Sorbonne Université
Cryptologie, cryptographie algébrique
4M035 - 2021/22 - Enseignement à distance
Alain Kraus

Correction du second devoir

1) Avec les notations de la définition 4.1, on a $a = b = 1$. On a $4a^3 + 27b^2 = 31$, qui n'est pas nul, donc E est une courbe elliptique définie sur $\mathbb{F}_7$.
2) En notant O le point à l'infini, on vérifie que l'on a
$$E(\mathbb{F}_7) = \Big\{O, (0,1), (0,6), (2,2), (2,5)\Big\}.$$
3) Soit f le polynôme caractéristique de l'endomorphisme de Frobenius de E (voir le paragraphe 3 page 26). L'ordre de $E(\mathbb{F}_7)$ vaut 5, donc la trace du Frobenius de E vaut 3 et on a
$$f = X^2 - 3X + 7.$$
Notons désormais α et β les racines complexes de f.
4) Soit $|E(\mathbb{F}_{7^2})|$ l'ordre cherché. D'après le théorème 4.8, on a
$$|E(\mathbb{F}_{7^2})| = 7^2 + 1 - (\alpha^2 + \beta^2).$$
On a les égalités
$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 3^2 - 14 = -5,$$
d'où $|E(\mathbb{F}_{7^2})| = 55$.
5) On a $55 = 5.11$. D'après la question précédente et le théorème de structure des groupes abéliens finis, $E(\mathbb{F}_{49})$ est donc isomorphe à $\mathbb{Z}/55\mathbb{Z}$.
6) On a
$$|E(\mathbb{F}_{7^3})| = 7^3 + 1 - (\alpha^3 + \beta^3).$$
On a les égalités
$$\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta) = -36,$$
d'où $|E(\mathbb{F}_{7^3})| = 380$.
7) Le polynôme considéré est de degré 3 et n'a pas de racines dans $\mathbb{F}_7$. Il est donc irréductible dans $\mathbb{F}_7[X]$.
8) On a
$$E[2] = \{O, (u,0), (v,0), (w,0)\},$$

où u, v, w sont les racines du polynôme $X^3 + X + 1$ dans une clôture algébrique de $\mathbb{F}_7$ (lemme 4.5). Parce que $X^3 + X + 1$ est irréductible sur $\mathbb{F}_7$, on a $\{v, w\} = \{u^7, u^{49}\}$. L'élément u est dans $\mathbb{F}_{7^3}$, il en est donc de même de v et w (on peut aussi évoquer le fait que l'extension $\mathbb{F}_{7^3}/\mathbb{F}_7$ est galoisienne), d'où le résultat.

9) On a $380 = 2^2.5.19$. On en déduit que $E(\mathbb{F}_{7^3})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/380\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/190\mathbb{Z}.$$

Le groupe $E[2]$ étant contenu dans $E(\mathbb{F}_{7^3})$, il en résulte que $E(\mathbb{F}_{7^3})$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par suite, $E(\mathbb{F}_{7^3})$ est isomorphe à

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/190\mathbb{Z}.$$

10) Posons $P_1 = (u, 0)$ et $P_2 = (u^7, 0)$. Alors, (P_1, P_2) est une base de $E[2]$ sur $\mathbb{F}_2$ car $P_1 \neq P_2$. Soit $\phi_7 : E[2] \to E[2]$ l'endomorphisme de Frobenius de E restreint à $E[2]$. On a $\phi_7(P_1) = P_2$ et $\phi_7(P_2) = (u^{49}, 0)$ (formule (27) du cours). Parce que u^{49} est distinct de u et u^7, on en déduit que $\phi_7(P_2) = P_1 + P_2$. La matrice de ϕ_7 dans la base (P_1, P_2) est donc $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$.

11) D'après le lemme 4.6 on a

$$G = 3X^4 + 6X^2 + 5X - 1 \in \mathbb{F}_7[X].$$

12) On a dans $\mathbb{F}_7[X]$ l'égalité

$$5G = X^4 + 2X^2 + 4X + 2.$$

En écrivant que l'on a $5G = (X^2 + aX + b)(X^2 + cX + d)$ avec $a, b, c, d \in \mathbb{F}_7$, on obtient

$$a + c = 0, \quad ac + b + d = 2, \quad ad + bc = 4, \quad bd = 2.$$

On a donc $b + d = 2 + a^2$. On a $a \neq 0$, sinon $c = 0$ ce qui contredit l'égalité $ad + bc = 4$. On en déduit que l'on a $b + d \in \{3, 4, 6\}$. On a $b \neq d$, sinon, $b(a + c) = 4$ or $a + c = 0$. Il en résulte que b et d sont racines de l'un des polynômes $X^2 - 3X + 2$ et $X^2 - 4X + 2$ (on a $b + d \neq 6$ car $X^2 - 6X + 2 = (X + 4)^2$ auquel cas $b = d$). Dans le premier cas, on a $\{b, d\} = \{1, 2\}$ et dans le second, on a $\{b, d\} = \{-1, -2\}$.
Supposons $\{b, d\} = \{1, 2\}$. On a $a + c = 0$ et $ad + bc = 4$ d'où $ac = -2$. Par ailleurs, on a $ac + b + d = 2$, ce qui conduit à une contradiction.
Par suite, on a $\{b, d\} = \{-1, -2\}$. Ainsi, $a^2 = 2$, d'où $a = \pm 3$. Quitte à échanger a et c on peut supposer que $a = 3$ et $c = -3$. Avec l'égalité $ad + bc = 4$, on en déduit alors que $b = -1$ et $d = -2$, d'où

$$5G = (X^2 + 3X - 1)(X^2 - 3X - 2),$$

qui est la décomposition cherchée.

13) D'après la question précédente, les abscisses des points non nuls de $E[3]$ appartiennent à $\mathbb{F}_{7^2}$ et ne sont pas dans $\mathbb{F}_7$. Par ailleurs, on a $|E(\mathbb{F}_{7^2})| = 55$, donc E n'a pas de points d'ordre 3 rationnels sur $\mathbb{F}_{7^2}$. Si (x, y) est un point non nul de $E[3]$, on a $y^2 = x^3+x+1$. Il en résulte que les ordonnées des points de $E[3]$ appartiennent à $\mathbb{F}_{7^4}$. On a donc $n = 4$.

14) On a

$$|E(\mathbb{F}_{7^4})| = 7^4 + 1 - (\alpha^4 + \beta^4).$$

On écrit que l'on a $\alpha^4 + \beta^4 = (\alpha^2 + \beta^2)^2 - 2(\alpha\beta)^2$, d'où

$$\alpha^4 + \beta^4 = 25 - 98 = -73,$$

puis $|E(\mathbb{F}_{7^4})| = 2475$.

15) On a $2475 = 3^2.5^2.11$. Le groupe $E[3]$ est contenu dans $E(\mathbb{F}_{7^4})$ (question 13). On en déduit que $E(\mathbb{F}_{7^4})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/825\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/165\mathbb{Z}.$$

Soit $E[5]$ le groupe des points de 5-torsion de E. D'après le fait admis, il existe un point $P = (x_0, y_0) \in E[5]$ tel que x_0 appartienne à $\mathbb{F}_{7^2}$ et que x_0 ne soit pas dans $\mathbb{F}_7$. Le point P est donc rationnel sur $\mathbb{F}_{7^4}$ (en fait P n'est pas rationnel sur $\mathbb{F}_{7^2}$ car $|E(\mathbb{F}_7)| = 5$ et $|E(\mathbb{F}_{7^2})| = 55$, mais peu importe ici). Le point P n'appartenant pas à $E(\mathbb{F}_7)$, le couple $\big((0, 1), P\big)$ est une base de $E[5]$ sur $\mathbb{Z}/5\mathbb{Z}$ (question 1). Par suite $E[5]$, qui est isomorphe à $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, est contenu dans $E(\mathbb{F}_{7^4})$. Il en résulte que $E(\mathbb{F}_{7^4})$ est isomorphe à

$$\mathbb{Z}/15\mathbb{Z} \times \mathbb{Z}/165\mathbb{Z}.$$