.9. *Soit $\{T_1, T_2\}$ une base de $E[n]$. Alors $e_n(T_1, T_2)$ est une racine primitive $n^{\text{ème}}$ de l'unité.*

Preuve. Posons $\zeta = e_n(T_1, T_2)$ avec $\zeta^d = 1$. Alors $e_n(T_1, dT_2) = 1$ par la linéarité de la deuxième composante. De plus, $e_n(T_2, dT_2) = e_n(T_2, T_2)^d = 1$ par la propriété 3 du théorème 1.8.

Soit $S \in E[n]$, alors $S = aT_1 + bT_2$ où a, b sont des entiers. Ainsi

$$e_n(S, dT_2) = e_n(T_1, T_2)^a e_n(T_2, T_2)^b = 1.$$

Puisque ceci est vrai pour tout $S \in E[n]$, alors $dT_2 = O$. Puisque $dT_2 = O$ si et seulement si $n|d$ (car T_2 est d'ordre n), ceci implique que ζ est une racine primitive $n^{\text{ème}}$ de l'unité. □

Corollaire 1.10 ([3] p.84)**.** *Si $E[n] \subseteq E(K)$, alors $\mu_n \subset K$.*

1.2 Courbes elliptiques sur un corps fini

En cryptographie on s'intéresse surtout aux courbes elliptiques sur des corps finis. En particulier, il est crucial de savoir calculer $\#E(\mathbb{F}_q)$ pour E une courbe elliptique définie sur $\mathbb{F}_q$. Dans ce paragraphe nous rappelons le théorème de Hasse. Une méthode algorithmique pour calculer $\#E(\mathbb{F}_q)$ sera donnée au chapitre 5.

Dans tout ce paragraphe nous considérons E une courbe elliptique sur un corps fini $\mathbb{F}_q$, avec $q = p^r$ pour un nombre premier p. On fixe une clôture algébrique $\overline{\mathbb{F}}_q$ de $\mathbb{F}_q$.

Commençons par donner une proposition dont la preuve se trouve en [2] p.375.

Théorème 1.11. *Si E est une courbe elliptique définie sur $\mathbb{F}_q$, alors il existe des entiers d_1 et d_2 tels que*

$$E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z},$$

avec $d_1|d_2$.

Endomorphisme de Frobenius

Définition 1.12. *Soit*

$$\begin{aligned} \phi_q : \overline{\mathbb{F}}_q &\longrightarrow \overline{\mathbb{F}}_q \\ x &\longmapsto x^q \end{aligned}$$

l'endomorphisme de Frobenius. On définit l'application :

$$\begin{aligned} \phi_q : E &\longrightarrow E \\ (x,y) &\longmapsto (x^q, y^q) \\ O &\longmapsto O. \end{aligned}$$

Lemme 1.13. *Soit* $(x,y) \in E(\overline{\mathbb{F}}_q)$.

1. $\phi_q(x,y) \in E(\overline{\mathbb{F}}_q)$,
2. $(x,y) \in E(\mathbb{F}_q)$ *si et seulement si* $\phi_q(x,y) = (x,y)$,
3. ϕ_q *est un endomorphisme.*

Preuve. Soient n, p tel que $q = p^n$ où p est premier et n un entier. La caractéristique de $\mathbb{F}_q$ est p. Nous avons donc $(a+b)^q = a^q + b^q$ pour $a, b \in \overline{F}_q$. De plus $a^q = a$ pour tout $a \in \mathbb{F}_q$. Soit

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

une courbe elliptique définie sur $\mathbb{F}_q$ (avec $a_i \in \mathbb{F}_q$). Si nous élevons les deux membres de cette équation à la puissance q et que nous utilisons ce que nous avons dit plus haut, nous obtenons :

$$(y^q)^2 + a_1x^qy^q + a_3y^q = (x^q)^3 + a_2(x^q)^2 + a_4x^q + a_6.$$

Ce qui veut dire que $(x^q, y^q) \in E(\overline{\mathbb{F}}_q)$, ce qui prouve 1.

Pour prouver le point 2, il faut rappeler que $x \in \mathbb{F}_q$ si et seulement si $\phi_q(x) = x$. Ainsi :

$$\begin{aligned} (x,y) \in E(\mathbb{F}_q) &\iff x, y \in \mathbb{F}_q \\ &\iff \phi_q(x) = x \text{ et } \phi_q(y) = y \\ &\iff \phi_q(x,y) = (x,y). \end{aligned}$$

Pour la preuve du point 3., le lecteur se référera à [3] pp.48-49.

□

Le théorème de Hasse nous permet de borner $\#E(\mathbb{F}_q)$.

Théorème 1.14 (Hasse)**.** *Soit E une courbe elliptique définie sur un corps fini* $\mathbb{F}_q$. *Alors*

$$|q + 1 - \#E(\mathbb{F}_q)| \leq 2\sqrt{q}.$$

Nous trouverons la preuve en [6].

Pour ce qui suit, posons $a = q + 1 - \#E(\mathbb{F}_q)$.

Théorème 1.15. *Soit E une courbe elliptique. Alors*

$$\phi_q^2 - a\phi_q + q = O$$

en tant qu'endomorphisme de E et a est le seul nombre entier qui satisfait cette équation. Autrement dit, pour $(x, y) \in E(\overline{\mathbb{F}}_q)$, nous avons

$$\left(x^{q^2}, y^{q^2}\right) - a(x^q, y^q) + q(x, y) = O.$$

Proposition 1.16. *Soit E une courbe elliptique défini sur un corps fini. Alors E est une courbe supersingulière si et seulement si $a \equiv 0 \pmod{p}$, i.e si et seulement si*

$$\#E(\mathbb{F}_q) \equiv 1 \pmod{p}.$$

De plus si $q = p \geq 5$, E est supersingulière si et seulement si

$$\#E(\mathbb{F}_p) = p + 1.$$

La preuve des deux affirmations ci-dessus se trouve en [3] p.121.
Nous allons donner une proposition que nous utiliserons dans le chapitre 2.

Proposition 1.17. *Soit q une puissance d'un nombre premier impair et $q \equiv 2 \pmod{3}$. Soit $b \in \mathbb{F}_q^*$. Alors la courbe elliptique $E : y^2 = x^3 + b$ est supersingulière.*

Preuve. Soit $\psi : \mathbb{F}_q^* \to \mathbb{F}_q^*$ l'homomorphisme défini par $\psi(x) = x^3$. Puisque $q - 1$ n'est pas un multiple de 3, il n'y a pas d'éléments d'ordre 3 dans $\mathbb{F}_q^*$, et donc le noyau de ψ est trivial. Ainsi ψ est injective. De plus ψ est surjective puisque l'application va d'un groupe fini dans lui-même. En particulier, tout élément de $\mathbb{F}_q$ a une racine cubique unique dans $\mathbb{F}_q$.
Pour chaque $y \in \mathbb{F}_q$ il existe exactement un $x \in \mathbb{F}_q$ tel que $(x, y) \in E$. En fait, x est l'unique racine cubique de $y^2 - b$. Puisqu'il y a q valeurs de y possibles, nous trouvons q points finis. Il faut encore rajouter le point à l'infini 0. Ainsi

$$\#E(\mathbb{F}_q) = q + 1,$$

et donc E est supersingulière ([3] p.121). □

1.3 Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$

Nous pouvons nous demander s'il est possible de généraliser la notion de courbe elliptique, c'est-à-dire de la définir sur un anneau au lieu d'un corps. Plus particulièrement nous nous intéressons aux anneaux du type $\mathbb{Z}/n\mathbb{Z}$ où n est un nombre entier positif pas forcément premier et voir qu'il existe une structure de groupe pour une courbe elliptique définie sur $\mathbb{Z}/n\mathbb{Z}$. Il ne suffit pas de considérer la courbe sur $\mathbb{Q}$, de multiplier l'équation par le PPMC des dénominateurs et de réduire modulo

n. Donnons un exemple.

Exemple. Soit la courbe elliptique E donnée par $y^2 = x^3 - x + 1$. Réduisons cette équation naïvement modulo 25. Supposons que nous voulons calculer $(1,1)+(21,4)$. En utilisant les formules de 1.3, la pente de la droite passant par ces deux points est $3/20$. Le dénominateur n'est pas nul mod 25, mais 20 n'est pas non plus inversible modulo 25 ! Ainsi la pente n'est ni finie, ni infinie modulo 25. Nous ne pouvons pas simplement réduire cette pente modulo 25 car $3/20$ n'a pas de sens modulo 25. Il nous faut donc trouver un autre moyen de définir une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$.

Pour pouvoir développer la théorie des courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$, il nous faut définir le concept de plan projectif.

Plan projectif Nous allons tout d'abord définir la notion de plan projectif dans le cas d'un corps K et ensuite la généraliser à $\mathbb{Z}/n\mathbb{Z}$. Nous verrons alors que le bon point de vue pour étudier les courbes elliptiques est l'espace projectif.

Définition 1.18. *Soient K un corps et n un nombre entier positif. Soient des points $x = (x_1, \cdots, x_{n+1}), y = (y_1, \cdots, y_{n+1}) \in K^{n+1}\backslash\{0\}$. On dit que x est équivalent à y et on note x y s'il existe $\lambda \in K^*$ tel que $x = \lambda y$. La classe d'équivalence de x se note $(x_1 : \cdots : x_{n+1})$.On appelle plan projectif l'ensemble suivant :*

$$\mathbb{P}^n(K) := \big(K^{n+1}\backslash\{0\}\big)/\sim .$$

Nous allons nous intéresser plus particulièrement au plan projectif $\mathbb{P}^2(K)$ et voir que nous pouvons regarder une courbe elliptique E définie sur K comme une courbe dans $\mathbb{P}^2(K)$ en la modifiant un peu. Ceci permet de mieux définir le point à l'infini 0 qui est l'élément neutre du groupe de $E(K)$.

Définition 1.19. *Soient K un corps et $E : y^2 = x^3 + Ax + B$ une courbe elliptique définie sur K. L'équation homogène de E est*

$$y^2z = x^3 + Axz^2 + Bz^3.$$

Remarques.

- Si $z = 1$ dans l'équation homogène de E, on retrouve E. Si $(x, y, z) \in K^3\backslash\{0\}$ est une solution de l'équation homogène de E, alors pour tout $\lambda \in K^*$, $(\lambda x, \lambda y, \lambda z)$ est aussi une solution (il suffit de multiplier l'équation homogène par λ^3). Ainsi, dans $\mathbb{P}^2(K)$, ça a un sens de considérer tout une classe $(x : y : z)$ comme solution de l'équation homogène.
- On peut injecter K^2 dans $\mathbb{P}^2(K)$ de la manière suivante :

$$\begin{aligned} K^2 &\hookrightarrow \mathbb{P}^2(K) \\ (x, y) &\mapsto (x : y : 1) \end{aligned}$$

- Si $(x : y : z) \in \mathbb{P}^2(K)$ avec $Z \neq 0$, alors $(x : y : z) = (x/z : y/z : 1)$. C'est un point fini de $\mathbb{P}^2(K)$. Par contre si $z = 0$, alors diviser par z nous donne ∞ dans au moins une des coordonnées x, y. C'est pourquoi on appelle les points ayant la forme $(x : y : 0)$ les points à l'infini dans $\mathbb{P}^2(K)$.

- Dans le cas d'une courbe elliptique sous forme homogène $y^2z = x^3+Axz^2+Bz^3$ si $z = 0$, alors $x = 0$ est donc $y \neq 0$, c'est à dire il n'y a qu'un seul point à l'infini dans $\mathbb{P}^2(K)$ qui est $(0 : 1 : 0)$. Puisque $(0 : 1 : 0) = (0 : -1 : 0)$, il n'y qu'une seule "direction" pour aller à l'infini. C'est ce point là que nous définissons comme étant O.

Nous allons maintenant définir la notion de plan projectif pour $\mathbb{Z}/n\mathbb{Z}$, où n est un entier positif.

Définition 1.20. *Soient $n, x_1, x_2, x_3 \in \mathbb{Z}$ avec $n > 0$ tels que*

$$\mathrm{PGDC}(n, x_1, x_2, x_3) = 1.$$

Alors on dit que (x_1, x_2, x_3) est primitif dans $(\mathbb{Z}/n\mathbb{Z})^3$.
On définit la relation d'équivalence suivante : deux triplets primitifs (x, y, z) et (x', y', z') dans $(\mathbb{Z}/n\mathbb{Z})^3$ sont équivalents s'il existe $u \in (\mathbb{Z}/n\mathbb{Z})^*$ tel que

$$(x', y', z') = (ux, uy, uz).$$

On définit le plan projectif de dimension 2 sur $\mathbb{Z}/n\mathbb{Z}$ ainsi

$$\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) := \big\{(x, y, z) \in (\mathbb{Z}/n\mathbb{Z})^3 \big| (x, y, z) \text{ est primitif}\big\}/\sim$$

où $\sim$ est la relation d'équivalence définie ci-dessus et on note la classe d'équivalence de (x, y, z), $(x : y : z)$.

Puisque nous voulons travailler sur des courbes elliptiques définie sur $\mathbb{Z}/n\mathbb{Z}$, il faut que $2 \in (\mathbb{Z}/n\mathbb{Z})^*$ et si nous voulons travailler avec l'équation de Weierstrass, il faut aussi que $3 \in (\mathbb{Z}/n\mathbb{Z})^*$.

Définition 1.21. *Supposons que $2, 3 \in (\mathbb{Z}/n\mathbb{Z})^*$, une courbe elliptique E sur $\mathbb{Z}/n\mathbb{Z}$ est le lieu dans $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$ d'une équation de la forme*

$$y^2z = x^3 + Axz^2 + Bz^3$$

avec $A, B \in \mathbb{Z}/n\mathbb{Z}$ tels que $4A^3 + 27B^2 \in (\mathbb{Z}/n\mathbb{Z})^*$. On pose

$$E(\mathbb{Z}/n\mathbb{Z}) = \big\{(x : y : z) \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) \big|\ y^2z = x^3 + Axz^2 + Bz^3\big\}.$$

Nous pouvons définir une addition sur cet ensemble de manière à obtenir un groupe. Mais nous n'allons pas la définir ici puisque se sont de longues formules qui ne nous apportent pas grand chose pour ce qui va suivre ([3] pp.62-64), étant donné que nous allons travailler plus loin avec ce genre de groupe de manière naïve, c'est-à-dire comme dans l'exemple ci-dessus.

Notons tout de même que dans un groupe de type $E(\mathbb{Z}/n\mathbb{Z})$, il n'y a pas, en général, qu'un seul point ayant zéro comme troisième coordonnée ; contrairement au courbes elliptiques définies sur un corps où le seul point ayant zéro comme troisième coordonnée est $(0 : 1 : 0)$. C'est une des raisons pour laquelle il est plus aisé de travailler dans le plan projectif.

Nous allons encore énoncer un théorème découlant du théorème chinois mais que nous ne démontrerons pas ici, voir [3] p.65.

Théorème 1.22. *Soient E une courbe elliptique et $n_1, n_2 \in \mathbb{Z}$ tels que n_1 et n_2 soient premiers entre eux. Alors*

$$E(\mathbb{Z}/n_1 n_2 \mathbb{Z}) \cong E(\mathbb{Z}/n_1\mathbb{Z}) \oplus E(\mathbb{Z}/n_2\mathbb{Z}).$$

Chapitre 2

Cryptosystèmes basés sur les courbes elliptiques

Nous allons présenter deux cryptosystèmes basés sur les courbes elliptiques. Mais commençons par donner une idée des différents types de cryptosystème. Il en existe principalement deux types :

- *Les systèmes à clé publique ou cryptosystèmes asymétriques* : la clé pour coder le message est connue de tout le monde mais ne permet pas d'en déduire la clé qui permet de décrypter le message. Cette clé-ci n'est connue que par le destinataire. Par exemple le RSA est un tel cryptosystème.
- *Les systèmes à clé privée ou cryptosystèmes symétriques* : dans ce cas les correspondants se mettent d'accord sur une clé secrète que seul eux connaissent. Il leur faut alors un moyen sûr pour s'échanger la clé. Par exemple le protocole de Diffie-Hellmann, que nous allons présenter ci-dessous, permet d'échanger une clé en toute sécurité.

2.1 Protocole d'échange de clés de Diffie-Hellmann

Alice et Bob veulent avoir une clé en commun pour s'échanger des données en toute sécurité. Supposons que leur seul moyen de communication soit public. Un des moyens de sécuriser leurs données est qu'ils établissent une clé privée entre eux. La méthode de Diffie-Hellmann permet justement de faire cela (en général on utilise cette méthode avec des groupes $\mathbb{F}_q^*$, mais nous présentons cette méthode adaptée pour les courbes elliptiques).

1. Alice et Bob choisissent une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ tel que le logarithme discret (voir juste après) soit difficile à résoudre. Il choisissent aussi un point $P \in E(\mathbb{F}_q)$ tel que le sous-groupe généré par P ait un ordre de grande taille. (En général, la courbe E et le point P sont choisis de manière à ce que l'ordre soit un grand nombre premier.)
2. Alice choisit un nombre entier secret a, calcule $P_a = aP$ et envoie P_a à Bob.
3. Bob choisit un nombre entier secret b, calcule $P_b = bP$ et envoie P_b à Alice.

4. Alice calcule $aP_b = abP$.
5. Bob calcule $bP_a = baP$.
6. Alice et Bob utilisent une méthode quelconque connue pour extraire une clé secrète de abP. Par exemple, ils peuvent utiliser les derniers 256 bits de la première coordonnée de abP comme clé, ou ils peuvent hâcher une des coordonnées de abP avec une fonction de hâchage (voir la définition 2.5) pour laquelle ils se sont mis d'accord.

Problème du logarithme discret Commençons par définir ce qu'est le problème du logarithme discret dans un groupe G quelconque.

Définition 2.1. *Soient G un groupe et $g \in G$. Le problème du logarithme discret dans G en base g est, pour $y \in G$ donné, de trouver un entier x tel que*

$$g^x = y$$

($xg = y$ si G est noté additivement).
Dans le cas où $G = E$ est une courbe elliptique, le problème du logarithme discret en base $P \in E$ est de trouver, étant donné $Q \in E$, un entier x tel que

$$Q = xP$$

si un tel x existe.

Nous parlerons plus spécialement du problème du logarithme discret dans le chapitre 3.

Revenons au protocole de Diffie-Hellmann. Les seules informations qu'un espion peut connaître sont la courbe E, le corps $\mathbb{F}_q$ et les points P, aP, bP. Ainsi si il veut pouvoir connaître la clé secrète, l'espion doit résoudre le problème suivant :

Problème de Diffie-Hellmann
Connaissant P, aP, bP des points de $E(\mathbb{F}_q)$, peut-on trouver abP ?

Si l'espion peut résoudre le problème du logarithme discret sur $E(\mathbb{F}_q)$, alors il peut résoudre le problème de Diffie-Hellmann. Actuellement, on ne connaît pas de moyen de trouver abP sans d'abord résoudre le problème du logarithme discret.

Une autre question est la suivante :

Problème de décision de Diffie-Hellmann
Connaissant P, aP, bP des points de $E(\mathbb{F}_q)$ et un point $Q \in \mathbb{F}_q$, peut-on déterminer si

$$Q = abP?$$

Autrement dit, si quelqu'un fournit à l'espion un point Q en lui affirmant qu'il est égal à abP, l'espion a-t-il un moyen de vérifier si l'information est correcte ?

Le problème de Diffie-Hellmann et le problème de décision de Diffie-Hellmann peuvent être posés pour des groupes arbitraires. Pour les courbes elliptiques, l'accouplement de Weil peut être utilisé pour résoudre le problème de décision de Diffie-Hellmann dans certains cas. Voyons ceci.

Résolution du problème de Diffie-Hellmann pour une famille de courbes elliptiques

Lemme 2.2. *Soit q comme dans la proposition 1.17 et b un carré de $\mathbb{F}_q^*$. Considérons la courbe supersingulière $E : y^2 = x^3 + b$. Cette courbe est supersingulière par la proposition ci-dessus. Soit $\omega \in \overline{\mathbb{F}}_q$ une racine cubique primitive de l'unité. Remarquons que $\omega \notin \mathbb{F}_q$ puisque l'ordre de $\mathbb{F}_q^*$ est $q-1$ qui n'est pas un multiple de 3. Définissons l'application*

$$\begin{aligned} \beta : E &\to E \\ (x, y) &\mapsto (\omega x, y) \\ O &\mapsto O. \end{aligned}$$

Pour $(x, y) \in E(\mathbb{F}_q)$, nous avons bien $(\omega x, y) \in E(\mathbb{F}_q)$ puisque $\omega^3 = 1$.

Preuve. On peut vérifier que cette application est un homomorphisme (voir [3] p.161). Mais nous pouvons voir que β est bijective. En effet, ω^{-1} est aussi une racine cubique primitive de l'unité et l'application

$$(x, y) \mapsto (\omega^{-1} x, y)$$

est l'inverse de β.

□

Lemme 2.3. *Soit $P \in E$ un point d'ordre n. Alors $\beta(P)$ est aussi d'ordre n car β est un isomorphisme. Supposons que $3 \nmid n$. Si $P \in E(\mathbb{F}_q)$ est d'ordre n avec $E : y^2 = x^3 + b$, $b \in \mathbb{F}_q$ un carré, alors $e_n(P, \beta(P))$ est une racine primitive $n^{\text{ème}}$ de l'unité.*

Preuve. Commençons par montrer que P et $\beta(P)$ forment une base de $E[n]$. Soient u, v des nombres entiers tels que

$$uP = v\beta(P).$$

Alors

$$\beta(vP) = v\beta(P) = uP \in E(F_q).$$

Si $vP = O$, alors $uP = O$ et donc $u \equiv 0 \pmod{n}$. Si $vP \neq O$, écrivons $vP = (x, y)$ avec $x, y \in \mathbb{F}_q$. Alors

$$(\omega x, y) = \beta(vP) \in E(\mathbb{F}_q).$$

Puisque $\omega \notin \mathbb{F}_q$, nous devons avoir $x = 0$. Ainsi $vP = (0, \pm\sqrt{b})$ qui est d'ordre 3. Ceci est impossible puisque, par hypothèse, $3 \nmid n$. Ceci implique que les seules relations $uP = v\beta(P)$ sont pour $u, v \equiv 0 \pmod{n}$, et donc P et $\beta(P)$ forment une base de $E[n]$. Par le corollaire 1.9, $e_n(P, \beta(P))$ est une racine primitive $n^{\text{ème}}$ de l'unité. □

Supposons maintenant que nous connaissons P, aP, bP, Q et nous voulons savoir si $Q = abP$.

Lemme 2.4. *Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et $P, Q \in E(\mathbb{F}_q)$ tel que N est l'ordre de P et $\mathrm{PGDC}(N, q) = 1$. Il existe un entier k tel que $Q = kP$ si et seulement si $Q \in E[N]$ et $e_N(P, Q) = 1$.*

Preuve. Supposons que $Q = kP$, alors $NQ = kNP = O$. De plus,

$$e_N(P, Q) = e_N(P, P)^k = 1^k = 1.$$

Réciproquement, si $NQ = O$, alors $Q \in E[N]$. Puisque $\mathrm{PGCD}(N, q) = 1$, nous avons

$$E[N] = \mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$$

par le théorème 1.5. Soit $R \in E[N]$ un point tel que $\{P, R\}$ soit une base de $E[N]$. Alors il existe des entiers a, b tels que

$$Q = aP + bQ.$$

Par le corollaire 1.9, $e_N(P, R) = \zeta$, une racine primitive $N^{\text{ème}}$ de l'unité. Ainsi, puisque $e_N(P, Q) = 1$, nous obtenons

$$1 = e_N(P, Q) = e_N(P, P)^a e_N(P, Q)^b = \zeta^b.$$

Ce qui implique que $b \equiv 0 \pmod{N}$, donc $bR = O$. Ainsi, $Q = aP$. □

Ce lemme nous permet de savoir si Q est un multiple de P.

Si $e_n(P, Q) \neq 1$ alors Q n'est pas un multiple de P.

Si $e_n(P, Q) = 1$ (l'ordre de P est n) alors il existe un t tel que $Q = tP$. Remarquons tout d'abord que

$$e_n(abP, \beta(P)) = e_n(aP, \beta(bP)).$$

Alors

$$ab \equiv t \pmod{n} \Rightarrow tP = Q = abP \Rightarrow e_n(Q, \beta(P)) = e_n(aP, \beta(bP)).$$

Supposons que $3 \nmid n$. Alors $e_n(P, \beta(P))$ est une racine primitive $n^{\text{ème}}$ de l'unité par le lemme 2.3. Supposons aussi que $e_n(Q, \beta(P)) = e_n(aP, \beta(bP))$. Alors

$$\begin{aligned} e_n(Q, \beta(P)) &= e_n(abP, \beta(P)) \\ \Rightarrow e_n(P, \beta(P))^t &= e_n(P, \beta(P))^{ab} \\ \Rightarrow e_n(P, \beta(P))^{t-ab} &= 1 \\ \Rightarrow t - ab &\equiv 0 \pmod{n}. \end{aligned}$$

Ces implications viennent du fait que e_n est bilinéaire et du fait que $e_n(P, \beta(P))$ est une racine primitive $n^{\text{ème}}$ de l'unité.

En résumé, si $3 \nmid n$, nous avons

$$Q = abP \Leftrightarrow t \equiv ab \pmod{n} \Leftrightarrow e_n(aP, b\beta(P)) = e_n(Q, \beta(P)).$$

Ceci résout le problème de décision de Diffie-Hellmann dans ce cas puisque Q, P, aP et bP sont des informations que l'espion connaît et $e_n(aP, \beta(bP))$ est calculable. Remarquons que nous n'avons jamais dû résoudre le problème du logarithme discret, il nous a juste fallu calculer l'accouplement de Weil.

2.2 La méthode d'ElGamal

Alice veut envoyer un message secret à Bob. Tout d'abord, Bob fabrique une clé publique de la manière suivante. Il choisit une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ de telle manière que le problème du logarithme discret soit plus difficile à résoudre sur $E(\mathbb{F}_q)$ que sur $\mathbb{F}_q$. Il choisit aussi un point P sur E tel que l'ordre de P soit un grand nombre premier. Il choisit un nombre entier secret s et calcule $B = sP$. La courbe E, le corps fini $\mathbb{F}_q$ et les points P et B sont la clé publique de Bob. La clé secrète de Bob est s. Pour envoyer le message, Alice fait comme suit :

1. Elle télécharge la clé publique de Bob.
2. Elle transforme son message en un point $M \in E(\mathbb{F}_q)$.
3. Elle choisit un nombre entier secret k et calcule $M_1 = kP$.
4. Elle calcule $M_2 = M + kB$.
5. Elle envoie M_1 et M_2 à Bob.

Bob déchiffre le message en calculant

$$M = M_2 - sM_1.$$

Nous avons cette égalité parce que

$$M_2 - sM_1 = (M + kB) - s(kP) = M + k(sP) - skP = M.$$

Un espion connaît la clé publique et les points M_1 et M_2. Si l'espion savait résoudre le problème du logarithme discret, il pourrait utiliser P et B pour trouver s et ainsi calculer $M_2 - sM_1$. L'espion pourrait aussi utiliser P et M_1 pour trouver k et calculer

$$M = M_2 - kB.$$

Actuellement, on ne connaît pas de moyen plus rapide pour retrouver le message initial en ne sachant que ce qui est rendu public du système de cryptage. Donc, a priori, la fiabilité de ce genre de cryptosystèmes dépend fortement des progrès fait en matière de résolution du logarithme discret.

Remarque. Il est important qu'Alice utilise, à chaque fois qu'elle envoie un message crypté à Bob avec la même clé, un k différent. En effet, si elle utilise le même k pour deux messages différents M et M', alors $M_1 = M_1'$. Un espion ayant intercepté les deux messages codés s'en apercevra et pourra calculer

$$M_2' - M_2 = M' - kB - (M - kB) = M' - M.$$

Supposons que pour une raison quelconque le message M soit rendu public dès que l'information n'est plus d'actualité, alors l'espion calculera sans peine M' qui vaut $M - M_2 + M_2'$.

2.3 Signature électronique d'ElGamal

Il nous reste un problème. Comment prouver à Bob que le message a bien été envoyé par Alice ? En effet, nous ne sommes pas sûrs de l'authenticité du message. Un imposteur ou un espion pourrait très bien se faire passer pour Alice en créant lui-même un système de clés privées et publiques et dire que ce sont les clés d'Alice. L'idée est de joindre au message une signature électronique, l'équivalent de l'autographe dans le monde physique, qui certifie au destinataire l'identité de l'expéditeur.

Nous allons présenter un modèle de signature basée sur les courbes elliptiques et réputé difficilement falsifiable. Ce modèle utilise les fonctions de hâchages, nous allons donc commencer par donner la définition de ces fonctions.

Définition 2.5. *Soient G et G' des ensembles quelconques, par exemple, pour ce qui va suivre $G = E(\mathbb{F}_q)$. Une fonction de hâchage H est une fonction*

$$H : G \to G'$$

telle que l'image par H de n'importe quel élément (grande longueur) est un élément ayant une longueur plus petite, par exemple, de 160 bits. De plus, elle doit satisfaire les propriétés suivantes :

1. *Pour un nombre n donné, $H(n)$ se calcule très rapidement.*
2. *Pour un nombre y donné, il est très difficile de trouver un nombre n tel que $H(n) = y$.*
3. *Il est très difficile de trouver deux nombres distincts n_1 et n_2 tels que*

$$H(n_1) = H(n_2).$$

(Dans ce cas, on dit que H est fortement sans collision).

Remarques. Les conditions 2 et 3 empêchent un espion de falsifier la signature. Il existe plusieurs bonnes fonctions de hâchages. Par exemple, la fonction MD5 est une fonction de hâchage inventée par Ron Rivest. Elle donne des "hâchés" de 128 bits. Des faiblesses ont été trouvées et son utilisation se raréfie ([7]). Une autre fonction de hâchage est la fonction SHA1. Elle renvoie une empreinte de 160 bits. C'est l'un des algorithmes les plus utilisés avec le MD5 ([4]).

Supposons donc qu'Alice envoie un message à Bob et qu'elle veuille signer électroniquement son message. Si elle utilise la signature ElGamal voici comment elle doit s'y prendre.

Alice doit tout d'abord créer une clé publique. Pour cela, elle choisit une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$, de manière que le problème du logarithme discret soit difficile sur $E(\mathbb{F}_q)$. Elle choisit aussi un point $A \in E(\mathbb{F}_q)$, tel que l'ordre n de A est un grand nombre premier. De plus, elle choisit un nombre secret a et calcule $B = aA$. Finalement, Alice choisit encore deux fonctions, une fonction de hâchage $H : \mathbb{N} \to \mathbb{N}$ et une fonction

$$f : E(\mathbb{F}_q) \to \mathbb{Z}.$$

Par exemple, si q est un nombre premier, elle peut prendre $f(x, y) = x \pmod q$. La fonction f doit avoir les propriétés suivantes :

- la cardinalité de $f(E(\mathbb{F}_q))$ doit être grande.
- un élément de l'image de f n'a qu'un petit nombre d'antécédents. (Par exemple, pour $f(x, y) = x$, il y a au plus deux points (x, y) qui ont pour image x.)

L'information publique d'Alice est $(E, \mathbb{F}_q, A, B, H, f)$. Elle garde secret le nombre a. L'ordre n de A n'est pas forcément gardé secret, cela n'entrave pas la sécurité du système. Pour signer son document, Alice fait comme suit :

1. Elle représente son document sous forme d'un nombre entier m et le hâche, c'est-à-dire calcule $H(m)$ (n étant un grand nombre premier, $H(m) \leq n$. Si tel n'est pas le cas, on sépare le message en morceaux $m_1, \ldots, m_k$ tels que chaque $H(m_i) \leq n, 1 \leq i \leq k$.).
2. Elle choisit un nombre entier k avec $\text{PGDC}(k, n) = 1$ et calcule
$$R = kA.$$
3. Elle calcule $s \equiv k^{-1}(H(m) - af(R)) \pmod{n}$.

Le message signé est (m, s, R). Si Alice veut garder son message secret, elle peut par exemple le crypter avec le RSA ([1]) et utiliser le message crypté au lieu de m.

Pour vérifier l'authenticité de la signature d'Alice, Bob procède de la manière suivante :

1. Il télécharge l'information publique d'Alice.
2. Il calcule
$$V_1 = f(R)B + sR \text{ et } V_2 = H(m)A.$$
3. Si $V_1 = V_2$ alors la signature est valide.

Montrons tout d'abord que si la signature est valide, alors $V_1 = V_2$.

$$\begin{aligned} V_1 &= f(R)B + sR \\ &= f(R)aA + (k^{-1}(H(m) - af(R)) + zn)kA \\ &= f(R)aA + (H(m) - af(R))A \\ &= H(m)A \\ &= V_2, \end{aligned}$$

où z est un nombre entier et nous utilisons le fait que l'ordre de A est n. C'est pour cela que nous définissons s modulo n.

En fait, $V_1 = V_2$ n'implique pas forcément que la signature soit valide mais il est très difficile de trouver un nombre s' tel que

$$f(R)B + s'R = H(m)A$$

sans connaître ni a, ni k. C'est l'utilisation de la fonction de hâchage qui nous garantit ceci.

Nous allons donner deux exemples où l'on peut falsifier la signature si nous n'utilisons pas de fonction de hâchage, i.e que nous utilisons m tel quel.

Exemple 1. Supposons que nous signions un message avec une signature ElGamal sans utiliser de fonction de hâchage. Le message signé est (m, R, s) comme ci-dessus, à ceci près que $s \equiv k^{-1}(m - af(R)) \pmod{n}$. Soit h un nombre entier tel que $\text{PGDC}(h, n) = 1$. Supposons que $\text{PGDC}(f(R), n) = 1$ et posons

$$\begin{aligned} R' &= hR, \\ s' &\equiv sf(R')f(R)^{-1}h^{-1} \pmod{n}, \\ m' &\equiv mf(R')f(R)^{-1} \pmod{n}. \end{aligned}$$

Alors (m', R', S') est une signature valide. En effet,

$$\begin{aligned} V_1 &= f(R')B + s'R' \\ &= f(R')aA + sf(R')f(R)^{-1}kA \\ &= f(R')aA + k^{-1}(m - af(R))f(R')f(R)^{-1}kA \\ &= mf(R')f(R)^{-1}A \\ &= m'A \\ &= V_2. \end{aligned}$$

Donc dans ce cas, il suffit que $\text{PGDC}(f(R), n) = 1$, pour qu'il soit possible de falsifier la signature. Par contre si Alice utilise une fonction de hâchage il est très difficile de trouver un nombre m' tel que

$$H(m') = H(m)f(R')f(R)^{-1} \pmod{n},$$

par la propriété 2 des fonctions de hâchage.

Exemple 2. Utilisons les mêmes notations que pour la signature ElGamal. Soient u, v deux entiers tels que $\text{PGDC}(v, n) = 1$ et $R = uA + vB$. Posons

$$s' \equiv -v^{-1}f(R) \pmod{n} \text{ et } m' \equiv su \pmod{n}.$$

Alors (m', R, s') est une signature valide. En effet,

$$\begin{aligned} V_1 &= f(R)B + s'R \\ &= f(R)B + (-v^{-1})f(R)R \\ &= f(R)v^{-1}(R - uA) - v^{-1}f(R)R \\ &= -f(R)v^{-1}uA \\ &= s'uA \\ &= m'A \\ &= V_2. \end{aligned}$$

Pour falsifier le message, il suffit de trouver un v tel que $\text{PGDC}(v, n) = 1$.

Là encore, si Alice utilise une fonction de hâchage, cette méthode ne fonctionne pas. Il faudrait pour cela trouver un nombre m' tel que $H(m') \equiv s'u \pmod{n}$ ce qui

est très difficile à cause de la propriété 2 des fonctions de hâchage.

Remarque. Dans la signature ElGamal, l'équation de vérification

$$f(R)B + sR = mA$$

requiert trois calculs d'un multiple d'un point. C'est la partie la plus coûteuse de l'algorithme. Il existe une variante de cette méthode qui ne fait que deux tels calculs. Voyons cette méthode.

Algorithme de signature digitale avec courbe elliptique Comme avant, Alice veut signer un message m qu'elle envoie à Bob. Pour cela, Alice choisit une courbe elliptique E définie sur un corps fini $\mathbb{F}_q$ telle que

$$\#E(\mathbb{F}_q) = fr,$$

où r est un grand nombre premier et f un petit nombre entier (généralement 1,2 ou 4) et une fonction de hâchage H. Elle choisit un point de base $B \in E(\mathbb{F}_q)$ ayant pour ordre r et un nombre entier secret a. Elle calcule $Q = aG$ et rend public

$$(\mathbb{F}_q, E, r, B, Q, H).$$

Pour signer le message m, Alice fait ce qui suit.

1. Elle choisit un nombre entier k tel que $1 \leq k < r$ et calcule $R = kB = (x, y)$.
2. Elle calcule $s \equiv k^{-1}(H(m) + ax) \pmod{r}$.

Le document signé est

$$(m, R, s).$$

Pour vérifier l'authenticité de la signature Bob fait ceci.

1. Il calcule $u_1 \equiv s^{-1}H(m) \pmod{r}$ et $u_2 \equiv s^{-1}x \pmod{r}$.
2. Il calcule $V = u_1B + u_2Q$.
3. Si $V = R$, la signature est valide.

Si le message est valide alors nous avons bien :

$$\begin{aligned} V &= u_1B + u_2Q \\ &= s^{-1}H(m)B + s^{-1}xQ \\ &= s^{-1}(H(m)B + xaB) \\ &= kB \\ &= R. \end{aligned}$$

Pour cette méthode aussi Alice doit choisir E tel que le problème du logarithme discret soit difficile à résoudre dans $E(\mathbb{F}_q)$.

Ici, il ne faut calculer que deux fois un multiple d'un point de la courbe.

2.4 Cryptosystème basé sur l'accouplement de Weil

Nous allons présenter ici une méthode due à Boneh et Franklin basée sur l'accouplement de Weil sur les courbes supersingulières. Nous verrons plus loin (paragraphe 3.2) que ces courbes donnent des cryptosystèmes moins solides mais ce qui nous intéresse ici c'est surtout la rapidité de calcul, en effet l'accouplement de Weil se calcule rapidement. De plus, il est intéressant de voir comment nous pouvons employer l'accouplement de Weil pour créer un cryptosystème.

Dans le système que nous allons décrire, chaque utilisateur possède une clé publique basée sur son identité, comme une adresse e-mail. Une autorité centrale assigne une clé privée à chaque utilisateur. Dans beaucoup de systèmes à clés publiques, lorsque Alice veut envoyer un message à Bob, elle vérifie l'authenticité de la clé publique de Bob. Il lui faut donc un moyen d'être sûr que cette clé appartienne bien à Bob, que se ne soit pas un imposteur qui se fait passer pour Bob. Dans le système présenté ici, l'authentification se fait lors de la première communication entre Bob et l'autorité centrale. Après cela, Bob est le seul possédant l'information nécessaire pour décrypter les messages encryptés avec sa clé publique.

Nous allons décrire comment se déroule ce cryptosystème.

L'autorité centrale fait ce qui suit.

1. Elle choisit un grand nombre premier $p = 6l - 1$, $p \geq 5$ (ainsi $p \equiv 2 \pmod 3$), où l est aussi premier.
2. Elle choisit une courbe elliptique $E : y^2 = x^3 + b$ avec $b \in \mathbb{F}_p^*$ un carré[1].
3. Elle choisit un point $P \in E(\mathbb{F}_p)$ d'ordre l. (Ceci n'est pas très difficile puisque en prenant un point quelconque $K \in E(\mathbb{F}_p)$, $6K$ est soit d'ordre 1, soit d'ordre l).
4. Elle choisit deux fonctions de hâchages $H_1 : \mathbb{N} \to E[l]$ et $H_2 : \mathbb{F}_{p^2}^* \to \mathbb{N}$. La fonction H_2 renvoie une valeur de longueur n, où n est la longueur du message qui va être envoyé.
5. Elle choisit une valeur secrète $s \mod l$, avec $s \not\equiv 0 \pmod l$ et calcule
$$P_{pub} = sP.$$
6. Elle rend publique $p, H_1, H_2, n, P, P_{pub}$ et garde s secret.

Remarques .

Nous allons, ce qui suit, utiliser l'application β définie dans le lemme 2.2.

Par le lemme 2.3, $e_n(P, \beta(P))$ est une racine primitive $n^{\text{ème}}$ de l'unité.

Puisque E est supersingulière et $q \geq 5$, l'ordre de $E(\mathbb{F}_p)$ est $p + 1$. Supposons maintenant que $q = 6l - 1$ pour ce qui suit, avec l un nombre premier. Alors $6P$ est d'ordre soit l, soit 1 pour tout $P \in E(\mathbb{F}_p)$. Il est donc facile de trouver des points d'ordre 6.

[1] Cette courbe elliptique est supersingulière par la proposition 1.17.

Si un utilisateur ayant l'identité ID veut une clé privée, l'autorité centrale fait ce qui suit.

1. Elle calcule $Q_{ID} = H_1(ID)$ qui est un point sur E d'ordre l.
2. Elle calcule $D_{ID} = sQ_{ID}$.
3. Après avoir vérifié que ID est bien l'identification de l'utilisateur avec qui elle communique, elle envoie D_{ID} à celui-ci.

Si Alice veut envoyer un message M à Bob elle fait ce qui suit.

1. Alice regarde l'identité de Bob, par exemple $ID = bob@epfl.ch$ (écrit en binaire) et calcule $Q_{ID} = H_1(ID)$.
2. Elle choisit un entier $r \mod l$, avec $r \not\equiv 0 \pmod{l}$.
3. Elle calcule $g_{ID} = e_l(Q_{ID}, \beta(P_{pub}))$.
4. Le message crypté est la paire

$$c = (rP, M \oplus H_2(g_{ID}^r)),$$

où $\oplus$ signifie l'addition bit par bit mod 2.

On remarque, puisque E est supersingulière, $E[l] \subset E(\mathbb{F}_{p^2})$ (proposition 3.1). $H_2(g_{ID}^r)$ est donc bien défini car $\mu_l \subset \mathbb{F}_{p^2}^*$ par le corollaire 1.10.

Pour décrypter le message $c = (u, v)$ Bob fait ce qui suit.

1. Il utilise sa clé privé D_{ID} pour calculer $h_{ID} = e_l(D_{ID}, \beta(u))$.
2. Il calcule $m = v \oplus H_2(h_{ID})$.

Bob retrouve bien le message M car

$$e_l(D_{ID}, \beta(u)) = e_l(sQ_{ID}, \beta(rP)) = e_l(Q_{ID}, \beta(P))^{sr} = e_l(Q_{ID}, \beta(P_{pub}))^r = g_{ID}^r.$$

Ainsi

$$m = v \oplus H_2(e_l(D_{ID}, \beta(u))) = (M \oplus H_2(g_{ID}^r)) \oplus H_2(g_{ID}^r) = M.$$

Remarque. Ce système n'est pas sécurisé contre certaines attaques (voir [3] p.174).

Chapitre 3

Le problème du logarithme discret

Nous allons, dans ce chapitre, traiter du problème du logarithme discret. Nous présenterons plusieurs méthodes qui permettent, dans certains cas, de résoudre ce problème. En effet, puisque le cryptage des messages avec des courbes elliptiques se base sur la difficulté de résoudre le problème du logarithme discret en un temps raisonnable généralement, il est important de savoir dans quels cas nous pouvons le résoudre rapidement pour éviter ces cas là. Nous parlerons plus précisément du Baby Step, Giant Step qui est apparemment l'un des algorithmes les plus efficaces ([3]) ; mais nous parlerons aussi de l'algorithme MOV qui ramène le problème au cas du logarithme discret dans $\mathbb{F}_{p^m}^*$ pour un certain nombre premier p.

3.1 Baby Step, Giant Step

Cette méthode, développée par D. Shanks ([3] p.136), fait environ $\sqrt{N}$ pas et stocke environ $\sqrt{N}$ données. C'est pourquoi elle ne fonctionne bien que pour des N de taille modérée.

Par commodité, dans ce paragraphe, nous exposons la méthode du Baby Step, Giant Step pour un groupe de la forme $E(\mathbb{F}_q)$ avec E une courbe elliptique sur $\mathbb{F}_q$ mais elle est valable pour un groupe quelconque.
Nous supposerons qu'il existe un nombre entier k tel que $Q = kP$ avec $P, Q \in E(\mathbb{F}_q)$ et que N, l'ordre de E, est connu.

L'algorithme se déroule comme suit :

1. Choisir un entier $m \geq \sqrt{N}$ et calculer mP.
2. Calculer et stocker dans une liste les iP pour $0 \leq i < m$.
3. Calculer les points $Q - jmP$ pour $j = 0, 1, \ldots, m-1$ jusqu'à ce qu'un de ces éléments correspondent à un iP de la liste précédente.
4. Si $iP = Q - jmP$, nous avons $Q = kP$ avec $k \equiv i + jm \pmod{N}$.

Nous allons maintenant regarder pourquoi cet algorithme fonctionne. Puisque $m^2 > N$, nous avons $0 \leq k < m^2$. Ecrivons $k = k_0 + mk_1$, ainsi $k \equiv k_0 \pmod{m}$ avec $0 \leq k_0 < m$ et $k_1 = (k - k_0)/m$ et donc $0 \leq k_1 < m$. Posons $i = k_0$ et $j = k_1$, nous obtenons donc

$$Q - k_1 mP = kP - k_1 mP = k_0 P$$

est la relation voulue.

Le point iP est calculé en ajoutant P ("baby step") à $(i-1)P$. Le point $Q - jmP$ est trouvé en ajoutant $-mP$ ("giant step") à $Q - (j-1)mP$.

Remarquons que nous ne devons pas connaître l'ordre exact de $E(\mathbb{F}_q)$. Nous devons juste connaître une borne supérieure de N. Ainsi pour une courbe elliptique définie sur un corps fini $\mathbb{F}_q$, nous pouvons prendre un m tel que

$$m^2 \geq q + 1 + 2\sqrt{q}$$

par le théorème de Hasse.

Donnons un exemple pour illustrer ceci :

Exemple. Soit $G = E(\mathbb{F}_{41})$, où E est donné par

$$y^2 = x^3 + 2x + 1.$$

Soient $P = (0, 1)$ et $Q = (30, 40)$. Par le théorème de Hasse, nous savons que l'ordre de G est au plus 56, posons $m = 8$. Les points iP pour $0 \leq i \leq 7$ sont

$$(0, 1), (1, 39), (8, 23), (38, 38), (23, 23), (20, 28), (26, 9).$$

Calculons $Q - jmP$ pour $j = 0, 1, 2$

$$(30, 40), (9, 25), (26, 9),$$

où nous nous arrêtons puisque le troisième point correspond à $7P$. Nous avons donc

$$Q = (7 + 2 \cdot 8)P = 23P$$

et nous trouvons $k = 23$.

3.2 L'algorithme MOV

Nous allons, maintenant, présenter un algorithme spécifique pour résoudre le problème du logarithme discret dans le cas des courbes elliptiques, contrairement à l'algorithme précédent qui peut être utilisé sur un groupe quelconque.

Le MOV, développé par Menezes, Okamoto et Vanstone ([3] p.144), utilise l'accouplement de Weil pour transformer un problème de logarithme discret dans $E(\mathbb{F}_q)$ en un problème de logarithme discret dans $\mathbb{F}_{q^m}^*$ pour un certain entier m. Puisque le problème du logarithme discret sur un corps fini peut être résolu par la méthode du calcul d'index, il peut être résolu plus vite sur $\mathbb{F}_{q^m}^*$ que sur $E(\mathbb{F}_q)$ tant que $\#\mathbb{F}_{q^m}^*$

n'est pas beaucoup plus grand que $\#\mathbb{F}_q^*$.

En fait, l'entier m de $E(\mathbb{F}_{q^m})$ peut très bien être grand, auquel cas le problème du logarithme discret dans le groupe $\mathbb{F}_{q^m}^*$, qui est d'ordre $q^m - 1$, est aussi difficile à résoudre que le problème du logarithme discret dans $E(\mathbb{F}_q)$, qui a un ordre d'environ q, par le théorème de Hasse. Par contre, pour une courbe supersingulière, nous pouvons en général prendre $m = 2$, comme nous allons le montrer par suite.

Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soient $P, Q \in E(\mathbb{F}_q)$ et N l'ordre de P. Supposons que

$$\mathrm{PGDC}(q, N) = 1.$$

Nous cherchons un entier k tel que $Q = kP$. Le lemme 2.4 page 14 nous permet de voir si un tel k existe.

Puisque tout point de $E[N]$ a ses coordonnées dans $\overline{\mathbb{F}}_q = \bigcup_{j\geq 1} \mathbb{F}_{q^j}$, il existe un m tel que

$$E[N] \subseteq E(\mathbb{F}_{q^m}).$$

Par le corollaire 1.10, le groupe μ_N des racines $N^{\text{ème}}$ de l'unité est alors contenu dans $\mathbb{F}_{q^m}$.

L'algorithme MOV se déroule ainsi.

1. Choisir un point $T \in E(\mathbb{F}_{q^m})$.
2. Calculer M, l'ordre de T.
3. Soit $d = \mathrm{PGDC}(M, N)$. Posons $T_1 = (M/d)T$, l'ordre de T_1 est d. Celui-ci divise N, ainsi $T_1 \in E[N]$.
4. Calculer $\zeta_1 = e_N(P, T_1)$ et $\zeta_2 = e_N(Q, T_1)$. Donc ζ_1 et ζ_2 sont dans $\mu_d \subseteq \mu_N \subseteq \mathbb{F}_{q^m}^*$. En effet,

   $$1 = e_N(P, O) = e_N(P, dT_1) = e_N(P, T_1)^d = \zeta_1^d,$$

   idem pour ζ_2.
5. Résoudre le problème du logarithme discret pour

   $$\zeta_2 = \zeta_1^k$$

   dans $\mathbb{F}_{q^m}^*$. Nous trouvons $k \pmod d$.
6. Recommencer avec des points T choisis au hasard jusqu'à ce que nous ayons $\mathrm{PGDC}(M, N) = N$. Ceci détermine $k \pmod N$.

Remarque. A priori, on pourrait penser que le cas $d = 1$ apparaisse très fréquemment. En réalité, il se passe le contraire. Voyons pourquoi.
Rappelons que

$$E(\mathbb{F}_{q^m}) \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z}$$

pour des entiers n_1, n_2 tels que $n_1 | n_2$. Ainsi $N | n_2$, puisque n_2 est l'ordre le plus grand possible pour un élément du groupe $E(\mathbb{F}_{q^m})$. Soient B_1, B_2 des points d'ordres n_1, n_2 respectivement tels qu'ils engendrent $E(\mathbb{F}_{q^m})$. Nous pouvons donc écrire

$$T = a_1 B_1 + a_2 B_2.$$

Soit $l^e|N$ avec l premier. Donc $l^f|n_2$ avec $f \geq e$. Si $l \nmid a_2$, alors $l^f|M$, l'ordre de T. En effet,

$$O = MT = Ma_1B_1 + Ma_2B_2,$$

puisque B_1, B_2 engendrent $E(\mathbb{F}_{q^m})$, cela implique que $Ma_1B_1 = Ma_2B_2 = O$ et donc que $n_2|Ma_2$, de plus $l \nmid a_2$ et $l^f|n_2$, donc $l^f|M$. Ainsi $l^e|d$, avec $d = \text{PGDC}(M, N)$. La probabilité que $l \nmid a_2$ est de $1 - 1/l$, et donc la probabilité que $d \neq 1$ est au moins $1 - 1/l$. Ainsi, après avoir choisi plusieurs T différents nous devrions trouver un $d \neq 1$, et après quelques itérations de l'algorithme trouver k.

Montrons maintenant que dans le cas d'une courbe elliptique supersingulière nous pouvons, en général, prendre $m = 2$.

Soit E une courbe elliptique définie sur $\mathbb{F}_q$, où q est la puissance d'un nombre premier p. Alors

$$\#E(\mathbb{F}_q) = q + 1 - a,$$

où a est un entier. Rappelons qu'une courbe E est appelée supersingulière si $a \equiv 0 \pmod{p}$. Nous savons aussi ([3] p.121) que ceci est équivalent à $a = 0$ lorsque $q \geq 5$ et q est premier.

Proposition 3.1. *Soit E une courbe elliptique sur $\mathbb{F}_q$ et supposons que $a = 0$, i.e. E est supersingulière. Soit N un nombre entier positif premier à p où $q = p^j$. S'il existe un point $P \in E(\mathbb{F}_q)$ d'ordre N, alors*

$$E[N] \subseteq E(\mathbb{F}_{q^2}).$$

Preuve. L'endomorphisme de Frobenius (1.12) ϕ_q satisfait la relation

$$\phi_q^2 - a\phi_q + q = 0.$$

Puisque $a = 0$ par hypothèse, nous avons $\phi_q^2 = -q$. Soit $S \in E[N]$, puisque $\#E(\mathbb{F}_q) = q + 1$ et qu'il existe un point d'ordre N, nous avons $N|(q + 1)$, c'est-à-dire $-q \equiv 1 \pmod{N}$. Ainsi

$$\phi_q^2(S) = -qS = S.$$

Par le lemme 1.13, $S \in E(\mathbb{F}_{q^2})$ car $\phi_q^2 = \phi_{q^2}$. □

Ainsi, l'algorithme MOV est très efficace lorsque $E(\mathbb{F}_q)$ est supersingulière et que $a = 0$ puisque nous pouvons nous ramener à un problème de logarithme discret sur $\mathbb{F}_{q^2}$.

3.3 Courbes à anomalies

Etant donné que nous savons résoudre le problème du logarithme discret sur les courbes supersingulières, nous pourrions espérer qu'il soit difficile pour les courbes ordinaires. En fait, il y a encore une classe de courbes elliptiques pour laquelle nous savons résoudre le problème du logarithme discret e même encore lus facilement que pour les courbes supersingulières.

Définition 3.2. *Une courbe elliptique E définie sur $\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = q$ s'appelle une courbe à anomalie.*

Malheureusement, le problème du logarithme discret peut être résolu très facilement sur une telle courbe. Nous allons ici voir comment nous pouvons résoudre ce problème dans le cas d'une courbe à anomalie.

Nous ne traiterons que le cas $q = p$, où p est un nombre premier.

Remarquons encore que le fait d'être à anomalie dépend du corps sur lequel la courbe est définie. Si E est à anomalie sur $\mathbb{F}_q$, elle ne l'est pas forcément sur $\mathbb{F}_{q^n}$, avec $n \geq 2$. Ceci contraste avec le fait d'être super singulier, qui est bel et bien une propriété de la courbe elliptique définie sur une clôture algébrique.

Nous devons tout d'abord relever la courbe elliptique E définie sur $\mathbb{F}_p$ et les points $P, Q \in E(\mathbb{F}_p)$ sur une courbe elliptique sur $\mathbb{Z}$. Ceci est possible par la proposition qui suit.

Proposition 3.3. *Soient E une courbe elliptique sur $\mathbb{F}_p$ et $P, Q \in E(\mathbb{F}_p)$. Supposons que E soit écrite sous la forme d'une équation de Weierstrass $y^2 = x^3 + Ax + B$. Alors il existe des entiers $\tilde{A}, \tilde{B}, x_1, x_2, y_1, y_2$ et une courbe elliptique $\tilde{E}$ donnée par*

$$y^2 = x^3 + \tilde{A}x + \tilde{B}$$

telle que $\tilde{P} = (x_1, y_1), \tilde{Q} = (x_2, y_2) \in \tilde{E}(\mathbb{Z})$ et telle que

$$A \equiv \tilde{A},\ B \equiv \tilde{B},\ P \equiv \tilde{P},\ Q \equiv \tilde{Q} \pmod{p}.$$

Nous ne faisons pas la preuve ici ([3] pp.147-148).

Remarque. Si nous avons la relation $Q = kP$ pour un certain entier k, nous n'avons pas, en général, $\tilde{Q} = k\tilde{P}$ dans $\tilde{E}$. Ce qui est remarquable sur les courbes à anomalies est que malgré que même si $\tilde{Q}$ et $\tilde{P}$ sont indépendants, nous pouvons obtenir suffisamment d'informations pour trouver k.

Définition 3.4. *Soit $a/b \neq 0$ un nombre rationnel, où a, b sont des entiers premiers entre eux. Ecrivons $a/b = p^r a_1/b_1$ avec p premier et $p \nmid a_1 b_1$. On définit la valuation p-adic comme suit*

$$v_p(a/b) = r.$$

On pose $v_p(0) = +\infty$.

Par exemple,

$$v_2(7/40) = -3,\ v_3(9/2) = 2,\ v_{13}(8/5) = 0.$$

Soit $\tilde{E}$ une courbe elliptique sur $\mathbb{Z}$ donnée par $y^2 = x^3 + \tilde{A}x + \tilde{B}$. Soit $r \geq 1$ un entier. On pose

$$\tilde{E}_r = \big\{(x, y) \in \tilde{E}(\mathbb{Q}) \big| v_p(x) \leq -2r, v_p(y) \leq -3r\big\} \cup \big\{0\big\}.$$

C'est l'ensemble des points tels que x a au moins le facteur p^{2r} au dénominateur et y au moins le facteur p^{3r} au dénominateur. Il est clair que

$$\tilde{E}_r \supseteq \tilde{E}_{r+1} \supseteq \cdots .$$

Théorème 3.5. *Soit $\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$, avec $\tilde{A}, \tilde{B}$ des entiers. Soient encore p un nombre premier et r un entier positif. Alors*

1. *$\tilde{E}_1$ est un sous-groupe de $\tilde{E}(\mathbb{Q})$.*
2. *Si $(x, y) \in \tilde{E}(\mathbb{Q})$, alors $v_p(x) < 0$ si et seulement si $v_p(y) < 0$. Dans ce cas, il existe un entier $r \geq 1$ tel que $v_p(x) = -2r, v_p(y) = -3r$.*
3. *L'application*

$$\begin{aligned} \lambda_r : \tilde{E}_r/\tilde{E}_{5r} &\to \mathbb{Z}/p^{4r}\mathbb{Z} \\ (x, y) &\mapsto p^{-r}x/y \pmod{p^{4r}} \\ O &\mapsto O \end{aligned}$$

   est un homomorphisme injectif.
4. *Si $(x, y) \in \tilde{E}_r$ mais que $(x, y) \notin \tilde{E}_{r+1}$, alors $\lambda_r(x, y) \not\equiv 0 \pmod{p}$.*

Nous ne faisons pas la preuve ici ([3] pp.189-197). Nous allons par contre vérifier si λ_r est bien définie.

Par l'assertion 1 du théorème, nous savons que $\tilde{E}_1 \subseteq \tilde{E}(\mathbb{Q})$. Nous savons aussi par l'assertion 2 que si $(x, y) \in \tilde{E}_1$, alors il existe un $r \geq 1$ tel que $v_p(x) = -2r$ et $v_p(y) = -3r$. Ainsi si $(a/b, c/d) \in \tilde{E}_r$ mais $(a/b, c/d) \notin \tilde{E}_{5r}$ où a, b, c, d sont des entiers non nuls, alors $a/b = p^{-2ir}a_1/b_1, c/d = p^{-3ir}c_1/d_1$, avec $p \nmid a_1b_1c_1d_1$ et $i = 1, 2, 3, 4$. Nous avons donc

$$\begin{aligned} \lambda_r(a/b, c/d) &= p^{-r}p^{-2ir}p^{3ir}a_1b_1^{-1}d_1c_1^{-1} \pmod{p^{4r}} \\ &= p^{(i-1)r}a_1b_1^{-1}c_1d_1^{-1} \pmod{p^{4r}} \end{aligned}$$

Remarquons encore que b_1, d_1 sont bien inversible dans $\mathbb{Z}/p^{4r}\mathbb{Z}$ car

$$\mathrm{PGDC}(b_1, p) = \mathrm{PGDC}(d_1, p) = 1$$

et que λ_r est bien injectif car $\lambda(x, y) = 0$ si $i \geq 5$.

Il nous faut encore énoncer une proposition que nous ne montrerons pas non plus ([3] p.66).

Proposition 3.6. *On définit la réduction modulo p comme suit :*

$$\begin{aligned} \mathrm{red}_p : \tilde{E}(\mathbb{Q}) &\to \tilde{E} \pmod{p} \\ (x, y) &\mapsto (x, y) \pmod{p} \text{ si } (x, y) \notin \tilde{E}_1 \\ \tilde{E}_1 &\to \{O\}. \end{aligned}$$

L'application red_p *est un homomorphisme dont le noyau est $\tilde{E}_1$.*

Nous pouvons, maintenant, regarder comment et pourquoi marche l'algorithme pour résoudre les problèmes de logarithme discret dans le cas de courbes à anomalies. Soient E une courbe elliptique sur $\mathbb{F}_p$ à anomalies, $P, Q \in E(\mathbb{F}_p)$. Nous cherchons k tel que $Q = kP$. Supposons que $k \neq 0$. Puisque E est une courbe à anomalie sur $\mathbb{F}_q$, $\#E(\mathbb{F}_p) = p$. L'algorithme se déroule ainsi :

1. Relever E, P, Q dans $\mathbb{Z}$ pour obtenir $\tilde{E}, \tilde{P}, \tilde{Q}$ comme dans la proposition 3.3.
2. Soient $\tilde{P}_1 = p\tilde{P}, \tilde{Q}_1 = p\tilde{Q}$. Remarquons que $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1$ puisque
$$\mathrm{red}_p(p\tilde{P}) = p \cdot \mathrm{red}_p(\tilde{P}) = O$$
(car E est une courbe à anomalie sur $\mathbb{F}_q$).
3. Si $\tilde{P}_1 \in \tilde{E}_2$, choisir des nouveaux $\tilde{E}, \tilde{P}, \tilde{Q}$ et réessayer. Sinon, soient $l_1 = \lambda_1(\tilde{P}_1)$ et $l_2 = \lambda_1(\tilde{Q}_1)$, l_1, l_2 sont bien définis puisque $\tilde{P}_1, \tilde{Q}_1 \in \tilde{E}_1$. Nous avons
$$k \equiv l_2 l_1^{-1} \pmod{p}.$$

Remarquons que l_1 est inversible modulo p car $\tilde{P}_1 \notin E_2$, ce qui veut dire que la puissance de p de $\lambda_1(\tilde{P}_1)$ est 0.

Pourquoi est-ce que ça marche ? Soit $\tilde{K} = k\tilde{P} - \tilde{Q}$. Nous avons :
$$0 = kP - Q = \mathrm{red}_p(k\tilde{P} - \tilde{Q}) = \mathrm{red}_p(\tilde{K}).$$
Ainsi $\tilde{K} \in \tilde{E}_1$ et donc $\lambda_1(\tilde{K})$ est défini et
$$\lambda_1(p\tilde{K}) = p\lambda_1(\tilde{K}) \equiv 0 \pmod{p}.$$
Ainsi,
$$kl_1 - l_2 = \lambda_1(k\tilde{P}_1 - \tilde{Q}_1) = \lambda_1(kp\tilde{P} - p\tilde{Q}) = \lambda_1(p\tilde{K}) \equiv 0 \pmod{p}.$$
Ce qui veut dire que $k \equiv l_2 l_1^{-1} \pmod{p}$.

Il faut noter que le fait que E soit à anomalies est crucial. En effet, si $E(\mathbb{F}_p)$ est d'ordre n, nous devons multiplier $\tilde{P}, \tilde{Q}$ par n pour les amener dans $\tilde{E}_1$, où λ_1 est défini. La différence $\tilde{K} = k\tilde{P} - \tilde{Q}$ doit aussi être multiplié par n. Si n est un multiple de p, nous avons $\lambda_1(n\tilde{K}) \equiv 0 \pmod{p}$ et la contribution de $\tilde{K}$ disparaît de nos calculs.

Si p est un grand nombre premier, nous rencontrons des difficultés lors de l'implémentation de l'algorithme parce que les coordonnées du point $\tilde{P}_1$ sont des nombres trop grands pour être manipulés rapidement par un ordinateur. Dans ce cas il faut utiliser un autre algorithme que nous ne développerons pas ici (voir [3] pp.150-152).

Remarque. Nous pouvons très facilement calculer la multiplication par un entier d'un point de $E(\overline{\mathbb{F}}_q)$ si E est une courbe anomalie sur $\mathbb{F}_q$, où $q = p^r$, p un nombre premier.

Soit E, une courbe elliptique définie à anomalie sur $\mathbb{F}_q$. Alors, l'endomorphisme de Frobenius ϕ_q satisfait l'équation suivante :
$$\phi_q^2 - \phi_q + q = O,$$
puisque $a = q + 1 - \#E(\mathbb{F}_q) = 1$. Nous avons donc $q = \phi_q - \phi_q^2$. Ainsi
$$q(x, y) = (x^q, y^q) + (x^{q^2}, -y^{q^2}) \text{ pour tout } (x, y) \in E(\overline{\mathbb{F}}_q).$$

Le calcul de x^q est très rapide dans un corps fini. Ainsi, contrairement à la méthode standard (voir [3] p.18), la multiplication par q est à peine plus coûteuse qu'une seule addition de deux points. Dans ce cas, pour calculer kP pour un entier k, on exprime $k = k_0 + k_1 q + k_2 q^2 + \cdots + k_g q^g$ en base q, puis on calculons $k_i P$ pour chaque $i = 0, \ldots, g$, puis $q^i k_i P$, pour finalement les additionner ensemble et obtenir kP.

Chapitre 4

Factorisation et primalité

Deux autres applications des courbes elliptiques sont indirectement utilisées en cryptographie. Par exemple, le système de cryptage RSA ([1]) se base sur le fait qu'il est difficile de factoriser de grands nombres et nécessite de grands nombres premiers pour fabriquer la clé publique. Il nous faut donc d'un côté des tests de primalité pour être sûr que les nombres que nous employons sont bien premiers. D'un autre côté si nous voulons décrypter un message codé avec le RSA sans avoir la clé privée, un des moyens est de savoir factoriser les grands nombres. Nous allons ici présenter une méthode de factorisation et un test de primalité utilisant toutes les deux les courbes elliptiques.

4.1 Factoriser avec des courbes elliptiques

Dans les années 1980, un algorithme de factorisation utilisant les courbes elliptiques a été mis au point. Il s'est vite avéré que cet algorithme est très efficace pour factoriser les nombres de l'ordre de 10^{60} et pour les nombres plus grands s'ils ont des facteurs premiers de l'ordre de 10^{20} à 10^{30}.

Remarque. Dans cette partie, nous allons regarder les courbes elliptiques sur des anneaux $\mathbb{Z}/n\mathbb{Z}$ de manière naïve, c'est-à-dire en réduisant les coefficients des courbes elliptiques et les coordonnées des points sur ces courbes modulo n. C'est pourquoi nous n'utiliserons pas la notation $E(\mathbb{Z}/n\mathbb{Z})$ mais $E \pmod{n}$.

L'idée est de regarder une courbe elliptique E sur l'anneau $\mathbb{Z}/n\mathbb{Z}$, où n est le nombre que nous voulons factoriser, mais de manière naïve, c'est-à-dire que pour additionner deux points nous calculons la pente de la droite passant par ces points et la réduisons modulo n. Il est clair que si n n'est pas premier, cette pente n'existera pas toujours car les nombres qui ne sont pas premiers avec n ne sont pas inversibles modulo n. L'idée clé de cette méthode est justement se retrouver dans une telle situation. En effet, dans ce cas nous aurons une pente dont le dénominateur d n'est pas inversible modulo n, ce qui veut dire que $\mathrm{PGDC}(n, d) \neq 1$ et nous aurons trouvé un facteur non trivial de n.

Rappelons (théorème 1.22) tout d'abord que si $n_1, n_2 \in \mathbb{Z}$ sont premiers entre

eux, alors

$$E(\mathbb{Z}/n_1n_2\mathbb{Z}) \cong E(\mathbb{Z}/n_1\mathbb{Z}) \oplus E(\mathbb{Z}/n_2\mathbb{Z}).$$

Soit $n = p_1^{e_1} \cdots p_r^{e_r}$ le nombre que nous voulons factoriser et p_1, p_r les facteurs premiers distincts de n. Soient une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$ et un point P sur E. Nous voulons trouver un nombre entier k tel que $kP = O \pmod{p_i^{e_i}}$ pour un $1 \leq i \leq r$ mais pas pour tout les i. En effet, lorsque nous calculons kP sur $E \pmod{n}$ de manière naïve, nous n'y arrivons pas parce que nous avons $kP = O$ modulo $p_i^{e_i}$ pour un certain i. C'est pourquoi la pente de la droite entre $(k-1)P$ et kP modulo $p_i^{e_i}$ vaut 0 et donc la pente aura pour dénominateur un multiple de $p_i^{e_i}$. Pour cette raison il faut qu'il y ait au moins un i entre 1 et r qui ne satisfasse pas $kP = O$ modulo $p_i^{e_i}$, sinon nous aurions pour dénominateur de la pente un multiple de n lui-même, ce qui ne nous avance pas beaucoup.

En fait, il est difficile de trouver un tel k pour une courbe elliptique particulière. Par contre, comme nous le verrons plus loin, si nous essayons avec suffisamment de courbes nous avons une forte probabilité d'avoir une courbe où ça marche.

Donnons un exemple pour illustrer ceci.

Exemple. Nous voulons factoriser 4453. Soit E la courbe elliptique d'équation

$$y^2 = x^3 + 3x \pmod{4453}$$

et soit $P = (1, 2)$. Essayons de calculer $6P$. Calculons tout d'abord $2P$, la pente de la tangente au point P est

$$\frac{3x^2 + 3}{2y} = \frac{3}{2} \equiv 2228 \pmod{4453}.$$

En effet $\text{PGDC}(2, 4453) = 1$, donc 2 est inversible mod 4453 et $2^{-1} \equiv 2227 \pmod{4453}$. Utilisant la pente, nous trouvons $2P = (x, y)$, avec

$$x \equiv 3340,\ y \equiv 1669 \pmod{4453}.$$

Nous calculons maintenant $3P$ en additionnant P et $2P$. La pente est

$$\frac{1669 - 2}{3340 - 1} = \frac{1667}{3339} \equiv 746 \pmod{4453}.$$

En effet $\text{PGDC}(3339, 4453) = 1$, donc 3339 est inversible modulo 4453 et

$$3339^{-1} \equiv 1483 \pmod{4453}.$$

Nous pouvons donc trouver $3P = (x, y)$ avec

$$x \equiv 1003,\ y \equiv 610 \pmod{4453}.$$

Calculons maintenant $6P = 3P + 3P$. Si nous regardons le dénominateur de la pente, qui est $2 \cdot 610 = 1220$, nous voyons $\text{PGDC}(1220, 4453) = 61 \neq 1$. Ainsi nous ne pouvons pas inverser 1220 modulo 4453 et ne pouvons pas trouver la pente

voulue. Par contre, nous avons trouvé que 61 est un facteur de 4453 et nous pouvons factoriser $4453 = 61 \cdot 73$.

Nous avons que :

$$E(\mathbb{Z}/4453\mathbb{Z}) \cong E(\mathbb{Z}61\mathbb{Z}) \oplus E(\mathbb{Z}/73\mathbb{Z}).$$

Regardons les multiples de $P \pmod{61}$

$$P \equiv (1,2), 2P \equiv (46,22), 3P \equiv (27,0), 6P = O, \ldots \pmod{61}.$$

Les multiples de $P \pmod{73}$ sont

$$P \equiv (1,2), 2P \equiv (55,63), 3P \equiv (54,26), 6P \equiv (65,11), \ldots \pmod{73}.$$

Ainsi, lorsque nous calculons $6P \pmod{4453}$, nous obtenons O modulo 61 et un point fini modulo 73 .

Pour factoriser un nombre n par la méthode des courbes elliptiques il nous faut donc différentes courbes elliptiques E_i définies sur $\mathbb{Z}/n\mathbb{Z}$ et des points P_i sur ces courbes. Un moyen pour trouver ceci est de choisir des entiers $A_i \pmod{n}$ et un point $P_i = (u_i, v_i) \pmod{n}$. Nous définissons ensuite les C_i tels que

$$C_i = v_i^2 - u_i^3 - Au \pmod{n}.$$

Nous obtenons ainsi des courbes elliptiques $E_i : y^2 = x^3 + A_i x + C_i$ avec un point P_i. Cette méthode est beaucoup plus efficace que de choisir des entiers A_i, C_i, u_i et ensuite de chercher v_i puisque calculer la racine carrée $\mod n$ est équivalent à factoriser n ([3] p.182).

Algorithme. Pour factoriser un entier n avec la méthode des courbes elliptiques nous pouvons procéder comme suit :

1. Choisir entre dix et vingt courbes elliptiques $E_i : y^2 = x^3 + A_i x + C_i$ et des points $P_i \pmod{n}$ sur les courbes E_i par la méthode énoncée ci-dessus.
2. Choisir un entier B (de l'ordre de 10^8) et calculer $(B!)P_i$ sur E_i pour chaque i.
3. Si l'étape 2. bloque parce que l'une des pentes n'existe pas $\mod n$, alors nous avons trouver un facteur de n.
4. Sinon augmenter la valeur de B ou recommencer à l'étape 1.

Cette méthode est très efficace pour trouver des facteurs premiers p de n lorsque $p < 10^{40}$. Les valeurs de n qui sont utilisées en cryptographie sont généralement choisies telles que $n = pq$ avec p et q de l'ordre de 10^{75}. Dans ce cas, cette méthode n'est plus efficace et il faut avoir recours à des méthodes plus performantes.

Regardons pourquoi cette méthode fonctionne dans le cas $n = p_1 \cdots p_r$ où les p_i sont des nombres premiers pour $1 \leq i \leq r$. Commençons par donner une définition.

Définition 4.1. *Soit m, B des entiers positifs. On dit que m est B-lisse si tous les facteurs premiers de m sont inférieurs ou égaux à B.*

Remarque. Si m n'a aucun facteur premier p tel que $B/2 \leq p^2 \leq B$, alors m divise $B!$.

Une courbe elliptique $E \pmod n$ peut être regardée comme une courbe elliptique mod p_i. Nous savons par le théorème de Hasse que

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p}.$$

En fait, on peut montrer ([3] p.183) que pour tout élément a dans l'intervalle

$$(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}),$$

il existe une courbe elliptique E telle que $\#E(\mathbb{F}_p) = a$

Soit p_k un des diviseur premier de n. Si nous choisissons un entier B de taille raisonnable alors la densité des entiers B-lisse dans cet intervalle est assez grande. Ainsi il y aura suffisamment de courbes elliptiques E qui ont un ordre B-lisse et donc si nous prenons plusieurs courbes elliptiques, il y en aura probablement une ayant un ordre B-lisse. A supposer que l'ordre de cette courbe elliptique E ne soit pas divisible par le carré d'un nombre premier supérieur ou égal à $B/2$, nous avons

$$(B!)P = O \pmod{p_k},$$

où P est un point de la courbe E. Il est peu probable que nous ayons

$$(B!)P = O \pmod{p_j},$$

pour un $j \neq k, 1 \leq j \leq r$. Ainsi lorsque nous calculons $(B!)P \pmod n$, nous trouverons une pente dont le dénominateur d est divisible par p_k mais pas par les autres p_j et donc le $\mathrm{PGDC}(n, d) = p$.

La force de cette méthode est que si nous avons une courbe elliptique E telle que $\#E(\mathbb{F}_p)$ ne soit pas B-lisse, pour un entier B de taille raisonnable, il nous suffit de prendre d'autres courbes elliptiques jusqu'à ce qu'une soit B-lisse.

4.2 Test de primalité

Pour des nombres de tailles raisonnables, il est assez aisé de déterminer si ces nombres sont composés ou premiers avec certitude. Par contre, pour un nombre de plusieurs centaines de chiffres, il devient plus difficile de dire si celui-ci est premier de manière déterministe. Il existe des tests probabilistes qui nous permettent de dire si un nombre est premier avec une certaine probabilité (par exemple les tests de pseudoprimalité [1]). Mais, pour qu'un système de type RSA soit sûr, il nous faut être certain que les nombres que nous employons soient premiers.

Nous allons, ici, présenter un test de primalité déterministe basé sur les courbes elliptiques. Ce test s'appelle le test de primalité de Goldwasser-Kilian (voir [2] p.467-470).

Ce test n'est utilisé que pour des nombres n qui ont passé un grand nombre de tests de pseudo-primalité avant. Nous pouvons donc travailler avec n comme s'il était premier. Ainsi, nous pouvons supposer que tous les nombres différent de zéro

modulo n sont inversibles modulo n. Dans le cas malheureux où un nombre $l \not\equiv 0 \pmod{n}$ n'est pas inversible, nous saurons non seulement que n n'est pas premier mais nous aurons aussi trouvé un facteur de n qui est $\mathrm{PGDC}(n, l)$.

Considérons maintenant une courbe elliptique E définie sur $\mathbb{Z}/n\mathbb{Z}$. Nous additionnons des points sur cette courbe comme si n était premier. Puisque la loi de groupe de E n'utilise que des additions et multiplications/divisions dans $\mathbb{Z}/n\mathbb{Z}$, la seule chose qui peut se passer si n n'est pas premier est qu'une division soit impossible et nous aurons donc trouvé un facteur de n.

Nous supposerons pour la suite que toutes les opérations que nous ferons ne posent pas de problèmes.

Proposition 4.2. *Soit n un entier, $n > 1$, $\mathrm{PGDC}(n, 6) = 1$ et E une courbe elliptique modulo n. Supposons que nous connaissions un nombre entier m et un point $P \in E(\mathbb{Z}/n\mathbb{Z})$ satisfaisant les conditions suivantes :*

1. *Il existe un nombre premier q divisant m tel que*
$$q > \left(\sqrt[4]{n} + 1\right)^2.$$
2. *$mP = O = (0 : 1 : 0)$.*
3. *$(m/q)P = (x : y : t)$ avec $t \in (\mathbb{Z}/n\mathbb{Z})^*$.*

Alors n est premier.

Preuve. Soit p un facteur premier de n. En réduisant modulo p, nous savons que dans le groupe $E(\mathbb{Z}/p\mathbb{Z})$, l'image de P a un ordre divisant m, mais ne divisant pas m/q puisque $t \in (\mathbb{Z}/n\mathbb{Z})^*$. Puisque q est premier, alors q divise l'ordre de l'image de P dans $E(\mathbb{Z}/p\mathbb{Z})$ et donc $q \leq \#E(\mathbb{Z}/p\mathbb{Z})$. Par le théorème de Hasse (1.14), nous avons que
$$q \leq (\sqrt{p} + 1)^2.$$
Supposons que n ne soit pas premier. Nous pouvons alors choisir un nombre premier p diviseur de n tel que $p \leq \sqrt{n}$. Nous aurions donc $q \leq (\sqrt[4]{n}+1)^2$, ce qui est absurde. Le nombre n est donc premier.

□

La proposition que nous venons d'énoncer ne nous permet pas de trouver un tel m. Il nous dit juste que si nous en avons un qui satisfait les hypothèses, alors n est premier. La proposition 4.2 affirme que si nous déterminons un entier m satisfaisant les hypothèses 1,2,3, alors n est premier, mais ne donne pas de méthode pour trouver un tel m. Cependant il est assez naturel de prendre $m = \#E(\mathbb{Z}/n\mathbb{Z})$. Ainsi l'hypothèse 2 sera automatiquement satisfaite. En fait on a la proposition suivante.

Proposition 4.3. *Soient n un nombre premier tel que $\mathrm{PGDC}(n, 6) = 1$, E une courbe elliptique définie sur $\mathbb{Z}/n\mathbb{Z}$ et soit*
$$m = \#E(\mathbb{Z}/n\mathbb{Z}).$$
S'il existe un nombre premier q avec $q|m$ tel que
$$q > \left(\sqrt[4]{n} + 1\right)^2,$$

alors il existe un point $P \in E(\mathbb{Z}/n\mathbb{Z})$ *tel que*

$$mP = O \text{ et } (m/q)P = (x : y : t) \text{ avec } t \in (\mathbb{Z}/n\mathbb{Z})^*.$$

Preuve. Posons $G = E(\mathbb{Z}/n\mathbb{Z})$. Remarquons tout d'abord que pour tout $P \in G$ nous avons $mP = O$. De plus, puisque n est premier, $t \in (\mathbb{Z}/n\mathbb{Z})^*$ veut dire que $t \neq 0$ et donc que $(m/q)P \neq O$ pour la condition 2.

Supposons que pour tout $P \in G$ nous avons $(m/q)P = O$. Alors l'ordre de G divise m/q.

Par le théorème 1.11, nous avons

$$G \cong \mathbb{Z}/d_1\mathbb{Z} \oplus \mathbb{Z}/d_2\mathbb{Z} \text{ avec } d_2|d_1.$$

Ainsi l'ordre de G est d_1, puisque $\#G = d_1 d_2 \leq d_1^2$. Nous avons donc

$$m = \#G \leq d_1^2 \leq (m/q)^2,$$

ce qui veut dire que $q^2 \leq m$. Utilisant notre hypothèse sur la taille de q et le théorème de Hasse (1.14), nous avons

$$\left(\sqrt[4]{n} + 1\right)^2 < \sqrt{n} + 1,$$

ce qui est absurde. □

Remarques. La cardinalité de $E(\mathbb{Z}/n\mathbb{Z})$ se calcule avec l'algorithme de Schoof que nous présentons plus loin (voir 5.1), où nous travaillons avec n comme s'il était premier. Si l'algorithme de Schoof s'arrête nous saurons que n est composé.

Le principe de l'algorithme de Goldwasser-Kilian est le suivant. Une fois que $m = \#E(\mathbb{Z}/n\mathbb{Z})$ a été calculée, nous essayons de diviser m par de petits premiers et espérons que le quotient q soit un nombre pseudo-premier large (i.e. plus grand que $(\sqrt[4]{n} + 1)^2$). Dans ce cas nous supposons que q est premier et cherchons un point $P \in E(\mathbb{Z}/n\mathbb{Z})$ qui satisfait les hypothèses de la proposition 4.2. Ceci est possible par la proposition 4.3.

Si un tel point P est trouvé, il nous faut prouver que q est bien premier. Pour cela nous utilisons l'algorithme récursivement. Puisque $q \leq m/2 \leq (n + 2\sqrt{n} + 1)/2$, les nombres que nous testons diminuerons au moins de moitié à chaque itération. Le nombre d'itérations de l'algorithme est $O(\log n)$. L'algorithme s'arrête dès que les nombres à tester deviennent assez petit pour employer d'autres tests.

Résumons finalement l'algorithme de Goldwasser-Kilian.

Algorithme de Goldwasser-Kilian.

Soit n un entier positif différent de 1 et premier avec 6. Si n n'est pas premier, l'algorithme le détectera ou tournera indéfiniment. C'est pourquoi il faut absolument utiliser le test de Rabin-Miller[1] avant d'utiliser cet algorithme.

1. Posons $i = 0$ et $n_i = n$.

[1]Le lecteur peut se référer à [2] p.422 pour plus de détails sur le test de Rabin-Miller.

2. Si $n_i < 2^{30}$, diviser par tous les premiers jusqu'à 2^{15}. Si n_i n'est pas premier aller à l'étape 9.
3. Choisir a et b dans $\mathbb{Z}/n_i\mathbb{Z}$ et vérifier que $4a^3 + 27b^2 \in (\mathbb{Z}/n_i\mathbb{Z})^*$. Poser E : $y^2 = x^3 + ax + b$.
4. Avec l'algorithme de Schoof, calculer $m = \#E(\mathbb{Z}/n_i\mathbb{Z})$. Si l'algorithme de Schoof bloque, aller à l'étape 9.
5. Diviser m par des petits nombres premiers dont on note m' le produit. On suppose $m = m'q$ avec $q > (\sqrt[4]{n} + 1)^2$ ayant passé le test de Rabin-Miller. Si ce n'est pas le cas, aller à l'étape 3.
6. Choisir un $x \in \mathbb{Z}/n_i\mathbb{Z}$ tel que le symbole de Legendre $(\frac{x^3+ax+b}{n_i}) = 0$ ou 1. Utiliser l'algorithme de Tonelli-Shanks (voir [2] p.34) pour trouver $y \in \mathbb{Z}/n_i\mathbb{Z}$ tel que $y^2 = x^3 + ax + b$. Si l'algorithme bloque, aller à l'étape 9.
7. Calculer $P_1 = mP$ et $P_2 = (m/q)P$. Si pendant les calculs une division était impossible, aller à l'étape 9. Sinon vérifier si $P_1 = O$, i.e. $P_1 = (0 : 1 : 0)$. Si $P_1 \neq O$, aller à l'étape 9. Si $P_2 = O$, aller à l'étape 6.
8. Poser $i = i + 1$ et $n_i = q$ et aller à l'étape 2.
9. Si $i = 0$, n est composé, on arrête. Sinon, poser $i = i - 1$ et aller à l'étape 3.

Ce test a été utilisé pour prouver la primalité de nombres de l'ordre de 10^{1000}.

Chapitre 5

Compter les points d'une courbe elliptique sur un corps fini

Nous avons vu qu'il est très important de connaître $\#E(\mathbb{F}_q)$ pour les méthodes de cryptages utilisant les courbes elliptiques. Dans cette partie nous allons montrer qu'il est facile de calculer l'ordre d'une courbe $E(\mathbb{F}_{q^n})$ si nous connaissons son ordre pour $E(\mathbb{F}_q)$. Ensuite nous allons donner un algorithme qui nous permet de calculer $\#E(\mathbb{F}_p)$ pour un p premier.

Théorème 5.1. *Soit $\#E(\mathbb{F}_q) = q + 1 - a$. Posons $X^2 - aX + q = (X - \alpha)(X - \beta)$, où $\alpha, \beta \in \overline{\mathbb{F}}_q$. Alors*

$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

pour tout $n \geq 1$.

Preuve. Commençons par montrer que $\alpha^n + \beta^n$ est un nombre entier.

Posons $s_n = \alpha^n + \beta^n$, alors $s_0 = 2$ et $s_1 = a$. Montrons que

$$s_{n+1} = as_n - qs_{n-1}$$

pour tout $n \geq 1$.

En effet, en multipliant la relation $\alpha^2 - a\alpha + q = 0$ par α^{n-1}, nous obtenons

$$\alpha^{n+1} = a\alpha^n - q\alpha^{n-1}.$$

Nous faisons de même pour β et nous trouvons

$$\beta^{n+1} = a\beta^n - q\beta^{n-1}.$$

En additionnant ces deux égalités ensembles nous avons bien

$$s_{n+1} = as_n - qs_{n-1}.$$

Posons

$$f(X) = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n.$$

Alors $X^2 - aX + q = (X - \alpha)(X - \beta)$ divise $f(X)$ car α et β sont des racines de f. Ainsi, il existe un polynôme $Q \in \mathbb{Z}[X]$ tel que

$$f(X) = Q(X)(X^2 - aX + q).$$

Et donc,

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = O,$$

comme endomorphisme de E, par le théorème 1.15. De plus, remarquons que

$$\phi_q^n = \phi_{q^n}.$$

Par le théorème 1.15, il n'y a qu'un unique nombre entier k qui satisfait

$$\phi_{q^n}^2 - k\phi_{q^n} + q^n = O$$

et ce k est donné par $k = q^n + 1 - \#E(\mathbb{F}_{q^n})$. Ainsi,

$$\alpha^n + \beta^n = q^n + 1 - \#E(\mathbb{F}_{q^n}).$$

□

Donnons un exemple de calcul.

Exemple. Considérons la courbe elliptique $E : y^2 = x^3 + 2$ définie sur $\mathbb{F}_7$,

$$E(\mathbb{F}_7) = \big\{O, (0,3), (0,4), (3,1), (3,6), (5,1), (5,6), (6,1), (6,6)\big\}.$$

Ainsi $\#E(\mathbb{F}_7) = 9$ et $a = 7 + 1 - 9 = -1$ et nous avons le polynôme suivant

$$X^2 + X + 7 = \left(X - \frac{-1 + \sqrt{-27}}{2}\right)\left(X - \frac{-1 - \sqrt{-27}}{2}\right).$$

Nous pouvons donc calculer la cardinalité de tout groupe $E(\mathbb{F}_{7^n})$. Par exemple

$$\left(\frac{-1 + \sqrt{-27}}{2}\right)^{60} + \left(\frac{-1 - \sqrt{-27}}{2}\right)^{60} = 180498585261198848060064 98,$$

et donc

$$\begin{aligned}\#E(\mathbb{F}_{7^{60}}) &= 7^{60} + 1 - 180498585261198848060064 98 \\ &= 508021860739623365322188179602357975652549718829504.\end{aligned}$$

Grâce à ce théorème nous pouvons très vite calculer la cardinalité d'un groupe $E(\mathbb{F}_{q^n})$ du moment que nous connaissons $\#E(\mathbb{F}_q)$.

5.1 L'algorithme de Schoof

Nous allons maintenant présenter un algorithme dû à René Schoof qui permet de calculer $\#E(\mathbb{F}_p)$ pour un grand nombre premier p. Sa complexité est $O(\ln^8 p)$ ([2] p.398). Ainsi nous pourrons calculer $\#E(\mathbb{F}_{p^n})$ grâce au théorème 5.1.

Soit $E : y^2 = x^3 + Ax + B$ une courbe elliptique définie sur $\mathbb{F}_p$ avec p un nombre premier et soit $a = p + 1 - \#E(\mathbb{F}_p)$. L'idée de cet algorithme est de déterminer $a \mod l$ pour de petits nombres premiers l. Par le théorème de Hasse (1.14) nous avons

$$p + 1 - 2\sqrt{p} < \#E(\mathbb{F}_p) < p + 1 + 2\sqrt{p},$$

i.e. $|a| \leq 2\sqrt{p}$. Il nous suffit donc de prendre tous les k premiers nombres premiers l_i de manières à avoir

$$\prod_{i=1}^{k} l_i > 4\sqrt{p}$$

pour pouvoir déterminer $\#E(\mathbb{F}_p)$ de manière unique grâce au théorème chinois. Notons S l'ensemble de ces premiers. On remarque que puisque p est grand, les premiers l_i sont petits par rapport à p et $l_i \neq p$.

Nous allons maintenant voir comment déterminer $a \mod l_i$ pour les différents $l_i \in S$.

Cas $l = 2$: Si $\#E(\mathbb{F}_p) \equiv 0 \pmod 2$ ça veut dire que l'ordre du groupe est pair, sinon son ordre est impair. Nous savons que les seuls éléments d'ordre 2 de $E(\mathbb{F}_p)$ sont de la forme $(e, 0)$ avec $e \in \mathbb{F}_p$, i.e. e est une racine de $x^3 + Ax + B$ et donc $p + 1 - a \equiv 0 \pmod 2$ ce qui veut dire que

$$a \equiv 0 \pmod 2.$$

Si $x^3 + Ax + B$ n'a pas de racine dans $\mathbb{F}_p$, alors $\#E(\mathbb{F}_p) \equiv 1 \pmod 2$ et donc

$$a \equiv 1 \pmod 2.$$

Pour déterminer si $x^3 + Ax + B$ possède des racines dans $\mathbb{F}_p$, il suffit de se rappeler que les éléments de $\mathbb{F}_p$ sont exactement les racines de $x^p - x$. Ainsi $x^3 + Ax + B$ a une racine dans $\mathbb{F}_p$ si et seulement s'il a une racine en commun avec $x^p - x$, i.e si et seulement si

$$\mathrm{PGDC}(x^3 + Ax + B, x^p - x) \neq 1.$$

Pour faire ce calcul, nous utilisons l'algorithme d'Euclide appliqué aux polynômes. Si p est grand, le polynôme x^p est de degré grand. Il est donc préférable de calculer

$$[x] \equiv x^p \pmod{x^3 + Ax + B}$$

et d'utiliser le résultat suivant :

$$\mathrm{PGDC}([x] - x, x^3 + Ax + B) = \mathrm{PGDC}(x^p - x, x^3 + Ax + B).$$

Ceci termine le cas $l = 2$.

Cas $l \neq 2$: D'après le théorème 1.15, pour déterminer $a \pmod{l_i}$, il suffit d'éxaminer quelle relation du type $\phi_p^2 - k\phi_p + p$ peut avoir lieu sur $E[l_i]$. On aura alors $k \equiv a \pmod{l_i}$.

Polynômes de division

Définition 5.2. *Nous définissons les polynômes de division $\psi_m \in \mathbb{Z}[x, y, A, B]$ comme suit :*

$$\begin{aligned}
\psi_0 &= 0 \\
\psi_1 &= 1 \\
\psi_2 &= 2y \\
\psi_3 &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\psi_4 &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\psi_{2m+1} &= \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3, \ m \geq 2 \\
\psi_{2m} &= (2y)^{-1}\psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \ m \geq 2.
\end{aligned}$$

Nous allons énoncer quelques propriétés des polynômes de division que nous ne démontrerons pas ([3] pp.77-79), mais qui nous serons utiles pour la suite.

Proposition 5.3.

1. *Si n est impair, alors $\psi_n \in \mathbb{Z}[x, y^2, A, B]$.*
2. *Soit n un nombre impair, alors le degré de $\psi_n \in \mathbb{Z}[x]$ est $(n^2 - 1)/2$.*
3. *Soient $(x, y) \in E(\overline{\mathbb{F}}_p)$ et $n \in \mathbb{N}$, alors*

$$(x, y) \in E[n] \Leftrightarrow \psi_n(x) = 0.$$

Soit $l \in S$ avec $l \neq 2$. Soit $(x, y) \in E(\mathbb{F}_p) \cap E[l]$. Alors

$$\begin{cases} \left(x^{p^2}, y^{p^2}\right) + p(x, y) = a(x^p, y^p) \\ \psi_l(x) = 0 \end{cases}$$

La deuxième équation permet de travailler modulo ψ_l dans tout ce qui suit (voir la remarque p. 44). Soit $p_l \in [-l/2, l/2]$ tel que $p_l \equiv p \pmod{l}$. Comme $(x, y) \in E[l]$, nous avons encore $p(x, y) = p_l(x, y)$ et donc

$$\left(x^{p^2}, y^{p^2}\right) + p_l(x, y) = a(x^p, y^p).$$

Ceci nous permet de travailler avec des valeurs plus petites. Puisque (x^p, y^p) est aussi d'ordre l (car ϕ_p est un endomorphisme), la relation ci-dessus détermine a mod l. L'idée est de calculer tous les termes de cette expression excepté a, puis de déterminer a pour que cette relation soit satisfaite. Notons que si cette relation est satisfaite pour un point de $(x, y) \in E[l]$, alors nous avons déterminer $a \mod l$ et donc elle sera vraie pour tout $(x, y) \in E[l]$.

1er cas : Supposons tout d'abord que $\left(x^{p^2}, y^{p^2}\right) \neq \pm p_l(x,y)$ pour $(x,y) \in E[l]$. Posons

$$(x', y') := \left(x^{p^2}, y^{p^2}\right) + p_l(x,y) \neq O,$$

ainsi $a \not\equiv 0 \pmod{l}$. Vu comment nous avons défini la loi de groupe sur E, nous avons que $x^{p^2} \neq x$. Posons

$$j(x,y) = (x_j, y_j)$$

pour j un entier. Nous avons

$$x' = \left(\frac{y^{p^2} - y_{p_l}}{x^{p^2} - x_{p_l}}\right)^2 - x^{p^2} - x_{p_l}.$$

Nous pouvons pouvons exprimer $\left(y^{p^2} - y\right)^2$ en fonction de x, en effet

$$\begin{aligned}\left(y^{p^2} - y\right)^2 &= y^2\left(y^{p^2-1} - 1\right)^2 \\ &= (x^3 + Ax + B)\left((x^3 + Ax + B)^{(p^2-1)/2} - 1\right)^2;\end{aligned}$$

il en va de même pour x_{p_l}. Nous pouvons donc exprimer x' comme une fonction rationnelle de x.

Nous cherchons j de telle manière à avoir

$$(x', y') = (x_j^p, y_j^p).$$

Regardons tout d'abord la première coordonnée. Nous avons $(x,y) \in E[l]$, avec $(x', y') = \pm(x_j^p, y_j^p)$ si et seulement si $x' = x_j^p$. Nous avons dit plus haut que si cette relation est vraie pour un point de $E[l]$, alors elle est vraie pour tout point de $E[l]$. Puisque les racines de ψ_l sont les premières coordonnées des points finis de $E[l]$, ceci implique que

$$x' - x_j^p \equiv 0 \pmod{\psi_l}.$$

Il faut aussi se rendre compte que les racines de ψ_l sont simples. En effet, il y a $l^2 - 1$ points finis d'ordre l (car $E[l] \cong \mathbb{Z}/l\mathbb{Z} \oplus \mathbb{Z}/l\mathbb{Z}$ par 1.5). Il y a donc $(l^2-1)/2$ points de $E[l]$ ayant la première coordonnée distincte des autres, puisque si $(x,y) \in E[l]$ alors $(x,-y) = -(x,y) \in E[l]$. De plus, par 5.3, le degré de ψ_l est $(l-1)/2$, donc ψ_l n'a que des racines simples. Ainsi $\psi_l | x' - x^p$. Nous calculons donc $(x^p)_j$ pour $1 \leq j \leq (l-1)/2$ jusqu'à ce que $x' - x_j^p \equiv 0 \pmod{\psi_l}$ soit satisfait.

Supposons maintenant que nous ayons trouvé un tel j. Alors

$$x', y' = \pm(x_j^p, y_j^p) = (x_j^p, \pm y_j^p).$$

Pour déterminer le signe de a il nous faut regarder y'. Les expressions y'/y et y_j^p/y sont des fonctions de x ([5]). Si

$$(y' - y_j^p)/y \equiv 0 \pmod{\psi_l},$$

alors

$$a \equiv j \pmod{l}.$$

Sinon nous avons

$$(y' + y_j^p)/y \equiv 0 \pmod{l},$$

et donc

$$a \equiv j \pmod{l}.$$

$\underline{2^{\text{ème}} \text{ cas :}}$ Il nous reste à considérer le cas où $\left(x^{p^2}, y^{p^2}\right) = \pm p(x,y)$ pour tout $(x,y) \in E[l]$. Si nous avons

$$\phi_p^2(x,y) = -p(x,y),$$

alors $aP = (\phi_p^2 + p)(P) = O$ pour tout $P \in E[l]$. Ainsi

$$a \equiv 0 \pmod{l}.$$

Si

$$\phi_p^2(x,y) = \left(x^{p^2}, y^{p^2}\right) = p(x,y),$$

alors

$$a\phi_p(x,y) = \phi_p^2(x,y) + p(x,y) = 2p(x,y),$$

autrement dit,

$$a^2 p(x,y) = a^2 \phi_p^2(x,y) = (2p)^2(x,y).$$

Ainsi, $a^2 p \equiv 4p^2 \pmod{l}$, i.e $p \equiv a^2(2^{-1})^2 \pmod{l}$, ce qui veut dire que p est un carré $\mod l$. Posons $w^2 \equiv p \pmod{l}$. Nous avons

$$(\phi_p - w)(\phi_p + w)(x,y) = \phi_p^2(x,y) = O$$

pour tout $(x,y) \in E[l]$. Soit $P \in E[l]$, alors soit $(\phi_p - w)(P) = O$, et donc

$$\phi_p(P) = wP,$$

soit $(\phi_p - w)(P) = P'$ est un point fini avec

$$(\phi_p + w)(P') = O.$$

Dans tous les cas, il existe un point $P \in E[l]$ avec

$$\phi_p(P) = \pm wP.$$

Supposons qu'il existe un point $P \in E[l]$ tel que $\phi_p(P) = wP$. Alors

$$O = (\phi_p^2 - a\phi_p + p)(P) = (p - aw + p)(P),$$

ainsi $aw \equiv 2p \equiv 2w^2 \pmod{l}$ et donc

$$a \equiv 2w \pmod{l}.$$

De la même manière, s'il existe P tel que $\phi_p(P) = -wP$, alors

$$a \equiv -2w \pmod{l}.$$

Ainsi si $\phi_p^2(x,y) = p(x,y)$ nous avons forcément que p est un carré modulo l. Nous procédons donc ainsi, nous regardons si p est un carré modulo l en calculant le symbole de Legendre $\left(\frac{p}{l}\right)$ qui est assez facile à calculer.

Si p n'est pas un carré modulo l alors nous somme forcément dans le cas

$$\phi_p^2(x,y) = -p(x,y)$$

qui a été traité plus haut. Si nous avons que p est un carré modulo l, il faut regarder s'il existe un point $P \in E[l]$ tel que $\phi_p(P) = \pm wP$ où $w^2 = p$. Pour le savoir, il suffit de calculer

$$\text{PGDC}(\text{numérateur}(x^p - x_w), \psi_l).$$

Si ce pgdc est différent de 1, alors il existe un tel point (x,y) qui est dans $E[l]$ tel que $\phi_p(x,y) = \pm w(x,y)$. Pour déterminer le signe, il nous faut encore calculer

$$\text{PGDC}(\text{numérateur}(y^p - y_w)/y), \psi_l)$$

S'il est différent de 1, alors $a \equiv 2w \pmod{l}$. Sinon $a \equiv -2w \pmod{l}$.

Si $\text{PGDC}(\text{numérateur}(x^p - x_w), \psi_l) = 1$, alors nous nous retrouvons dans le cas $\phi_p^2(P) = -pP$ et donc $a \equiv 0 \pmod{l}$.

Remarque. Ici nous calculons les pgdc et ne regardons pas si nous avons $0 \mod \psi_l$ parce que ce ne sont pas tous les points de $E[l]$ qui satisfont $\phi_p(P) = wP$ et donc nous voulons juste voir s'il y a une racine en commun.

En résumé : l'algorithme de Schoof se déroule ainsi. Soit une courbe elliptique $E : y^2 = x^3 + Ax + B$ définie sur $\mathbb{F}_p$, nous voulons calculer $\#E(\mathbb{F}_p) = p + 1 - a$.

1. Soit S l'ensemble défini plus haut.
2. Si $l = 2$, $a \equiv 0 \pmod{2}$ si et seulement si $\text{PGDC}(x^3 + Ax + B, x^p - x) \neq 1$.
3. Pour chaque nombre premier $l \in S$ avec $l \neq 2$, faire ce qui suit.
   (a) Posons $p_l \equiv p \pmod{l}$ avec $|p_l| < l/2$.
   (b) Calculer x', la première coordonnée de
   $$(x', y') = \left(x^{p^2}, y^{p^2}\right) + p_l(x,y) \pmod{\psi_l}.$$
   (c) Pour $j = 1, \cdots, (l-1)/2$, faire ce qui suit.
      i. Calculer x_j, la première coordonnée de
      $$(x_j, y_j) = j(x,y).$$
      ii. Si $x' - x_j^p \equiv 0 \pmod{\psi_l}$, aller à l'étape (iii). Sinon, essayer la prochaine valeur de j à l'étape (c). Si toutes les valeurs de $1 \leq j \leq (l-1)/2$ ont été essayées aller à l'étape (d).
      iii. Calculer y' et y_j. Si $(y' - y_j)/y \equiv 0 \pmod{\psi_l}$, alors $a \equiv j \pmod{l}$. Sinon, $a \equiv -j \pmod{l}$.

(d) Si toutes les valeurs $1 \leq j \leq (l-1)/2$ ont été essayées sans succès, posons

$$w^2 \equiv p \pmod{l}.$$

Si p n'est pas un carré modulo l, alors $a \equiv 0 \pmod{l}$.

(e) Si PGDC(numérateur$(x^p - x_w), \psi_l) = 1$, alors $a \equiv 0 \pmod{l}$. Sinon, calculer PGDC(numérateur$((y^p - y_w)/y, \psi_l)$. Si le PGDC n'est pas 1, alors $a \equiv 2w \pmod{l}$. Sinon, $a \equiv -2w \pmod{l}$.

4. Connaissant $a \pmod{l}$ pour chaque $l \in S$, nous pouvons calculer

$$a \mod \prod_{l \in S} l$$

par le théorème chinois. Choisir la valeur de a qui satisfait cette congruence et telle que $|a| \leq 2\sqrt{p}$. Alors

$$\#E(\mathbb{F}_p) = p + 1 - a.$$

Remarque. Les polynômes avec lesquels nous travaillons, par exemple x^p ou x^{p^2}, ne sont pas utilisés tels quels dans la pratique mais réduit modulo ψ_l avec $l \in S$, ce qui nous permet de travailler avec des polynômes ayant un degré qui n'est pas trop grand.

Conclusion

Nous avons donc présenté des cryptosystèmes basés sur les courbes elliptiques et différents problèmes qui y sont liés. Evidemment nous n'avons abordé que certains aspects des choses, surtout mathématiques, en particulier nous ne nous sommes pas vraiment attardé sur la complexité des algorithmes ni sur les aspects purement informatiques qui sortaient du cadre de ce travail.

Nous avons tout de même pu constater que la cryptographie est une étude à la fois théorique et pratique qui touche différents domaines. Mais contrairement aux mathématiques, en cryptographie certaines choses sont prouvées empiriquement.

Bibliographie

[1] Lindsay N. Childs. *A Concrete Introduction to Higher Algebra*. Springer, second edition, 2000.

[2] Henri Cohen. *A Course in Computational Algebraic Number Theory*. Springer, 1993.

[3] Lawrence C.Washington. *Elliptic curves Number Theory and Cryptography*. Chapman & Hall/CRC, 2003.

[4] Didier Müller. www.apprendre-en-ligne.net/crypto/moderne/integrite.html/.

[5] René Schoof. Elliptic curves over finite fields and the computation of square roots. *Mathematics of Computation*, Vol. 44, N°382, avril 1985.

[6] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 1986.

[7] Pierre Vandeginste. Le hachage était presque parfait... *La recherche*, N°382, janvier 2005.