Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22
Travaux dirigés
Alain Kraus

Correction des exercices - Chapitre IV

Courbes elliptiques

Exercice 1

1) On a $4 \times 2^3 + 27 = 59 \neq 0$, donc E est une courbe elliptique définie sur $\mathbb{Q}$ (définition 4.1 du cours).

2) Un point $[x, y, z]$ de $\mathbb{P}^2$ appartient à D si et seulement si le déterminant de la matrice

$$\begin{pmatrix} 1 & 0 & x \\ 2 & 1 & y \\ 1 & 1 & z \end{pmatrix}$$

est nul. Il s'agit donc de la droite d'équation $y = x + z$.

3) Reprenons les notations de la proposition 4.1 du cours. On a $P \neq Q$, $P \neq O$ et $Q \neq O$. Par ailleurs, on a $x_P = 1$, $y_P = 2$, $x_Q = 0$ et $y_Q = 1$, d'où (alinéa 1.1)

$$\lambda = -1 \quad \text{et} \quad \nu = 1.$$

D'après la formule (10), on obtient $f(P, Q) = (0, 1) = Q$. Par suite, on a

$$D \cap E = \{P, Q\}.$$

(La droite D est donc la tangente à E au point Q.)

4) En utilisant la formule (14) du théorème 4.1, on obtient

$$P + Q = (0, -1).$$

D'après la formule (16), on a donc

$$P + Q = -Q \quad \text{puis} \quad P + 2Q = O.$$

5) Le polynôme $X^3 + 2X + 1$ est irréductible sur $\mathbb{Q}$, car il est de degré 3 et n'a pas de racines dans $\mathbb{Q}$; en effet, soient a et b des entiers premiers entre eux, avec $a \in \mathbb{N}$, tels que $\frac{a}{b}$ soit racine de $X^3 + 2X + 1$. On a $a^3 + 2ab^2 + b^3 = 0$, d'où $a = 1$ et $b = \pm 1$.

Or ± 1 ne sont pas racines de ce polynôme. Par suite, E n'a pas de points d'ordre 2 rationnels sur $\mathbb{Q}$ (lemme 4.5).

Exercice 2

1) On a $4 \times (-3)^3 + 27 \times 16 = 2^2 \times 3^4$, qui est non nul dans $\mathbb{F}_p$ car $p \geq 5$, donc E est une courbe elliptique sur $\mathbb{F}_p$.

2) On vérifie que l'on a

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

3) Notons f le polynôme caractéristique de ϕ_5. Suivant la terminologie page 27 du cours, on a dans $\mathbb{Z}[X]$ l'égalité

$$f = X^2 - tX + 5,$$

avec $t = 5 + 1 - |E(\mathbb{F}_5)|$, où $|E(\mathbb{F}_5)|$ est l'ordre du groupe $E(\mathbb{F}_5)$. On a $|E(\mathbb{F}_5)| = 7$, d'où $t = -1$, puis

$$f = X^2 + X + 5.$$

4) D'après le théorème 4.6, pour tout $P \in E$ on a

$$\phi_5^2(P) + \phi_5(P) + 5P = O.$$

Il en résulte que P est dans $E[5]$ si et seulement si on a $\phi_5^2(P) + \phi_5(P) = O$. Autrement dit, pour tout $P \in E$, on a l'équivalence

$$P \in E[5] \iff \phi_5\big(\phi_5(P) + P\big) = O.$$

Parce que ϕ_5 est injectif, cette condition se traduit par l'égalité $\phi_5(P) = -P$, d'où le résultat.

5) Soit $P = (x, y)$ un point de $E[5]$. Il appartient à $E(\mathbb{F}_{25})$ si et seulement si on a $x^{25} = x$ et $y^{25} = y$. Cette condition signifie que l'on a $\phi_5^2(P) = P$, ce qui est le cas d'après la question précédente.

6) Soient α et β les racines de f dans $\mathbb{C}$. On a (théorème 4.8)

$$\big|E(\mathbb{F}_{25})\big| = 5^2 + 1 - (\alpha^2 + \beta^2).$$

On a $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$. Les égalités $\alpha + \beta = -1$ et $\alpha\beta = 5$ entraînent alors $\big|E(\mathbb{F}_{25})\big| = 35$.

7) L'ordre du groupe abélien $E(\mathbb{F}_{25})$ est sans facteurs carrés. Par suite, $E(\mathbb{F}_{25})$ est cyclique d'ordre 35.

Exercice 3

1) Le discriminant du polynôme $X^3 - 2 \in \mathbb{F}_5[X]$ est 2. Il est non nul, donc E est une courbe elliptique sur $\mathbb{F}_5$.

2) Un point (x, y) de E est d'ordre 2 si et seulement si $y = 0$. Par ailleurs, la décomposition de $X^3 - 2$ en produit de polynômes irréductibles dans $\mathbb{F}_5[X]$ est donnée par l'égalité

$$X^3 - 2 = (X + 2)(X^2 + 3X - 1).$$

La somme de ses racines dans $\overline{\mathbb{F}_5}$ est nulle. Les racines dans $\overline{\mathbb{F}_5}$ de $X^3 - 2$ sont donc $3, \alpha$ et $2 - \alpha$. En posant $O = [0, 1, 0]$, on a ainsi

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

3) Une base de $E[2]$ est par exemple (P_1, P_2) où $P_1 = (3, 0)$ et $P_2 = (\alpha, 0)$.

4) L'endomorphisme de Frobenius ϕ_5 de E est le morphisme de groupes qui à un point $(x, y) \in E$ associe (x^5, y^5). On a $\phi_5(P_1) = P_1$ et $\phi_5(P_2) = (\alpha^5, 0)$. Puisque α^5 est racine du polynôme $X^2 + 3X - 1$ et que α n'est pas dans $\mathbb{F}_5$, on a $\alpha^5 = 2 - \alpha$ (on peut aussi vérifier directement cette égalité). Par suite, on a

$$\phi_5(P_2) = P_1 + P_2.$$

Dans la base (P_1, P_2), la matrice de ϕ_5 restreint à $E[2]$ est donc $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Exercice 4

1) Soit $f = X^2 - tX + p \in \mathbb{Z}[X]$ le polynôme caractéristique du Frobenius de E. Soient α et β les racines de f dans $\mathbb{C}$. Posons $s_n = \alpha^n + \beta^n$. On a (théorème 4.8)

$$|E(\mathbb{F}_{p^n})| = p^n + 1 - s_n.$$

De plus, on a $s_{n+1} \equiv ts_n \mod p$ (lemme 4.11). On a $s_1 = t$, d'où $s_n \equiv t^n \mod p$, ce qui conduit à la congruence annoncée.

2) Soit (x, y) un point de E d'ordre p. Le groupe $E[p]$ étant d'ordre p, on a l'égalité $\mathbb{F}_p(E[p]) = \mathbb{F}_p(x, y)$. Soit n le degré de $\mathbb{F}_p(E[p])$ sur $\mathbb{F}_p$. On a $\mathbb{F}_p(E[p]) = \mathbb{F}_{p^n}$ et n est le plus petit entier $k \geq 1$ tel que p divise $|E(\mathbb{F}_{p^k})|$. D'après la question précédente, n est donc l'ordre de t modulo p, d'où le résultat.

Exercice 5

1) Soit t la trace du Frobenius de E. Par définition, on a

$$|E(\mathbb{F}_q)| = q + 1 - t.$$

Par hypothèse, on a $|E(\mathbb{F}_q)| = q+1$, d'où $t = 0$.

2) Pour tout $P \in E(\mathbb{F}_q)$, on a l'égalité (théorème 4.6)

$$\phi_q^2(P) - t\phi_q(P) + qP = O,$$

où le point O est l'élément neutre de $E(\mathbb{F}_q)$. On a $t = 0$, d'où l'assertion.

3) Soit P un point de $E[n]$. Il s'agit de montrer que P est dans $E\big(\mathbb{F}_{q^2}\big)$. Parce qu'il existe un point d'ordre n dans $E(\mathbb{F}_q)$ et que $|E(\mathbb{F}_q)| = q+1$, on a $q \equiv -1$ mod. n. Il en résulte que l'on a

$$qP = -P.$$

D'après la question précédente, on a donc

$$(\phi_q \circ \phi_q)(P) = P.$$

On peut supposer $P \neq O$. Posons $P = (x, y)$. On a ainsi

$$\big(x^{q^2}, y^{q^2}\big) = (x, y),$$

d'où $x^{q^2} = x$ et $y^{q^2} = y$, ce qui implique que x et y sont dans $\mathbb{F}_{q^2}$, d'où le résultat.

4.1) On a l'égalité (proposition 4.3)

$$|E(\mathbb{F}_q)| = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + x}{q} \right).$$

Puisque $q \equiv 3$ mod. 4, on a $\left(\frac{-1}{q}\right) = -1$. Pour tout $x \in \mathbb{F}_q$, on a ainsi

$$\left(\frac{(-x)^3 + (-x)}{q} \right) = -\left(\frac{x^3 + x}{q} \right),$$

d'où $|E(\mathbb{F}_q)| = q + 1$.

4.2) Notons $E(\mathbb{F}_q)[2]$ le groupe des points de 2-torsion de E rationnels sur $\mathbb{F}_q$. Considérons un point $P = (x, y)$ de $E(\mathbb{F}_q)[2]$. On a $x^3 + x = 0$ i.e. $x(x^2+1) = 0$. Puisque -1 n'est pas un carré dans $\mathbb{F}_q$, on en déduit que $x = 0$, d'où $P = (0, 0)$. On a donc

$$E(\mathbb{F}_q)[2] = \Big\{ O, (0,0) \Big\}.$$

Par ailleurs, il existe des entiers n_1 et n_2 tels que le groupe $E(\mathbb{F}_q)$ soit isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$, et que n_1 divise n_2 et n_1 divise $q-1$ (théorème 4.5). Parce que n_1 divise $q+1$, on a donc $n_1 \leq 2$. Le fait que $E(\mathbb{F}_q)$ possède un unique point d'ordre 2 entraîne $n_1 = 1$, donc $E(\mathbb{F}_q)$ est cyclique.

4.3) Le polynôme caractéristique du Frobenius de E dans $\mathbb{Z}[X]$ est

$$X^2 + q.$$

Soient α et β ses racines dans $\mathbb{C}$. On a (théorème 4.8)

$$|E(\mathbb{F}_{q^2})| = q^2 + 1 - (\alpha^2 + \beta^2).$$

On a $\alpha + \beta = 0$ et $\alpha\beta = q$, d'où $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = -2q$. On obtient

$$|E(\mathbb{F}_{q^2})| = (q+1)^2.$$

4.4) On a $|E(\mathbb{F}_q)| = q + 1$ et $E(\mathbb{F}_q)$ possède un élément d'ordre $q + 1$. D'après la question 3, le groupe $E[q+1]$ est donc contenu dans $E(\mathbb{F}_{q^2})$. Le groupe $E[q+1]$ étant d'ordre $(q+1)^2$, la question précédente implique alors l'égalité $E[q+1] = E(\mathbb{F}_{q^2})$.

Exercice 6

1) Le discriminant du polynôme $X^3 - X + 1 \in \mathbb{F}_5[X]$ est $-23 = 2$. Il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) On vérifie que l'on a

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

où $O = [0,1,0]$.

3) Le groupe $E(\mathbb{F}_5)$ est abélien d'ordre 8. Il est donc isomorphe à l'un des groupes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/8\mathbb{Z}.$$

Par ailleurs, un point (x, y) de E est d'ordre 2 si et seulement si $y = 0$. Le point $(3, 0)$ est donc le seul point d'ordre 2 de $E(\mathbb{F}_5)$. Ainsi $E(\mathbb{F}_5)$ contient un unique sous-groupe d'ordre 2. Il est donc isomorphe à $\mathbb{Z}/8\mathbb{Z}$.
(Remarquons que la première possibilité ne se produit jamais, vu qu'une courbe elliptique possède au plus quatre points de 2-torsion.)

4) Notons f le polynôme caractéristique du Frobenius de E. Parce que l'ordre de $E(\mathbb{F}_5)$ est 8, la trace du Frobenius de E est $6 - 8 = -2$. On a donc

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

5) Soient α et β les racines de f dans $\mathbb{C}$. On a (théorème 4.8)

$$\big|E(\mathbb{F}_{25})\big| = 5^2 + 1 - (\alpha^2 + \beta^2).$$

Les égalités $\alpha + \beta = -2$ et $\alpha\beta = 5$ entraînent

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = -6.$$

On obtient

$$\left|E(\mathbb{F}_{25})\right| = 32.$$

6) Le point $(3, 0)$ est d'ordre 2 dans $E(\mathbb{F}_5)$. Les abscisses des deux autres points d'ordre 2 de E sont donc racines d'un polynôme de degré 2 de $\mathbb{F}_5[X]$ (qui est $X^2 + 3X + 3$). Elles sont ainsi dans $\mathbb{F}_{25}$, d'où l'assertion.

7) Le groupe $E(\mathbb{F}_{25})$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ qui n'est pas cyclique, donc $E(\mathbb{F}_{25})$ n'est pas un groupe cyclique.

8) Le groupe $E(\mathbb{F}_{25})$ est d'ordre 32. Il n'est pas cyclique et il contient au plus quatre points de 2-torsion (en fait ici exactement quatre). Il en résulte qu'il est isomorphe à l'un des groupes

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}.$$

Supposons $E(\mathbb{F}_{25})$ isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. Il contient alors un sous-groupe isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Cela entraîne que le sous-groupe des points de 4-torsion de E est contenu dans $E(\mathbb{F}_{25})$. D'après l'assertion admise, on obtient ainsi une contradiction. Par suite, $E(\mathbb{F}_{25})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$.

Exercice 7

1) Il s'agit de montrer que n divise $q - 1$. D'après l'hypothèse faite, c'est par exemple une conséquence du théorème de structure du groupe $E(K)$ (théorème 4.5).
On peut aussi procéder comme suit. On déduit de l'hypothèse que le groupe $E[n]$ des points de n-torsion de E est d'ordre n^2, et donc que n est premier avec la caractéristique de K (théorème 4.2). Par ailleurs, $E[n]$ est contenu dans $E(K)$. Le groupe des racines n-ièmes de l'unité est donc contenu dans K (théorème 4.3). C'est un sous-groupe d'ordre n de K^*, ce qui entraîne que n divise $q - 1$.

2) D'après le théorème de Hasse (théorème 4.4), on a

$$|t| \leq 2\sqrt{q}.$$

En élevant les deux membres de cette inégalité au carré, on obtient

$$4 + r^2n^2 + 4rn \leq 4q = 4n^2 + 4rn + 4,$$

d'où $r^2 \leq 4$, puis $|r| \leq 2$.

3) On a

$$q = n^2 + rn + 1.$$

Puisque r vaut 0, ± 1 ou ± 2, cette égalité implique le résultat.

4) Pour tout entier a, on vérifie que a^2+1 est congru à $1, 2, 5$ ou 10 modulo 12, et que $a^2 \pm a + 1$ est congru à $1, 3, 7$ ou 9 modulo 12. Par ailleurs, un carré n'étant pas congru à -1 modulo 4, cela entraîne l'assertion.

Exercice 8

1) Supposons $E[\ell]$ contenu dans $E(\mathbb{F}_{q^n})$. Parce que ℓ ne divise pas q, le groupe des racines ℓ-ièmes de l'unité (dans une clôture algébrique de $\mathbb{F}_q$) est contenu dans $\mathbb{F}_{q^n}^*$ (théorème 4.3). Par suite, ℓ divise $q^n - 1$.
Inversement, supposons que ℓ divise $q^n - 1$. L'entier ℓ divise $|E(\mathbb{F}_q)|$ donc il existe un point $P \in E(\mathbb{F}_q)$ d'ordre ℓ. Soit Q un point de $E[\ell]$ tel que (P, Q) soit une base du $\mathbb{F}_\ell$-espace vectoriel $E[\ell]$. Soit ϕ_q l'endomorphisme de Frobenius de E. Il existe a et b dans $\mathbb{F}_\ell$ tels que la matrice de $(\phi_q)_\ell$ soit de la forme $\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}$. D'après la seconde égalité du théorème 4.7, on a $b = q$ modulo ℓ. Pour tout $m \in \mathbb{N}$, on a ainsi

$$M^m = \begin{pmatrix} 1 & a(1+q+\cdots+q^{m-1}) \\ 0 & q^m \end{pmatrix}.$$

Parce que ℓ ne divise pas $q-1$, on déduit alors de l'hypothèse faite que l'on a

$$M^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Ainsi, ϕ_q^n agit trivialement sur $E[\ell]$. Soit $R = (x, y)$ un point de $E[\ell]$ dans un modèle donné de E sur $\mathbb{F}_q$. On a

$$(\phi_q)_\ell^n(R) = \left(x^{q^n}, y^{q^n}\right) = (x, y).$$

Par suite, x et y appartiennent à $\mathbb{F}_{q^n}$, donc $E[\ell]$ est contenu dans $E(\mathbb{F}_{q^n})$, d'où l'assertion.

2) On vérifie que l'équation considérée définie une courbe elliptique sur $\mathbb{F}_7$ et que l'on a

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

3) On a $|E(\mathbb{F}_7)| = 6$. Par suite, 3 divise $|E(\mathbb{F}_7)|$ et $E[3]$, qui est d'ordre 9, n'est pas contenu dans $E(\mathbb{F}_7)$.

4) Le polynôme f n'a pas de racines dans $\mathbb{F}_7$ et il est de degré 3, donc il est irréductible sur $\mathbb{F}_7$. On vérifie que P et Q sont des points de E. Par ailleurs, le polynôme de $\mathbb{F}_7[X]$ donnant les abscisses des points de $E[3]$ est $3(X+1)f$. Il en résulte que P et Q sont dans $E[3]$ (lemme 4.6). De plus, (P, Q) est une base de $E[3]$ car P et Q sont $\mathbb{F}_3$-linéairement indépendants. (En particulier, on a $\mathbb{F}_7(E[3]) = \mathbb{F}_7(\alpha)$.)

5) On vérifie que l'on a

$$\phi_7(Q) = (\alpha^2 + 2\alpha + 6, \alpha^2 + 2\alpha + 5) = 2P + Q.$$

La matrice de $(\phi_7)_3$ dans la base (P, Q) est donc $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$.

Exercice 9

1) Le discriminant du polynôme $X^3 - X \in \mathbb{F}_5[X]$ est 4. Il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) On vérifie que l'on a

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

où O est le point à l'infini de E. En particulier, $E(\mathbb{F}_5)$ est d'ordre 8.

3) Un point (x, y) de E est d'ordre 2 si et seulement si $y = 0$. Les points d'ordre 2 de $E(\mathbb{F}_5)$ sont donc les points $(0,0)$, $(1,0)$ et $(4,0)$.

4) Le groupe $E(\mathbb{F}_5)$ étant abélien d'ordre 8, il est isomorphe à l'un des groupes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/8\mathbb{Z}.$$

D'après la question précédente, le groupe des points de 2-torsion de E est contenu dans $E(\mathbb{F}_5)$. Il est d'ordre 4 isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il en résulte que $E(\mathbb{F}_5)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

5) Le groupe $E(\mathbb{F}_5)$ étant d'ordre 8, la trace du Frobenius de E vaut est $6 - 8 = -2$. En notant F le polynôme caractéristique du Frobenius de E, on a donc

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

6) Soient a et b les racines de F dans $\mathbb{C}$. On a (Théorème 4.8)

$$\big|E(\mathbb{F}_{25})\big| = 5^2 + 1 - (a^2 + b^2).$$

Les égalités $a + b = -2$ et $ab = 5$ entraînent

$$a^2 + b^2 = (a + b)^2 - 2ab = -6.$$

On obtient $\big|E(\mathbb{F}_{25})\big| = 32$.

7.1) En utilisant la formule (15) du théorème 4.1 et l'égalité $y^2 = x^3 - x$, on vérifie que l'on a $2P = (u, v)$, où

$$u = \frac{(x^2+1)^2}{4(x^3 - x)} \quad \text{et} \quad v = \frac{x^6 - 5x^4 - 5x^2 + 1}{8y(x^3 - x)} = \frac{x^6 + 1}{8y(x^3 - x)}.$$

7.2) Le point P est d'ordre 4 si et seulement si $2P$ est d'ordre 2. Supposons que P soit d'ordre 4. On a $y \neq 0$, sinon P serait d'ordre 2. L'égalité $v = \frac{x^6+1}{8y(x^3-x)}$ impliquent alors $x^6 + 1 = 0$. Inversement, supposons $x^6 + 1 = 0$. Vérifions que l'on a $y \neq 0$. Dans le cas contraire, on aurait $P = (x, 0)$ d'où $P \in \{(0, 0), (1, 0), (4, 0)\}$ (question 3), or aucun de ces points ne vérifient l'égalité $x^6 + 1 = 0$. D'après la question précédente, on en déduit que $2P$ est d'ordre 2, donc P est d'ordre 4, d'où le résultat.

8) Le polynôme $X^2 - 2$ est irréductible dans $\mathbb{F}_5[X]$, d'où l'égalité annoncée. On a $\alpha^2 = 2$, d'où $(1 + \alpha)^3 = 5\alpha + 7 = 2$ i.e. on a $w = 2$.

9) Les points P et Q appartiennent à $E(\mathbb{F}_5)$. Par ailleurs, on a les égalités (question 8)

$$(1 + \alpha)^3 - (1 + \alpha) = 1 - \alpha = (2 + \alpha)^2,$$

ce qui prouve que R appartient à $E(\mathbb{F}_{25})$. Par ailleurs, on a $2^6 + 1 = 65 = 0$ et $3^6 + 1 = 730 = 0$. D'après la question 7, les points P et Q sont donc d'ordre 4. De plus, on a

$$(1 + \alpha)^6 + 1 = \big((1 + \alpha)^3\big)^2 + 1 = 2^2 + 1 = 0,$$

donc R est aussi d'ordre 4.

10) Il y a deux éléments d'ordre 4 dans $\mathbb{Z}/16\mathbb{Z}$. On en déduit qu'il y a exactement quatre d'éléments d'ordre 4 dans $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$. Ce sont en fait les éléments $(0, 4)$, $(0, 12)$, $(1, 4)$ et $(1, 12)$.

11) On déduit de la question 9, que $E(\mathbb{F}_{25})$ possède au moins six points d'ordre 4, à savoir $\pm P$, $\pm Q$ et $\pm R$. Ainsi, $E(\mathbb{F}_{25})$ n'est pas isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}$ (question 10).

12) Le groupe $E(\mathbb{F}_{25})$ est d'ordre 32 (question 6). Il n'est pas cyclique, car par exemple son sous-groupe $E(\mathbb{F}_5)$ ne l'est pas. Par suite, en tenant compte du fait que E a exactement trois points d'ordre 2, le groupe $E(\mathbb{F}_{25})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z}.$$

D'après la question précédente, on en déduit que $E(\mathbb{F}_{25})$ est isomorphe au groupe $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$.

13) Notons comme ci-dessus a et b les racines dans $\mathbb{C}$ du polynôme $F = X^2+2X+5 \in \mathbb{Z}[X]$. On a (Théorème 4.8)

$$\big|E(\mathbb{F}_{125})\big| = 5^3 + 1 - (a^3 + b^3).$$

Par ailleurs, on a les égalités

$$a^3 + b^3 = (a + b)^3 - 3ab(a + b) = -8 + 30 = 22.$$

On obtient $|E(\mathbb{F}_{125})| = 104$.

14) On a $104 = 8.13$. Le groupe des points de 2-torsion de E étant d'ordre 4, il en résulte que $E(\mathbb{F}_{125})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/104\mathbb{Z}.$$

Le groupe $E(\mathbb{F}_{125})$ contient $E(\mathbb{F}_5)$ qui n'est pas cyclique (question 4). Par suite, $E(\mathbb{F}_{125})$ n'est pas cyclique, donc $E(\mathbb{F}_{125})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/52\mathbb{Z}$.

Exercice 10

1) Le discriminant du polynôme $X^3 + X + 1 \in \mathbb{F}_5[X]$ est $-31 = -1$. Il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) On vérifie que l'on a

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

où $O = [0,1,0]$ est le point à l'infini.

3) On vérifie que l'on a

$$2.(0,1) = (4,2), \quad 2.(2,1) = (2,-1), \quad 2.(3,1) = (0,1), \quad 2.(4,2) = (3,-1).$$

Parce que l'opposé du point (a,b) est $(a,-b)$, on en déduit que l'on a

$$2.(0,-1) = (4,-2), \quad 2.(2,-1) = (2,1), \quad 2.(3,-1) = (0,-1), \quad 2.(4,-2) = (3,1).$$

4) D'après la question précédente, pour tout point $P \in E(\mathbb{F}_5)$, on a $2P = -P$ si et seulement si P est l'un des points O, $(2,1)$ et $(2,-1)$. Le sous-groupe des points de 3-torsion de $E(\mathbb{F}_5)$ est donc

$$\{O, (2,1), (2,-1)\}.$$

5) Le groupe $E(\mathbb{F}_5)$ est abélien d'ordre 9 (question 1). Il est donc isomorphe à l'un des groupes $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ et $\mathbb{Z}/9\mathbb{Z}$. Il possède exactement deux points d'ordre 3, par suite $E(\mathbb{F}_5)$ est isomorphe à $\mathbb{Z}/9\mathbb{Z}$.

6) Notons χ_E le polynôme caractéristique du Frobenius de E. L'ordre de $E(\mathbb{F}_5)$ étant 9, la trace du Frobenius de E est -3 (égalité (28) du chapitre IV du cours). On a ainsi

$$\chi_E = X^2 + 3X + 5 \in \mathbb{Z}[X].$$

7) Soient a et b les racines de χ_E dans $\mathbb{C}$. On a (Théorème 4.8)

$$\big|E(\mathbb{F}_{25})\big| = 5^2 + 1 - (a^2 + b^2).$$

On a $a+b=-3$ et $ab=5$ d'où $a^2+b^2=(a+b)^2-2ab=-1$. On en déduit que l'on a

$$\big|E(\mathbb{F}_{25})\big| = 27.$$

Par ailleurs, on a

$$\big|E(\mathbb{F}_{125})\big| = 5^3+1-(a^3+b^3).$$

On a $a^3+b^3=(a+b)^3-3ab(a+b)$. On obtient $a^3+b^3=18$, d'où

$$\big|E(\mathbb{F}_{125})\big| = 108.$$

Le polynôme f, qui est de degré 2, n'a pas de racines dans $\mathbb{F}_5$, il est donc irréductible sur $\mathbb{F}_5$.

8) On a $\alpha^2=\alpha-2$. Il en résulte que l'on a les égalités

$$(2\alpha+3)^2 = \alpha+1 = (\alpha+3)^3+(\alpha+3)+1,$$

d'où l'assertion.

9) On vérifie que l'on a $2Q=(\alpha+3,3\alpha+2)\in E(\mathbb{F}_{25})$.

Notons désormais $E[3]$ le groupe des points de 3-torsion de E.

10) D'après la question précédente, on a $2Q=-Q$, autrement dit, Q est un point de $E[3]$. D'après la question 4, le point P est aussi dans $E[3]$. Par ailleurs, Q n'appartient pas à $E(\mathbb{F}_5)$. On en déduit que (P,Q) est une famille libre du $\mathbb{F}_3$-espace vectoriel $E[3]$, d'où le résultat.

11) Le groupe $E(\mathbb{F}_{25})$ étant d'ordre 27 (question 7), il est donc isomorphe à l'un des groupes $\mathbb{Z}/27\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}$ et $(\mathbb{Z}/3\mathbb{Z})^3$. Ce dernier cas est impossible car $E[3]$ est d'ordre 9. Par ailleurs, le groupe $E[3]$ est isomorphe à $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$ (Théorème 4.2) et d'après la question 10, il est contenu dans $E(\mathbb{F}_{25})$. Il en résulte que $E(\mathbb{F}_{25})$ est isomorphe à

$$\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}.$$

12) Le polynôme $X^3+X+1\in\mathbb{F}_5[X]$ est de degré 3 et on vérifie qu'il n'a pas de racines dans $\mathbb{F}_5$, d'où l'assertion.

13) Les points de 2-torsion non nuls de E sont ceux de la forme $(u,0)$ où $u^3+u+1=0$. D'après la question précédente, $\mathbb{F}_{125}$ est donc le corps de rationalité des points de 2-torsion de E.

14) Le groupe $E(\mathbb{F}_{125})$ est d'ordre 108 (question 7) et on a $108=2^2.3^3$. Parce que $E[3]$ est d'ordre 9 et que $E(\mathbb{F}_{125})$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (question 13), on en déduit que $E(\mathbb{F}_{125})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/27\mathbb{Z} \quad\text{et}\quad \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/9\mathbb{Z}.$$

D'après la question 10, les points de 3-torsion de E sont rationnels sur $\mathbb{F}_{25}$, sans l'être tous sur $\mathbb{F}_5$. Ainsi $\mathbb{F}_{25}$ est le corps de rationalité de $E[3]$. Le corps $\mathbb{F}_{25}$ (qui est de degré 2 sur $\mathbb{F}_5$) n'est pas contenu dans $\mathbb{F}_{125}$ (qui est de degré 3 sur $\mathbb{F}_5$). Par suite, $E[3]$ n'est pas contenu dans $E(\mathbb{F}_{125})$ i.e. $E(\mathbb{F}_{125})$ ne contient pas de sous-groupes isomorphes à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. On en déduit que $E(\mathbb{F}_{125})$ est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/27\mathbb{Z}$, autrement dit que $E(\mathbb{F}_{125})$ est isomorphe à

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/54\mathbb{Z}.$$

Exercice 11

1) Le discriminant du polynôme $X^3 - 6X$ est $2^5 \times 3^3$. Il est non nul dans $\mathbb{F}_p$, donc E est une courbe elliptique sur $\mathbb{F}_p$.

2) On a l'égalité (proposition 4.3)

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 - 6x}{p} \right).$$

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

$$\left(\frac{(-x)^3 - 6(-x)}{p} \right) = -\left(\frac{x^3 - 6x}{p} \right),$$

ce qui entraîne l'assertion (voir l'exemple 4.15).

3) Notons $E[2]$ le sous-groupe des points de 2-torsion de E. Le point $(0, 0)$ est dans $E[2]$ et est rationnel sur $\mathbb{F}_p$. Par suite, $E[2]$ est contenu dans $E(\mathbb{F}_p)$ si et seulement si 6 est un carré dans $\mathbb{F}_p$, autrement dit si on a

$$\left(\frac{2}{p}\right) = -1 \quad \text{et} \quad \left(\frac{3}{p}\right) = -1 \qquad \text{ou bien} \qquad \left(\frac{2}{p}\right) = 1 \quad \text{et} \quad \left(\frac{3}{p}\right) = 1.$$

En utilisant la loi de réciprocité quadratique, on obtient

$$\left(\frac{2}{p}\right) = -1 \quad \text{et} \quad \left(\frac{3}{p}\right) = -1 \iff p \equiv 3 \text{ mod. } 8 \quad \text{et} \quad p \equiv 1 \text{ mod. } 3,$$

$$\left(\frac{2}{p}\right) = 1 \quad \text{et} \quad \left(\frac{3}{p}\right) = 1 \iff p \equiv 7 \text{ mod. } 8 \quad \text{et} \quad p \equiv 2 \text{ mod. } 3.$$

Il en résulte que l'on a

$$\left(\frac{2}{p}\right) = -1 \quad \text{et} \quad \left(\frac{3}{p}\right) = -1 \iff p \equiv 19 \text{ mod. } 24,$$

$$\left(\frac{2}{p}\right) = 1 \quad \text{et} \quad \left(\frac{3}{p}\right) = 1 \iff p \equiv 23 \text{ mod. } 24.$$

Cela établit l'équivalence annoncée.

4) Supposons $E(\mathbb{F}_p)$ cyclique. Tous les sous-groupes de $E(\mathbb{F}_p)$ sont alors cycliques, donc $E(\mathbb{F}_p)$ ne contient pas de sous-groupes isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ainsi, E n'a pas tous ses points d'ordre 2 rationnels sur $\mathbb{F}_p$. D'après la question précédente, p n'est donc pas congru à 19 ou 23 modulo 24. Par hypothèse on a $p \equiv 3$ mod. 4, donc p est congru à 7 ou 11 modulo 24.
Inversement, supposons p congru à 7 ou 11 modulo 24. D'après le théorème de structure du groupe abélien $E(\mathbb{F}_p)$ (théorème 4.5), il existe un unique couple d'entiers naturels (n_1, n_2) tel que $E(\mathbb{F}_p)$ soit isomorphe au groupe produit

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

D'après la question 2, n_1 divise $p+1$. Par suite, on a $n_1 \leq 2$. D'après l'hypothèse faite, E n'a pas tous ses points d'ordre 2 rationnels sur $\mathbb{F}_p$, donc $E(\mathbb{F}_p)$ ne contient pas de sous-groupes isomorphes à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Il en résulte que $n_1 = 1$, puis que $E(\mathbb{F}_p)$ est cyclique. (Cet argument est analogue à celui utilisé dans l'exemple 4.12.)

5) On utilise la formule (15) du théorème 4.1. Avec ses notations, on a

$$\lambda = \frac{3u^2 - 6}{2v}.$$

L'abscisse de $2Q$ est $\lambda^2 - 2u$. L'égalité $v^2 = u^3 - 6u$ entraîne alors le résultat.

6) Supposons qu'il existe $Q \in E(\mathbb{F}_p)$ tel que $2Q = P$. D'après la question précédente, l'abscisse de P est un carré dans $\mathbb{F}_p$. Par ailleurs, -2 n'est pas un carré dans $\mathbb{F}_p$ si p est congru à 7 modulo 24, d'où une contradiction et le résultat.

7) On a $p \geq 5$ donc $\ell \geq 3$. On a ainsi $p \equiv 7$ mod. 8 et $p \equiv 1$ mod. 3, d'où $p \equiv 7$ mod. 24.

8) D'après la question 4, $E(\mathbb{F}_p)$ est cyclique et d'après la question 6, P n'est pas un double dans $E(\mathbb{F}_p)$. L'indication de l'énoncé entraîne alors le résultat.

9) Parce que l'ordre de P est $p+1 = 2^\ell$, le point $2^{\ell-1}P$ est d'ordre 2. Compte tenu de la question 3, $(0,0)$ est le seul point d'ordre 2 de $E(\mathbb{F}_p)$, d'où $2^{\ell-1}P = (0,0)$.

Exercice 12 (Cryptosystème de Menezes-Vanstone)

1) Alice détermine le point

$$s(kP) = kA = (x, y).$$

Elle déchiffre alors le message $m = (m_1, m_2)$ en effectuant (xy est non nul)

$$x^{-1}(m_1 x) = m_1 \quad \text{et} \quad y^{-1}(m_2 y) = m_2.$$

2) Le discriminant de E est 4, il est non nul, donc E est une courbe elliptique sur $\mathbb{F}_{11}$.

3) Pour tout $z \in \mathbb{F}_{11}$, notons $\chi(z) = \left(\frac{z}{11}\right)$ le symbole de Legendre. On a l'égalité (Proposition 4.3)

$$|E(\mathbb{F}_{11})| = 12 + \sum_{x \in \mathbb{F}_{11}} \chi(x^3 + x + 6).$$

Pour tout $x \in \mathbb{F}_{11}$, on détermine $\chi(x^3 + x + 6)$. Pour cela, on vérifie d'abord que l'ensemble des carrés de $\mathbb{F}_{11}$ (qui est de cardinal 6) est $\Big\{0, 1, 3, 4, 5, 9\Big\}$. Il en résulte que l'ensemble des couples $\big(x, \chi(x^3 + x + 6)\big)$ pour x parcourant $\mathbb{F}_{11}$ est

$$\Big\{(0,-1), (1,-1), (2,1), (3,1), (4,-1), (5,1), (6,-1), (7,1), (8,1), (9,-1), (10,1)\Big\},$$

d'où $|E(\mathbb{F}_{11})| = 13$. On peut vérifier par ailleurs que l'on a

$$E(\mathbb{F}_{11}) = \Big\{O, (2, \pm 4), (3, \pm 5), (5, \pm 2), (7, \pm 2), (8, \pm 3), (10, \pm 2)\Big\}.$$

4) Il s'agit de calculer le point $A = 7P$. On vérifie que l'on a

$$2P = (5, 2), \quad 4P = (10, 2), \quad 6P = (7, 9),$$

d'où $A = (7, 2)$.

5) Conformément au cryptosystème utilisé, Bob calcule les points

$$6P \quad \text{et} \quad 6A = (x, y).$$

On a $6A = 42P = 3P$ (car $13P = O$), d'où $6A = (8, 3)$, puis $x = 8$ et $y = 3$. Bob explicite le couple

$$(9x, y) = (6, 3) \in \mathbb{F}_{11} \times \mathbb{F}_{11},$$

et il envoie à Alice le point $6P$ et le couple $(6, 3)$.

6) Alice retrouve le message m en procédant comme suit. Avec sa clé secrète, elle calcule le point $7(6P) = 6A$, ce qui lui permet de déterminer (x, y). Elle en déduit le message m, vu que l'on a $8^{-1} = 7$ et que $(8^{-1}6, 3^{-1}3) = (9, 1)$.