Université Pierre et Marie Curie
Cours de cryptographie MM067 - 2009/10
Alain Kraus

# Chapitre VII - Courbes elliptiques

On va présenter dans ce chapitre une introduction à la théorie des courbes elliptiques et en donner des applications à la cryptographie. On verra l'analogue elliptique de certains cryptosystèmes à clés publiques, et des applications aux problèmes de primalité et de factorisation des entiers. Le lien entre « cryptographie et courbes elliptiques » est apparu il y a une trentaine d'années. Par exemple, la théorie des courbes elliptiques sur un corps fini est très utile pour la cryptographie à clé publique. On sera amené à admettre quelques résultats essentiels qui seraient trop longs à démontrer ici, mais que l'on pourra utiliser librement, aussi bien d'un point de vue théorique que pratique.

**Table des matières**

1. Définition - Généralités 1
2. Loi de groupe 7
3. Points de torsion 15
4. Courbes elliptiques sur les corps finis 23
5. Méthodes de comptage 32
6. Cryptosystèmes elliptiques 37
7. Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$ 41
8. Primalité - Théorème ECPP 47
9. Méthode de factorisation ECM 51

## 1. Définition - Généralités

On ne va pas donner ici la définition la plus générale d'une courbe elliptique définie sur un corps commutatif. Elle n'est pas indispensable pour nos objectifs. Pour cette raison, on se placera dans la situation où la caractéristique du corps de base est distincte de 2 et 3. Plus précisément, dans tout le chapitre, la lettre $K$ désignera

un corps de caractéristique 0, ou un corps fini de caractéristique distincte de 2 et 3.

On notera $\overline{K}$ une clôture algébrique de $K$ choisie implicitement.

### 1. Définition

Nous adopterons la définition suivante.

**Définition 7.1.** *Une courbe elliptique définie sur $K$ est une courbe projective plane d'équation*

$$y^2z = x^3 + axz^2 + bz^3, \tag{1}$$

*où $a$ et $b$ sont des éléments de $K$ vérifiant la condition*

$$4a^3 + 27b^2 \neq 0. \tag{2}$$

Il convient d'en expliquer la signification. Rappelons pour cela que le plan projectif sur $\overline{K}$, que l'on notera $\mathbb{P}^2\big(\overline{K}\big)$ ou $\mathbb{P}^2$, est l'ensemble quotient

$$\overline{K}^3 - \big\{(0,0,0)\big\}\big/ \sim$$

où $\sim$ est la relation d'équivalence telle que pour tous $(x,y,z)$ et $(x',y',z')$ non nuls de $\overline{K}^3$,

$$(x,y,z) \sim (x',y',z') \iff \text{ il existe } \lambda \in \overline{K}^* \text{ tel que } (x',y',z') = \lambda(x,y,z).$$

Il s'identifie à l'ensemble des droites vectorielles de $\overline{K}^3$. Pour tout $(x,y,z)$ non nul dans $\overline{K}^3$, on note $[x,y,z]$ sa classe d'équivalence.

Considérons des éléments $a$ et $b$ de $K$. Dans l'anneau des polynômes $K[X,Y,Z]$, posons

$$F = Y^2Z - (X^3 + aXZ^2 + bZ^3).$$

C'est un polynôme homogène de degré 3. Si $(x,y,z)$ est un élément non nul de $\overline{K}^3$, la condition $F(x,y,z) = 0$, ne dépend que de sa classe dans $\mathbb{P}^2\big(\overline{K}\big)$.

**Terminologie.** Soit $P = [x,y,z]$ un point de $\mathbb{P}^2\big(\overline{K}\big)$. On dit que $P$ est un zéro de $F$ dans $\overline{K}$, ou plus simplement un zéro de $F$, si l'on a $F(x,y,z) = 0$. On signifie par, courbe projective plane d'équation (1), l'ensemble des zéros de $F$ dans $\overline{K}$.

Quant à la condition (2), elle signifie que les racines dans $\overline{K}$ du polynôme

$$f = X^3 + aX + b$$

sont simples. Plus précisément :

**Lemme 7.1.** *Le discriminant*[(1)] *de $f$ est $-(4a^3+27b^2)$. En particulier, les racines de $f$ sont simples si et seulement si $4a^3+27b^2$ est non nul.*

Démonstration : Soit $\Delta$ le discriminant de $f$. Notons $\alpha$, $\beta$ et $\gamma$ les racines de $f$ dans $\overline{K}$ et $f'$ le polynôme dérivé de $f$. Vérifions que l'on a

$$\Delta = -f'(\alpha)f'(\beta)f'(\gamma). \tag{3}$$

On a $f=(X-\alpha)(X-\beta)(X-\gamma)$, d'où

$$f' = (X-\alpha)(X-\beta)+(X-\alpha)(X-\gamma)+(X-\beta)(X-\gamma),$$

puis les égalités

$$f'(\alpha)=(\alpha-\beta)(\alpha-\gamma),\quad f'(\beta)=(\beta-\alpha)(\beta-\gamma),\quad f'(\gamma)=(\gamma-\alpha)(\gamma-\beta),$$

ce qui implique (3). Par suite, on a

$$\Delta = -(3\alpha^2+a)(3\beta^2+a)(3\gamma^2+a),$$

autrement dit,

$$\Delta = -\Big(27(\alpha\beta\gamma)^2+9a(\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2)+3a^2(\alpha^2+\beta^2+\gamma^2)+a^3\Big).$$

Par ailleurs, on a

$$\alpha^2\beta^2+\alpha^2\gamma^2+\beta^2\gamma^2 = (\alpha\beta+\alpha\gamma+\beta\gamma)^2-2\alpha\beta\gamma(\alpha+\beta+\gamma),$$

$$\alpha^2+\beta^2+\gamma^2 = (\alpha+\beta+\gamma)^2-2(\alpha\beta+\alpha\gamma+\beta\gamma).$$

Les relations entre les coefficients et les racines de $f$,

$$\alpha+\beta+\gamma=0,\quad \alpha\beta+\alpha\gamma+\beta\gamma=a\quad\text{et}\quad \alpha\beta\gamma=-b,$$

entraînent alors le résultat.

---

(1) Soit $g$ un polynôme unitaire à coefficients dans $K$ de degré $n\geq 1$. Soient $\alpha_1,\cdots,\alpha_n$ ses $n$ racines dans $\overline{K}$ comptées avec multiplicités. Le discriminant $\Delta$ de $g$ est défini par l'égalité

$$\Delta = \prod_{i<j}(\alpha_i-\alpha_j)^2.$$

C'est un élément de $K$.

**Terminologie.** Les éléments $a$ et $b$ vérifiant la condition (2), on dit que la courbe elliptique d'équation (1) est définie sur $K$ pour préciser que $a$ et $b$ sont dans $K$.

**Remarque 7.1.** En toute caractéristique, une courbe elliptique sur un corps peut être définie comme étant une courbe projective lisse d'équation

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \tag{4}$$

où les $a_i$ sont dans le corps de base. Le mot «lisse» signifie qu'il n'existe pas de point $[x_0, y_0, z_0] \in \mathbb{P}^2$ tel que, en posant

$$F(x, y, z) = y^2z + a_1xyz + a_3yz^2 - (x^3 + a_2x^2z + a_4xz^2 + a_6z^3),$$

on ait

$$F(x_0, y_0, z_0) = \frac{\partial F}{\partial x}(x_0, y_0, z_0) = \frac{\partial F}{\partial y}(x_0, y_0, z_0) = \frac{\partial F}{\partial z}(x_0, y_0, z_0) = 0.$$

On peut démontrer que, $K$ étant de caractéristique distincte de 2 et 3, une courbe lisse d'équation (4) est «isomorphe sur $K$» à une courbe de la forme (1) pour laquelle la condition (2) est satisfaite. Dans notre situation, la définition 7.1 n'est donc pas restrictive.

**2. Partie affine - Point à l'infini**

Posons

$$U = \Big\{[x, y, z] \in \mathbb{P}^2\big(\overline{K}\big) \mid z \neq 0\Big\}.$$

On dispose de l'application $\Phi : U \to \overline{K}^2$ définie par

$$\Phi([x, y, z]) = \Big(\frac{x}{z}, \frac{y}{z}\Big).$$

C'est une bijection, dont l'application réciproque est donnée par la formule

$$\Phi^{-1}(x, y) = [x, y, 1].$$

Considérons des éléments $a$ et $b$ de $K$ tels que $4a^3 + 27b^2 \neq 0$. Soit $E$ la courbe elliptique définie sur $K$ d'équation

$$y^2z = x^3 + axz^2 + bz^3.$$

L'ensemble des points $[x, y, z] \in E$ tels que $z = 0$ est réduit au singleton $\big\{O\big\}$ où

$$O = [0, 1, 0].$$

Par ailleurs, $E \cap U$ s'identifie via $\Phi$ à l'ensemble des éléments $(x, y)$ de $\overline{K}^2$ vérifiant l'égalité

$$y^2 = x^3 + ax + b. \tag{5}$$

**Terminologie.** On dira que $E \cap U$ est la partie affine de $E$ et que $O$ est le point à l'infini de $E$.

Dans toute la suite, on identifiera $E \cap U$ et le sous-ensemble de $\overline{K}^2$ formé des éléments $(x, y)$ vérifiant (5). Avec cette identification, on a

$$E = \Big\{(x, y) \in \overline{K} \times \overline{K} \mid y^2 = x^3 + ax + b\Big\} \cup \Big\{O\Big\}. \tag{6}$$

Ainsi, $E$ est la courbe affine d'équation (5) à laquelle on adjoint le point à l'infini $O$. C'est pourquoi on définira souvent une courbe elliptique par sa partie affine, sans préciser le point $O$. Cela étant, il ne faudra pas perdre de vue l'importance du point à l'infini, comme on s'en rendra compte notamment dans la définition de la loi de groupe sur $E$ que l'on verra plus loin.

**Remarque 7.2.** On retiendra qu'une courbe affine d'équation de la forme (5) est une courbe elliptique si et seulement si, par définition, la condition (2) est satisfaite.

### 3. Points rationnels d'une courbe elliptique

Soit $L$ une extension de $K$ dans $\overline{K}$.

**Définition 7.2.** *Soit $P = [x, y, z]$ un point de $\mathbb{P}^2$. On dit que $P$ est rationnel sur $L$ s'il existe $\lambda \in \overline{K}^*$ tel que $\lambda x$, $\lambda y$ et $\lambda z$ soient dans $L$. On note $\mathbb{P}^2(L)$ l'ensemble des points de $\mathbb{P}^2$ rationnels sur $L$.*

Cela justifie la notation $\mathbb{P}^2 = \mathbb{P}^2\big(\overline{K}\big)$.

**Remarque 7.3.** Étant donné un point $[x_1, x_2, x_3] \in \mathbb{P}^2$, le fait qu'il soit rationnel sur $L$ n'implique pas que les $x_i$ soient dans $L$. Cela signifie qu'il existe $i$ tel que $x_i$ soit non nul, et que chaque $\frac{x_j}{x_i}$ appartienne à $L$.

Soit $E$ une courbe elliptique définie sur $K$ d'équation (1).

**Définition 7.3.** *Un point de $E$ est dit rationnel sur $L$ s'il appartient à $E \cap \mathbb{P}^2(L)$. On note $E(L)$ l'ensemble des points de $E$ rationnels sur $L$.*

Par définition, on a donc

$$E = E\big(\overline{K}\big). \tag{7}$$

Le point $O = [0, 1, 0]$ appartient à $E(K)$. Soit $(x, y) \in \overline{K}^2$ un point de la partie affine de $E$. Par définition, il est rationnel sur $L$ si et seulement si $x$ et $y$ sont dans $L$. Il en résulte que l'on a

$$E(L) = \Big\{(x, y) \in L \times L \;\Big|\; y^2 = x^3 + ax + b\Big\} \cup \Big\{O\Big\}. \tag{8}$$

**Exemples 7.1.**

1) Soit $E$ la courbe elliptique définie sur $\mathbb{F}_5$ d'équation

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

(On notera que la condition (2) est satisfaite). On vérifie que l'on a

$$E(\mathbb{F}_5) = \Big\{(0,1), (0,4), (2,1), (2,4), (3,1), (3,4), (4,2), (4,3)\Big\} \cup \Big\{O\Big\}.$$

Soit $\mathbb{F}_{25}$ le sous-corps de $\overline{\mathbb{F}_5}$ à vingt-cinq éléments. On a

$$\mathbb{F}_{25} = \mathbb{F}_5(\alpha) \quad \text{où } \alpha \in \overline{\mathbb{F}_5} \quad \text{vérifie} \quad \alpha^2 + \alpha + 1 = 0.$$

On constate que l'on a

$$E(\mathbb{F}_{25}) = \Big\{(0, \pm 1), (2, \pm 1), (3, \pm 1), (4, \pm 2), (1 + \alpha, \pm 2\alpha), \big(2 + 2\alpha, \pm(4 + \alpha)\big),$$

$$(2 + 3\alpha, \pm 2), (4 + 2\alpha, \pm 2), \big(3\alpha, \pm(2 + \alpha)\big), \big(4, \pm(2 + 2\alpha)\big), \big(1, \pm(3 + \alpha)\big),$$

$$\big(1 + 3\alpha, \pm(3 + \alpha)\big), \big(3 + 2\alpha, \pm(3 + \alpha)\big)\Big\} \cup \Big\{O\Big\}.$$

Le cardinal de $E(\mathbb{F}_5)$ est 9 et celui de $E(\mathbb{F}_{25})$ est 27. En particulier, le cardinal de $E(\mathbb{F}_5)$ divise celui de $E(\mathbb{F}_{25})$. On verra que cela n'est pas un hasard.

2) Considérons la courbe elliptique $E$ sur $\mathbb{Q}$ d'équation

$$y^2 = x^3 + 45.$$

On peut démontrer que $E(\mathbb{Q}) = \big\{O\big\}$. Ce n'est pas un résultat facile, mais on peut l'obtenir relativement simplement à condition de développer suffisamment la théorie des courbes elliptiques sur $\mathbb{Q}$. Cela étant, il est facile de trouver des corps quadratiques $K$ pour lesquels $E(K)$ n'est pas trivial. Par exemple, $\big(0, 3\sqrt{5}\big)$ est un point de $E$ rationnel sur $\mathbb{Q}\big(\sqrt{5}\big)$, ou encore $\big(-1, 2\sqrt{11}\big)$ est un point de $E$ rationnel sur $\mathbb{Q}\big(\sqrt{11}\big)$.
Limitons nous ici à prouver qu'il n'existe pas de points $(x, y) \in E(\mathbb{Q})$ avec $x$ et $y$ dans $\mathbb{Z}$. Supposons qu'il existe un tel point $(x, y)$. L'entier $x$ est impair (car le carré d'un nombre impair est congru à 1 modulo 8) et est congru à 3 modulo 4. On a donc $x \equiv 3, 7$ mod. 8.

De plus, $x$ n'est pas multiple de 3. En effet, si $x = 3X$, on a $y = 3Y$, d'où $Y^2 = 3X^3 + 5$. On obtient $Y^2 \equiv 2$ mod. 3 et une contradiction. L'idée est alors de trouver un entier $a$ convenable de sorte que $y^2 - 2a^2$ soit divisible par un nombre premier $p$ impair non congru à $\pm 1$ modulo 8, et ne divisant pas $a$. L'existence d'un tel entier $a$ entraîne alors une contradiction. En effet, on a dans ce cas $y^2 \equiv 2a^2$ mod. $p$ et $a$ étant inversible modulo $p$, cela entraîne que 2 est un carré dans $\mathbb{F}_p$, or $p$ est impair non congru à $\pm 1$ modulo 8. Supposons $x \equiv 3$ mod. 8. Avec $a = 6$, on obtient

$$y^2 - 2.6^2 = x^3 - 27 = (x-3)(x^2 + 3x + 9).$$

On a $x^2 + 3x + 9 \equiv 3$ mod. 8, donc $x^2 + 3x + 9$ possède un diviseur premier $p$ impair non congru à $\pm 1$ modulo 8. On a $p \neq 3$, sinon 3 diviserait $x$, d'où la contradiction cherchée. Supposons $x \equiv 7$ mod. 8. Avec $a = 3$, on a

$$y^2 - 2.3^2 = x^3 + 27 = (x+3)(x^3 - 3x + 9).$$

On a $x^3 - 3x + 9 \equiv 3$ mod. 8, et l'on aboutit à la même conclusion, d'où notre assertion.

3) Soient $a$ un entier relatif impair et $E$ la courbe elliptique définie sur $\mathbb{Q}$ d'équation

$$y^2 = x^3 + (2a)^3 - 1.$$

Vérifions que $E$ n'a pas de points $(x, y) \in \mathbb{Z}^2$. Supposons qu'il existe un tel point $(x, y)$. On a les égalités

$$y^2 + 1 = (x + 2a)\big((x-a)^2 + 3a^2\big).$$

Nécessairement, $x$ est impair donc $x - a$ est pair, d'où $(x-a)^2 + 3a^2 \equiv 3$ mod. 4. Par suite, $(x-a)^2 + 3a^2$ possède un diviseur premier $p \equiv 3$ mod. 4. Le fait que $p$ divise $y^2 + 1$ conduit alors à une contradiction. En particulier, il existe une infinité d'entiers qui ne s'écrivent pas comme la différence d'un carré et d'un cube d'entiers.

## 2. Loi de groupe

Soit $E$ une courbe elliptique définie sur $K$. Pour toute extension $L$ de $K$ dans $\overline{K}$, on va munir $E(L)$ d'une structure naturelle de groupe abélien, d'élément neutre le point à l'infini.

### 1. Droites de $\mathbb{P}^2$

**Définition 7.4.** *Une droite de $\mathbb{P}^2$ est une partie de $\mathbb{P}^2$ formée des points $[x, y, z]$ tels que*

$$ux + vy + wz = 0,$$

*où $u$, $v$ et $w$ sont des éléments non tous nuls de $\overline{K}$.*

On parle alors de la droite d'équation $ux+vy+wz=0$. Une droite d'équation $x=\lambda z$, où $\lambda$ est dans $\overline{K}$, est dite verticale. Une telle droite passe par le point $O=[0,1,0]$. En fait, toute droite passant par $O$ a une équation de la forme $ux+wz=0$. On dit souvent que la droite d'équation $z=0$ est la droite à l'infini. En identifiant la partie de $\mathbb{P}^2$ formée des points $[x,y,z]$ tels que $z\neq 0$ avec $\overline{K}^2$, le plan projectif s'interprète comme la réunion de $\overline{K}^2$ avec la droite à l'infini.

**Lemme 7.2.** *Soient $P=[a_1,a_2,a_3]$ et $Q=[b_1,b_2,b_3]$ deux points distincts de $\mathbb{P}^2$. Il existe une unique droite de $\mathbb{P}^2$ passant par $P$ et $Q$. C'est l'ensemble des points $[x,y,z]\in\mathbb{P}^2$ tels que le déterminant de la matrice*

$$\begin{pmatrix} a_1 & b_1 & x \\ a_2 & b_2 & y \\ a_3 & b_3 & z \end{pmatrix}$$

*soit nul. Autrement dit, c'est la droite d'équation $ux+vy+wz=0$, avec*

$$u=a_2b_3-a_3b_2,\quad v=a_3b_1-a_1b_3,\quad w=a_1b_2-a_2b_1.$$

Démonstration : Les éléments $u,v$ et $w$ ne sont pas tous nuls car $P$ et $Q$ sont distincts. L'équation $ux+vy+wz=0$ est donc celle d'une droite contenant $P$ et $Q$. Considérons alors une droite de $\mathbb{P}^2$ passant par $P$ et $Q$ d'équation

$$u'x+v'y+w'z=0.$$

Soient $f$ et $g$ les formes linéaires $\overline{K}^3\to\overline{K}$ définies par

$$f(x,y,z)=ux+vy+wz\quad\text{et}\quad g(x,y,z)=u'x+v'y+w'z.$$

Le noyau de $f$ et $g$ est le plan de $\overline{K}^3$ engendré par $(a_1,a_2,a_3)$ et $(b_1,b_2,b_3)$. En particulier, $f$ et $g$ ont le même noyau. Dans le dual de $\overline{K}^3$, l'orthogonal du noyau de $f$ (resp. $g$) est la droite engendrée par $f$ (resp. $g$). Il existe donc $\lambda\in\overline{K}$ non nul tel que $f=\lambda g$, d'où l'assertion d'unicité.

### 2. Tangente à $E$ en un point

Notons désormais

$$y^2z=x^3+axz^2+bz^3$$

l'équation de $E$, où $a$ et $b$ sont dans $K$. Posons

$$F=Y^2Z-(X^3+aXZ^2+bZ^3)\in K[X,Y,Z],$$

$$F_X=\frac{\partial F}{\partial X},\quad F_Y=\frac{\partial F}{\partial Y},\quad F_Z=\frac{\partial F}{\partial Z}.$$

On a

$$F_X = -(3X^2 + aZ^2), \quad F_Y = 2YZ, \quad F_Z = Y^2 - (2aXZ + 3bZ^2). \tag{9}$$

**Lemme 7.3.** *Il n'existe pas de point $P \in E$ tel que*

$$F_X(P) = F_Y(P) = F_Z(P) = 0.$$

Démonstration : Supposons qu'il existe un tel point $P$. On a $F_Z(O) = 1$, donc $P$ est distinct de $O$. Posons $P = [x, y, 1]$. La caractéristique de $K$ étant distincte de 2, on a $y = 0$. On obtient

$$3x^2 + a = 0 \quad \text{et} \quad 2ax + 3b = 0.$$

Supposons $a \neq 0$. On a alors $x = -\frac{3b}{2a}$, d'où $4a^3 + 27b^2 = 0$. Si $a = 0$, vu que la caractéristique de $K$ n'est pas 3, on a $b = 0$. On obtient ainsi une contradiction et le résultat.

**Définition 7.5.** *Pour tout point $P \in E$, la tangente à $E$ en $P$ est la droite d'équation*

$$F_X(P)x + F_Y(P)y + F_Z(P)z = 0.$$

**Lemme 7.4.** *1) L'équation de la tangente à $E$ au point $O$ est $z = 0$.*
*2) Soit $P = [x_0, y_0, 1]$ un point de $E$ distinct de $O$. L'équation de la tangente à $E$ en $P$ est*

$$F_X(P)(x - x_0 z) + F_Y(P)(y - y_0 z) = 0.$$

Démonstration : Cela résulte des formules (9) et de l'égalité $y_0^2 = x_0^3 + ax_0 + b$.

**Exemple 7.2.** Soit $\alpha$ une racine dans $\overline{K}$ du polynôme $X^3 + aX + b$. Le point $P = (\alpha, 0)$ appartient à $E$. On a $F_X(P) = -(3\alpha^2 + a) \neq 0$ (lemme 7.1) et $F_Y(P) = 0$. La tangente à $E$ en $P$ est donc verticale et a pour équation

$$x = \alpha z.$$

En particulier, elle passe par $O$.

### 3. Loi de composition des cordes-tangentes

On va définir ici une loi de composition interne sur $E$, qui va s'avérer ne pas être une loi de groupe, mais qu'il suffira de modifier « à l'aide d'une symétrie convenable » pour obtenir la loi de groupe que l'on a en vue. Pour tout point $R$ de $E$ distinct de $O$, on notera $R = [x_R, y_R, 1]$.

**Proposition 7.1.** *Soient $P$ et $Q$ des points de $E$. Soit $D$ la droite de $\mathbb{P}^2$ passant par $P$ et $Q$ si $P \neq Q$, ou bien la tangente à $E$ en $P$ si $P = Q$. On a*

$$D \cap E = \Big\{P, Q, f(P,Q)\Big\},$$

*où $f(P,Q)$ désigne le point de $E$ défini par les conditions suivantes.*

*1) Supposons $P \neq Q$, $P \neq O$ et $Q \neq O$.*

*1.1) Supposons $x_P \neq x_Q$. Posons*

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad et \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

*On a*

$$f(P,Q) = \Big[\lambda^2 - x_P - x_Q, \lambda\big(\lambda^2 - x_P - x_Q\big) + \nu, 1\Big]. \tag{10}$$

*1.2) Si $x_P = x_Q$, on a $f(P,Q) = O$.*

*2) Supposons $P \neq O$ et $Q = O$. On a*

$$f(P,O) = \big[x_P, -y_P, 1\big]. \tag{11}$$

*De même, si $P = O$ et $Q \neq O$, on a $f(O,Q) = [x_Q, -y_Q, 1]$.*

*3) Si $P = Q = O$, on a $f(O,O) = O$.*

*4) Supposons $P = Q$ et $P \neq O$.*

*4.1) Si $y_P = 0$, on a $f(P,P) = O$.*

*4.2) Supposons $y_P \neq 0$. Posons*

$$\lambda = \frac{3x_P^2 + a}{2y_P} \quad et \quad \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

*On a*

$$f(P,P) = \Big[\lambda^2 - 2x_P, \lambda\big(\lambda^2 - 2x_P\big) + \nu, 1\Big]. \tag{12}$$

Démonstration : 1) Supposons $x_P \neq x_Q$. D'après le lemme 7.2, l'équation de $D$ est

$$y = \lambda x + \nu z.$$

Soit $M$ un point de $D \cap E$. Puisque $O$ n'est pas sur $D$, il existe $x_0$ et $y_0$ dans $\overline{K}$ tels que $M = [x_0, y_0, 1]$. On a les égalités

$$y_0^2 = x_0^3 + ax_0 + b \quad \text{et} \quad y_0 = \lambda x_0 + \nu.$$

Ainsi, $x_0$ est une racine du polynôme

$$H = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

La somme de ses racines est $\lambda^2$. On a $H(x_P) = H(x_Q) = 0$ et $x_P \neq x_Q$. Par suite, les racines de $H$ sont

$$x_P, \quad x_Q \quad \text{et} \quad \lambda^2 - x_P - x_Q.$$

Il en résulte que $D \cap E$ est formé de $P$, $Q$ et du point $f(P,Q)$ défini par la formule (10).

Supposons $x_P = x_Q$. Puisque $P$ et $Q$ sont distincts, on a alors $y_P = -y_Q$. D'après le lemme 7.2, l'équation de $D$ est

$$x = x_P z.$$

Le point $O$ est donc sur $D \cap E$. Soit $M$ un point $D \cap E$ distinct de $O$. Si $M = [x_0, y_0, 1]$, on a $x_0 = x_P$ puis $y_0 = \pm y_P$. On a donc $M = P$ ou $M = Q$. On en déduit que l'on a $D \cap E = \big\{P, Q, O\big\}$, d'où l'assertion dans ce cas.

2) Supposons $P \neq O$. La droite $D$ passant par $P$ et $O$ a pour équation

$$x = x_P z.$$

Si $M = [x_0, y_0, 1]$ est un point $D \cap E$, on a donc $x_0 = x_P$ d'où $y_0 = \pm y_P$. On a ainsi $D \cap E = \big\{P, O, f(P,O)\big\}$, où $f(P,O)$ est défini par la formule (11).

3) La tangente $D$ à $E$ en $O$ a pour équation $z = 0$ (lemme 7.4). Par suite, $O$ est le seul point de $D \cap E$, d'où $f(O,O) = O$.

4) On a $P = Q$ et $P \neq O$. L'équation de la tangente $D$ à $E$ en $P$ a donc pour équation (*loc. cit.*)

$$F_X(P)(x - x_P z) + F_Y(P)(y - y_P z) = 0.$$

Si $y_P = 0$, on a $F_Y(P) = 0$. Puisque $x_P$ est racine simple du polynôme $X^3 + aX + b$, on a $F_X(P) \neq 0$. Ainsi, $D$ a pour équation

$$x = x_P z.$$

Le seul point de $D \cap E$ distinct de $P$ est donc le point $O$, d'où $D \cap E = \big\{P, O\big\}$ et l'assertion.

Supposons $y_P \neq 0$. L'équation de $D$ est dans ce cas

$$y = \lambda x + \nu z.$$

Le point $O$ n'est pas sur $D$. Soit $M = [x_0, y_0, 1]$ un point de $E \cap D$. On a

$$y_0^2 = x_0^3 + a x_0 + b \quad \text{et} \quad y_0 = \lambda x_0 + \nu.$$

Par suite, $x_0$ est racine du polynôme

$$G = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

Le polynôme dérivé de $G$ est

$$G' = 3X^2 - 2\lambda^2 X + a - 2\lambda\nu.$$

On a $G(x_P) = 0$, et en utilisant l'égalité $y_P^2 = x_P^3 + ax_P + b$, on vérifie que $G'(x_P) = 0$. Ainsi, $x_P$ est une racine d'ordre au moins 2 de $G$. Les racines de $G$ sont donc

$$x_P \quad \text{et} \quad \lambda^2 - 2x_P.$$

On obtient $D \cap E = \big\{P, f(P,P)\big\}$, où $f(P,P)$ est défini par la formule (12), d'où le résultat.

On obtient une loi de composition interne sur $E$, appelée loi de composition des cordes-tangentes, $f : E \times E \to E$ qui à tout couple $(P,Q) \in E \times E$ associe le point $f(P,Q) \in E$ défini dans la proposition. Elle est commutative, mais n'est pas associative.

**Exemple 7.3.** Soit $E$ la courbe elliptique sur $\mathbb{Q}$ d'équation

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

Les points $P = (1,2)$, $Q = (0,0)$ et $R = \big(\frac{1}{4}, -\frac{7}{8}\big)$ sont dans $E(\mathbb{Q})$. On vérifie que l'on a

$$f(P,Q) = (3,6), \quad f(Q,R) = (12,-42).$$

$$f\big(f(P,Q),R\big) = (3,6), \quad f\big(P,f(Q,R)\big) = (3,-6).$$

**4. Loi de groupe sur $E$**

Considérons comme précédemment $a$ et $b$ des éléments de $K$ tels que $4a^3 + 27b^2 \neq 0$ et $E$ la courbe elliptique définie sur $K$ d'équation

$$y^2 = x^3 + ax + b.$$

Notons $+$ la loi de composition interne sur $E$, définie pour tous $P$ et $Q$ dans $E$ par l'égalité

$$P + Q = f\big(f(P,Q), O\big). \tag{13}$$

Géométriquement, $P + Q$ s'obtient à partir de $f(P,Q)$ par symétrie «par rapport à l'axe des abscisses». Cette loi de composition est une loi de groupe sur $E$.

**Théorème 7.1.** *Le couple $(E,+)$ est un groupe abélien, d'élément neutre $O$. La loi interne $+$ est décrite explicitement par les formules suivantes.*

*Soient $P$ et $Q$ des points de $E$ distincts de $O$. Posons $P=(x_P,y_P)$ et $Q=(x_Q,y_Q)$.*

*1) Supposons $x_P\neq x_Q$. Posons*

$$\lambda=\frac{y_P-y_Q}{x_P-x_Q}\quad et\quad \nu=\frac{x_Py_Q-x_Qy_P}{x_P-x_Q}.$$

*On a*

$$P+Q=\big(\lambda^2-x_P-x_Q,-\lambda(\lambda^2-x_P-x_Q)-\nu\big). \tag{14}$$

*2) Si $x_P=x_Q$ et $P\neq Q$, on a $P+Q=O$.*

*3) Supposons $P=Q$ et $y_P\neq 0$. Posons*

$$\lambda=\frac{3x_P^2+a}{2y_P}\quad et\quad \nu=\frac{-x_P^3+ax_P+2b}{2y_P}.$$

*On a*

$$2P=\big(\lambda^2-2x_P,-\lambda(\lambda^2-2x_P)-\nu\big). \tag{15}$$

*4) Si $P=Q$ et $y_P=0$, on a $2P=O$.*

*5) L'opposé de $P$ est le point*

$$-P=(x_P,-y_P). \tag{16}$$

Démonstration : Compte tenu de (13), les formules (14) et (15) résultent directement des égalités (10), (11) et (12). Supposons $x_P=x_Q$ et $P\neq Q$. D'après l'assertion 1.2 de la proposition 7.1 on a $f(P,Q)=O$, d'où $P+Q=f(O,O)=O$. Si $P=Q$ et $y_P=0$, on a $f(P,P)=O$ (assertion 4.1 de la prop. 7.1), d'où $2P=f(O,O)=O$. Cela établit les formules d'addition de $P$ et $Q$.
Par ailleurs, pour tous points $R$ et $S$ de $E$, on a $f(R,S)=f(S,R)$. La loi $+$ est donc commutative. Le fait que cette loi soit associative peut par exemple se vérifier au cas par cas, en utilisant les formules ci-dessus et un logiciel de calculs. C'est assez long et nous l'admettrons ici. Les assertions 2 et 3 de la proposition 7.1 impliquent

$$R+O=f\big(f(R,O),O\big)=R,$$

donc $O$ est l'élément neutre. En ce qui concerne la formule (16), si $P = (x_P, 0)$, on a $2P = O$ d'après l'assertion 4 établie ci-dessus. Si $y_P \neq 0$, en posant $Q = (x_P, -y_P)$, on a $P + Q = O$ d'après l'assertion 2 , d'où la formule (16) et le théorème.

**Remarque 7.3.** Par définition de cette loi de groupe, trois points de $E$ sont alignés si et seulement si leur somme est nulle.

Supposons que les points $P$ et $Q$ de $E = E\big(\overline{K}\big)$ soient rationnels sur une extension $L$ de $K$ contenue dans $\overline{K}$. Dans ce cas, comme on le constate directement dans l'énoncé du théorème, le point $P - Q$ est aussi rationnel sur $L$. Par ailleurs $O$ est dans $E(L)$. Ainsi, l'ensemble $E(L)$ des points de $E$ rationnels sur $L$ est un sous-groupe de $E\big(\overline{K}\big)$. Plus généralement :

**Proposition 7.2.** *Soient $L$ et $L'$ des extensions de $K$ dans $\overline{K}$ telles que $L$ soit contenue dans $L'$. Alors, $E(L)$ est un sous-groupe de $E(L')$.*

**Remarque 7.4.** Dans le premier exemple 7.1, cela explique pourquoi le cardinal de $E(\mathbb{F}_5)$ divise celui de $E\big(\mathbb{F}_{25}\big)$, vu que $E(\mathbb{F}_5)$ est un sous-groupe de $E\big(\mathbb{F}_{25}\big)$.

**Exemple 7.4.** Soit $E$ la courbe elliptique sur $\mathbb{Q}$ d'équation

$$y^2 = x^3 + x + 3. \tag{17}$$

Le point $P = (-1, 1)$ appartient à $E(\mathbb{Q})$. On vérifie que l'on a

$$2P = (6, -15), \quad 3P = \Big(\frac{11}{49}, \frac{617}{343}\Big), \quad 4P = \Big(\frac{1081}{900}, -\frac{65771}{27000}\Big),$$

$$5P = \Big(\frac{179051}{80089}, \frac{91814227}{22665187}\Big), \quad 6P = \Big(-\frac{6465234}{18653761}, -\frac{130201927155}{80565593759}\Big), \cdots.$$

En fait, $P$ est un point d'ordre infini et on a

$$E(\mathbb{Q}) = \Big\{nP \;\Big|\; n \in \mathbb{Z}\Big\},$$

de sorte que $E(\mathbb{Q})$ est isomorphe à $\mathbb{Z}$. Ce n'est pas un résultat simple, il faut développer la théorie des courbes elliptiques sur $\mathbb{Q}$ pour l'établir.

**Remarque 7.5.** Pour toute courbe elliptique $E$ définie sur $\mathbb{Q}$, on peut démontrer que le groupe $E(\mathbb{Q})$ est de type fini (théorème de Mordell-Weil sur $\mathbb{Q}$). Autrement dit, $E(\mathbb{Q})$ est isomorphe à un groupe de la forme $\mathbb{Z}^r \times T$ où $T$ est un groupe fini. Nous n'utiliserons pas ce résultat. L'entier $r$ s'appelle le rang de $E$ sur $\mathbb{Q}$. Il est généralement difficile à déterminer. En revanche, on peut expliciter assez simplement le sous-groupe de torsion de

$E(\mathbb{Q})$. Signalons par ailleurs que grâce à un théorème difficile de Mazur établi en 1977, on sait que ce sous-groupe de torsion est isomorphe à l'un des groupes suivants :

$$\mathbb{Z}/n\mathbb{Z} \quad \text{avec} \quad 1 \leq n \leq 10 \text{ ou } n = 12,$$

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} \quad \text{avec} \quad 1 \leq n \leq 4.$$

**Exemple 7.5.** Soit $p$ un nombre premier $\geq 5$. L'équation (17) définit une courbe elliptique $E$ sur $\mathbb{F}_p$ pour $p$ distinct de 13 et 19. On vérifie que l'on a

$$E(\mathbb{F}_5) = \Big\{O, (1,0), (-1, \pm 1)\Big\}.$$

Ce groupe est cyclique d'ordre 4 engendré par $(-1, 1)$. On a

$$E(\mathbb{F}_7) = \Big\{O, (5,0), (4, \pm 1), (6, \pm 1)\Big\},$$

qui est cyclique d'ordre 6 engendré par $(4, 1)$. On a

$$E(\mathbb{F}_{11}) = \Big\{O, (3,0), (0, \pm 5), (1, \pm 4), (4, \pm 4), (5, \pm 1), (6, \pm 4), (7, \pm 1), (9, \pm 2), (10, \pm 1)\Big\}.$$

Le point $(3, 0)$ est d'ordre 2 et $(4, 4)$ est d'ordre 9, donc $E(\mathbb{F}_{11})$ est cyclique d'ordre 18 engendré par le point $(3, 0) + (4, 4) = (9, -2)$.

## 3. Points de torsion

Considérons une courbe elliptique $E$ définie $K$. Étant donné un entier $n \geq 2$, posons

$$E[n] = \Big\{P \in E\big(\overline{K}\big) \;\Big|\; nP = O\Big\}.$$

C'est un sous-groupe de $E\big(\overline{K}\big)$, qui est l'ensemble des points de $E$ d'ordre divisant $n$.

**Terminologie.** Un point $P \in E\big(\overline{K}\big)$ est dit de $n$-torsion s'il appartient à $E[n]$. Le groupe $E[n]$ s'appelle le sous-groupe des points de $n$-torsion de $E$.

### 1. Théorème fondamental

Notons $\mathrm{car}(K)$ la caractéristique de $K$. On admettra le résultat essentiel suivant.

**Théorème 7.2.** *Soit $n$ un entier $\geq 2$.*

*1) Supposons que $\mathrm{car}(K)$ ne divise pas $n$ (tel est le cas si $\mathrm{car}(K) = 0$). Alors, $E[n]$ est un groupe d'ordre $n^2$ isomorphe à $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.*

*2) Supposons $\mathrm{car}(K) = p$ où $p$ est un diviseur premier de $n$. Posons $n = p^r n'$ où $p$ ne divise pas $n'$. Alors, $E[n]$ est isomorphe à l'un des groupes*

$$\mathbb{Z}/n'\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n'\mathbb{Z}.$$

En particulier :

**Corollaire 7.1.** *Pour tout $n \geq 2$, le groupe $E[n]$ est fini d'ordre au plus $n^2$.*

Par ailleurs, si $\mathrm{car}(K) = p$, le groupe $E[p]$ est trivial ou est cyclique d'ordre $p$. On reviendra sur ce point.

**Corollaire 7.2.** *Soit $\ell$ un un nombre premier distinct de $\mathrm{car}(K)$. Le groupe $E[\ell]$ est un $\mathbb{F}_\ell$-espace vectoriel de dimension 2.*

Pour tout nombre premier $\ell$ distinct de $\mathrm{car}(K)$, si $(P_1, P_2)$ est une base de $E[\ell]$ sur $\mathbb{F}_\ell$, tout point de $P \in E[\ell]$ s'écrit ainsi de manière unique sous la forme

$$P = n_1 P_1 + n_2 P_2,$$

où $n_1$ et $n_2$ sont des entiers compris entre 0 et $\ell - 1$.

Le théorème 7.2 est facile à démontrer pour $n = 2$ et $n = 3$. En effet, soit

$$y^2 = x^3 + ax + b$$

l'équation de $E$ sur $K$.

**Lemme 7.5.** *Soient $\alpha$, $\beta$, $\gamma$ les racines dans $\overline{K}$ du polynôme $X^3 + aX + b \in K[X]$. On a*

$$E[2] = \Big\{O, (\alpha, 0), (\beta, 0), (\gamma, 0)\Big\}.$$

*En particulier, $E[2]$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.*

Démonstration : Soit $P$ un point de $E$ distinct de $O$. Posons $P = (x, y) \in E\big(\overline{K}\big)$. D'après les assertions 3 et 4 du théorème 7.1, le point $P$ est dans $E[2]$ si et seulement si $y = 0$, d'où le résultat, vu que $\alpha$, $\beta$, $\gamma$ sont distincts deux à deux (lemme 7.1).

**Lemme 7.6.** *Posons $G = 3X^4 + 6aX^2 + 12bX - a^2 \in K[X]$.*

*1) Le polynôme $G$ possède quatre racines distinctes dans $\overline{K}$.*

*2) Soit $P = (x, y)$ un point de $E\big(\overline{K}\big)$. On a l'équivalence*

$$P \in E[3] \Longleftrightarrow G(x) = 0.$$

*En particulier, $E[3]$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

Démonstration : 1) On vérifie que le discriminant de $G$ est

$$-2^8.3^3(4a^3 + 27b^2)^2.$$

Puisque $\mathrm{car}(K) \geq 5$ et que $4a^3 + 27b^2 \neq 0$, il n'est pas nul, d'où la première assertion.

2) Supposons que $P$ appartienne à $E[3]$. On a alors $2P = -P$. Par ailleurs, on a $2P \neq 0$ (car $P$ est par hypothèse distinct de $O$), donc $y$ est non nul (lemme 7.5). D'après les assertions 3 et 5 du théorème 7.1, on obtient

$$\lambda^2 - 2x = x \quad \text{avec} \quad \lambda = \frac{3x^2 + a}{2y}. \tag{18}$$

Compte tenu de l'égalité $y^2 = x^3 + ax + b$, il en résulte que $G(x) = 0$.
Inversement, supposons $G(x) = 0$. On vérifie que l'on a

$$(3X^2 + 4a)G - (X^3 + aX + b)(9X^3 + 21aX + 27b) = -(4a^3 + 27b^2).$$

Par suite, $G$ et $X^3 + aX + b$ n'ont pas de racines communes. On a donc $x^3 + ax + b \neq 0$ i.e. $y$ est non nul. L'égalité $G(x) = 0$ entraîne alors que la condition (18) est satisfaite. L'abscisse de $2P$ est donc celle de $P$. On a ainsi $2P = \pm P$, puis $2P = -P$ i.e. $P$ est dans $E[3]$, d'où l'équivalence annoncée.
Par ailleurs, chaque racine de $G$ dans $\overline{K}$ est l'abscisse de deux points distincts de $E$. Le groupe $E[3]$ est donc d'ordre 9, d'où le résultat.

**Exemples 7.6.**

1) Soit $E$ la courbe elliptique sur $\mathbb{Q}$ d'équation

$$y^2 = x^3 - 2.$$

Soient $\zeta$ une racine primitive cubique de l'unité dans $\mathbb{C}$ et $\alpha$ la racine cubique réelle de 2. D'après le lemme 7.5, on a

$$E[2] = \Big\{O, (\alpha, 0), (\zeta\alpha, 0), (\zeta^2\alpha, 0)\Big\}.$$

Les points d'ordre 2 de $E$ sont donc rationnels sur le corps $\mathbb{Q}\big(\zeta, \alpha\big)$ qui est une extension galoisienne de $\mathbb{Q}$ de degré 6. Son groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathbb{S}_3$ (le groupe symétrique de $\big\{1, 2, 3\big\}$). Les points $(\alpha, 0)$ et $(\zeta\alpha, 0)$ forment une base de $E[2]$ sur $\mathbb{F}_2$.
Par ailleurs, avec les notations du lemme 7.6, on a

$$G = 3X^4 - 24X = 3X(X - 2)(X^2 + 2X + 4).$$

Les abscisses des points d'ordre 3 de $E$ sont donc

$$0, \quad 2, \quad -1 + \sqrt{-3}, \quad -1 - \sqrt{-3}.$$

On en déduit que l'on a

$$E[3] = \Big\{O, \big(0, \pm\sqrt{-2}\big), \big(-1 + \sqrt{-3}, \pm\sqrt{6}\big), \big(-1 - \sqrt{-3}, \pm\sqrt{6}\big), \big(2, \pm\sqrt{6}\big)\Big\}.$$

On constate que tous les points d'ordre 3 de $E$ sont rationnels sur le corps $\mathbb{Q}\big(\sqrt{-2},\sqrt{6}\big)$, qui est une extension galoisienne de degré 4 de $\mathbb{Q}$. Elle contient $\mathbb{Q}\big(\sqrt{-3}\big)$ qui n'est autre que $\mathbb{Q}(\zeta)$ (cela n'est pas un hasard). Son groupe de Galois sur $\mathbb{Q}$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$. Une base de $E[3]$ sur $\mathbb{F}_3$ est formée des points $\big(0,\sqrt{-2}\big)$ et $\big(-1+\sqrt{-3},\sqrt{6}\big)$.

2) Reprenons l'exemple 7.4, avec la courbe elliptique $E$ sur le corps $\mathbb{F}_{11}$ d'équation

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

Dans $\mathbb{F}_{11}[X]$, on a $X^3+X+3 = (X-3)(X^2+3X-1)$. Le seul point de $E(\mathbb{F}_{11})$ d'ordre 2 est donc $(3,0)$, et les deux autres points d'ordre 2 de $E$ sont rationnels sur l'extension quadratique de $\mathbb{F}_{11}$, qui est $\mathbb{F}_{11}(\alpha)$ où $\alpha^2+3\alpha-1=0$. On vérifie alors que l'on a

$$E[2] = \Big\{O,(3,0),(\alpha,0),(-\alpha+8,0)\Big\}.$$

Avec les notations du lemme 7.6, on a

$$G = 3X^4+6X^2+36X-1 = (X-1)(X-2)(X^2+3X+9) \in \mathbb{F}_{11}[X].$$

On en déduit que $(1,\pm 4)$ sont les points d'ordre 3 de $E(\mathbb{F}_{11})$. Soit $\beta$ une racine carrée de 13 dans $\overline{\mathbb{F}_{11}}$. Les points $(2,\pm\beta)$ sont dans $E[3]$. On vérifie que les racines de $X^2+3X+9$ sont $4\pm 3\beta$. Par suite, on a

$$E[3] = \Big\{O,(1,\pm 4),(2,\pm\beta),\big(4+3\beta,\pm(2+9\beta)\big),\big(4-3\beta,\pm(2+2\beta)\big)\Big\}.$$

Tous les points de $E[3]$ sont donc rationnels sur l'extension quadratique de $\mathbb{F}_{11}$ (il en existe une seule dans $\overline{\mathbb{F}_{11}}$. Cela étant, il est visible ici que $\mathbb{F}_{11}(\alpha)=\mathbb{F}_{11}(\beta)$).

### 2. Morphismes de groupes de $E\big(\overline{K}\big)$

Considérons un morphisme de groupes $f : E\big(\overline{K}\big) \to E\big(\overline{K}\big)$. Soit $n$ un entier $\geq 2$ non divisible par $\mathrm{car}(K)$. Le groupe $E[n]$ est un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2 (th. 7.2). L'image par $f$ de $E[n]$ est contenue dans $E[n]$. Par suite, $f$ induit un endomorphisme du $\mathbb{Z}/n\mathbb{Z}$-module $E[n]$. Dans toute base $(P_1,P_2)$ de $E[n]$ sur $\mathbb{Z}/n\mathbb{Z}$, il est donc représenté par une matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

qui décrit l'action de $f$ sur $E[n]$.

**Exemples 7.7.**

1) Pour tout $m\in\mathbb{Z}$, l'application qui à tout point $P$ de $E$ associe $mP$ est un morphisme de groupes.

2) Le morphisme de multiplication par 2 sur $E$ vaut moins l'identité sur $E[3]$.

3) Soit $E$ une courbe elliptique définie sur $\mathbb{R}$. Soit $\tau : E(\mathbb{C}) \to E(\mathbb{C})$ l'application définie pour tout $P = (x, y) \in E(\mathbb{C})$ par

$$\tau(P) = \big(\overline{x}, \overline{y}\big) \quad \text{et} \quad \tau(O) = O,$$

où $\overline{x}$ désigne le nombre complexe conjugué de $x$. Cette application est bien définie, car $E$ étant définie sur $\mathbb{R}$, si $P$ est dans $E(\mathbb{C})$ il en est de même de $\tau(P)$. Il résulte directement du théorème 7.1 que c'est un morphisme de groupes. On dit que $\tau$ est le morphisme de la conjugaison complexe

4) On peut généraliser l'exemple précédent. Notons $\mathrm{Gal}\big(\overline{K}/K\big)$ le groupe de Galois de $\overline{K}$ sur $K$ i.e. l'ensemble des automorphismes de $\overline{K}$ qui fixent $K$. Pour toute courbe elliptique $E$ définie sur $K$, le groupe $\mathrm{Gal}\big(\overline{K}/K\big)$ opère sur $E\big(\overline{K}\big)$. En effet, soient $y^2 = x^3 + ax + b$ l'équation de $E$ sur $K$, $\sigma$ un élément de $\mathrm{Gal}\big(\overline{K}/K\big)$ et $P = (x, y)$ un point de $E$. L'élément

$$\sigma(P) = \big(\sigma(x), \sigma(y)\big) \tag{19}$$

est un point de $E$, car $a$ et $b$ étant dans $K$, ils sont fixés par $\sigma$. En posant $\sigma(O) = O$, l'application qui à tout point $P \in E$ associe $\sigma(P)$, est un morphisme de groupes bijectif i.e. est un automorphisme de $E\big(\overline{K}\big)$. Dans l'exemple précédent, la conjugaison complexe qui à $z$ associe $\overline{z}$ est l'élément non trivial du groupe de Galois de $\mathbb{C}$ sur $\mathbb{R}$.

5) Soit $E$ la courbe elliptique sur $\mathbb{Q}$ d'équation $y^2 = x^3 - 2$. Décrivons l'action de la conjugaison complexe $\tau$ sur le groupe $E[2]$. On a vu que

$$E[2] = \Big\{O, P_1, P_2, P_1 + P_2\Big\} \quad \text{avec} \quad P_1 = (\alpha, 0),\ P_2 = (\zeta\alpha, 0),$$

où $\zeta$ est une racine primitive cubique de l'unité et $\alpha$ la racine cubique réelle de 2. On a

$$\tau(P_1) = P_1 \quad \text{et} \quad \tau(P_2) = P_1 + P_2.$$

Par suite, dans la base $(P_1, P_2)$, la matrice de $\tau$ agissant sur $\mathbb{F}_2$-espace vectoriel $E[2]$ est

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

### 3. Corps des points de torsion

Ce paragraphe nécessite quelques connaissances de théorie de Galois. Poursuivons l'exemple 4 ci-dessus. Soit $n$ un entier $\geq 2$ non divisible par $\mathrm{car}(K)$. Pour tout élément $\sigma \in \mathrm{Gal}\big(\overline{K}/K\big)$, on dispose de l'automorphisme $\rho(\sigma) : E\big(\overline{K}\big) \to E\big(\overline{K}\big)$ qui à $P$ associe

$\sigma(P)$ défini par (19). Il induit un automorphisme du $\mathbb{Z}/n\mathbb{Z}$-module $E[n]$. Notons $\mathrm{Aut}\big(E[n]\big)$ le groupe des automorphismes de $E[n]$. On obtient ainsi une application

$$\rho_n : \mathrm{Gal}\big(\overline{K}/K\big) \to \mathrm{Aut}\big(E[n]\big),$$

qui à $\sigma$ associe $\rho(\sigma)$ restreint à $E[n]$. C'est un morphisme de groupes i.e. pour tous $\sigma$ et $\tau$ dans $\mathrm{Gal}\big(\overline{K}/K\big)$, on a $\rho_n(\sigma \circ \tau) = \rho_n(\sigma) \circ \rho_n(\tau)$. Son noyau $\mathrm{Ker}(\rho_n)$ joue un rôle très important dans l'étude de $E[n]$. Un élément $\sigma \in \mathrm{Gal}\big(\overline{K}/K\big)$ est dans $\mathrm{Ker}(\rho_n)$ si et seulement si pour tout $P \in E[n]$ on a $\sigma(P) = P$. Notons

$$K\big(E[n]\big)$$

le sous-corps de $\overline{K}$ laissé fixe par $\mathrm{Ker}(\rho_n)$. Par définition, $K\big(E[n]\big)$ est formé des éléments $x \in \overline{K}$ tels que pour tout $\sigma \in \mathrm{Ker}(\rho_n)$ on ait $\sigma(x) = x$.

**Terminologie.** Le corps $K\big(E[n]\big)$ s'appelle le corps des points de $n$-torsion de $E$.

**Lemme 7.7.** *Le corps $K\big(E[n]\big)$ est le sous-corps de $\overline{K}$ obtenu en adjoignant à $K$ les coordonnées des points de $E[n]$.*

Démonstration : Soient $L$ le sous-corps de $\overline{K}$ obtenu en adjoignant à $K$ les coordonnées des points de $E[n]$ et $H$ le groupe de Galois de $\overline{K}$ sur $L$. Pour tout $\sigma \in H$ et tout $P \in E[n]$, on a $\sigma(P) = P$. Ainsi $H$ est contenu dans $\mathrm{Ker}(\rho_n)$, par suite $K\big(E[n]\big)$ est contenu dans $L$. Inversement, soit $(P_1, P_2)$ une base de $E[n]$. En posant $P_i = (x_i, y_i)$, on a $L = K[x_1, y_1, x_2, y_2]$. En particulier, tout élément de $\ker(\rho_n)$ fixe $L$. Par définition, $L$ est donc contenu dans $K\big(E[n]\big)$, d'où le résultat.

Le corps des points de $n$-torsion de $E$ est une extension finie galoisienne de $K$. Une question arithmétique importante, que nous n'aborderons pas ici, concerne la détermination du degré $[K\big(E[n]\big) : K]$ de $K\big(E[n]\big)$ sur $K$. Limitons-nous à remarquer que le groupe de Galois de $K\big(E[n]\big)$ sur $K$ est isomorphe à un sous-groupe de $\mathrm{Aut}\big(E[n]\big)$. Par le choix d'une base de $E[n]$ sur $\mathbb{Z}/n\mathbb{Z}$, le groupe $\mathrm{Aut}\big(E[n]\big)$ s'identifie au groupe $\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$ des matrices inversibles de tailles $(2,2)$ à coefficients dans $\mathbb{Z}/n\mathbb{Z}$. Il en résulte que l'on a

$$[K\big(E[n]\big) : K] \leq |\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})|,$$

où $|\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})|$ est l'ordre de $\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})$. À titre indicatif, déterminons cet ordre. Rappelons qu'une matrice de taille $(2,2)$ à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ est inversible si et seulement si son déterminant est inversible dans $\mathbb{Z}/n\mathbb{Z}$.

**Lemme 7.8.** *On a*

$$\big|\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z})\big| = n^4 \prod_{p|n} \Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{p^2}\Big),$$

*où $p$ parcourt l'ensemble des diviseurs premiers de $n$.*

Démonstration : Soit $n = p_1^{n_1} \cdots p_s^{n_s}$ la décomposition de $n$ en facteurs premiers $p_i$ distincts deux à deux. D'après le théorème chinois, l'anneau des matrices $(2,2)$ à coefficients dans $\mathbb{Z}/n\mathbb{Z}$ est isomorphe, via l'application de réduction, à l'anneau produit des matrices $(2,2)$ à coefficients dans $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$. Leurs groupes des éléments inversibles le sont donc aussi. Par suite, l'application de réduction

$$\mathbb{GL}_2(\mathbb{Z}/n\mathbb{Z}) \to \mathbb{GL}_2(\mathbb{Z}/p_1^{n_1}\mathbb{Z}) \times \cdots \times \mathbb{GL}_2(\mathbb{Z}/p_s^{n_s}\mathbb{Z}),$$

est un isomorphisme de groupes. On se ramène ainsi au cas où $n = p^r$ avec $p$ premier. Le morphisme de réduction $\mathbb{GL}_2(\mathbb{Z}/p^r\mathbb{Z}) \to \mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$ est surjectif et son noyau est formé des matrices

$$\begin{pmatrix} a + p^r\mathbb{Z} & b + p^r\mathbb{Z} \\ c + p^r\mathbb{Z} & d + p^r\mathbb{Z} \end{pmatrix},$$

où $a, b, c, d$ sont des entiers compris entre 1 et $p^r$ tels que

$$a, d \equiv 1 \text{ mod. } p \quad \text{et} \quad b, c \equiv 0 \text{ mod. } p.$$

Il y a $p^{r-1}$ multiples de $p$ et $p^{r-1}$ entiers de la forme $1 + kp$ entre 1 et $p^r$. L'ordre de ce noyau est donc $p^{4(r-1)}$. Puisque $\mathbb{GL}_2(\mathbb{Z}/p\mathbb{Z})$ est d'ordre $(p^2-1)(p^2-p)$ (c'est le nombre de bases d'un plan vectoriel sur $\mathbb{F}_p$), il en résulte que

$$|\mathbb{GL}_2(\mathbb{Z}/p^r\mathbb{Z})| = p^{4(r-1)}(p^2-1)(p^2-p) = p^{4r}\Big(1 - \frac{1}{p}\Big)\Big(1 - \frac{1}{p^2}\Big),$$

ce qui entraîne le résultat.

Examinons le cas où $n = 2$. Supposons que soit $E$ définie par l'équation $y^2 = F(x)$ où $F = X^3 + aX + b \in K[X]$.

**Lemme 7.9.** *Soit $d$ le degré de $K\big(E[2]\big)$ sur $K$.*

*1) On a $d \leq 6$.*

*2) Si $F$ a tous ses racines dans $K$, on a $d = 1$.*

*3) Si $F$ a une seule racine dans $K$, on a $d = 2$.*

*4) Supposons $F$ irréductible sur $K$. On a $d = 3$ ou $d = 6$. De plus, on a l'équivalence*

$$d = 3 \Longleftrightarrow -(4a^3 + 27b^2) \text{ est un carré dans } K.$$

Démonstration : Soient $\alpha$, $\beta$, $\gamma$ les racines de $F$ dans $\overline{K}$. Posons

$$\Delta = -(4a^3 + 27b^2).$$

On a l'égalité (lemme 7.1)

$$\Delta = \big((\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)\big)^2. \tag{20}$$

D'après le lemme 7.7, on a

$$K\big(E[2]\big) = K(\alpha,\beta,\gamma). \tag{21}$$

Le groupe de Galois de $K\big(E[2]\big)$ sur $K$ est isomorphe à un sous-groupe de $\mathbb{GL}_2(\mathbb{F}_2)$, qui est d'ordre 6, d'où $d \leq 6$. Les assertions 2 et 3 résultent directement de (21).

Supposons $F$ irréductible sur $K$ i.e. que ses racines ne soient pas dans $K$. Dans ce cas, $K(\alpha)$ est une extension de degré 3 de $K$, donc 3 divise $d$. D'après l'égalité (20), le corps $K\big(\sqrt{\Delta}\big)$ est contenu dans $K\big(E[2]\big)$. Il en résulte que si $\Delta$ n'est pas un carré dans $K$, alors 2 divise $d$, d'où $d = 6$.
Inversement, supposons que $\Delta$ soit un carré dans $K$. Montrons alors que l'on a

$$K\big(E[2]\big) = K(\alpha), \tag{22}$$

ce qui établira le résultat. On a

$$F = (X-\alpha)(X^2 - (\beta+\gamma)X + \beta\gamma),$$

donc $\beta+\gamma$ et $\beta\gamma$ sont dans $K(\alpha)$, et il en est de même de $(\alpha-\beta)(\gamma-\alpha)$. De l'égalité

$$(\beta-\gamma)^2 = \frac{\Delta}{(\alpha-\beta)^2(\gamma-\alpha)^2}, \tag{23}$$

on déduit alors que $\beta-\gamma$ appartient à $K(\alpha)$. Cela entraîne que $2\beta$ et $2\gamma$ sont dans $K(\alpha)$. Le corps $K$ étant de caractéristique différente de 2, les éléments $\beta$ et $\gamma$ sont donc aussi dans $K(\alpha)$. L'égalité (21) entraîne alors (22).

**Remarque 7.6.** Reprenons les notations du lemme précédent et de sa démonstration. Supposons que $F$ ait une seule racine dans $K$. Dans ce cas, on a

$$K\big(E[2]\big) = K\big(\sqrt{\Delta}\big). \tag{24}$$

Pour le vérifier, vu que l'on a $d = 2$ et que $K\big(\sqrt{\Delta}\big)$ est contenu dans $K\big(E[2]\big)$, il suffit de montrer que $\Delta$ n'est pas un carré dans $K$. Soit $\alpha$ la racine de $F$ dans $K$. On constate comme ci-dessus que $\beta+\gamma$, $\beta\gamma$ et $(\alpha-\beta)(\gamma-\alpha)$ sont dans $K$. Si $\Delta$ était un carré dans $K$, alors $\beta-\gamma$ serait dans $K$ (égalité (23)), donc $\beta$ et $\gamma$ aussi, d'où une contradiction et l'égalité (24).

On utilisera plus loin, le résultat important suivant que l'on admettra, concernant la rationalité des points de $n$-torsion de $E$, où rappelons que $n$ est premier avec la caractéristique de $K$. Notons $\mu_n$ le sous-groupe des racines $n$-ièmes de l'unité de $\overline{K}^*$ : ce sont les racines du polynôme $X^n - 1$ dans $\overline{K}$.

**Théorème 7.3.** *Le groupe $\mu_n$ est contenu dans $K\big(E[n]\big)$.*

**Remarque 7.7.** Cet énoncé est évident si $n = 2$. Il est assez facile à démontrer si $n = 3$. En effet, soit $y^2 = F(x)$ l'équation de $E$ avec $F = X^3 + aX + b \in K[X]$. Le polynôme donnant les abscisses des points de $E[3]$ est (lemme 7.6)

$$X^4 + 2aX^2 + 4bX - \frac{a^2}{3}.$$

Notons $x_1, x_2, x_3, x_4$ ses quatre racines dans $\overline{K}$. Posons

$$z_1 = x_1x_2 + x_3x_4, \quad z_2 = x_1x_3 + x_2x_4, \quad z_3 = x_1x_4 + x_2x_3.$$

On vérifie que l'on a

$$z_1 + z_2 + z_3 = 2a, \quad z_1z_2 + z_2z_3 + z_1z_3 = \frac{4a^2}{3}, \quad z_1z_2z_3 = 16b^2 + \frac{8a^3}{3}.$$

Par suite, les $z_i$ sont racines du polynôme

$$H = Z^3 - 2aZ^2 + \frac{4a^2}{3}Z - \Big(16b^2 + \frac{8a^3}{3}\Big).$$

On a l'égalité

$$H = \Big(Z - \frac{2a}{3}\Big)^3 - \frac{16}{27}(4a^3 + 27b^2).$$

Il en résulte que $16(4a^3 + 27b^2)$ est un cube dans $K\big(E[3]\big)$. Posons $\delta^3 = 16(4a^3 + 27b^2)$ où $\delta \in K\big(E[3]\big)$. Puisque $K\big(E[3]\big)$ est une extension galoisienne de $K$, si $\zeta$ est une racine primitive cubique de l'unité, $\zeta\delta$ est aussi dans $K\big(E[3]\big)$. Ainsi, $\zeta$ appartient à $K\big(E[3]\big)$, d'où le résultat.

## 4. Courbes elliptiques sur les corps finis

Dans tout ce paragraphe, $K$ désigne un corps fini de caractéristique $\geq 5$ et $E$ une courbe elliptique définie sur $K$ d'équation

$$y^2 = x^3 + ax + b. \tag{25}$$

Notons $q$ le cardinal de $K$. Le corps $K$ est donc est « le » corps fini à $q$ éléments. Pour toute extension finie $L$ de $K$, le groupe $E(L)$ est fini. On notera $|E(L)|$ son ordre.

## 1. Théorème de Hasse

Un résultat fondamental de la théorie des courbes elliptiques sur les corps finis est le théorème ci-dessous, démontré par Hasse vers 1933, concernant l'ordre de $E(K)$. Remarquons d'abord que pour chaque valeur de $x \in K$, il y a au plus deux valeurs de $y$ satisfaisant l'équation (25). On a donc évidemment

$$|E(K)| \leq 2q + 1.$$

Puisque qu'un élément de $K$ choisi au hasard a environ une chance sur deux d'être un carré dans $K$, on doit donc s'attendre à ce que l'ordre de grandeur de $|E(K)|$ soit $q$. Cette heuristique est confirmée par l'énoncé suivant.

**Théorème 7.4 (Hasse).** *On a l'inégalité*

$$\big|q + 1 - |E(K)|\big| \leq 2\sqrt{q}.$$

Nous l'admettrons ici. Il peut se reformuler par l'inégalité

$$\big|\sqrt{|E(K)|} - \sqrt{q}\big| \leq 1.$$

En fait, la détermination de l'ordre $E(K)$ a de nombreuses applications en cryptographie. On dit parfois que

$$H_q = [q + 1 - 2\sqrt{q}, q + 1 + 2\sqrt{q}]$$

est l'intervalle de Hasse pour $q$.

Le théorème de Hasse permet parfois de déterminer facilement l'ordre de $E(K)$ si l'on parvient à détecter un point de $E(K)$ d'ordre $d$ assez grand. En effet, si $d$ est assez grand, les multiples de $d$ dans l'intervalle $H_q$ sont peu nombreux, ce qui laisse un petit nombre de possibilités pour l'ordre de $E(K)$. Si par exemple, il y a un seul multiple $N$ de $d$ dans $H_q$, alors on a $|E(K)| = N$. Illustrons cette idée à travers deux exemples.

**Exemples 7.8.**

1) Prenons $K = \mathbb{F}_{101}$ et pour $E$ la courbe elliptique d'équation

$$y^2 = x^3 + 7x + 1.$$

Le point $(0, 1)$ appartient à $E(K)$. On vérifie que son ordre est 116. L'ordre de $E(K)$ est donc multiple de 116. Puisque l'on a (th. 7.4)

$$82 \leq |E(K)| \leq 122,$$

on obtient $|E(K)| = 116$.

2) Prenons $K = \mathbb{F}_{557}$ et pour $E$ la courbe elliptique d'équation

$$y^2 = x^3 - 10x + 21.$$

On constate que $(2, 3)$ est un point de $E(K)$ d'ordre 189. Le seul multiple de 189 dans $H_{557}$ étant 567, on a donc $|E(K)| = 567$.

Nous verrons plus loin une méthode de comptage pour déterminer l'ordre du groupe des points d'une courbe elliptique sur $\mathbb{F}_p$ qui formalise cette idée.

## 2. Structure du groupe $E(K)$

Le théorème de structure du groupe abélien $E(K)$ est le suivant.

**Théorème 7.5.** *Il existe un unique couple d'entiers naturels $(n_1, n_2)$ tel que $E(K)$ soit isomorphe au groupe produit*

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z} \quad \textit{et que} \quad n_1 \textit{ divise } n_2 \quad \textit{et} \quad n_1 \textit{ divise } q - 1.$$

Démonstration : D'après le théorème de structure des groupes abéliens finis[(2)], il existe au plus un couple d'entiers naturels $(n_1, n_2)$ réalisant la condition de cet énoncé. Il suffit donc de démontrer l'assertion d'existence. Il existe des entiers naturels non nuls $n_1, \cdots, n_t$ tels que $E(K)$ soit isomorphe au groupe produit

$$\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_t\mathbb{Z} \quad \text{et que} \quad n_i \text{ divise } n_{i+1}.$$

Pour chaque indice $i$, vu que $n_1$ divise $n_i$, le groupe $\mathbb{Z}/n_i\mathbb{Z}$ contient $n_1$ éléments d'ordre divisant $n_1$. Par suite, $E(K)$ possède $n_1^t$ éléments annulés par $n_1$. D'après le corollaire 7.1, $E(K)$ possède au plus $n_1^2$ points de $n_1$-torsion. On a donc

$$t \leq 2.$$

Il reste à établir que $n_1$ divise $q - 1$. On remarque pour cela que $\mathbb{Z}/n_2\mathbb{Z}$ contient un sous-groupe isomorphe à $\mathbb{Z}/n_1\mathbb{Z}$ (car $n_1$ divise $n_2$). Ainsi $E(K)$ contient un sous-groupe isomorphe à

$$\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}.$$

---

(2) Soit $G$ un groupe abélien fini. Il existe des entiers naturels $a_1, \cdots a_r$ uniques tels que $a_i$ divise $a_{i+1}$ et que $G$ soit isomorphe au groupe produit

$$\mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_r\mathbb{Z}.$$

Les $a_i$ (ou les idéaux $a_i\mathbb{Z}$) s'appellent les facteurs invariants de $G$.

Le groupe de $E[n_1]$ formé des points de $n_1$-torsion de $E\big(\overline{K}\big)$ est donc contenu dans $E(K)$. Soit $p$ la caractéristique de $K$. L'entier $n_1$ n'est pas divisible par $p$, sinon $E(K)$ contiendrait un sous-groupe isomorphe à $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, ce qui n'est pas (th. 7.2). D'après le théorème 7.3, on en déduit que le groupe des racines $n_1$-ièmes de l'unité de $\overline{K}^*$ est contenu dans $K^*$. Puisque $p$ ne divise pas $n_1$, il est d'ordre $n_1$, donc $n_1$ divise $q-1$, d'où le résultat.

**Exemple 7.9.** Soit $E$ la courbe elliptique sur $\mathbb{F}_7$ d'équation

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

Vérifions que $E(\mathbb{F}_7)$ est isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, autrement dit que l'on a $E(\mathbb{F}_7) = E[3]$. D'après le théorème de Hasse, l'ordre de $E(\mathbb{F}_7)$ est compris entre 3 et 13. Par ailleurs, le point $P = (-1, 1)$ est d'ordre 3. Puisque $Q = (0, 4)$ est aussi un point d'ordre 3 de $E(\mathbb{F}_7)$, sans être sur la droite vectorielle sur $\mathbb{F}_3$ engendrée par $P$, cela entraîne l'assertion.

### 3. Endomorphisme de Frobenius

Considérons l'application $\sigma_q : \overline{K} \to \overline{K}$ définie pour tout $x \in \overline{K}$ par

$$\sigma_q(x) = x^q.$$

C'est un isomorphisme de corps, qui s'appelle le morphisme de Frobenius de $\overline{K}$. Pour tout $x \in K$, on a l'équivalence (Chap. III)

$$\sigma_q(x) = x \iff x \in K. \tag{26}$$

On dispose donc de l'application

$$\phi_q : E\big(\overline{K}\big) \to E\big(\overline{K}\big),$$

définie pour tout $(x, y) \in E\big(\overline{K}\big)$ par

$$\phi_q(x, y) = (x^q, y^q) \quad \text{et} \quad \phi_q(O) = O. \tag{27}$$

Remarquons que $\phi_q$ est bien définie car si $(x, y)$ est un point de $E$, on a $y^2 = x^3 + ax + b$, et vu que $a$ et $b$ sont dans $K$, $(x^q, y^q)$ est aussi un point de $E$ (condition (26)). Comme conséquence du théorème 7.1, on obtient :

**Lemme 7.10.** *L'application $\phi_q$ est un morphisme de groupes.*

Compte tenu de (26) et (27), pour tout $P \in E\big(\overline{K}\big)$, on a

$$\phi_q(P) = P \iff P \in E(K).$$

**Terminologie.** On dit que $\phi_q$ est l'endomorphisme de Frobenius de $E$.

Il joue un rôle crucial dans la théorie des courbes elliptiques sur les corps finis. On va maintenant énoncer deux théorèmes décrivant ses principales propriétés. Leurs démonstrations sont du même niveau de difficulté que celle du théorème de Hasse. Nous les admettrons donc aussi.

D'après le théorème de Hasse, on a

$$|E(K)| = q + 1 - t \quad \text{avec} \quad |t| \leq 2\sqrt{q}. \tag{28}$$

**Terminologie.** L'entier $t$ s'appelle la trace du Frobenius de $E$. Le polynôme

$$X^2 - tX + q \in \mathbb{Z}[X]$$

s'appelle le polynôme caractéristique du Frobenius de $E$.

**Théorème 7.6.** *On a l'égalité*

$$\phi_q^2 - t\phi_q + q = 0. \tag{29}$$

*De plus, $t$ est l'unique entier $k$ tel que $\phi_q^2 - k\phi_q + q = 0$.*

L'égalité (29) signifie que l'on a

$$(\phi_q \circ \phi_q)(P) - t\phi_q(P) + qP = O \quad \text{pour tout } P \in E\big(\overline{K}\big),$$

autrement dit, si $P = (x, y)$ est un point de $E\big(\overline{K}\big)$, on a

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

Par ailleurs, pour tout entier $n \geq 2$, $\phi_q$ induit un endomorphisme de $E[n]$. Notons

$$(\phi_q)_n : E[n] \to E[n]$$

ce morphisme de groupes. Si $n$ n'est pas divisible par la caractéristique de $K$, alors $E[n]$ est un $\mathbb{Z}/n\mathbb{Z}$-module libre de rang 2. En choisissant une base de $E[n]$ on peut représenter $(\phi_q)_n$ par une matrice de taille $(2, 2)$ à coefficients dans $\mathbb{Z}/n\mathbb{Z}$, et considérer sa trace et son déterminant. Ils sont donnés par l'énoncé suivant.

**Théorème 7.7.** *Soit $n$ un entier $\geq 2$ non divisible par la caractéristique de $K$. On a*

$$\mathrm{Trace}(\phi_q)_n = t + n\mathbb{Z} \quad \textit{et} \quad \det(\phi_q)_n = q + n\mathbb{Z}.$$

**Exemple 7.10.** Soit $E$ la courbe elliptique sur $\mathbb{F}_{11}$ d'équation

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

Soit $\beta$ une racine carrée de 13 dans $\overline{\mathbb{F}_{11}}$. On a vu que les points

$$P_1 = (1, 4) \quad \text{et} \quad P_2 = (2, \beta)$$

forment une base de $E[3]$ (cf. exemples 7.6) Déterminons l'action de $\phi_{11}$ sur $E[3]$. Puisque $P_1$ est rationnel sur $\mathbb{F}_{11}$, on a $\phi_{11}(P_1) = P_1$. Par ailleurs, on a

$$\phi_{11}(P_2) = (2^{11}, \beta^{11}) = (2, -\beta) = -P_2.$$

(On a $\beta^{11} = -\beta$ vu que $\beta^{11}$ est racine du polynôme $X^2 - 13 \in \mathbb{F}_{11}[X]$ et que $\beta^{11}$ est distinct de $\beta$). La matrice de $(\phi_{11})_3$ dans la base $(P_1, P_2)$ est donc

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Notons que l'ordre de $E(\mathbb{F}_{11})$ est 18, de sorte que l'on a $t = -6$. On retrouve dans ce cas particulier les égalités annoncées du théorème 7.7.

### 4. L'ordre de $E\big(\mathbb{F}_{q^n}\big)$

Notons $\mathbb{F}_{q^n}$ l'extension de degré $n$ de $\mathbb{F}_q = K$ dans $\overline{K}$ [3]. La courbe elliptique $E$ étant définie sur $K$, il est facile de calculer l'ordre du groupe $E\big(\mathbb{F}_{q^n}\big)$, pourvu que l'on sache déterminer celui de $E(K)$, autrement dit, le polynôme caractéristique du Frobenius de $E$.

**Théorème 7.8.** *Soient $\alpha$ et $\beta$ les racines dans $\mathbb{C}$ du polynôme caractéristique du Frobenius de $E$. On a*

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

Démonstration : Commençons par établir que $\alpha^n + \beta^n$ est un entier. C'est une conséquence directe du lemme suivant :

**Lemme 7.11.** *Pour tout $k \in \mathbb{N}$ posons $s_k = \alpha^k + \beta^k$. On a*

$$s_0 = 2, \quad s_1 = t \quad \text{et} \quad s_{k+1} = ts_k - qs_{k-1} \quad (k \geq 1).$$

[3] Étant donné un entier $n \geq 1$, rappelons pourquoi il existe une unique extension de degré $n$ de $K$ contenue dans $\overline{K}$. Tout d'abord, une telle extension existe car $K[X]$ possède des polynômes irréductibles sur $K$ de degré $n$ (chapitre III). Soient $K_1$ et $K_2$ des extensions de degré $n$ de $K$ dans $\overline{K}$. Le cardinal de $K_1$ est $q^n$, donc pour tout $x \in K_1$, on a $x^{q^n} = x$. Par suite, $K_1$ est l'ensemble des racines dans $\overline{K}$ du polynôme $X^{q^n} - X$. Tel est aussi le cas de $K_2$, d'où $K_1 = K_2$.

Démonstration : On a $X^2 - tX + q = (X - \alpha)(X - \beta)$, d'où $t = \alpha + \beta$. Considérons un entier $k \geq 1$. On a $\alpha^2 - t\alpha + q = 0$, d'où

$$\alpha^{k+1} - t\alpha^k + q\alpha^{k-1} = 0,$$

puis le résultat en additionnant cette égalité avec la même obtenue en remplaçant $\alpha$ par $\beta$.

Terminons la preuve du théorème. Posons

$$f = (X^n - \alpha^n)(X^n - \beta^n) = X^{2n} - (\alpha^n + \beta^n)X^n + q^n \in \mathbb{Z}[X].$$

Puisque $X - \alpha$ et $X - \beta$ divisent respectivement $X^n - \alpha^n$ et $X^n - \beta^n$, le polynôme $f$ est divisible par $X^2 - tX + q$. Puisque ce dernier est unitaire, il existe donc $H \in \mathbb{Z}[X]$ tel que

$$f = (X^2 - tX + q)H.$$

Dans l'anneau $\mathbb{Z}[\phi_q]$, on obtient ainsi (th. 7.6)

$$\phi_q^{2n} - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = (\phi_q^2 - t\phi_q + q)H(\phi_q) = 0. \tag{30}$$

D'après le théorème 7.6 appliqué avec le corps $\mathbb{F}_{q^n}$, il existe un unique entier $r$ tel que

$$\phi_{q^n}^2 - r\phi_{q^n} + q^n = 0, \tag{31}$$

et on a (formule (28))

$$r = q^n + 1 - \left|E\left(\mathbb{F}_{q^n}\right)\right|.$$

Par ailleurs, on a

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

Il résulte alors de (30) et (31) que l'on a $r = \alpha^n + \beta^n$, d'où le résultat.

**Exemple 7.11.** Soit $E$ la courbe elliptique définie sur $\mathbb{F}_5$ d'équation

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

Le polynôme caractéristique de Frobenius de $E$ est

$$X^2 + X + 5 \in \mathbb{Z}[X].$$

On a donc

$$\alpha = \frac{-1 + \sqrt{-19}}{2} \quad \text{et} \quad \beta = \frac{-1 - \sqrt{-19}}{2}.$$

En utilisant le lemme 7.11, on constate que l'on a

$$\alpha^{50} + \beta^{50} = -164775798123330249.$$

Par suite, on a

$$\left|E\left(\mathbb{F}_{5^{50}}\right)\right| = 888178419700125233986663315705958 75.$$

Ce nombre est facile à factoriser par la méthode des divisons successives, on trouve

$$\left|E\left(\mathbb{F}_{5^{50}}\right)\right| = 5^3 \times 7 \times 11^2 \times 461 \times 1201 \times 17401 \times 4419101 \times 19704014845201.$$

### 5. Courbes elliptiques ordinaires et supersingulières

Soit $p$ la caractéristique de $K$. On a vu que l'on a

$$E[p] = \left\{O\right\} \quad \text{ou} \quad E[p] \simeq \mathbb{Z}/p\mathbb{Z}.$$

**Définition 7.6.** *On dit que $E$ est ordinaire si $E[p]$ est d'ordre $p$, et que $E$ est supersingulière si $E[p]$ est le groupe trivial.*

Comme conséquence du théorème 7.8, on va établir l'énoncé suivant qui permet de savoir si $E$ est ordinaire ou supersingulière, si l'on connaît l'ordre de $E(K)$.

**Théorème 7.9.** *La courbe elliptique $E$ est supersingulière si et seulement si on a*

$$|E(K)| \equiv 1 \text{ mod. } p. \tag{32}$$

**Remarque 7.8.** Puisque $|E(K)| = q + 1 - t$, et que $q$ est une puissance de $p$, la condition (32) signifie que l'on a $t \equiv 0$ mod. $p$.

Démonstration : Posons

$$X^2 - tX + q = (X - \alpha)(X - \beta) \quad \text{où} \quad \alpha, \beta \in \mathbb{C}.$$

Pour tout entier $n \geq 1$, en posant $s_n = \alpha^n + \beta^n$, on a (lemme 7.11)

$$s_0 = 2, \quad s_1 = t \quad \text{et} \quad s_{n+1} = ts_n - qs_{n-1}.$$

Supposons la congruence (32) satisfaite. Il s'agit de montrer que $E\left(\overline{K}\right)$ n'a pas de points d'ordre $p$. Soient $n$ un entier $\geq 1$ et $\mathbb{F}_{q^n}$ l'extension de degré $n$ de $K$ dans $\overline{K}$. Tout

revient à montrer que $E(\mathbb{F}_{q^n})$ ne possède pas de points d'ordre $p$. L'entier $t$ étant divisible par $p$, on a

$$s_n \equiv 0 \text{ mod. } p.$$

D'après le théorème 7.8, on en déduit que

$$\left|E\left(\mathbb{F}_{q^n}\right)\right| \equiv 1 \text{ mod. } p.$$

En particulier, l'ordre de $E\left(\mathbb{F}_{q^n}\right)$ n'est pas divisible par $p$, d'où notre assertion.
Inversement, supposons $t$ non divisible par $p$. Pour tout $n \geq 1$, on a

$$s_{n+1} \equiv t s_n \text{ mod. } p.$$

Vu que $s_1 = t$, il en résulte que l'on a

$$s_n \equiv t^n \text{ mod. } p.$$

On obtient

$$\left|E\left(\mathbb{F}_{q^n}\right)\right| \equiv 1 - t^n \text{ mod. } p.$$

D'après le petit théorème de Fermat, on $t^{p-1} \equiv 1$ mod. $p$. Ainsi l'ordre du groupe $E\left(\mathbb{F}_{q^{p-1}}\right)$ est divisible par $p$. Il contient donc un élément d'ordre $p$, ce qui prouve que $E$ est ordinaire, d'où le théorème.

**Corollaire 7.3.** *Supposons $E$ définie sur $\mathbb{F}_p$ où $p$ est un nombre premier $\geq 5$. Alors, $E$ est supersingulière si et seulement si $|E(\mathbb{F}_p)| = p + 1$, autrement dit, si et seulement si $t = 0$.*

Démonstration : Supposons $E$ supersingulière. On a $t \equiv 0$ mod. $p$ (th. 7.9). D'après le théorème de Hasse, on a $|t| \leq 2\sqrt{p}$. L'inégalité $p \geq 5$ implique alors $t = 0$, d'où l'assertion.

**Exemple 7.12.** Supposons $q \equiv 2$ mod. 3. Soient $u$ un élément non nul de $K$ et $E$ la courbe elliptique sur $K$ d'équation

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

Vérifions que $E$ est supersingulière. Considérons pour cela l'application $f : K^* \to K^*$ qui à $x$ associe $x^3$. C'est un morphisme de groupes. Il est injectif car on a $q \equiv 2$ mod. 3 (si $K^*$ avait un élément d'ordre 3, $q - 1$ serait divisible par 3). Par suite, $f$ est une bijection, donc tous les éléments de $K$ possèdent une unique racine cubique dans $K$. Pour chaque $y \in K$, il existe donc un unique élément $x \in K$ tel que $y^2 - u = x^3$. En comptant le point à l'infini, on obtient

$$|E(K)| = q + 1, \tag{33}$$

d'où l'assertion (th. 7.9). On peut en déduire que $E(K)$ est cyclique. En effet, d'après le théorème 7.5, il existe des entiers $n_1$ et $n_2$ tels que $n_1$ divise $n_2$, $n_1$ divise $q-1$, et que

$$E(K) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}.$$

D'après (33), l'entier $n_1$ divise $q+1$. Puisque $n_1$ divise $q-1$, on a donc $n_1 \leq 2$. Par ailleurs, $E[2]$ n'est pas contenu dans $E(K)$ car, comme on l'a vu ci-dessus, le polynôme $X^3+u$ a une seule racine dans $K$. Le groupe $E(K)$ contenant un sous-groupe isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_1\mathbb{Z}$, on a donc $n_1 = 1$, d'où le résultat.

## 5. Méthodes de comptage

On considère dans ce paragraphe un nombre premier $p \geq 5$. Soit $E$ une courbe elliptique sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 + ax + b.$$

Dans les algorithmes de primalité et de factorisation utilisant les courbes elliptiques, il importe de pouvoir disposer de courbes elliptiques sur $\mathbb{F}_p$, pour lesquelles on sache déterminer l'ordre de $E(\mathbb{F}_p)$. On va décrire deux méthodes permettant parfois d'y parvenir.

### 1. Méthode du symbole de Legendre

Soit $\chi : \mathbb{F}_p \to \{-1, 0, 1\}$ l'application définie pour tout $x \in \mathbb{F}_p$ par

$$\chi(x) = \Big(\frac{x}{p}\Big).$$

Rappelons que l'on a $\chi(0) = 0$, $\chi(x) = 1$ si $x$ est un carré non nul dans $\mathbb{F}_p$ et $\chi(x) = -1$ si $x$ n'est pas un carré dans $\mathbb{F}_p$.

**Proposition 7.3.** *On a l'égalité*

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \chi\big(x^3 + ax + b\big).$$

Démonstration : Pour tout $x \in \mathbb{F}_p$, il y a deux points d'abscisse $x$ dans $E(\mathbb{F}_p)$ si $\chi(x^3+ax+b) = 1$. Il n'y en a pas si $\chi(x^3+ax+b) = -1$ et il y en a un seul si $x^3+ax+b = 0$. Par suite, en comptant le point à l'infini, on obtient

$$|E(\mathbb{F}_p)| = 1 + \sum_{x \in \mathbb{F}_p} \big(1 + \chi(x^3 + ax + b)\big),$$

ce qui conduit à l'égalité annoncée.

**Exemple 7.13.** Prenons pour $E$ la courbe elliptique sur $\mathbb{F}_{11}$ d'équation

$$y^2 = x^3 + x + 5.$$

On a

$$|E(\mathbb{F}_{11})| = 12 + \sum_{x \in \mathbb{F}_{11}} \chi\big(x^3 + x + 5\big),$$

autrement dit,

$$|E(\mathbb{F}_{11})| = 12 + \chi(5) + \chi(7) + \chi(4) + \chi(2) + \chi(7) + \chi(3) + \chi(7) + \chi(3) + \chi(8) + \chi(6) + \chi(3).$$

On vérifie que l'on a

$$\chi(3) = \chi(4) = \chi(5) = 1 \quad \text{et} \quad \chi(2) = \chi(6) = \chi(7) = \chi(8) = -1.$$

On obtient ainsi

$$|E(\mathbb{F}_{11})| = 11.$$

En fait, cette méthode de comptage fonctionne bien, disons pour les nombres premiers $p$ plus petits que $10^6$ ou à la limite $10^7$.

**Exemple 7.14.** Prenons pour $E$ la courbe elliptique d'équation

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

Avec $p = 10^6 + 3$, on trouve en une seconde avec le logiciel de calculs Pari que

$$\sum_{x \in \mathbb{F}_p} \chi\big(x^3 + x + 1\big) = 723,$$

d'où $|E(\mathbb{F}_p)| = 1000727$.
Avec $p = 10^7 + 19$, on trouve en douze secondes que

$$\sum_{x \in \mathbb{F}_p} \chi\big(x^3 + x + 1\big) = -1439,$$

d'où $|E(\mathbb{F}_p)| = 9998581$.

**Exemple 7.15.** Supposons $p \equiv 3$ mod. 4. Soient $u$ un élément non nul de $\mathbb{F}_p$ et $E$ la courbe elliptique sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 - ux.$$

Vérifions que l'on a $|E(\mathbb{F}_p)| = p+1$. En particulier, $E$ est supersingulière (cor. 7.3). Pour tout $x \in \mathbb{F}_p$, on a l'égalité

$$\chi\big((-x)^3 - u(-x)\big) = \chi(-1)\chi(x^3 - ux).$$

Puisque $p \equiv 3$ mod. 4, on a $\chi(-1) = -1$. Pour tout $x \in \mathbb{F}_p$, on a ainsi

$$\chi\big((-x)^3 - u(-x)\big) = -\chi(x^3 - ux).$$

La somme des $\chi(x^3 - ux)$ pour $x$ parcourant $\mathbb{F}_p$ est donc nulle, d'où l'assertion.

### 2. Méthode de Shanks - L'algorithme Baby step - Giant step

L'algorithme qui suit est dû à Shanks. Rappelons que

$$H_p = [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$$

est l'intervalle de Hasse pour $p$.

1) On choisit un point $P$ aléatoirement dans $E(\mathbb{F}_p)$. Pour cela, on détermine une abscisse $x$ au hasard jusqu'à ce que $x^3+ax+b$ soit un carré dans $\mathbb{F}_p$ et on extrait une racine carrée $y$ de $x^3+ax+b$ pour obtenir l'ordonnée. On prend alors $P = (x, y)$.

2) On détermine ensuite un entier $m$ tel que

$$mP = O \quad \text{et} \quad m \in H_p. \tag{34}$$

Il existe un tel entier $m$, car $|E(\mathbb{F}_p)|P = O$ et $|E(\mathbb{F}_p)|$ est dans $H_p$. Si $m$ est le seul entier de $H_p$ réalisant cette condition, alors $m$ est l'ordre de $E(\mathbb{F}_p)$ (on a déjà rencontré cette idée dans les exemples 7.8). En fait, la longueur de $H_p$ étant $4\sqrt{p}$, il est coûteux de vérifier, si $p$ est grand, que $m$ est le seul entier de $H_p$ satisfaisant (34) si tel est le cas. On peut procéder autrement.

**Lemme 7.12.** *Soit $d$ l'ordre de $P$. Supposons que l'on ait*

$$d > 4\sqrt{p}.$$

*Soit $m$ un entier vérifiant la condition* (34)*. Alors, $m$ est l'ordre de $E(\mathbb{F}_p)$. De plus, $m$ est l'unique multiple de $d$ dans $H_p$.*

Démonstration : L'entier $d$ divise $m$ et l'ordre de $E(\mathbb{F}_p)$. Parce que la longueur de $H_p$ est $4\sqrt{p}$, il y a un seul multiple de $d$ dans $H_p$. On a donc $m = |E(\mathbb{F}_p)|$.

Si l'on parvient à déterminer un entier $m$ satisfaisant (34), ainsi que sa factorisation en produit de nombres premiers, on peut facilement déterminer l'ordre de $P$. On peut alors éventuellement conclure en utilisant le lemme précédent.

Supposons qu'il existe deux entiers $m$ et $m'$ dans $H_p$ tels que $mP = m'P = O$, ce qui arrive rarement en pratique. Cela peut se produire si l'exposant du groupe $E(\mathbb{F}_p)$ est petit. Dans ce cas, on calcule l'ordre $d$ de $P$, et on recommence l'algorithme avec un autre point de $E(\mathbb{F}_p)$, en utilisant l'information que $d$ divise $|E(\mathbb{F}_p)|$.

**Exemples 7.16.** Prenons pour $E$ la courbe elliptique sur $\mathbb{F}_p$ d'équation

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

Le point $P = (0, 1)$ appartient à $E(\mathbb{F}_p)$.

1) Avec $p = 10^6 + 3$, en une demie seconde environ, on trouve que

$$m = 1000727$$

est le seul entier dans $H_p$ tel que $mP = O$, d'où $|E(\mathbb{F}_p)| = m$. En fait, l'ordre de $P$ est 76979, qui est plus grand que $4\sqrt{p}$. Par ailleurs, on a $m = 7^2 \times 13 \times 1571$ et 7 ne divise par $p - 1$. Compte tenu du théorème 7.5, cela entraîne que $E(\mathbb{F}_p)$ est cyclique d'ordre $m$.

2) Avec $p = 10^{10} + 19$, on trouve en une minute quinze secondes environ que

$$m = 9999881780$$

est le seul entier de $H_p$ tel que $mP = O$, d'où $|E(\mathbb{F}_p)| = m$. Vérifions que $E(\mathbb{F}_p)$ est cyclique. Pour cela, on constate que l'on a

$$m = 2^2 \times 5 \times 7^2 \times 17 \times 600233.$$

Le polynôme $X^3 + X + 1$ ayant une seule racine modulo $p$, le groupe $E[2]$ n'est pas contenu dans $E(\mathbb{F}_p)$, autrement dit, $E(\mathbb{F}_p)$ ne contient pas un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Puisque 7 ne divise pas $p - 1$, le théorème 7.5 implique l'assertion.

**L'algorithme Baby step - Giant step**

Le point $P \in E(\mathbb{F}_p)$ étant donné, il s'agit alors d'expliquer comment trouver un entier $m$ vérifiant la condition (34). On peut, comme dans les exemples ci-dessus, tester les entiers de $H_p$ jusqu'à en trouver un vérifiant cette condition, ce qui peut nécessiter $4\sqrt{p}$ tests. L'algorithme Baby step-Giant step permet en fait de se limiter à environ $4p^{\frac{1}{4}}$ tests. On procède comme suit.

1) On calcule $Q = (p + 1)P$.

2) On choisit un entier $s > p^{\frac{1}{4}}$, par exemple $s = \left[p^{\frac{1}{4}}\right] + 1$ et l'on dresse la liste des points

$$jP \quad \text{pour} \quad j = 0, \cdots, s.$$

Connaissant $jP$, on connaît aussi $-jP$. On détermine ainsi $2s+1$ points de $E(\mathbb{F}_p)$. L'appellation baby step est relative à ce calcul pour le passage de $jP$ à $(j+1)P$.

3) On calcule les points

$$Q + k(2sP) \quad \text{pour} \quad k \in [-s, s].$$

Pour cela, on calcule au départ le point $Q+2sP$. On obtient alors $Q+(k+1)(2sP)$ (resp. $Q+(k-1)(2sP)$) à partir de $Q+k(2sP)$ en lui ajoutant $2sP$ (resp. $-2sP$). L'appellation giant step est relative à ce passage.

**Proposition 7.4.** *Il existe des entiers $j$ et $k$ tels que l'on ait*

$$jP = Q + k(2sP) \quad \textit{avec} \quad j, k \in [-s, s] \quad \textit{et} \quad |j - 2ks| \leq 2\sqrt{p}.$$

*Si $j$ et $k$ sont des entiers satisfaisant ces conditions, en posant*

$$m = p + 1 + 2ks - j, \tag{35}$$

*on a $mP = O$ et $m$ est dans $H_p$.*

Démonstration : Vérifions pour cela le lemme suivant :

**Lemme 7.13.** *Soit $c$ un entier relatif tel que $|c| \leq 2s^2$. Il existe des entiers $c_0$ et $c_1$ tels que l'on ait*

$$c = c_0 + 2sc_1 \quad \textit{avec} \quad c_0, c_1 \in [-s, s].$$

Démonstration : Il existe un entier $c_0$ tel que l'on ait

$$c \equiv c_0 \text{ mod. } 2s \quad \text{avec} \quad c_0 \in [-s, s].$$

Posons $c - c_0 = 2sc_1$. On a

$$|c_1| \leq \frac{2s^2 + s}{2s} < s + 1,$$

d'où l'assertion.

On en déduit la proposition comme suit. Appliquons ce lemme avec $t = p+1-|E(\mathbb{F}_p)|$. D'après le choix de $s$, on a $s^2 > \sqrt{p}$, d'où $|t| \leq 2s^2$ (théorème de Hasse). Il existe donc $j, k \in [-s, s]$ tels que $t = j - 2ks$. On a alors $|j - 2ks| \leq 2\sqrt{p}$ et les égalités

$$Q + k(2sP) = (p + 1 + 2sk)P = (p + 1 + j - t)P = (|E(\mathbb{F}_p)| + j)P = jP,$$

ce qui entraîne le résultat.

**Exemples 7.17.** Soit $E$ la courbe elliptique sur $\mathbb{F}_p$ d'équation

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

Posons $P = (0, 1) \in E(\mathbb{F}_p)$. On reprend les notations de la proposition 7.4.

1) Prenons $p = 10^{15} + 37$. Avec $s = 5624$, on trouve

$$j = 3111 \quad \text{et} \quad k = -164,$$

d'où (formule (35))

$$m = 999999998152255.$$

On vérifie que $m$ est l'ordre de $P$ et que $m > 4\sqrt{p}$. Par suite, $E(\mathbb{F}_p)$ est cyclique d'ordre $m$ (lemme 7.12). Le temps pour effectuer ces opérations est d'environ deux secondes.

2) Prenons $p = 10^{20} + 39$. Avec $s = 100001$, on obtient

$$j = 78499 \quad \text{et} \quad k = -31624,$$

ce qui conduit à

$$m = 99999999993675058293.$$

On a $m > 4\sqrt{p}$ et $P$ est d'ordre $m$, donc $E(\mathbb{F}_p)$ est cyclique d'ordre $m$. Le temps de calcul est d'environ deux minutes.

## 6. Cryptosystèmes elliptiques

On peut utiliser en cryptographie des cryptosystèmes à clés publiques utilisant la théorie des courbes elliptiques. Dans l'étude faite au chapitre IV, on a vu que l'efficacité de certains cryptosystèmes à clés publiques repose sur la difficulté de pouvoir résoudre le problème du logarithme discret dans des corps finis bien choisis. On va remplacer ici le groupe multiplicatif d'un corps fini par le groupe des points rationnels d'une courbe elliptique sur un tel corps. L'un des avantages est que, un corps fini $K$ étant donné, on dispose généralement de nombreux choix de courbes elliptiques $E$ sur $K$, autrement dit de nombreux groupes $E(K)$, pour utiliser efficacement un cryptosystème elliptique à clé publique, contrairement à la théorie classique, où l'on ne dispose que du groupe $K^*$.

### 1. Le problème du logarithme discret elliptique

Il est analogue à celui déjà défini pour le groupe multiplicatif d'un corps fini. Soient $K$ un corps fini et $E$ une courbe elliptique définie sur $K$. Soit $A$ un point de $E(K)$. Le problème du logarithme discret sur $E$ de base $A$ est le suivant.

**Problème.** Soit $P$ un point de $E(K)$. Trouver un entier $n$, s'il existe, tel que

$$nA = P.$$

Un tel entier $n$ n'existe pas toujours. De plus, $E(K)$ n'est pas nécessairement cyclique. Afin d'essayer de résoudre ce problème, on peut, comme dans le cas des corps finis, utiliser par exemple l'algorithme de Silver, Pohlig et Hellman ou l'algorithme Baby step - Giant step. On se limitera à décrire ce dernier dans le cadre qui nous occupe ici. Posons

$$N = |E(K)|.$$

**Algorithme Baby step - Giant step.** Supposons que $n$ existe et, ce qui n'est pas restrictif, que l'on a $0 \leq n \leq N$. Cet algorithme permet de trouver $n$ en $O\big(\sqrt{N}\big)$ opérations.

1) On fixe un entier $m > \sqrt{N}$ et on calcule $mA$.

2) On établit la liste des points

$$jA \quad \text{pour} \quad j = 0, \cdots, m-1.$$

3) On détermine les points

$$P - k(mA) \quad \text{pour} \quad k = 0, \cdots, m-1,$$

jusqu'à en trouver un qui soit égal à l'un des $jA$ précédemment calculés.

Il y a toujours une coïncidence :

**Lemme 7.14.** *Il existe $j$ et $k$ dans $\big\{0, \cdots, m-1\big\}$ tels que l'on ait*

$$jA = P - kmA.$$

*En particulier, on a $nA = P$ avec $n = j + km$.*

Démonstration : Puisque $N < m^2$, on a

$$0 \leq n < m^2.$$

Il existe des entiers naturels $n_0$ et $n_1$ tels que l'on ait (division euclidienne)

$$n = mn_1 + n_0 \quad \text{avec} \quad 0 \leq n_0 < m.$$

On a alors

$$n_1 = \frac{n - n_0}{m} \leq \frac{n}{m} < m.$$

On obtient

$$P - n_1(mA) = nA - n_1(mA) = (n - n_1 m)A = n_0 A,$$

d'où assertion.

**Exemple 7.18.** Prenons $K = \mathbb{F}_{53}$ et pour $E$ la courbe elliptique d'équation

$$y^2 = x^3 + 5x + 2.$$

Il est facile de vérifier que $E(K)$ est cyclique d'ordre 63 engendré par le point

$$A = (-1, 7).$$

Le point $P = (20, 24)$ appartient à $E(K)$. Cherchons l'entier naturel $n < 63$ tel que

$$nA = P.$$

Prenons $m = 8$. Les points $jA$ pour $j = 0, \cdots 7$, sont (par indices croissants)

$$O, \quad (-1, 7), \quad (51, 39), \quad (20, 29), \quad (50, 38), \quad (19, 38), \quad (6, 6), \quad (8, 17).$$

Par ailleurs, les points $P - kmA$ pour $k = 0, \cdots 7$, sont (par indices croissants)

$$P, \quad (35, 4), \quad (33, 45), \quad (16, 16), \quad (49, 17), \quad (5, 24), \quad (13, 12), \quad (50, 38).$$

La coïncidence a lieu pour $k = 7$, ce qui a donc rendu nécessaire le calcul de sept points, et pour $j = 4$. On obtient

$$n = 60.$$

**Remarque 7.8.** Afin de résoudre le problème du logarithme discret dans $E(K)$, il n'est pas nécessaire de déterminer l'ordre de $E(K)$. En supposant qu'il existe $n$ tel que $nA = P$, il suffit en fait de savoir que l'on peut prendre pour $n$ un entier plus petit qu'une borne explicite. Tel est le cas dans notre situation, vu que $|E(K)|$ est plus petit que $q + 1 + 2\sqrt{q}$ où $q$ est le cardinal de $K$. Si l'entier $n$ cherché existe, on peut donc supposer que l'on a $n \leq q + 1 + 2\sqrt{q}$. Ainsi, l'algorithme précédent fonctionne en choisissant au départ un entier $m$ vérifiant l'inégalité $m^2 > q + 1 + 2\sqrt{q}$, auquel cas, on a de nouveau $n < m^2$, et l'énoncé du lemme 7.14 est encore valable, avec la même démonstration.

Le problème du logarithme discret est généralement beaucoup plus difficile à résoudre dans le groupe des points rationnels d'une courbe elliptique $E$ sur un corps fini $K$, que celui dans $K^*$. Il convient toutefois de prendre certaines précautions sur le choix de $E$. Il faut par exemple que l'ordre de $E(K)$ soit divisible par un grand nombre premier, disons ayant plus de cinquante chiffres décimaux. Il faut par ailleurs éviter que $E$ soit supersingulière. En effet, Menezes, Okamoto et Vanstone ont découvert une méthode permettant de plonger le groupe $E(K)$ dans dans une extension finie $L$ de $K$ de degré assez petit. Leur méthode utilise l'accouplement de Weil, que l'on ne verra pas ici. Dans ce cas, le problème du logarithme discret dans $E(K)$ se ramène ainsi à celui dans $L^*$. Moyennant un choix

convenable de $E$, les seuls algorithmes connus pour résoudre le problème du logarithme discret dans $E(K)$, sont de complexité asymptotique exponentielle. Par ailleurs, il semble que les cryptosystèmes elliptiques utilisant des clés de chiffrement de taille environ 160-bits soient aussi sécurisés que, par exemple, le système RSA utilisé avec un entier de 1024-bits. Cela renforce l'intérêt de leur utilisation, puisque l'on travaille avec des clés de plus petite taille qu'avec les autres cryptosystèmes, et avec le même niveau de sécurité.

On va maintenant décrire les analogues elliptiques du protocole de Diffie-Hellman et de l'algorithme de El Gamal que l'on a rencontrés au chapitre IV.

### 2. L'analogue du protocole de Diffie-Hellman

Deux personnes Alice et Bob se mettent d'accord pour se construire une clé secrète commune, leur seul moyen de communication étant public. Pour cela, ils suivent le procédé suivant.

1) Ils choisissent un corps fini $K$ et une courbe elliptique $E$ définie sur $K$, de telle sorte que le problème du logarithme discret soit difficile à résoudre dans le groupe $E(K)$. Ils choisissent un point $P \in E(K)$ tel que l'ordre du sous-groupe de $E(K)$ engendré par $P$ soit grand. En pratique, l'ordre de ce groupe est un grand nombre premier. Le triplet $(K, E, P)$ est public.

2) Alice choisit secrètement un entier naturel $a$, elle calcule le point $P_a = aP$, et transmet publiquement $P_a$ à Bob.

3) Bob choisit de même secrètement un entier naturel $b$, il calcule le point $P_b = bP$, et transmet publiquement $P_b$ à Alice.

4) Alice détermine le point $aP_b = abP$.

5) Bob détermine le point $bP_a = baP$.

Leur clé secrète commune est alors le point $abP$. Ils peuvent aussi fabriquer leur secrète à partir $abP$ par un procédé précis. Par exemple, ils peuvent utiliser les cent derniers chiffres de l'abscisse de $abP$ comme clé secrète.

Toute l'efficacité de ce protocole repose sur le problème suivant :

**Problème de Diffie-Hellman.** Connaissant $P$, $aP$ et $bP$ dans $E(K)$, comment déterminer $abP$ ?

On ne sait pas à ce jour résoudre ce problème sans calculer $a$ ou $b$, autrement dit, sans savoir résoudre le problème du logarithme discret dans $E(K)$. Cela étant, on n'a pas la preuve qu'il n'existe pas d'autres moyens pour y parvenir.

### 3. L'analogue de l'algorithme de El Gamal

Une personne, Alice souhaite pouvoir se faire envoyer des messages confidentiels. Elle choisit pour cela un corps fini $K$, une courbe elliptique $E$ définie sur $K$, de sorte que le

problème du logarithme discret soit difficile à résoudre dans le groupe $E(K)$. Elle choisit un point $P \in E(K)$, en pratique d'ordre premier assez grand. Elle choisit par ailleurs un entier naturel $s$ et calcule le point

$$A = sP.$$

La clé publique d'Alice est le quadruplet

$$(K, E, P, A).$$

Sa clé secrète est l'entier $s$.

Bob souhaite envoyer confidentiellement un message $M \in E(K)$ à Alice. Pour cela, il choisit secrètement un entier naturel $k$ et calcule les points

$$M_1 = kP \quad \text{et} \quad M_2 = M + kA.$$

Il transmet ensuite publiquement ces deux points à Alice. C'est la phase d'encryptage du message $M$.

Afin de décrypter $M$, Alice calcule le point

$$M_2 - sM_1.$$

Elle retrouve ainsi $M$, vu que l'on a

$$M_2 - sM_1 = M + kA - s(kP) = M + kA - kA = M.$$

Quiconque connaissant l'entier $s$, autrement dit le logarithme discret de base $P$ de $A$, peut intercepter le message $M$. De même, si un intrus parvient à déterminer $k$, il obtient $M$ en calculant $M_2 - kA$. On ne connaît pas de moyens de trouver $M$, autrement qu'en déterminant $s$ ou $k$.

## 7. Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$

Dans les applications de la théorie des courbes elliptiques aux problèmes de primalité et de factorisation, on est amené à évoquer la notion de «courbe elliptique sur l'anneau $\mathbb{Z}/n\mathbb{Z}$», où $n$ n'est pas nécessairement premier.

### 1. Le plan projectif $\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$

Soit $n$ un entier $\geq 2$. Pour tous $x, y, z$ dans $\mathbb{Z}/n\mathbb{Z}$, posons

$$\text{pgcd}(x, y, z, n) = \text{pgcd}(\tilde{x}, \tilde{y}, \tilde{z}, n),$$

où $\tilde{x}$, $\tilde{y}$, $\tilde{z}$ sont des représentants de $x, y, z$ dans $\mathbb{Z}$. Cette définition a un sens car elle ne dépend pas des représentants choisis. Posons alors

$$T = \Big\{(x,y,z) \in \big(\mathbb{Z}/n\mathbb{Z}\big)^3 \;\Big|\; \text{pgcd}(x,y,z,n) = 1\Big\}.$$

Un élément $(x,y,z)$ est dans $T$ si et seulement si l'idéal engendré par $x, y$ et $z$ est $\mathbb{Z}/n\mathbb{Z}$ tout entier. Par définition, on a

$$\mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) = T/\sim,$$

la relation d'équivalence $\sim$ étant telle que

$$(x,y,z) \sim (x',y',z') \iff \text{il existe } u \in \big(\mathbb{Z}/n\mathbb{Z}\big)^* \text{ tel que } (x,y,z) = u(x',y',z').$$

Autrement dit, deux éléments de $T$ sont équivalents s'ils diffèrent multiplicativement par un élément inversible de $\mathbb{Z}/n\mathbb{Z}$. On note $[x,y,z]$ la classe d'équivalence de $(x,y,z)$.

**Exemple 7.19.** L'ensemble $\mathbb{P}^2(\mathbb{Z}/4\mathbb{Z})$ est de cardinal 28. Les éléments $[x,y,z]$ de $\mathbb{P}^2(\mathbb{Z}/4\mathbb{Z})$ pour lesquels $z$ est inversible sont les $[x,y,1]$ où $x$ et $y$ parcourent $\mathbb{Z}/4\mathbb{Z}$. Il y en a seize. Ceux pour lesquels $z$ n'est pas inversible et $x = 1$ sont

$$[1,0,0], \quad [1,1,0], \quad [1,2,0], \quad [1,3,0], \quad [1,0,2], \quad [1,1,2], \quad [1,2,2], \quad [1,3,2].$$

Ceux pour lesquels $z$ et $x$ ne sont pas inversibles sont,

$$[0,1,0], \quad [2,1,0], \quad [0,1,2], \quad [2,1,2].$$

Plus généralement :

**Lemme 7.15.** *Soient $p$ un nombre premier et $r$ un entier $\geq 1$. On a*

$$\big|\mathbb{P}^2(\mathbb{Z}/p^r\mathbb{Z})\big| = p^{2r}\left(1 + \frac{1}{p} + \frac{1}{p^2}\right).$$

Démonstration : Soit $(x,y,z)$ un élément $\big(\mathbb{Z}/p^r\mathbb{Z}\big)^3$. Il est dans $T$ si et seulement si l'un (au moins) des éléments $x$, $y$ et $z$ n'est pas divisible par $p$. Il en résulte que $\mathbb{P}^2(\mathbb{Z}/p^r\mathbb{Z})$ est la réunion disjointe des trois ensembles

$$A = \Big\{[a,b,1] \;\Big|\; a,b \in \mathbb{Z}/p^r\mathbb{Z}\Big\}, \quad B = \Big\{[1,a,pb] \;\Big|\; a,b \in \mathbb{Z}/p^r\mathbb{Z}\Big\},$$

$$C = \Big\{[pa,1,pb] \;\Big|\; a,b \in \mathbb{Z}/p^r\mathbb{Z}\Big\}.$$

On a

$$|A| = p^{2r}, \quad |B| = p^r p^{r-1}, \quad |C| = \left(p^{r-1}\right)^2.$$

Le cardinal cherché est donc $p^{2r} + p^{2r-1} + p^{2r-2}$, d'où le résultat.

**Remarque 7.9.** Dans le cas où $r = 1$, on retrouve le fait que le cardinal de $\mathbb{P}^2(\mathbb{F}_p)$, qui est le nombre de droites d'un espace vectoriel de dimension 3 sur $\mathbb{F}_p$, est

$$\frac{p^3 - 1}{p - 1} = 1 + p + p^2.$$

### 2. Courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$ - Définition

Soit $n$ un entier naturel premier avec 6. Nous appellerons courbe elliptique $E$ sur $\mathbb{Z}/n\mathbb{Z}$, une courbe projective d'équation

$$y^2 z = x^3 + axz^2 + bz^3, \tag{36}$$

où $a$ et $b$ sont des éléments de $\mathbb{Z}/n\mathbb{Z}$ tels que

$$4a^3 + 27b^2 \text{ soit un élément inversible de } \mathbb{Z}/n\mathbb{Z}. \tag{37}$$

Dans le cas où $n$ est composé, et dans ce cas seulement, on signifie ici que $E$ est l'ensemble $E(\mathbb{Z}/n\mathbb{Z})$ formé des points

$$[x, y, z] \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z})$$

vérifiant l'égalité (36). Il contient la partie, que l'on appellera affine,

$$E_{\text{aff}}(\mathbb{Z}/n\mathbb{Z}) = \left\{ [x, y, 1] \in \mathbb{P}^2(\mathbb{Z}/n\mathbb{Z}) \mid y^2 = x^3 + ax + b \right\}$$

ainsi que le point $O = [0, 1, 0]$. On désignera par $(x, y)$ le point $[x, y, 1]$ et on notera

$$V_{n,E} = E_{\text{aff}}(\mathbb{Z}/n\mathbb{Z}) \cup \{O\}.$$

Si $n$ est premier, on a $V_{n,E} = E(\mathbb{F}_n)$. La situation est plus compliquée si $n$ est composé. Il y a d'autres points dans $E(\mathbb{Z}/n\mathbb{Z})$.

**Exemple 7.20.** Considérons la cubique projective sur $\mathbb{Z}/25\mathbb{Z}$ d'équation

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

La condition (37) étant satisfaite, c'est une courbe elliptique $E$ sur $\mathbb{Z}/25\mathbb{Z}$. Explicitons $E(\mathbb{Z}/25\mathbb{Z})$. On vérifie que $V_{25,E}$ est formé, avec le point $O$, des vingt-cinq points suivants :

$$(0,\pm 1),(2,\pm 3),(5,\pm 1),(7,\pm 12),(10,\pm 1),(12,\pm 2),(15,\pm 1),(17,\pm 8),$$

$$(20,\pm 1)(22,\pm 7),(24,0),(24,\pm 5),(24,\pm 10).$$

On a donc $|V_{25,E}| = 26$. Par ailleurs, soit $[x,y,z]$ un point de $E(\mathbb{Z}/25\mathbb{Z})$ avec $z$ non inversible. Alors $x$ n'est pas inversible, donc $y$ l'est i.e. $y$ est premier avec 5, et on peut supposer $y = 1$. On constate que l'on a $z = 0$, et on obtient les quatre autres points

$$[5,1,0], \quad [10,1,0], \quad [15,1,0], \quad [20,1,0].$$

L'ensemble $E(\mathbb{Z}/25\mathbb{Z})$ est donc de cardinal 30.

**Remarque 7.10.** On peut démontrer que pour tout entier $n$, premier avec 6, l'ensemble $E(\mathbb{Z}/n\mathbb{Z})$ est muni d'une structure de groupe qui généralise celle que l'on a définie si $n$ est premier. Cela étant, les formules définissant cette structure de groupe ne sont pas données par celles établies dans le cas où $n$ est premier. Cela est dû au fait que si $n$ est composé, et si $x_1$ et $x_2$ sont distincts dans $\mathbb{Z}/n\mathbb{Z}$, l'élément $x_1 - x_2$ peut ne pas être inversible. Pour les applications que l'on a en vue, nous n'utiliserons pas la structure de groupe sur $E(\mathbb{Z}/n\mathbb{Z})$. En fait, pour les problèmes de primalité et de factorisation, seule la partie $V_{n,E}$ est importante.

### 3. Algorithme de pseudo-addition sur $V_{n,E}$

Soit $E$ une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$ définie par une équation de la forme (36). Pour tout diviseur premier $p$ de $n$, en réduisant les coefficients de $E$ modulo $p$ via le morphisme canonique $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$, on obtient une courbe elliptique sur $\mathbb{F}_p$, que l'on notera encore $E$. On dispose alors de l'application de réduction modulo $p$

$$E(\mathbb{Z}/n\mathbb{Z}) \to E(\mathbb{Z}/p\mathbb{Z})$$

qui à $[x,y,z] \in E(\mathbb{Z}/n\mathbb{Z})$ associe $[u,v,w]$, où $u$, $v$ et $w$ sont respectivement les images de $x, y$ et $z$ par le morphisme $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$. Pour tout point $P$ de $V_{n,E}$, on notera $P_p$ son image dans $E(\mathbb{Z}/p\mathbb{Z})$.

On va décrire un algorithme, que l'on appellera pseudo-addition sur $V_{n,E}$, qui étant donnés $P$ et $Q$ dans $V_{n,E}$ permet, ou bien de trouver un diviseur non trivial de $n$, ou bien de construire un point $R$ de $V_{n,E}$ tel que l'on ait

$$R_p = P_p + Q_p \quad \text{pour tout diviseur premier } p \text{ de } n. \tag{38}$$

1) si $P = O$ (resp. $Q = O$), on pose $R = Q$ (resp. $R = P$).

Supposons $P$ et $Q$ distincts de $O$. Posons

$$P = (x_1, y_1), \quad Q = (x_2, y_2) \quad \text{et} \quad d = \operatorname{pgcd}\big(x_2 - x_1, n\big).$$

2) Si $d$ est distinct de 1 et $n$, alors $d$ est un diviseur non trivial de $n$.

3) Si $d = 1$, l'élément $x_2 - x_1$ est inversible. On pose alors (comme pour les corps)

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

auquel cas

$$R = \big(\lambda^2 - x_1 - x_2, -\lambda(\lambda^2 - x_1 - x_2) - \nu\big). \tag{39}$$

4) Supposons $d = n$. Dans ce cas, on a $x_1 = x_2$. Posons

$$d' = \operatorname{pgcd}(y_1 + y_2, n).$$

4.1) Si $d'$ est distinct de 1 et $n$, on a trouvé un diviseur non trivial de $n$.

4.2) Si $d' = n$, on alors $y_1 = -y_2$, et on pose

$$R = O.$$

4.3) Supposons $d' = 1$. Les égalités

$$y_1^2 = x_1^3 + ax_1 + b \quad \text{et} \quad y_2^2 = x_2^3 + ax_2 + b,$$

et le fait que $x_1 = x_2$, impliquent

$$(y_1 - y_2)(y_1 + y_2) = 0.$$

Puisque $d' = 1$, $y_1 + y_2$ est inversible, et l'on obtient $y_1 = y_2$, autrement dit, on a

$$P = Q.$$

Par hypothèse, $n$ est impair, donc $2y_1$ est inversible. On pose alors (comme pour les corps)

$$\lambda = \frac{3x_1^2 + a}{2y_1} \quad \text{et} \quad \nu = \frac{-x_1^3 + ax_1 + 2b}{2y_1},$$

puis

$$R = \big(\lambda^2 - 2x_1, -\lambda(\lambda^2 - 2x_1) - \nu\big). \tag{40}$$

Par construction, et compte tenu du théorème 7.1, la condition (38) est satisfaite et cet algorithme possède ainsi les propriétés annoncées.

On peut ainsi essayer de calculer dans $V_{n,E}$ «comme si $\mathbb{Z}/n\mathbb{Z}$ était un corps». En particulier, si $P$ est un point de $V_{n,E}$ et $m$ un entier naturel, on peut essayer de calculer le point

$$mP.$$

Ou bien l'algorithme de pseudo-addition fonctionne et l'on détermine, comme dans le cas d'un corps, effectivement ce point, ou bien on ne peut pas effectuer le calcul jusqu'au bout, et on a alors trouvé un diviseur non trivial de $n$.

**Remarque 7.11.** Le calcul de $mP$ dépend a priori de la façon dont on l'effectue. Par exemple, il se peut que l'on puisse calculer $9P$ et effectuant les opérations

$$3P + 6P,$$

et que l'algorithme de pseudo-addition ne fonctionne pas avec la chaîne d'opérations

$$P + 4P + 4P.$$

Il en est ainsi avec la courbe elliptique sur $\mathbb{Z}/77\mathbb{Z}$ d'équation

$$y^2 = x^3 + x + 1 \quad \text{avec} \quad P = (0, 1).$$

On vérifie que l'on a

$$3P = (72, 72), \quad 6P = (0, 43) \quad \text{et} \quad 3P + 6P = (14, 69).$$

Par ailleurs, on a

$$4P = (28, 27) \quad \text{et} \quad 4P + 4P = 8P = (44, 23),$$

et on ne peut pas calculer $P + 8P$, vu que l'on a $\text{pgcd}(44, 77) = 11$. On ne peut pas non plus calculer $P + 4P$, car on a $\text{pgcd}(28, 77) = 7$.

Cela étant si deux chaînes de calculs fonctionnent, on peut démontrer que le point obtenu est le même. Ce n'est pas évident a priori. En tout cas, cela donne un sens à $mP$ sous réserve que l'on puisse effectuer le calcul par quelque chaîne d'opérations que ce soit. Dans l'exemple ci-dessus, on a $9P = (14, 69)$.

## 8. Primalité - Théorème ECPP

La terminologie ECPP vient de l'anglais, elliptic curve primality proving. Goldwasser et Killian en 1986 ont utilisé la théorie des courbes elliptiques pour résoudre des problèmes de primalité. Le principe est le suivant. On dispose d'un grand entier $N$, ayant disons plus de mille chiffres décimaux, dont on est moralement sûr qu'il est premier, pour la raison que les critères de composition classiques, notamment le test de Miller, ont échoué à prouver qu'il est composé. Il s'agit alors de fournir la preuve que $N$ est effectivement premier. Le critère de primalité de Goldwasser et Killian est le résultat suivant, qui est un analogue elliptique du critère de Pocklington.

**Théorème 7.10 (Théorème ECPP).** *Soit $N$ un entier naturel premier avec 6 et distinct de 1. Soit $E$ une courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$. Soient $m$ un entier et $P$ un point de $V_{N,E}$ satisfaisant les conditions suivantes :*

*1) l'algorithme de pseudo-addition fonctionne pour le point $mP$ et l'on a $mP = O$.*

*2) Il existe un diviseur premier $q$ de $m$ tel que :*

*2.1) on a*

$$q > \left(\sqrt[4]{N} + 1\right)^2.$$

*2.2) L'algorithme de pseudo-addition fonctionne pour le point $\left(\frac{m}{q}\right)P$ et l'on a*

$$\left(\frac{m}{q}\right)P \neq O.$$

*Alors, $N$ est premier.*

Démonstration : Soit $p$ un diviseur premier de $N$. Soit $P_p \in E(\mathbb{F}_p)$ l'image de $P$ par l'application de réduction $E(\mathbb{Z}/N\mathbb{Z}) \to E(\mathbb{F}_p)$. Identifions $O$ et son image dans $E(\mathbb{F}_p)$. Compte tenu de la condition (38), on a

$$mP_p = O.$$

Par suite, l'ordre $d$ de $P_p$ dans $E(\mathbb{F}_p)$ divise $m$. D'après la condition 2.2, il existe $x$ et $y$ dans $\mathbb{Z}/N\mathbb{Z}$ tels que l'on ait $\left(\frac{m}{q}\right)P = [x, y, 1] \in V_{N,E}$. On a donc

$$\left(\frac{m}{q}\right)P_p \neq O.$$

Ainsi, $d$ ne divise pas $\frac{m}{q}$. Le fait que $q$ soit premier entraîne alors que $q$ divise $d$. En particulier, on a

$$q \leq |E(\mathbb{F}_p)|.$$

D'après le théorème de Hasse, on a donc l'inégalité

$$q \leq \left(\sqrt{p}+1\right)^2.$$

Supposons que $N$ ne soit pas premier. On a $N \neq 1$. Prenons pour $p$ le plus petit diviseur premier de $N$. On a $p \leq \sqrt{N}$, et l'on obtient

$$q \leq \left(\sqrt[4]{N}+1\right)^2,$$

ce qui contredit l'hypothèse faite sur $q$, d'où le résultat.

**Remarques 7.12.**

1) En pratique les calculs de $mP$ et de $\left(\frac{m}{q}\right)P$ ne poseront pas de problèmes, vu que $N$ est très certainement premier.

2) Le théorème ECPP est un analogue du critère de Pocklington, au sens où l'entier $m$ joue ici le rôle de l'entier $N-1$.

Voyons maintenant comment on utilise ce résultat en pratique. Autrement dit, comment choisir la courbe elliptique $E$, l'entier $m$ et le point $P$ ? Vu que notre objectif est de démontrer que $N$ est premier, on peut pour faire ces choix supposer que tel est le cas. En fait, seul le choix de l'entier $m$ est difficile a priori. Il est suggéré par l'énoncé suivant.

**Proposition 7.5.** *Soient $\ell$ un nombre premier $\geq 5$ et $E$ une courbe elliptique définie sur $\mathbb{F}_\ell$. Posons*

$$m = |E(\mathbb{F}_\ell)|.$$

*Supposons que $m$ possède un diviseur premier $q$ tel que*

$$q > \left(\sqrt[4]{\ell}+1\right)^2.$$

*Alors, il existe un point $P \in E(\mathbb{F}_\ell)$ tel que l'on ait*

$$mP = O \quad et \quad \left(\frac{m}{q}\right)P \neq O.$$

Démonstration : Vu que l'on a $m = |E(\mathbb{F}_\ell)|$, tout point $P \in E(\mathbb{F}_\ell)$ vérifie l'égalité $mP = O$. Procédons par l'absurde en supposant que pour tout point $P \in E(\mathbb{F}_\ell)$ on ait

$$\left(\frac{m}{q}\right)P = O.$$

Dans ce cas, l'ordre de tout point $P \in E(\mathbb{F}_\ell)$ divise $\frac{m}{q}$. En particulier, l'exposant de $E(\mathbb{F}_\ell)$, qui est le ppcm des ordres des éléments de $E(\mathbb{F}_\ell)$, divise $\frac{m}{q}$. Par ailleurs, $E(\mathbb{F}_\ell)$ est

isomorphe à un groupe produit de la forme $\mathbb{Z}/d_1\mathbb{Z}\times\mathbb{Z}/d_2\mathbb{Z}$, avec $d_1$ divisant $d_2$. L'exposant de $E(\mathbb{F}_\ell)$ est $d_2$ et son ordre est $d_1d_2$. On a ainsi

$$m = d_1d_2 \leq d_2^2 \leq \Big(\frac{m}{q}\Big)^2,$$

d'où l'inégalité

$$q^2 \leq m.$$

D'après le théorème de Hasse, on a

$$m \leq \big(\sqrt{\ell}+1\big)^2.$$

Compte tenu de l'hypothèse faite sur $q$, il en résulte que l'on a

$$\big(\sqrt[4]{\ell}+1\big)^2 < \sqrt{\ell}+1,$$

d'où une contradiction et le résultat.

Formalisons ce qui précède sous la forme de l'algorithme suivant.

**Algorithme de Goldwasser et Killian**

Soit $N$ un entier qui est très certainement premier.

1) On choisit des entiers $a$ et $b$ au hasard de sorte que

$$\mathrm{pgcd}(4a^3+27b^2, N) = 1,$$

et l'on considère la courbe elliptique $E$ sur $\mathbb{Z}/N\mathbb{Z}$ d'équation $y^2 = x^3+ax+b$.

2) On essaye de calculer le cardinal de $E(\mathbb{Z}/N\mathbb{Z})$

$$\text{« comme si } N \text{ était premier »}.$$

Si l'on y parvient, la proposition 7.5 suggère alors de choisir l'entier

$$m = |E(\mathbb{Z}/N\mathbb{Z})|.$$

Ce calcul est a priori difficile pour les grands entiers $N$ et des courbes elliptiques sans propriétés arithmétiques particulières, bien que l'on dispose d'algorithmes très performants à ce sujet. Signalons que pour pallier à cet inconvénient, Atkin a eu l'idée d'utiliser des courbes elliptiques pour lesquelles le cardinal de $E(\mathbb{Z}/N\mathbb{Z})$ soit connu à l'avance, tout au moins si $N$ est premier, ce sont les courbes à multiplications complexes. On ne verra pas ici cette démarche.

3) On essaye de factoriser $m$, en espérant que $m$ possède un diviseur premier

$$q > \left(\sqrt[4]{N} + 1\right)^2.$$

Si l'on y parvient pas, on change de courbe elliptique $E$.

4) Si $m$ a un tel diviseur premier $q$, on détermine alors un point $P = (x, y)$ de $V_{N,E}$. Pour cela, on choisit aléatoirement $x \in \mathbb{Z}/N\mathbb{Z}$ de sorte que l'on ait l'égalité du symbole de Jacobi

$$\left(\frac{x^3 + ax + b}{N}\right) = 1.$$

On utilise ensuite les algorithmes d'extraction de racines carrées modulo $N$ en supposant toujours implicitement que $N$ est premier, afin de déterminer $y \in \mathbb{Z}/N\mathbb{Z}$ tel que l'on ait $y^2 = x^3 + ax + b$. Si $N$ est effectivement premier, on aura automatiquement $mP = O$, et souvent en pratique on aura aussi $\left(\frac{m}{q}\right)P \neq O$, auquel cas les conditions du théorème ECPP sont satisfaites. On obtient alors la preuve que $N$ est premier. On dit que le quadruplet

$$(E, m, q, P)$$

est un certificat de primalité de $N$, puisque connaissant $(E, m, q, P)$ on peut vérifier sur machine très facilement que $N$ est premier.

**Exemple 7.21.** Prenons $N = 10^{25} + 13$. Le test de Miller laisse penser que $N$ est premier. Démontrons que tel est bien le cas. On prend pour $E$ la courbe elliptique sur $\mathbb{Z}/N\mathbb{Z}$ d'équation

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

On a $N \equiv 2$ mod. 3. Si $N$ est premier, on a vu que $|E(\mathbb{Z}/N\mathbb{Z})| = N + 1$ (exemple 7.12). Prenons donc

$$m = N + 1.$$

On vérifie ensuite que

$$q = 16423310748511,$$

est un diviseur premier de $m$ et que $q > \left(\sqrt[4]{N} + 1\right)^2$. Choisissons pour $P$ le point

$$P = (10^6, 45189585937662084063661 06) \in E(\mathbb{Z}/N\mathbb{Z}).$$

En fait, on choisit $x$ aléatoirement de sorte que

$$\left(\frac{x^3 + 1}{N}\right) = 1,$$

par exemple $x = 10^6$, et on extrait ensuite une racine carrée de $x^3+1$, toujours en supposant que $N$ est premier. On a $N \equiv 5$ mod. 8 et on vérifie que

$$(x^3+1)^{\frac{N-1}{4}} = 1.$$

Si $N$ est effectivement premier, alors

$$\pm(x^3+1)^{\frac{N+3}{8}},$$

sont les deux racines carrées de $x^3+1$ dans $\mathbb{Z}/N\mathbb{Z}$. Cela conduit au point $P$ choisi. On constate que l'on a $mP = O$ et que

$$\Big(\frac{m}{q}\Big)P = (633844304660660861339882 1, 771228741314168046759 1102) \neq O,$$

d'où le fait que $N$ soit premier.

## 9. Méthode de factorisation ECM

La méthode ECM (en anglais, elliptic curve method) a été découverte par H. Lenstra vers 1986. C'est une méthode de factorisation, qui est l'analogue elliptique de la méthode $p-1$ de Pollard. L'entier $p-1$, i.e. l'ordre de $\mathbb{F}_p^*$, est ici remplacé par l'ordre du groupe des points d'une courbe elliptique sur $\mathbb{F}_p$. Soit $n$ un entier composé premier avec 6, que l'on cherche à factoriser. Le principe de la méthode est le suivant.

1) On choisit une courbe elliptique $E$ sur $\mathbb{Z}/n\mathbb{Z}$ et un point $P$ de la partie affine $V_{n,E}$ de $E$.

2) On choisit une borne $B$, disons plus petite que $10^7$, et l'on essaye de calculer dans $V_{n,E}$ le point

$$B!P$$

avec l'algorithme de pseudo-addition.

3) Si le calcul ne s'effectue pas jusqu'au bout, car un certain dénominateur dans la chaîne d'opérations choisie pour calculer $B!P$ n'est pas premier avec $n$, alors on a trouvé un diviseur non trivial de $n$. Si le calcul s'effectue jusqu'à son terme, on n'a pas réussi à factoriser $n$. On change alors de courbe elliptique et on recommence à la première étape.

Voyons en quoi cette méthode est très efficace pour déterminer un facteur premier de $n$, pourvu qu'il ne soit pas trop grand, disons en pratique plus petit que $10^{40}$. Soit $E$ une courbe elliptique sur $\mathbb{Z}/n\mathbb{Z}$. Soient par ailleurs $P$ un point de $V_{n,E}$ et $B$ un entier plus petit que $10^7$. Supposons qu'il existe un diviseur premier $p$ de $n$ tel que

$$|E(\mathbb{F}_p)| \text{ soit } B\text{-friable}, \tag{41}$$

autrement dit, que l'ordre de $E(\mathbb{F}_p)$ n'ait que des facteurs premiers plus petits que $B$. Supposons de plus que ces facteurs premiers soient affectés de puissances pas trop grandes. Dans le groupe $E(\mathbb{F}_p)$, on a alors

$$B!P = O.$$

D'après l'algorithme de pseudo-addition dans $V_{n,E}$, cela signifie que dans la chaîne de calculs choisie pour calculer $B!P$, il existe deux multiples de $P$,

$$k_1P = (x_1, y_1) \quad \text{et} \quad k_2P = (x_2, y_2)$$

tels que $p$ divise $x_1 - x_2$. Si $n$ possède au moins deux grands facteurs premiers, il sera alors probable que l'on ait $\operatorname{pgcd}(x_1 - x_2, n) \neq n$, et l'on pourra détecter $p$ en calculant ce pgcd.

Pour que la méthode fonctionne, il s'agit de pouvoir trouver assez facilement des courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$ de sorte que la condition (41) soit satisfaite. En fait, on peut démontrer que tout entier de l'intervalle de Hasse $H_p$ est l'ordre du groupe des points d'une courbe elliptique convenable sur $\mathbb{F}_p$. Par ailleurs, les ordres des groupes des points des courbes elliptiques sur $\mathbb{F}_p$ se répartissent assez uniformément dans $H_p$. Une courbe elliptique sur $\mathbb{F}_p$ étant choisie au hasard, la probabilité pour que la condition (41) soit satisfaite est donc « analogue » à celle pour qu'un entier choisi au hasard dans $H_p$ soit $B$-friable. Or si $B$ est choisi assez grand, il y a une densité assez grande d'entiers $B$-friables dans $H_p$. On a ainsi au départ la possibilité de choisir de nombreuses courbes elliptiques sur $\mathbb{Z}/n\mathbb{Z}$ afin d'en trouver une pour laquelle la condition (41) soit réalisée. Par exemple, on peut essayer celles ayant une équation de la forme

$$y^2 = x^3 + ax + 1 \quad \text{avec} \quad P = (0, 1), \tag{42}$$

ou encore celles de la forme

$$y^2 = x^3 + ax - a \quad \text{avec} \quad P = (1, 1). \tag{43}$$

C'est l'avantage par rapport à la méthode $p - 1$ classique, car si l'entier $p - 1$ n'est pas $B$-friable, on ne peut définitivement pas conclure.

**Remarque 7.11 (Sur le choix de $B$).** On peut voir heuristiquement, et constater expérimentalement, que pour trouver les diviseurs premiers de $n$ plus petits que $A$, il convient souvent de choisir

$$B = L(A)^{\frac{1}{\sqrt{2}}} \quad \text{où} \quad L(A) = \exp\bigl(\sqrt{\log A \log\log A}\bigr). \tag{44}$$

Par exemple, on a

$$L(10^{12}) \simeq 872,$$

de sorte que pour rechercher des diviseurs premiers de $n$ ayant environ douze chiffres décimaux, la constante $B = 1000$ semble être bien adaptée. De même, on a

$$L(10^{25}) \simeq 49048,$$

donc une constante $B$ de l'ordre de 50000 semble être un bon choix pour la recherche de diviseurs premiers de $n$ ayant environ de vingt-cinq chiffres décimaux.

**Exemples 7.22.**

1) Factorisons $n = 10^{50} + 3$. On trouve par divisions successives les facteurs 19, 97 et 283. Reste à factoriser

$$n_1 = \frac{n}{19 \times 97 \times 283} = 1917291863588518489404086515878052568308315 87.$$

Avec la courbe elliptique $E$ sur $\mathbb{Z}/n_1\mathbb{Z}$ d'équation

$$y^2 = x^3 + 360x + 1,$$

le point $P = (0, 1)$ et comme constante

$$B = 1000,$$

on constate que $p = 994327748569$ est un diviseur premier de $n_1$. L'équation choisie de $E$ est de la forme (42) et $a = 360$ est le plus entier permettant de conclure avec cette valeur de $B$. On vérifie que l'on a

$$|E(\mathbb{F}_p)| = 2^3 \times 3 \times 5^2 \times 29 \times 41 \times 61 \times 73 \times 313,$$

qui est $B$-friable, donc la condition (41) est satisfaite dans ce cas. Posons ensuite

$$n_2 = \frac{n_1}{994327748569} = 1928229264795048279931642865705 23.$$

En prenant la courbe elliptique $E'$ sur $\mathbb{Z}/n_2\mathbb{Z}$ d'équation

$$y^2 = x^3 + 2016x + 1,$$

$P = (0, 1)$ et $B = 1000$, on trouve que $q = 61236769827829$ est un diviseur premier de $n_2$. Notons que l'on a dans ce cas

$$|E'(\mathbb{F}_q)| = 2 \times 3^2 \times 5 \times 19 \times 157 \times 521 \times 641 \times 683.$$

On obtient ainsi la décomposition complète de $n_2$, et donc celle de $n$,

$$n_2 = 61236769827829 \times 3148809563627188687.$$

2) Posons $n = 2^{211} - 1$. Il est facile de vérifier que l'on a

$$n = 15193 \times c_{60},$$

où $c_{60}$ est un nombre composé de soixante chiffres. Recherchons, a priori, des diviseurs premiers de $c_{60}$ ayant au plus vingt-cinq chiffres décimaux. Pour cela, on suit l'estimation (44), en prenant pour $B$ la constante

$$B = 1000 \prod_{j=169}^{5134} p_k, \tag{45}$$

où $p_k$ est le $k$-ième nombre premier, en tenant compte du fait que l'on a $p_{169} = 1009$ et $p_{5134} = 50021$. Soient $E$ la courbe elliptique sur $\mathbb{Z}/c_{60}\mathbb{Z}$ d'équation

$$y^2 = x^3 + 6x - 6$$

et $P$ le point $(1, 1)$. En essayant de calculer $B!P$, on trouve que

$$p = 60272956433838849161,$$

qui a vingt chiffres décimaux, est un diviseur premier de $c_{60}$. On a choisi ici une équation de la forme (43) et $a = 6$ est le plus petit entier permettant de conclure. On constate que l'on a

$$|E(\mathbb{F}_p)| = 2^4 \times 3^2 \times 5 \times 11 \times 293 \times 467 \times 947 \times 3517 \times 16699,$$

qui est $B$-friable. En posant

$$q = \frac{c_{60}}{p} = 35938757044958237573881998942687731534 39,$$

on vérifie que $q$ est premier, et l'on obtient la décomposition complète de $n$,

$$n = 15193 \times pq.$$

3) Factorisons l'entier

$$n = \frac{10^{131} - 1}{9}$$

qui a cent trente et un chiffres 1.

3.1) Par la méthode des divisions successives, on trouve les diviseurs premiers

$$q_1 = 80173 \quad \text{et} \quad q_2 = 109517.$$

3.2) Avec la méthode rho de Pollard, on trouve les diviseurs premiers

$$q_3 = 446790173, \quad q_4 = 141811693 \quad \text{et} \quad q_5 = 7370364319027.$$

Il reste à factoriser l'entier de quatre-vingt-onze chiffres

$$n_1 = \frac{n}{q_1 q_2 q_3 q_4 q_5}.$$

On utilise la méthode ECM, en prenant la même constante $B$ que (45), et des courbes elliptiques de la forme (42) avec le point $P = (0, 1)$.

3.3) Avec la courbe elliptique sur $\mathbb{Z}/n_1\mathbb{Z}$ d'équation

$$y^2 = x^3 + 34x + 1,$$

on détecte le diviseur premier de vingt-sept chiffres

$$q_6 = 180222062287834025451247081.$$

3.4) Posons $n_2 = \frac{n_1}{q_6}$. Avec la courbe elliptique sur $\mathbb{Z}/n_2\mathbb{Z}$ d'équation

$$y^2 = x^3 + 116x + 1,$$

on trouve le diviseur premier de vingt-deux chiffres

$$q_7 = 7317723970031057677693.$$

3.5) Posons $n_3 = \frac{n_2}{q_7}$. Avec la courbe elliptique sur $\mathbb{Z}/n_3\mathbb{Z}$ d'équation

$$y^2 = x^3 + 370x + 1,$$

on trouve le diviseur premier de vingt-quatre chiffres

$$q_8 = 131758351065116151205213.$$

3.6) On vérifie ensuite que

$$q_9 = \frac{n_3}{q_8} = 15594845538029429933$$

est un nombre premier. On obtient ainsi la décomposition complète de $n$,

$$n = \prod_{i=1}^{9} q_i.$$