Chapitre 1

Courbes elliptiques

La lettre k désigne le corps commutatif $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Q}$ ou $\mathbb{F}_q$.

1.1 Définition et invariants

1.1.1 Définition

Définition 1 *Une courbe elliptique E définie sur k est une courbe* lisse *donnée par une équation de Weierstrass :*

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1.1}$$

*où les coefficients a_1, a_2, a_3, a_4 et a_6 sont dans k. Le terme "*courbe lisse*" signifie que la propriété suivante est satisfaite : si $(x, y) \in \overline{k}^2$ vérifie l'équation (1.1) alors les nombres $2y + a_1x + a_3$ et $3x^2 + 2a_2x + a_4 - a_1y$ ne sont pas simultanément nuls.*

Si le couple $(x, y) \in \overline{k}^2$ vérifie l'équation (1.1), on dit que (x, y) est un point sur la courbe (cette notion sera plus clairement définie dans la suite).
On pose $P(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$, la condition "courbe lisse" de la définition affirme que si $P(x_1, y_1) = 0$, avec $(x_1, y_1) \in \overline{k}^2$, alors le vecteur $(\frac{\partial P}{\partial x}(x_1, y_1), \frac{\partial P}{\partial y}(x_1, y_1))$ n'est pas le vecteur nul. En d'autres termes, on peut définir une tangente à la courbe au point (x_1, y_1).

Exemples :
1- On prend $k = \mathbb{R}$, on pose :

$$E_1 \ : \ y^2 = x^3 + x \qquad \text{et} \qquad E_2 \ : \ y^2 = x^3 + x^2$$

Les courbes E_1 et E_2 sont bien définies sur $\mathbb{R}$ puisque tous les coefficients sont réels.
La courbe E_1 est lisse, en effet :

$$\left(\frac{\partial P}{\partial x}(x, y), \frac{\partial P}{\partial y}(x, y)\right) = (0, 0) \Leftrightarrow \left\{ \begin{array}{rcl} 3x^2 + 1 & = & 0 \\ 2y & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x & = & \pm i/\sqrt{3} \\ y & = & 0 \end{array} \right.$$

or les points $(\pm i/\sqrt{3}, 0)$ ne sont pas sur la courbe et E_1 est donc une courbe elliptique.

Pour E_2, le point $(0, 0)$ est un point sur la courbe et on vérifie aisément que

$\frac{\partial P}{\partial x}(0,0) = \frac{\partial P}{\partial y}(0,0) = 0$. On dit alors que le point $(0,0)$ est un point *singulier*. La courbe E_2 n'est pas lisse et n'est pas une courbe elliptique.

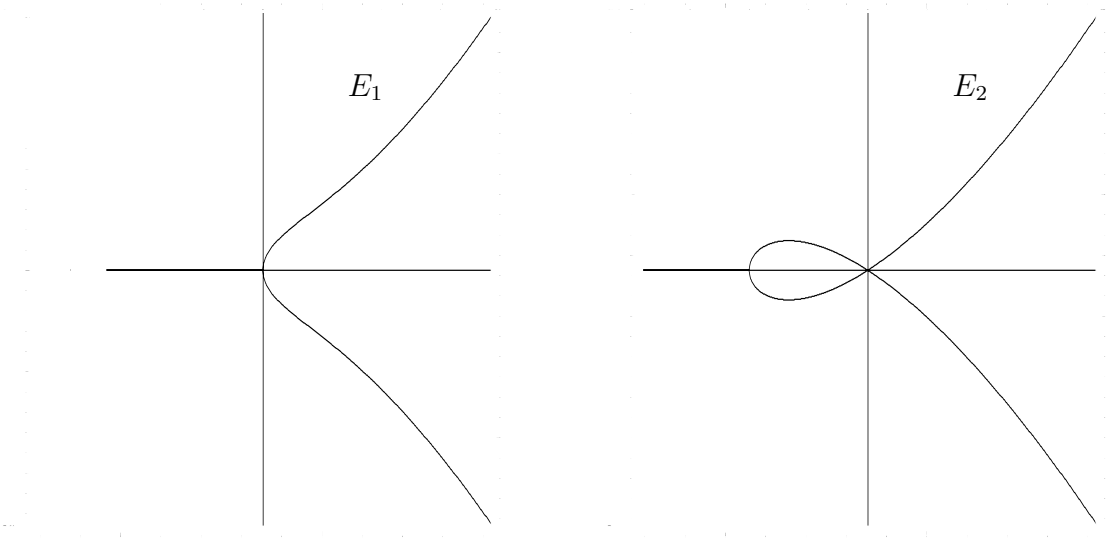

FIG. 1.1 – Graphes des courbes E_1 et E_2 sur $\mathbb{R}$. La courbe E_1 est lisse et la courbe E_2 possède un point singulier (un point double en $(0,0)$).

2- On pose $E\ :\ y^2 = x^3 + a$, $a \in k$. On vérifie que si $\operatorname{car} k \neq 2, 3$ alors E est une courbe elliptique si et seulement si on a $a \neq 0$.
Si $\operatorname{car}(k) = 2$, le point $(0, a^{1/2})$ est un point singulier de E ($a^{1/2}$ désigne la racine carré de a dans $\overline{k}$). La courbe E n'est pas une courbe elliptique.
Si $\operatorname{car}(k) = 3$, le point $(-a^{1/3}, 0)$ est un point singulier de E ($a^{1/3}$ désigne la racine cubique de a dans $\overline{k}$). La courbe E n'est pas une courbe elliptique.

1.1.2 Invariants

Supposons que $\operatorname{car} k \neq 2$, alors en complétant le carré du membre de gauche, l'équation (1.1) s'écrit :

$$\left(y + \frac{a_1}{2}x + \frac{a_3}{2}\right)^2 = x^3 + \frac{4a_2 + a_1^2}{4}x^2 + \frac{2a_4 + a_3a_1}{2}x + \frac{4a_6 + a_3^2}{4}$$

On pose $b_2 = (4a_2 + a_1^2)$, $b_4 = (2a_4 + a_3a_1)$ et $b_6 = (4a_6 + a_3^2)$ et on définit la courbe E' sur k par :

$$E'\ :\ Y^2 = X^3 + \frac{b_2}{2}X^2 + \frac{b_4}{2}X + \frac{b_6}{4}$$

On peut montrer que E' est une courbe elliptique si et seulement si E en est une. Les courbes E et E' sont *isomorphes* (mais on ne définira pas clairement cette notion dans ce cours). L'application suivante est une bijection de l'ensemble des points (x, y) sur E dans l'ensemble des points (X, Y) sur E'.

$$\begin{array}{ccc} E & \longrightarrow & E' \\ (x,y) & \longmapsto & (X,Y) = (x, y + \frac{a_1}{2}x + \frac{a_3}{2}) \end{array}$$

Cette application n'est rien d'autre qu'un changement linéaire des variables. La proposition suivante (dont la preuve est laissée en exercice) permet de donner un critère simple pour décider si la courbe E' est lisse ou non.

Proposition 1 *Soit k un corps de caractéristique $\neq 2$ et E une courbe définie sur k par $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ alors la courbe E est lisse si et seulement si le polynôme $x^3 + a_2x^2 + a_4x + a_6$ n'a pas de racine multiple dans $\overline{k}$.*

On rappelle qu'un polynôme P possède une racine multiple si et seulement si son *discriminant* , $\operatorname{disc}(P)$, est nul, or :

$$\operatorname{disc}(x^3 + a_2x^2 + a_4x + a_6) = -4a_6a_2^2 + (a_4a_2)^2 + 18a_6a_4a_2 - 4a_4^3 - 27a_6$$

On pose $\Delta(E) = 16 \operatorname{disc}(P)$ et ainsi $E : y^2 = x^3 + a_2x^2 + a_4x + a_6$ est une courbe elliptique si et seulement si $\Delta(E) = 0$.

Exemples :

- $E_1/\mathbb{R} : y^2 = x^3 + x$, on a $\Delta(E_1) = -64 \neq 0$.
- $E_2/\mathbb{R} : y^2 = x^3 + x^2$, on a $\Delta(E_2) = 0$.
- $E_3/k : y^2 = x^3 + a$, on a $\Delta(E_3) = -2^4 \times 3^3 \times a$. On vérifie directement que E_3 est une courbe elliptique si et seulement si $\operatorname{car} k \nmid 2 \times 3 \times a$.

Définition 2 *Soit $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ une courbe définie sur k. On pose :*

$$b_2 = a_1^2 + 4a_2 \qquad b_4 = a_1a_3 + 2a_4$$
$$b_6 = a_3^2 + 4a_6 \qquad b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2$$
$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

Le nombre $\Delta = \Delta(E)$ est appelé le discriminant de E. La courbe E est une courbe elliptique si et seulement si on a $\Delta \neq 0$. Dans ce cas, on pose $j(E) = \frac{(b_2^2 - 24b_4)^3}{\Delta}$, on dit que $j(E)$ est le j-invariant de E.

Remarque : Cette définition est valable en caractéristique 2. Les calculs précédents montrent que si $\operatorname{car} k \neq 2$, la courbe E est isomorphe à :

$$E' \ : \ y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4}$$

1.1.3 Équations réduites

Dans l'exercice 2, on montre que lorsque la caractéristique de k n'est ni 2 ni 3, on peut ramener l'équation (1.1) à une équation réduite avec $a_1 = a_2 = a_3 = 0$, c'est-à-dire on peut toujours supposer que la courbe est donnée par :

$$E \ : \ y^2 = x^3 + a_4x + a_6 \tag{1.2}$$

On dit alors que (1.2) est une équation de Weierstrass courte pour E. Dans ce cas, on a :

$$\Delta = -16(4a_4^3 + 27a_6^2) \quad \text{et} \quad j(E)(-48a_4)^3/\Delta$$

Lorsque la caractéristique de k vaut 2 ou 3, on a également une notion d'équation "courte".
Supposons tout d'abord que $\operatorname{car} k = 2$. On peut montrer qu'un changement linéaire des variables permet de ramener l'équation d'une courbe elliptique à l'une de deux équations suivantes :

$$\begin{aligned} E \ : \ y^2 + xy &= x^3 + a_2x^2 + a_6 \\ E \ : \ y^2 + a_3y &= x^3 + a_4x + a_6 \end{aligned}$$

Dans le premier cas, on a $\Delta = a_6$ et $j(E) = 1/a_6$. Dans le deuxième, on a $\Delta = a_3^4$ et $j(E) = 0$, dans ce cas, la courbe est *supersingulière* (on verra plus tard la définition d'une courbe supersingulière). L'utilisation d'une courbe supersingulière pour le problème du logarithme discret permet des attaques sous-exponentielles et ne sont pas utilisées en principe.

Lorsque $\operatorname{car} k = 3$, un changement linéaire des variables permet de ramener l'équation d'une courbe elliptique à l'une de deux suivantes :

$$\begin{aligned} E \ : \ y^2 &= x^3 + a_2x^2 + a_6 \\ E \ : \ y^2 &= x^3 + a_4x + a_6 \end{aligned}$$

Dans le premier cas, on a $\Delta = -a_2^3a_6$ et $j(E) = -a_2^3/a_6$. Dans le deuxième cas, on a $\Delta = -a_4^3$ et $j(E) = 0$, ici aussi la courbe est *supersingulière*.

L'invariant j ne dépend pas de la forme de l'équation de la courbe elliptique alors que Δ en dépend.

1.1.4 Exercices

Exercice 1 : À quelle(s) condition(s) sur k, la courbe d'équation $y^2 = x^3 + ax$ définie sur k est-elle une courbe elliptique ?

Exercice 2 :
1- Soit k un corps de caractéristique 2 et E la courbe elliptique définie sur k par :

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

Montrer alors que a_1 et a_3 ne peuvent être simultanément nuls.
2- Soit k un corps de caractéristique $\neq 2, 3$ et

$$E \ : \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (*)$$

Montrer qu'une transformation linéaire des variables permet de ramener l'équation $(*)$ à une équation de la forme :

$$E' \ : \ y^2 = x^3 + a_4{}'x + a_6{}'$$

Exercice 3 : Montrer la proposition 1.

Exercice 4 : On pose $E : y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5$ et $k = \mathbb{F}_{2011}$.
1- Calculer Δ et $j(E)$. (Réponse $\Delta = 1715$, $j(E) = 1430$).
2- Montrer que les points $(1, 2)$ et $(2, 470)$ sont sur la courbe.
3- Calculer $|\{(x, y) \in \mathbb{F}_{2011} | y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5\}|$. (Réponse 2003).

1.2 La loi de groupe

1.2.1 Points rationnels

Dans cette partie, on considère une courbe elliptique E définie sur k par :

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

Définition 3 *L'ensemble des points k-rationnels de E, noté E(k) est :*

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

Le point $\mathcal{O}$ est appelé "point à l'infini".

Remarques :
1- Par convention le point à l'infini $\mathcal{O}$ est défini sur k et sur toute extension de k. Ainsi, si K/k est une extension du corps k, E peut aussi être considérée comme une courbe elliptique définie sur K et $\mathcal{O}$ est encore le point à l'infini de E/K. On a :

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

de même :

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

Si $k \subset L \subset \overline{k}$, il vient alors $E(k) \subset E(L) \subset E(\overline{k})$.

2- Si E est définie sur $\mathbb{F}_q$ et si $n \in \mathbb{N}^*$ alors le groupe de galois $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) \simeq \mathbb{Z}/n\mathbb{Z}$, engendré par l'automorphisme de Frobenius σ_q, agit sur $E(\mathbb{F}_{q^n})$ par :

$$\begin{aligned} \sigma_q.(x, y) &= (x^q, y^q) \in E(\mathbb{F}_{q^n}) \\ \sigma_q.\mathcal{O} &= \mathcal{O} \in E(\mathbb{F}_{q^n}) \end{aligned}$$

On a la propriété fondamentale suivante :

$$E(\mathbb{F}_q) = \{P \in E(\mathbb{F}_{q^n}) | \sigma_q(P) = P\}$$

Exemples :
1- $E : y^2 = x^3 - x$, $k = \mathbb{F}_3$. On a :

$$E(\mathbb{F}_3) = \{\mathcal{O}, (0, 0), (2, 0), (1, 0)\}$$

On considère $\mathbb{F}_9 = \mathbb{F}_3[\theta]$ où $\theta^2 = -1$. On a :

$$\begin{aligned} E(\mathbb{F}_9) \ = \ & \{\mathcal{O}, (0, 0), (2, 0), (1, 0), (\theta, \theta + 2), (\theta, 2\theta + 1), (\theta + 1, \theta + 2), \\ & (\theta + 2, \theta + 2), (\theta + 2, 2\theta + 1), (2\theta, \theta + 1), (2\theta, 2\theta + 2), (2\theta + 1, \theta + 1), \\ & (2\theta + 1, 2\theta + 2), (2\theta + 2, \theta + 1), (2\theta + 2, 2\theta + 2), (\theta + 1, 2\theta + 1)\} \end{aligned}$$

2- $E : y^2 = x^3 - x$, $k = \mathbb{R}$. La figure (1.2) représente $E(\mathbb{R})$.

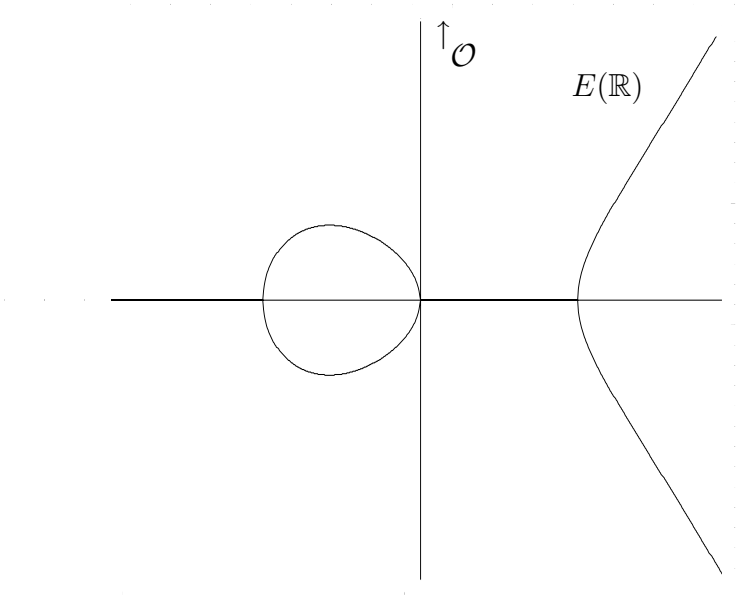

FIG. 1.2 – $E(\mathbb{R})$ pour E donné par l'équation $y^2 = x^3 - x$

1.2.2 Loi de groupe

On définit une loi de groupe abélien $\oplus$ sur $E(k)$ de la façon suivante (il faudrait vérifier à posteriori qu'il s'agit bien d'une loi de groupe commutatif) :

- $\mathcal{O}$ est l'élément neutre i.e. $(x_1, y_1) \oplus \mathcal{O} = \mathcal{O} \oplus (x_1, y_1) = (x_1, y_1)$ pour tout $(x_1, y_1) \in E(k)$.
- L'opposé de (x_1, y_1) est $\ominus(x_1, y_1) = (x_1, -y_1 - a_1x_1 - a_3)$.
- Soient P et Q deux points de $E(k)\backslash\{\mathcal{O}\}$, la droite passant par P et Q "recoupe" la courbe E en un troisième point $R \in E(k)$ qui est l'opposé de $P \oplus Q$ i.e. on a : $P \oplus Q = \ominus R$. Si $P = Q$, on considère la droite tangente en P à la courbe E au lieu de la droite (PQ).

Le troisième point peut aussi s'énoncer de la façon suivante : la somme de 3 points alignés est nulle (en admettant que la loi est associative).

On peut bien sûr obtenir des formules explicites pour l'addition de deux points. Pour cela, soient $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ deux points de $E(k)$ avec $P \neq \ominus Q$ (sinon, on reconnait de suite que Q est l'opposé de P et on a $P \oplus Q = \mathcal{O}$).

Supposons tout d'abord que $P \neq Q$. La droite passant par P et Q a pour équation $y = \lambda x + \mu$ avec :

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2} \quad \text{et} \quad \mu = y_1 - \lambda x_1$$

(Remarquons que λ est bien défini car si $x_1 = x_2$ alors $P = Q$ ou $P = \ominus Q$, ce qui est exclu par hypothèse). L'intersection de la droite (PQ) avec la courbe E est donnée par :

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6$$

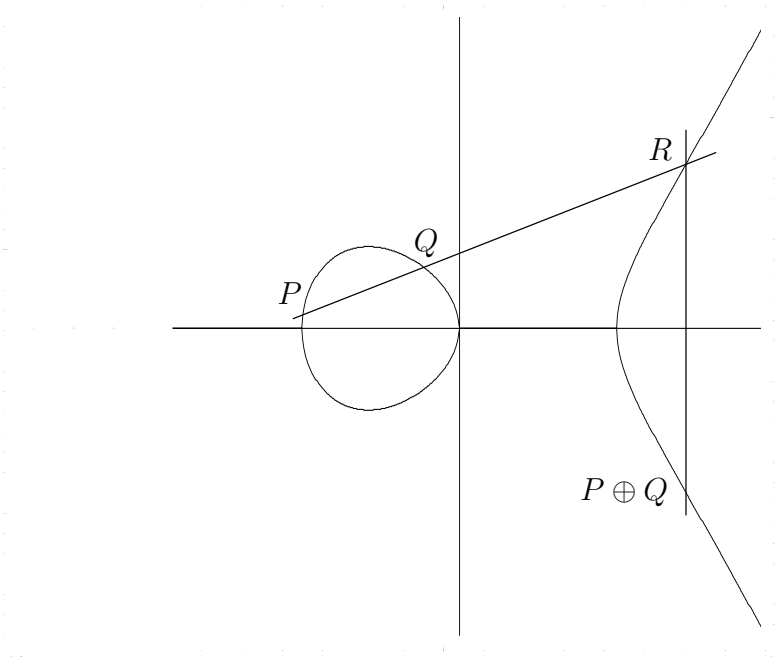

FIG. 1.3 – Loi de groupe sur $E(\mathbb{R})$ pour E donné par l'équation $y^2 = x^3 - x$

ce qui donne l'équation suivante :

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\lambda - a_3\mu)x + (a_6 - \mu^2 - a_3\mu) = 0$$

On connait deux solutions de cette équation à savoir x_1 et x_2. Or la somme de trois racines est l'opposé du coefficient de degré 2 et on pose donc :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{et} \quad \widetilde{y_3} = \lambda x_3 + \mu$$

Le point $(x_3, \widetilde{y_3})$ est le troisième point d'intersection cherché. On obtient alors :

$$\begin{aligned} P \oplus Q = (x_3, y_3) &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3) \end{aligned}$$

Supposons maintenant que $P = Q = (x_1, y_1)$. La droite tangente à la courbe E au point P a pour équation $y = \lambda x + \mu$ avec :

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} \quad \text{et} \quad \mu = y_1 - \lambda x_1$$

(Remarquons que λ est bien défini car si $2y_1 + a_1x_1 + a_3 = 0$ alors $P = \ominus P$, ce qui est exclu par hypothèse). L'intersection de la droite avec la courbe E est donnée par :

$$(\lambda x + \mu)^2 + (a_1x + a_3)(\lambda x + \mu) = x^3 + a_2x^2 + a_4x + a_6$$

ce qui donne l'équation suivante :

$$x^3 + (a_2 - \lambda^2 - a_1\lambda)x^2 + (a_4 - 2\lambda\mu - a_1\lambda - a_3\mu)x + (a_6 - \mu^2 - a_3\mu) = 0$$

On connait une racine double (à savoir x_1) de cette équation, on en déduit la dernière solution et on pose :

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \quad \text{et} \quad \widetilde{y_3} = \lambda x_3 + \mu$$

Le point $(x_3, \widetilde{y_3})$ est le troisième point d'intersection cherché et on obtient :

$$\begin{aligned} [2]P := P \oplus P = (x_3, y_3) &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, -\lambda x_3 - \mu - a_1 x_3 - a_3) \\ &= (\lambda^2 + a_1\lambda - a_2 - 2x_1, \lambda(x_1 - x_3) - y_1 - a_1 x_3 - a_3) \end{aligned}$$

Proposition 2 *On a les règles suivantes pour calculer la loi "$\oplus$".*
On pose $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ alors :

- $\ominus P = (x_1, -y_1 - a_1x_1 - a_3)$.
- $P \oplus Q = (x_3, y_3)$ *avec* $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3$) *et :*

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & si \quad P \neq Q, \ominus Q \\ \\ \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & si \quad P = Q \end{cases}$$

Si $P = Q$ et $2y_1 + a_1x_1 + a_3 = 0$ alors $P \oplus Q = P \oplus P = \mathcal{O}$.

Théorème 3 *Soit E une courbe elliptique définie sur k alors $(E(k), \oplus)$ est un groupe abélien de neutre $\mathcal{O}$. En particulier, on a $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.*

Preuve. La commutativité est évidente, il suffit alors seulement de vérifier par un calcul (long et fastidieux mais que l'on peut faire avec un logiciel de calcul formel) que la loi est associative.

Puisqu'il n'y aura aucune confusion possible dans la suite, la loi $\oplus$ sera noté $+$ (et donc, $\ominus$ sera noté $-$).

Exemple : Sur le corps $k = \mathbb{F}_{2011}$, on défini

$$E \ : \ y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5$$

On prend $P = (1, 2) \in E(\mathbb{F}_{2011})$ et $Q = (2, 470) \in E(\mathbb{F}_{2011})$.
On a $2P = P + P = (1161, 1551)$, $P + Q = (288, 128)$. De plus, on peut vérifier que l'on a $723P = Q$ (on peut voir cette dernière comme un problème, ou plutôt une solution, du logarithme discret dans $E(\mathbb{F}_{2011})$).

Théorème 4 *Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. Soit $n \in \mathbb{Z}$ et σ_q l'automorphisme de Frobenius engendrant le groupe* $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$. *On a*

$$\forall P, \ Q \in E(\mathbb{F}_{q^n}), \quad \sigma_q(P + Q) = \sigma_q(P) + \sigma_q(Q)$$

1.2.3 Exercices

Exercice 1 : On considère la courbe elliptique $E : y^2 = x^3 - 25x$ sur $k = \mathbb{Q}$.
1- Montrer que les points $P_1 = (-5, 0)$, $P_2 = (0, 0)$ et $P_3 = (5, 0)$ sont des points de 2-torsions (i.e. $2P_i = \mathcal{O}$).

2- Vérifier que le point $G = (-4, 6)$ appartient à $E(\mathbb{Q})$.
3- Calculer $G + P_1$, $G + P_2$, $G + P_3$ ainsi que $2G$, $3G$ et $4G$. Que remarquez-vous ?

On peut démontrer (mais on ne cherchera pas à le faire) que $E(\mathbb{Q}) = \{nG + \ell_1 P_1 + \ell_2 P_2 | n \in \mathbb{Z},\ \ell_1 = 0, 1\ , \ell_2 = 0, 1\}$.

Exercice 2 : Soit E la courbe elliptique définie sur $\mathbb{F}_7$ par l'équation :

$$E\ :\ y^2 = x^3 + 3x - 1$$

1- Calculer le discriminant et le j-invariant de E.
2- Trouver tous les points de $E(\mathbb{F}_7)$.
3- Montrer que $E(\mathbb{F}_7)$ est cyclique et donner un générateur.

Exercice 3 :
1- Montrer que le polynôme $P(X) = X^3 + X + 1$ est irréductible dans $\mathbb{F}_5[X]$. En déduire que l'on a $\mathbb{F}_{125} = \mathbb{F}_5[\theta]$ où $\theta^3 + \theta + 1 = 0$.
2- Calculer θ^{-1} en fonction de θ.
3- Calculer θ^{30} puis θ^{31}.

On considère la courbe E définie sur $\mathbb{F}_{125}$ d'équation :

$$E\ :\ y^2 = x^3 + \theta$$

4- Montrer que E est une courbe elliptique. Calculer son discriminant ainsi que son j-invariant.
5- Montrer que θ est un carré dans $\mathbb{F}_{125}$. En déduire qu'il existe un point sur E de la forme $(0, y)$.
6- Calculer $(2\theta^2 + \theta + 2)^2$. En déduire que le point $P = (0, 2\theta^2 + \theta + 2)$ est sur la courbe. Calculer $3P$.
7- Montrer que les points $P_1 = (1, 2\theta^2 + 1)$, $P_2 = (\theta, 2)$ et $P_3 = (\theta, -2)$ sont sur la courbe.
8- Calculer dans $E(\mathbb{F}_{125})$:

$$P_2 + P_3 \quad , \quad P_1 + P_3 \quad , \quad 2P_1$$

9- Montrer que θ est un cube dans F_{125}, en déduire qu'il existe un point Q de la forme $(x, 0) \in E(\mathbb{F}_{125})$. Montrer que $2Q = \mathcal{O}$.

1.3 Problème du logarithme discret

Soit k un corps et E une courbe elliptique définie sur k. Les points k-rationnels formant un groupe abélien, celui-ci donne un cadre pour le problème du logarithme discret.

Définition 4 *Soit E une courbe elliptique définie sur k et $G \in E(k)$. Connaissant le point $P \in E(k)$, le problème du logarithme discret consiste à trouver $n \in \mathbb{N}$, s'il existe, tel que $P = nG$.*

Si k est un corps fini, ce problème est réputé être un problème "difficile" en principe. À ce jour aucun algorithme sous-exponentiel général n'est connue pour le résoudre.

Cependant, il existe des attaques sous-exponentielles pour certaines courbes "faibles" du point de vue de la sécurité (par exemple les courbes supersingulières). Il faut donc faire attention au choix de E.

Réciproquement, connaissant E, k, G et n, il est facile de calculer $P = nG$ en utilsant un algorithme d'exponentation rapide. Par exemple :

Algorithme
- Entrées : une courbe elliptique E sur un corps k, un point $G \in E(k)$ et $n \in \mathbb{Z}$.
- Sortie : le point $nG \in E(k)$.

Étape 1 : Faire $P \leftarrow \mathcal{O}$. Si $n = 0$ retourner P, fin de l'algorithme. Si $n < 0$, faire $N \leftarrow -n$, $Q \leftarrow -G$, sinon faire $N \leftarrow n$ et $Q \leftarrow G$.
Étape 2 : Si N est impair, faire $P \leftarrow Q + P$.
Étape 3 : Faire $N \leftarrow \lfloor N/2 \rfloor$. Si $N = 0$ retourner le point P, fin de l'algorithme. Sinon, faire $Q \leftarrow 2Q$ et aller à l'étape 2.

Cet algorithme se termine (N décroît strictement) et on établit sa validité en montrant qu'à chaque fois que l'on débute l'étape 2 on a $nG = P + NQ$. On vérifie que la boucle est de longueur $\lfloor \log_2(|n|) \rfloor + 1$. À chaque étape, on doit effectuer une addition et/ou un doublement de points. Le coût de ces opérations dépendent du corps k dans lequel on effectue les calculs. Supposons que la courbe elliptique E soit donnée par une équation de Weierstrass courte :

$$E \ : \ y^2 = x^3 + a_4 x + a_6$$

C'est-à-dire, on suppose que $\operatorname{car} k > 3$ ou que $\operatorname{car} k = 3$ et que la courbe est supersingulière.
Soit $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ tels que $P \neq \pm Q$, on a $P + Q = (x_3, y_3)$ avec x_3 et y_3 donnés par :

$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

où $\lambda = (y_1 - y_2)/(x_1 - x_2)$. Le calcul de $P + Q$ demande donc *1 inversion* et *3 multiplications* dans le corps k (pour simplifier, nous avons considéré l'élévation au carré comme une multiplication et nous ne comptons ni les additions ni les soustractions dans k).
Pour calculer $2P = (x_3, y_3)$, on a :

$$x_3 = \lambda^2 - 2x_1 \qquad y_3 = \lambda(x_1 - x_3) - y_1$$

où $\lambda = (3x_1^2 + a_4)/(2y_1)$. Le calcul de $P + P$ demande ici *1 inversion* et *4 multiplications*.
On peut également faire une étude similaire en caractéristique 2 et pour les courbes non supersingulières en caractéristique 3.

Remarques :
1- L'algorithme d'exponentiation rapide que nous avons donné est un des nombreux algorithmes que l'on peut trouver. Il en existe bien d'autres qui sont plus fins et

plus efficaces (et aussi plus adaptés au cadre des courbes elliptiques). On peut aussi changer la façon de représenter les points sur la courbe elliptique afin d'optimiser le coût des opérations (addition, doublement de points...).

2- En général, pour le problème du logarithme discret à base de courbes elliptiques, les corps utilisés pour définir les courbes sont les corps $\mathbb{F}_p$, où p est un grand nombre premier, et les corps $\mathbb{F}_{2^r}$ avec r grand.

1.3.1 Exercices

Exercice 1 : Dans l'algorithme d'exponentiation rapide donné dans cette partie, calculer le nombre d'inversions et de multiplications à effectuer lorsque le corps est de caractéristique 2 (resp. 3) et que la courbe est donnée par une équation réduite.

Exercice 2 : Sur le corps $\mathbb{F}_{2011}$, on considère la courbe elliptique :

$$E \ : \ y^2 + xy + 3y = x^3 + 2x^2 + 4x + 5$$

On pose $P = (1, 2) \in E(\mathbb{F}_{2011})$.
En utilisant l'algorithme d'exponentiation rapide de cette partie calculer $723P$.
Combien d'additions/doublement de points avez-vous effectué ? (Réponse : 6 additions et 10 doublements).

1.4 Propriétés des points k-rationnels

1.4.1 Structure du groupe des points rationnels

On considère toujours une courbe elliptique E définie sur un corps k. Dans le cas où k est un corps fini $\mathbb{F}_q$, la structure du groupe des points $\mathbb{F}_q$-rationnels est donnée par le :

Théorème 5 *Le groupe $E(\mathbb{F}_q)$ est soit un groupe cyclique soit le produit de deux groupes cycliques. Dans le premier cas on a :*

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_2\mathbb{Z}$$

où $d_2 = |E(\mathbb{F}_q)|$. Dans le second cas, on a :

$$E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$$

où $d_1 \mid d_2$ et $d_1 | q - 1$.

Il existe également des résultats sur la structure points rationnels lorsque le corps k n'est pas un corps fini.

Soit $n \in \mathbb{Z}$, on dira qu'un point $P \in E(\overline{k})$ est un point de n-torsion si l'on a $nP = \mathcal{O}$. Le sous-groupe de $E(\overline{k})$ des points de n-torsion est noté $E[n]$ i.e. :

$$E[n] = \{P \in E(\overline{k}) | nP = \mathcal{O}\}$$

La structure des points de n-torsion est donnée par le théorème suivant :

Théorème 6 *Si* $\operatorname{car} k = 0$ *ou si* $(n, \operatorname{car} k) = 1$ *on a :*

$$E[n] \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

Si $\operatorname{car} k = p$ *et* $n = p^r$ *on a soit :*

$$E[p^r] = \{\mathcal{O}\} \text{ pour tout } r \geq 1$$

soit :

$$E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z} \text{ pour tout } r \geq 1$$

Définition 5 *Soit* $p = \operatorname{car} k \neq 0$*, si* $E[p^r] = \{\mathcal{O}\}$ *pour un (et donc pour tout)* $r \geq 1$*, la courbe elliptique* E *est dite* supersingulière*. Sinon,* E *est dite* ordinaire*.*

Exemple : Sur $k = \mathbb{F}_5$ on définit E par :

$$E \ : \ y^2 = x^3 + 4x + 1$$

On peut facilement énumérer tous les points de $E(\mathbb{F}_5)$:

$$E(\mathbb{F}_5) = \{\mathcal{O},\ (0,1),\ (0,4),\ (1,1),\ (1,4),\ (3,0),\ (4,1),\ (4,4)\}$$

Par exemple, le point $(0,1)$ est d'ordre 8 et le groupe $E(\mathbb{F}_5)$ est cyclique engendré par $(0,1)$ (ou par $(0,4)$, $(1,1)$ et $(1,4)$). Le groupe $E(\mathbb{F}_5)$ ne possède pas de point de 5-torsion non-trivial. Cependant, cette courbe n'est pas supersingulière car on a bien $E[5] \simeq \mathbb{Z}/5\mathbb{Z}$; pour montrer cela il suffit juste de trouver un point de 5-torsion $\neq \mathcal{O}$ dans $E(\overline{\mathbb{F}_5})$. Considérons le corps $\mathbb{F}_{5^8} \simeq \mathbb{F}_5[\theta]$ où $\theta^8 + 2 = 0$, on peut vérifier que le point :

$$P = (2\theta^4 + 1, 2\theta^6 + \theta^2)$$

est bien un point de 5-torsion ; P ne peut pas être défini sur une extension plus petite de $\mathbb{F}_5$.

L'utilisation des courbes elliptiques pour le problème du logarithme discret demande que l'on connaisse l'ordre du groupe $E(\mathbb{F}_q)$ (ou du moins l'ordre du point de base G dans $E(\mathbb{F}_q)$). Une estimation de cet ordre est donné par le théorème de Hasse-Weil :

Théorème 7 (Hasse-Weil) *Soit* E *une courbe elliptique définie sur* $\mathbb{F}_q$*, on a :*

$$|E(\mathbb{F}_q)| = q + 1 - t \text{ où } |t| \leq 2\sqrt{q}$$

De plus, si p est un nombre premier, alors pour toute valeur entière de t dans l'intervalle $[-2\sqrt{p}, 2\sqrt{p}]$, il existe une courbe elliptique E définie sur $\mathbb{F}_p$ telle que $|E(\mathbb{F}_p)| = p + 1 - t$. Supposons que nous connaissons un point $G \in E(\mathbb{F}_q)$ ainsi que son ordre $\ell \in \mathbb{N}$, alors si $\ell > \frac{q+1}{2} + \sqrt{q}$, le theorème de Hasse-Weil montre que le groupe $E(\mathbb{F}_q)$ est cyclique engendré par G et que ce groupe est d'ordre ℓ. L'utilisation directe de ce procédé est cependant assez rare car, en principe, on calcule d'abord l'ordre du groupe $E(\mathbb{F}_q)$ et on l'utilise pour trouver l'ordre du point G. La détermination du nombre de points $\mathbb{F}_q$-rationnels sur E est un problème important pour le logarithme discret et pour d'autres applications (test de primalité, factorisation etc.). Par exemple, si la courbe E est donnée par une équation de

Weierstrass courte : $y^2 = x^3+ax^2+bx+c$ sur $\mathbb{F}_q$ (donc, implicitement on a car $k \neq 2$), la formule :

$$|E(\mathbb{F}_q)| = p + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + ax^2 + bx + c}{q} \right) \tag{1.3}$$

permet de calculer $|E(\mathbb{F}_q)|$ avec une complexité $O(q^{1+\varepsilon})$ (le "ε" prenant en compte la complexité des opérations élémentaires dans $\mathbb{F}_q$ ainsi que celle du calcul du symbole de Legendre). Une adaptation fine de la méthode "Baby steps-Giant steps" permet de calculer $|E(\mathbb{F}_q)|$ avec une complexité $O(q^{1/2+\varepsilon})$. Des méthodes récentes très sophistiquées permettent d'obtenir $|E(\mathbb{F}_q)|$ avec une complexité en $O(\log(q)^{2+\mu})$ où μ est donné par la complexité de la multiplication dans $\mathbb{F}_q$.

Définition 6 *L'entier t définie dans le théorème précédent est appelé la* trace du Frobenius *ou la* trace de l'endomorphisme de Frobenius.

On peut caractériser les courbes supersingulière grâce à ce nombre t :

Proposition 8 *Soient E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et t la trace du Frobenius associée à E. La courbe E est supersingulière si et seulement si* $\operatorname{car} k \mid t$. *En particulier, si* $\operatorname{car} k = 2$ *ou* 3 *la courbe E est supersingulière si et seulement si $j(E) = 0$. Si $k = \mathbb{F}_p$, $p \geq 5$ premier, la courbe E est supersingulière si et seulement si $t = 0$.*

Si E est une courbe elliptique sur $\mathbb{F}_q$ et si t désigne la trace du Frobenius, on pose :

$$\chi_E(T) = T^2 - tT + q$$

si bien que $|E(\mathbb{F}_q)| = \chi_E(1)$. Le polynôme $\chi_E(T)$ est le polynôme caractéristique de l'endomorphisme de Frobenius, on a :

$$\chi_E(\sigma_q) = 0 \quad \text{(i.e. c'est l'endomorphisme nul)}$$

c'est-à-dire pour tout point $P \in E(\overline{\mathbb{F}_q})$, on a :

$$\sigma_q^2.P - t\,\sigma_q.P + qP = \mathcal{O}$$

Si on écrit $P = (x, y)$ cette dernière égalité s'écrit aussi :

$$(x^{q^2}, y^{q^2}) - t(x^q, y^q) + q(x, y) = \mathcal{O}$$

Théorème 9 *Soit E une courbe elliptique définie sur $\mathbb{F}_q$ et soient τ_1 et $\tau_2 = \overline{\tau_1}$ les deux racines* complexes *du polynômes $\chi_E(T)$. Pour tout $r \geq 1$, on a :*

$$|E(\mathbb{F}_{q^r})| = q^r + 1 - \tau_1^r - \tau_2^r$$

Ce théorème permet donc de calculer l'ordre du groupe $|E(\mathbb{F}_{q^r})|$ dès que l'on connait l'ordre de $|E(\mathbb{F}_q)|$.

Exemple : Reprenons l'exemple précédent où E est la courbe elliptique définie par : $y^2 = x^3 + 4x + 1$ sur le corps $\mathbb{F}_5$. On a déjà vu que $|E(\mathbb{F}_5)| = 8$ ainsi $t = -2$. Le polynôme $\chi_E(T)$ est donné par :

$$\chi_E(T) = T^2 + 2T + 5$$

Les racines complexes de ce polynômes sont $\tau_1 = -1 + 2i$ et $\tau_2 = -1 - 2i$. On en déduit que l'on a :

$$|E(\mathbb{F}_{25})| = 25 + 1 - \tau_1^2 - \tau_2^2 = 32$$

Le groupe $E(\mathbb{F}_{25})$ n'est pas cyclique et on a :

$$E(\mathbb{F}_{25}) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$$

Si on choisit de représenter les éléments de $\mathbb{F}_{25}$ comme des éléments de $\mathbb{F}_5[\theta]$ avec $\theta^2 = 2$, alors les points $(\theta + 1, 0)$ (d'ordre 2) et $(\theta, \theta + 3)$ (d'ordre 16) engendrent le groupe $E(\mathbb{F}_{25})$. Tous les éléments de $\mathbb{F}_{25}$ sont fixes par σ_5^2 et donc si le point $P = (x, y) \in E(\mathbb{F}_{25})$ on a :

$$\sigma_5^2.P + 2(\sigma.P) + 5P = (x, y) + 2(x^5, y^5) + 5(x, y) = 6(x, y) + 2(x^5, y^5) = \mathcal{O}$$

Prenons par exemple le point $P = (\theta, \theta + 3) \in E(\mathbb{F}_{25})$. On a :

$$6(\theta, \theta + 3) = (2\theta, -\theta - 2) \qquad \text{et} \qquad 2(x^5, y^5) = 2(-\theta, -\theta + 3) = (2\theta, \theta + 2)$$

Comme $t = -2 \not\equiv 0 \pmod 5$, la courbe E est ordinaire (ce que l'on savait déjà) ; il existe donc une extension $\mathbb{F}_{5^r}$ de $\mathbb{F}_5$ telle que $E(\mathbb{F}_{5^r})$ contienne un point de 5-torsion non-trivial i.e. il existe un entier $r \geq 1$ tel que $|E(\mathbb{F}_{5^r})|$ est divisible par 5. En calculant $|E(\mathbb{F}_{5^r})| = 5^r + 1 - \tau_1^r - \tau_2^r$ pour $r = 1, 2, \ldots$, on obtient pour $r = 8$:

$$|E(\mathbb{F}_{5^8})| = 391680 = 2^9 \times 3^2 \times 5 \times 17$$

1.4.2 Recherche des points rationnels

Pour donner un problème de logarithme discret à base d'une courbe elliptique $E/\mathbb{F}_q$, il faut avoir un point $\mathbb{F}_q$-rationnel sur E possédant, si possible, un grand ordre premier. Supposons, pour simplifier l'exposé, que $\operatorname{car} \mathbb{F}_q \geq 3$ et que la courbe E est définie par $y^2 = x^3 + ax^2 + bx + c$. Pour trouver un point $P \in E(\mathbb{F}_q)$, on choisit un élément x dans $\mathbb{F}_q$ tel que $A = x^3 + ax^2 + bx + c$ est un carré dans $\mathbb{F}_q$. Alors, le point $P = (x, y)$, où y est une racine carrée de A dans $\mathbb{F}_q$, est bien un point de $E(\mathbb{F}_q)$. Tout le problème consiste donc à pouvoir extraire une racine carrée dans un corps fini. Remarquons que si le corps est $\mathbb{F}_{2^r}$ alors tout élément $x \in \mathbb{F}_{2^r}$ est trivialement le carré de $x^{2^{m-1}}$.

Algorithme

- Entrées : un corps $\mathbb{F}_q$ de caractéristique $p \geq 3$, un élément $A \in \mathbb{F}_q$.
- Sortie : $r \in \mathbb{F}_q$ tel que $r^2 = A$ (s'il existe).

Étape 1 : Faire $\varepsilon \leftarrow \left(\frac{A}{q}\right)$.
Si $\varepsilon = -1$ alors A n'est pas un carré dans $\mathbb{F}_q$: fin.
Si $\varepsilon = 0$, sortir $r = 0$: fin.

Étape 2 : Choisir un élément $B \in \mathbb{F}_q$ tel que $\left(\frac{B^2 - 4A}{q}\right) = -1$.

Étape 3 : Dans le corps $\mathbb{F}_q[\theta] (\simeq \mathbb{F}_{q^2})$ où θ vérifie $\theta^2 - B\theta + A = 0$, faire $r \leftarrow \theta^{(q+1)/2}$.
Retourner r (ou $-r$).

Le choix de B dans l'étape 2 est probabiliste. Cependant, pour chaque élément $B \in \mathbb{F}_q$, on peut espérer qu'il y a, à peu près, une chance sur deux pour qu'un B pris au hasard convienne. Cette algorithme nécessite alors $O(\log q)$ multiplications dans $\mathbb{F}_q$ (essentiellement, des élevations à la puissance $\approx q/2$: autant que nécessaires pour trouver B et une pour calculer r). Pour montrer la validité de l'algorithme, il suffit juste de vérifier que $r^2 = A$. On a $r^2 = \theta^{q+1}$ et on peut écrire :

$$\theta = \frac{b+\delta}{2}$$

où $\delta^2 = B^2 - 4A \in \mathbb{F}_q[\theta]$. Si σ_q désigne l'automorphisne de Frobenius, on a $\sigma_q\delta = -\delta$ car $\sigma_q\delta$ est aussi une racine carrée de $B^2 - 4AC$ et $\delta \neq \sigma_q\delta$ (sinon $B^2 - 4A$ serait un carré dans $\mathbb{F}_q$). On peut aussi voir cela en utilisant directement l'expression du symbole de Legendre :

$$-1 = \left(\frac{B^2-4A}{q}\right) = (B^2-4A)^{\frac{q-1}{2}} = \delta^{q-1} \text{ donc } \delta^q = -\delta$$

Ceci étant, on a alors :

$$\begin{aligned}\theta^{q+1} = \left(\frac{b+\delta}{2}\right)^{q+1} &= \left(\frac{b+\delta}{2}\right)^q \left(\frac{b+\delta}{2}\right) = \left(\frac{b^q+\delta^q}{2^q}\right)\left(\frac{b+\delta}{2}\right) \\ &= \left(\frac{b-\delta}{2}\right)\left(\frac{b+\delta}{2}\right) = \left(\frac{b^2-\delta^2}{4}\right) = A\end{aligned}$$

Exemple : On pose $p = 1000033$, et on cherche la racine carrée de 69. Tout d'abord,

$$\left(\frac{69}{p}\right) = 69^{500016} = 1$$

et 69 est bien un carré dans $\mathbb{F}_p$. Ensuite, on essaie $B = 0$, 1, 2,... jusqu'à ce que $B^2 - 4A$ ne soit pas un carré dans $\mathbb{F}_p$: la valeur $B = 6$ convient. Dans le corps $\mathbb{F}_p[\theta]$, où $\theta^2 - 6\theta + 69 = 0$, on calcule $\theta^{(p+1)/2}$ et on trouve 736476, qui est bien une racine carrée de 69 dans $\mathbb{F}_p$.

Lorsque $q \equiv 3$, 5 ou 7 (mod 8), on peut éviter d'avoir recours à l'extension quadratique $\mathbb{F}_{q^2}/\mathbb{F}_q$, en effet :

Proposition 10 *On a : Si $q \equiv 3$ (mod 4) et si A est un carré dans $\mathbb{F}_q$ alors $A^{(q+1)/4}$ est une racine carrée de A.*
Si $q \equiv 5$ (mod 8) et si A est un carré dans $\mathbb{F}_q$, on pose $d = A^{(p-1)/4}$. Si $d = 1$ alors $r = A^{(q+3)/8}$ est une racine de A dans $\mathbb{F}_q$. Si $d = -1$ alors $r = 2A(4A)^{(p-5)/8}$ est une racine de A dans $\mathbb{F}_q$.

On a l'algorithme suivant pour trouver un point $\mathbb{F}_q$-rationnel sur E.

Algorithme
• Entrées : un corps $\mathbb{F}_q$ de caractéristique $p \geq 3$, $E : y^2 = x^3 + ax + b$ une courbe elliptique définie sur $\mathbb{F}_q$.
• Sortie : $P = (x, y) \in E(\mathbb{F}_q)$.

Étape 1 : Choisir x dans $\mathbb{F}_q$ tel que $\left(\frac{x^3+ax+b}{q}\right) = 1$.

Étape 2 : Calculer y une racine carrée de x^3+ax+b et retourner le point $P = (x, y)$.

Le choix de x à l'étape 1 est probabiliste, cependant on en trouve facilement un qui convient. Le coût de cet algorithme est également $O(\log(q))$ multiplications dans $\mathbb{F}_q$. On peut donner un algorithme similaire (mais plus technique) lorsque la caractéristique du corps est 2.

Exemple : Sur le corps $\mathbb{F}_p = \mathbb{F}_{1000033}$, on considère la courbe E définie par :

$$E \ : \ y^2 = x^3 + 33x + 69$$

On a calculé une racine carrée de 69, on a donc trouvé un point sur la courbe :

$$G = (0, 736476) \in E(\mathbb{F}_p)$$

Une fois que l'on a un point P sur la courbe elliptique, il faut aussi calculer son ordre ce qui se fait facilement si on connait $m = |E(\mathbb{F}_q)|$ et sa factorisation. De plus, pour le problème du logarithme discret, il faut que l'ordre de P soit un grand nombre premier. Ainsi, m doit être de la forme $m = s\ell$ où s est un petit entier et ℓ est un grand nombre premier : on peut donc supposer que $(s, \ell) = 1$. Si $sP = \mathcal{O}$ l'ordre de P est trop petit et il faut changer de point. Sinon, ℓ divise l'ordre de P et ℓ est exactement l'ordre de sP.

Exemple : Dans l'exemple précédent, on a $|E(\mathbb{F}_p)| = 1001041$, or 1001041 est un nombre premier, on en déduit que $E(\mathbb{F}_p)$ est cyclique engendré par G.

1.4.3 Exercices

Exercice 1 : Montrer que si $\operatorname{car} k = 2$ ou 3, la courbe E est supersingulière si et seulement si $j(E) = 0$.

Exercice 2 : Montrer la formule (1.3).

Exercice 3 : Soit E la courbe elliptique définie sur $\mathbb{F}_7$ par :

$$E \ : \ y^2 = x^3 - x - 2$$

1- Donner le discriminant et le j-invariant de E.
2- Calculer $|E(\mathbb{F}_7)|$ et énumérer tous les points de $E(\mathbb{F}_7)$.
3- Montrer que $E(\mathbb{F}_7)$ est cylclique engendré par le point $(2, 2)$. Écrire tous les éléments de $E(\mathbb{F}_7)$ comme multiple de $(2, 2)$.
4- Quelle est la plus petite extension de $\mathbb{F}_7$ sur laquelle on peut définir un point dans $E[7]$?
5- À l'aide d'un ordinateur, donner un point de 7-torsion sur cette extension.

Exercice 4 : Soit p un nombre premier impair tel que $p \equiv 2 \pmod 3$.
1- Montrer que l'application :

$$\begin{array}{ccc} \mathbb{F}_p & \longrightarrow & \mathbb{F}_p \\ x & \longmapsto & x^3 \end{array}$$

est bijective. En déduire que tout élément $x \in \mathbb{F}_p$ est le cube d'un unique élément dans $\mathbb{F}_p$.
Soit $a \in \mathbb{F}_p^*$ et E la courbe définie par :

$$E \quad y^2 = x^3 + a$$

2- Montrer que E est une courbe elliptique.
3- Calculer $|E(\mathbb{F}_p)|$ et en déduire la valeur t de la trace du Frobenius.
4- Donner une formule simple pour $|E(\mathbb{F}_{p^r})|$ lorsque $r \in \mathbb{N}$ (on pourra distinguer le cas r pair du cas r impair).
5- Montrer que pour tout $r \geq 1$, la courbe E considérée comme une courbe elliptique définie sur $\mathbb{F}_{p^r}$ est une courbe supersingulière.

Exercice 5 : Soit $p = 100003$, on considère les courbes elliptiques $E_b/\mathbb{F}_p$ définies par :

$$E_b \ : \ y^2 = x^3 + x + b$$

où $b = 5$, 9, 11, 12, 13 16, 25 ou 33.
1- Écrire un programme simple pour calculer $|E_b(\mathbb{F}_p)|$.
2- Trouver un point $G \in E_b(\mathbb{F}_p)$ dont l'ordre est exactement égal à $E_b(\mathbb{F}_p)$.

1.5 Protocole de signature

Le protocole d'authentification que nous allons donner repose sur le problème du logarithme discret sur une courbe elliptique. Dans ce cadre, il faut éviter certaines situations qui sont faibles du point de vue de la sécurité.

1.5.1 Choix du corps de définition

Il faut avant tout choisir le corps dans lequel on va définir la courbe elliptique. Pour éviter certaines attaques, il est préférable de choisir :

- Soit un corps premier $\mathbb{F}_p$ où p est un grand nombre premier.
- Soit un corps $\mathbb{F}_{p^r}$ de caractéristique p petite (par exemple $p = 2$) où r est un nombre premier tel que l'ordre de 2 dans $\mathbb{F}_r^*$ est grand (en particulier, il faut éviter les nombres premiers de Fermat et de Mersenne).

1.5.2 Choix de la courbe elliptique

Le corps $k = \mathbb{F}_q$ étant choisi, on note p sa caractéristique. Soit E la courbe elliptique considérée, t la trace du Frobenius, $G \in E(\mathbb{F}_q)$ le point de base et ℓ son ordre dans $E(\mathbb{F}_q)$. Également pour éviter certaines attaques, on note que :

- Si ℓ n'est pas premier, la réduction de Pohlig-Helman permet de simplifier le calcul du logarithme discret.

- Si $t = 1$, on dit que la courbe E est *anormale* (cas rare). Si de plus $q = p$ est premier, le problème du logarithme discret sur E peut être résolu en un temps linéaire (attaque de Smart).
- Si v est le plus petit entier tel que $\ell | q^v - 1$, alors grâce au *pairing de Weil*, on peut ramener le problème du logarithme discret sur la courbe elliptique à un problème de logarithme discret sur le corps fini $\mathbb{F}_{q^v}$ (attaque de Menezes-Okamoto-Vanstone).

On définit le degré MOV comme le plus petit entier v tel que $|E(\mathbb{F}_q)| \mid q^v - 1$. On doit donc s'assurer que v n'est pas petit (il n'est pas nécessaire de calculer exactement v). En particulier, la courbe E ne doit pas être supersingulière (si E est une courbe supersingulière, on peut montrer que son degré MOV est ≤ 6).

Exemple : On considère l'exemple de E définie par $y^2 = x^3 + 33x + 69$ dans le corps $\mathbb{F}_p = \mathbb{F}_{1000033}$. On a

- $\ell = 1001041$ qui est du même ordre de grandeur que p.
- $t = -1007$, la courbe n'est ni anormale, ni supersingulière.
- Le degré MOV de la courbe vaut 10320.

Calculer le degré MOV d'une courbe elliptique revient en fait à trouver v tel que $q^v \equiv 1 \pmod{|E(\mathbb{F}_q)|}$. C'est donc trouver l'ordre de q dans $(\mathbb{Z}/|E(\mathbb{F}_q)|\mathbb{Z})^*$.
Une bonne stratégie pour générer de "bonnes" courbes est de les construire au hasard et de s'assurer qu'elles semblent "raisonnables".

Algorithme

- Entrée : un corps fini k.
- Sorties : une courbe elliptique E/k, un point $G \in E(k)$ ayant un grand ordre.

  Étape 1 : Choisir au hasard une courbe elliptique E/k.

  Étape 2 : Calculer $|E(k)|$ et vérifier que la courbe n'est pas "anormale" et que son degré MOV est grand (sinon aller à l'étape 1).

  Étape 3 : Factoriser $|E(k)|$. Si cela prend trop de temps aller à l'étape 1. Si $|E(k)|$ n'est pas la forme $s\ell$ avec s petit et ℓ premier grand, aller à l'étape 1.

  Étape 4 : Chercher un point au hasard $P \in E(k)$; si $sP = \mathcal{O}$, aller à l'étape 4 (ou aller à l'étape 1 si la recherche d'un point convenable échoue). Sinon, retourner E et $G = sP$.

1.5.3 ECDSA

Le protocole "Elliptic Curve Digital Signature Algorithm" repose sur le problème du logarithme discret. Pour simplifier, nous allons supposer que les courbes sont définies sur un corps $\mathbb{F}_p$ où p est un (grand) nombre premier. Soit E une courbe elliptique définie sur $\mathbb{F}_p$ et G un point de $E(\mathbb{F}_p)$ d'ordre premier ℓ. Supposons alors qu'Alice et Bob communiquent et qu'ils veulent pouvoir authentifier les messages de chacun. Alice choisit un nombre aléatoire $1 < n_A < \ell - 1$ et calcule $P_A = n_A G$. Bob choisit également un nombre aléatoire $1 < n_B < \ell - 1$ et calcule $P_B = n_B G$. Alice publie sa clé publique : P_A. Sa clé secrète est n_A. Bob publie aussi sa clé publique et "protège" sa clé privée.

Algorithme (signature d'un message m par Alice)
• Entrée : un message m.
• Sortie : La signature du meesage m par Alice.
Étape 1 : Choisir un nombre aléatoire $1 < k < \ell - 1$ et calculer $kG = (x, y) \in E(\mathbb{F}_p)$. On peut toujours supposer que x est dans l'intervalle $[0, p-1]$ (c'est ce que l'on fait).
Étape 2 : Calculer r tel que $r = x \pmod{\ell}$. Si $r = 0$ retourner à l'étape 1.
Étape 3 : Calculer $s = k^{-1}(H(m) + n_A r) \pmod{\ell}$ où H est une fonction de hachage. Si $s = 0$ retourner à l'étape 1.
Étape 4 : Retourner la signature (r, s).

Dans l'étape 2, si $r = 0$ le nombre s de l'étape 3 ne dépend pas de n_A et la signature $(0, s)$ n'authentifie rien. Une signature du type $(r, 0)$ permettrait de retrouver la clé secrète d'Alice. De plus, on ne peut pas appliquer l'algorithme de vérification (car on a besoin de calculer s^{-1}). Comme k est choisi au hasard, la probabilité pour que $r = 0$ ou $s = 0$ est très faible.

Algorithme (vérification de la signature par Bob)
• Entrées : un message m et une signature (r, s).
• Sortie : Validation ou non de la signature d'Alice.
Étape 1 : Obtenir la clé publique d'Alice P_A.
Étape 2 : Si $(r, s) \notin [1, \ell - 1]^2$ ne pas valider la signature. Fin.
Étape 3 : Calculer $w = s^{-1} \pmod{\ell}$.
Étape 4 : Calculer $u_1 = H(m)w \pmod{\ell}$ et $u_2 = rw \pmod{\ell}$.
Étape 5 : Calculer $u_1 G + u_2 P_A = (x, y)$ et $v = x \pmod{\ell}$.
Étape 6 : Si $v \neq r$ ne pas valider la signature, sinon valider la signature.

1.5.4 Exercices

Exercice 1 : Calculer le degre MOV pour chacune des courbes de l'exercice 5 de la partie précédente.

Exercice 2 : Soit E une courbe elliptique définie sur un corps $\mathbb{F}_p$ avec p premier ≥ 5. On suppose que E est supersingulière, calculer le degré MOV de E.

Exercice 3 : Construire, sur un corps (à choisir) $\mathbb{F}_p$ avec p est premier $\approx 10^6$, un couple (E, G), où E est une courbe elliptique sur $\mathbb{F}_p$ et $G \in E(\mathbb{F}_p)$, qui semble raisonnable pour définir un problème du logarithme discret (comte tenu de la taille de p). En particulier, calculer le degré MOV, la trace du Frobenius etc.

Exercice 4 : Vérifier le protocole d'authentification ECDSA.

1.6 Factorisation à l'aide des courbes elliptiques

On peut également utiliser les courbes elliptiques pour factoriser certains entiers n. La méthode (ECM) dont nous allons donner le principe est due à Lenstra.

C'est l'analogue de la méthode $p-1$ de Pollard sur les corps $\mathbb{F}_p$.
L'idée générale est la suivante : supposons que nous voulions factoriser un entier n. On choisit aléatoirement une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$ (notons que nous n'avons pas défini ce qu'est une courbe elliptique sur un anneau mais une théorie générale existe). On fait alors des calculs sur la courbe elliptique (additions de points etc.) comme si $\mathbb{Z}/n\mathbb{Z}$ était un corps. Cependant, lorsque nous ajoutons deux points, nous devons inverser un certain nombre L dans $\mathbb{Z}/n\mathbb{Z}$ et cet anneau possède des diviseurs de zéro : il peut donc arriver que L ne soit pas inversible et que l'addition des deux points ne puisse pas se faire. Cet échec est en fait un succés pour nous ; car dire que L n'est pas inversible dans $\mathbb{Z}/n\mathbb{Z}$, c'est dire que L n'est pas premier avec n et $\text{pgcd}(n, L)$ est un diviseur non trivial de n.

1.6.1 Courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$

Soit n un entier non premier tel que $\text{pgcd}(n, 6) = 1$.

Définition 7 *Une courbe elliptique E définie $\mathbb{Z}/n\mathbb{Z}$ est donnée par une équation de Weierstrass courte :*

$$E \ : \ y^2 = x^3 + ax + b$$

telle que $\Delta(E) = 4a^3 + 27b^2$ est premier avec n.
L'ensemble des points de la courbe E, noté $E(\mathbb{Z}/n\mathbb{Z})$, est :

$$E(\mathbb{Z}/n\mathbb{Z}) = \{(x_1, y_1) \in (\mathbb{Z}/n\mathbb{Z})^2, \ \ y_1^2 = x_1^3 + ax_1 + b\} \cup \{\mathcal{O}\}$$

Le point $\mathcal{O}$ est appelé point à l'infini.

Exemple : On considère le nombre $n = 21$ et la courbe elliptique sur $\mathbb{Z}/21\mathbb{Z}$:

$$E \ : \ y^2 = x^3 + x + 1$$

On a $\Delta(E) = 8$ et :

$$\begin{aligned} E(\mathbb{Z}/21\mathbb{Z}) \ &= \ \{(0,1),(0,8),(0,13),(0,20),(7,6),(7,15),(9,2),(9,5),(9,16) \\ &\quad (9,19),(16,9),(16,12)\} \cup \{\mathcal{O}\} \end{aligned}$$

On peut définir une opération "+" partielle sur $E(\mathbb{Z}/n\mathbb{Z})$: si $P = (x_1, y_1)$ et $Q = (x_2, y_2)$ sont deux points de $E(\mathbb{Z}/n\mathbb{Z}) \setminus \{\mathcal{O}\}$, on pose :

- $P + \mathcal{O} = \mathcal{O} + P$.
- Si $x_1 = x_2$ et $y_1 \neq y_2$ alors $P + Q = \mathcal{O}$.
- Si $x_1 \neq x_2$ et si $L = x_2 - x_1$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $P + Q = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -y_1 + \lambda(x_1 - x_3) \ \text{ et } \ \lambda = (y_2 - y_1)L^{-1} \qquad (1.4)$$

- Si $P = Q$ et si $L = 2y_1$ est inversible dans $\mathbb{Z}/n\mathbb{Z}$ alors $P + Q = 2P = (x_3, y_3)$ avec

$$x_3 = \lambda^2 - 2x_1, \quad y_3 = -y_1 + \lambda(x_1 - x_3) \quad \text{et} \quad \lambda = (3x_1^2 + a)L^{-1} \qquad (1.5)$$

- Si $P = Q = (x_1, 0)$ alors $P + Q = P + P = \mathcal{O}$.

La loi que nous venons de définir n'est pas une une loi de groupe (sauf si n est premier). Si P est un point de la courbe, on peut, en utilisant ces formules, essayer de calculer P, $2P$, $3P$, $\cdots$. Si une de ces opérations ne peut pas se faire, nous mettons en évidence un facteur de n.

Exemple : Avec l'exemple précédent, si on prend $P = (0, 1)$, on calcule facilement $2P = (16, 12)$. Si maintenant, on veut calculer $2P + 2P$ on voit que l'on doit inverser le nombre $2 \times 12 = 3 \pmod{21}$ (équation (1.5)). Or, 3 n'est pas premier avec 21 et on obtient un facteur non trivial de 21 à savoir $\text{pgcd}(3, 21) = 3$.

Algorithme : Test avec E
• Entrées : un entier n à factoriser, une borne $B > 2$, une courbe elliptique E définie sur $\mathbb{Z}/n\mathbb{Z}$ et un point $P \in E(\mathbb{Z}/n\mathbb{Z})$.
• Sortie : un facteur non trivial de n ou un message d'échec pour ces paramètres.
Étape 1 : On pose $p \leftarrow 1$.
Étape 2 : On fait $p \leftarrow$ le nombre premier suivant p. Si $p > B$ retourner un message d'échec et terminer l'algorithme sinon faire $\ell \leftarrow 1$.
Étape 3 : Faire $\ell \leftarrow \ell p$, faire $P \leftarrow pP$. Si le calcul échoue, sortir le facteur mis en évidence. Si $\ell > B$ aller à l'étape 2. Sinon aller à l'étape 3.

On remarque que dans cet algorithme on essaie de calculer rP où :

$$r = \prod_{p \leq B} p^{\lfloor \log B / \log p \rfloor}$$

Si le calcul aboutit aucun facteur n'est trouvé.

1.6.2 Analyse de la méthode et réduction modulo p

Soit donc $n \in \mathbb{N}$, le nombre dont on cherche un facteur premier non-trivial, disons p. On considère une courbe elliptique aléatoire E définie sur l'anneau $\mathbb{Z}/n\mathbb{Z}$. Alors, si on réduit les coefficients de E modulo p, on obtient une courbe elliptique E_p définie sur $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. De même, si $P \in E(\mathbb{Z}/n\mathbb{Z})$, alors en reduisant les coordonnées de P modulo p, on obtient un point $P_p \in E_p(\mathbb{F}_p)$. On désignera par $\mathcal{O}_p$ le point à l'infini de $E(\mathbb{F}_p)$. Si P et Q sont deux points de $E(\mathbb{Z}/n\mathbb{Z})$, alors il est facile de voir que, si l'addition de P et de Q est possible, on a en fait $(P + Q)_p = P_p + Q_p$ (le premier signe "+" désigne l'opération partielle dans $E(\mathbb{Z}/n\mathbb{Z})$ alors que le deuxième signe "+" désigne la loi d'addition dans $E(\mathbb{F}_p)$). Si l'addition de P et Q n'est pas possible, c'est que le calcul de λ défini par (1.4) ou par (1.5) est impossible car on doit inverser un nombre L qui n'est justement pas premier avec n, il existe donc un nombre premier divisant le pgcd de n et de L, sans perdre de généralités nous pouvons supposer que c'est p et on a alors $P_p + Q_p = \mathcal{O}_p$. Ainsi, l'algorithme précédent détectera le facteur p (ou plutôt un multiple de p) si l'on a atteint un multiple m de l'ordre de P_p dans $E(\mathbb{F}_p)$ sans que m soit un multiple de l'ordre de P dans $E(\mathbb{Z}/n\mathbb{Z})$ (bien qu'il faudrait préciser cette notion un peu plus). Plus précisément, on détecte un facteur s'il existe deux nombres premiers p et q divisant n tels que m est un multiple de l'ordre de P_p dans $E_p(\mathbb{F}_p)$ et m n'est pas un multiple de l'ordre de P_q dans $E(\mathbb{F}_q)$.

Or, si la courbe E est choisi aléatoirement alors on peut considérer $|E_p(\mathbb{F}_p)|$ comme un nombre aléatoire compris entre $p+1-2\sqrt{p}$ et $p+1+2\sqrt{p}$ et il y a une probabilité non nulle pour que les facteurs premiers de $|E(\mathbb{F}_p)|$ soient "petits". Ainsi, si le nombre B de l'algorithme est assez grand, on a une chance non nulle pour qu'un produit de puissances de nombres premiers $< B$ soit en fait un multiple de $|E(\mathbb{F}_p)|$ et donc que l'algorithme détecte un facteur premier. Si l'algorithme n'aboutit pas, on recommence avec une autre courbe E.

1.6.3 Algorithme ECM

Comme n est composé, il est difficile de calculer une racine carrée modulo n et on ne peut pas utiliser les procédés de la partie 1.4.2 pour trouver un point P au hasard dans $E(\mathbb{Z}/n\mathbb{Z})$. Au lieu de cela, on choisit d'abord au hasard trois nombres a, x_1 et y_1 modulo n et on pose $b = y_1^2 - (x_1^3 + ax_1)$. Le point $P = (x_1, y_1)$ est alors un point de la courbe $E : y^2 = x^3 + ax + b$.

Les discussions précédentes suggèrent alors la méthode suivante :

Algorithme
- Entrées : un entier n à factoriser une borne $B \in \mathbb{N}$.
- Sortie : un facteur non trivial de n ou un message d'échec pour ces paramètres.

  Étape 1 : Choisir au hasard x_1, y_1 et a dans $\mathbb{Z}/n\mathbb{Z}$. Définir $E : y^2 = x^3 + ax + (y_1^2 - x_1^3 - ax_1)$.

  Étape 2 : Faire $d \leftarrow \text{pgcd}(\Delta(E), n)$. Si $1 < d < n$ retourner d, fin. Si $d = n$ retourner à l'étape 1.

  Étape 3 : Faire $P \leftarrow (x_1, y_1)$. Chercher un facteur de n en utilisant l'algorithme "Test avec E" pour les paramètres E, B et P. Si l'algorithme détecte un facteur, retourner ce facteur, fin. Sinon, aller à l'étape 1.

Une analyse détaillée montrent que l'on doit choisir :

$$B \approx \exp\left(\left(\frac{\sqrt{2}}{2} + \varepsilon\right) \log(p)^{1/2} \log(\log(p))^{1/2}\right)$$

où ε est un "petit" nombre réel (tendant vers 0 lorsque p tend vers l'infini). Le seul problème avec la formule précédente, c'est que l'on ne connait pas p ! Dans la pratique, on réitère le procédé en incrémentant B au fur et à mesure. On peut établir que la complexité de la méthode de courbes elliptiques est de l'ordre de

$$\exp((1+\varepsilon) \log(n)^{1/2} \log(\log(n))^{1/2})$$

(complexité sous-exponentielle). Cette méthode est en particulier très efficace pour factoriser des grands entiers qui admettent des facteurs premiers de l'ordre jusqu'à $\approx 10^{40}$.

Exemple : On veut factoriser avec la méthode des courbes elliptiques le nombre :

$$n = 203131958479987807 = 2011 \times 10000019 \times 10101023$$

Bien sûr, à priori on ne connait pas la factorisation à l'avance, mais on va voir comment la méthode des courbes elliptiques est capable de détecter le facteur premier $p = 2011$. Tout d'abord, on choisit le nombre B, pour cela on calcule :

$$\exp\left(\left(\frac{\sqrt{2}}{2}\right)\log(2011)^{1/2}\log(\log(2011))^{1/2}\right) \approx 16.08$$

On pose alors $B = 16$ (dans la pratique, on ne peut pas calculer B de cette manière puisque l'on ne connait pas le nombre p, mais on prend B de plus en plus grand jusqu'à ce que la méthode aboutisse). Ainsi le nombre r définit après l'algorithme "Test avec E" est donné par :

$$r = 2^4 \times 3^2 \times 5 \times 7 \times 11 \times 13$$

On choisit une courbe E aléatoirement sur $\mathbb{Z}/n\mathbb{Z}$ et on considère que le nombre $|E_{2011}(\mathbb{F}_{2011})|$ est un nombre au hasard plus petit que $2012 + 2\sqrt{2011}$. On peut montrer que les diviseurs premiers d'un tel nombre sont *tous* plus petits que B avec une probabilté $\approx 1/B$. En testant donc quelques dizaines de courbes, on a une bonne chance de détecter le facteur 2011. Nous prenons les courbes elliptiques suivantes :

$$E \ : \ y^2 = x^3 + x + (y_1^2 - x_1^3 - x_1)$$

pour x_1, $y_1 = 1, 2, 3$. Dans le tableau suivant, nous donnons la factorisation de $|E_{2011}(\mathbb{F}_{2011})|$ pour chacune de ces 9 courbes.

$y_1 \backslash x_1$	1	2	3
1	$2^2 \times 11 \times 47$	$2^2 \times 503$	$2 \times 7 \times 11 \times 13$
2	$2^5 \times 3^2 \times 7$	43×47	2×991
3	$2^2 \times 3 \times 167$	$2^2 \times 11 \times 47$	$2^2 \times 7 \times 73$

Ainsi, le couple $(x_1, y_1) = (3, 1)$ devrait permettre de détecter le facteur 2011. Dans ce cas, on a $P = (3, 1)$ et la courbe E est définie par $E : y^2 = x^3 + x - 29$ sur $\mathbb{Z}/n\mathbb{Z}$. On a successivement :

$$\begin{aligned}
P_1 = \quad 2^4 P \quad &= (113335492298694779, 120072510320811350) \\
P_2 = \quad 3^2 P_1 \quad &= (88473308409788250, 44958990040955827) \\
P_3 = \quad 5 \times P_2 \quad &= (62528891122227755, 4402639539853129) \\
P_4 = \quad 7 \times P_3 \quad &= (80943592970473600, 19944167038863674) \\
P_5 = \quad 11 \times P_4 \quad &= (176914498221880419, 88610394536361644)
\end{aligned}$$

Par contre le calcul de $13P_5$ aboutit à la détection du facteur 2011. En effet, par exemple, on calcule facilement :

$$12P_5 = (126794386927080337, 169864995554483396)$$

Maintenant, le calcul de $12P_5 + P_5 = 13P_5$ demande l'inversion de :

$$176914498221880419 - 126794386927080337 = 50120111294800082$$

Or, on a $\text{pgcd}(50120111294800082, n) = 2011$. Les multiplications par 3^2 et par 5 étaient inutiles mais on ne peut pas le savoir à l'avance !

1.6.4 Exercices

Exercice 1 : Expliquez ce qui se passe si on prend le couple $(x_1, y_1) = (1, 2)$ dans l'exemple précédent (en prenant $r = 2^5 \times 3^2 \times 7 \times 11 \times 13$).

Exercice 2 : Factoriser le nombre $10000019 \times 10101023 = 101010421919437$ en utilisant la courbe elliptique $E : y^2 = x^3 + x - 64$, le point $P = (4, 4)$ et $B = 113$.