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

Correction de l'examen du 16 juin 2022

Exercice 1

1) On calcule les premiers termes de la suite $(x_i)_{i\in\mathbb{N}}$ définie par $x_0 = 3$ et l'égalité $x_{i+1} = f(x_i)$ mod. 481. On a

$$x_0 = 3, \quad x_1 = 10, \quad x_2 = 101.$$

On a $\mathrm{pgcd}(x_2 - x_1, 481) = 13$, d'où l'égalité $481 = 13 \times 37$.

2) Compte tenu de la question précédente, on est amené à résoudre le système de congruence

$$\begin{cases} x \equiv 1 \text{ mod. } 13 \\ x \equiv -1 \text{ mod. } 37. \end{cases}$$

On vérifie avec l'algorithme d'Euclide étendu que l'on a

$$-17 \times 13 + 6 \times 37 = 1.$$

D'après la démonstration du théorème chinois, on en déduit que 443 est une solution particulière de ce système. L'ensemble cherché est donc $\{\pm 1, \pm 443\}$, autrement dit

$$\{1, 38, 443, 480\}.$$

Exercice 2

1) Le polynôme f est irréductible dans $\mathbb{F}_2[X]$ car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_2$. Par suite, K est un corps de cardinal 8.

2) La groupe K^* est cyclique d'ordre 7, donc α est un générateur de K^*.

3.1) La clé secrète d'Alice est le plus petit entier $a \geq 1$ tel que $\alpha^a = \alpha^2 + 1$. On a $\alpha^2 + 1 = (\alpha + 1)^2$. L'égalité $\alpha^3 = \alpha + 1$ entraîne alors $a = 6$.

3.2) Soit m le message décrypté. On a

$$m = (\alpha^2)^{-6}\alpha.$$

Par ailleurs, on a $\alpha^7 = 1$, d'où $(\alpha^2)^6 = \alpha^{12} = \alpha^5$, puis $(\alpha^2)^{-6} = \alpha^{-5} = \alpha^2$. On a donc

$$m = \alpha^3.$$

Exercice 3

1) Par hypothèse, E est supersingulière, on a donc $|E(\mathbb{F}_p)| = p+1$ (Corollaire 4.3).
2) Il existe des entiers n_1 et n_2 tels que $E(\mathbb{F}_p)$ soit isomorphe à $\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ avec $n_1 \mid n_2$ et $n_1 \mid p-1$ (Théorème 4.5). Vu que n_1 divise $p+1$ et $p-1$, on donc $n_1 \leq 2$. Si $n_1 = 2$, alors $E(\mathbb{F}_p)$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, en particulier 4 divise $p+1$, d'où $p \equiv 3$ mod. 4, ce qui contredit l'hypothèse faite. Par suite, on a $n_1 = 1$, ce qui montre que $E(\mathbb{F}_p)$ est cyclique.

Exercice 4

1) On vérifie directement que l'on a

$$E(\mathbb{F}_7) = \{O, (2,1), (2,6), (3,1), (3,6), (6,0)\},$$

où $O = [0,1,0]$ est le point à l'infini. En particulier, $E(\mathbb{F}_7)$ est cyclique d'orde 6.

2) Le point d'ordre 2 de $E(\mathbb{F}_7)$ est $(6,0)$.
3) Posons $G = 3X^4 + 12X^2 + 36X - 4 \in \mathbb{F}_7[X]$. On a $G(3) = 0$. D'après le lemme 4.6, le point P est donc d'orde 3. On peut aussi vérifier que $2P = (3,-1)$, d'où $2P = -P$, puis $3P = O$.
4) Les points P et $-P$ sont d'ordre 3 et $(6,0)$ est d'ordre 2. Le groupe $E(\mathbb{F}_7)$, qui est cyclique d'ordre 6, possède deux générateurs. Il en résulte que $(2,1)$ et $(2,6)$ sont les deux générateurs de $E(\mathbb{F}_7)$.
5) D'après la première question, la trace du Frobenius de E vaut 2 et donc que le polynôme caractéristique du Frobenius de E est (page 27 du chapitre IV)

$$f = X^2 - 2X + 7 \in \mathbb{Z}[X].$$

6) Soient α et β les racines complexes de f. On a (Théorème 4.8)

$$|E(\mathbb{F}_{49})| = 49 + 1 - (\alpha^2 + \beta^2).$$

On a $\alpha^2 + \beta^2 = (\alpha+\beta)^2 - 2\alpha\beta$ et $\alpha + \beta = 2$, $\alpha\beta = 7$, d'où $\alpha^2 + \beta^2 = -10$. On a donc

$$|E(\mathbb{F}_{49})| = 60.$$

7) Soit $E[2]$ le groupe des points de 2-torsion de E. On a $E[2] = \{O, (u,0), (v,0), (w,0)\}$ où u, v, w sont les racines dans une clôture algébrique de $\mathbb{F}_7$ du polynôme $X^3 + 2X + 3$ (Lemme 4.5). Le corps $\mathbb{F}_7(E[2])$ des points de 2-torsion de E est $\mathbb{F}_7(u,v,w)$ (Lemme 4.7). D'après la première question, le polynôme $X^3 + 2X + 3$ a une unique racine dans $\mathbb{F}_7$. Il en résulte que ses deux autres racines sont rationnelles sur $\mathbb{F}_{49}$. On a donc $\mathbb{F}_7(E[2]) = \mathbb{F}_{49}$.

8) On a $60 = 4 \times 15$. On a $|E(\mathbb{F}_{49})| = 60$, donc $E(\mathbb{F}_{49})$ est isomorphe à $\mathbb{Z}/60\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$. D'après la question précédente, $E(\mathbb{F}_{49})$ contient $E[2]$, donc $E(\mathbb{F}_{49})$ contient un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. On en déduit que $E(\mathbb{F}_{49})$ est isomorphe à

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

9) Supposons R non nul et posons $R = (x, y)$. Par définition, on a $\phi_7(R) = (x^7, y^7)$. On a donc $\Phi_7^n(R) = \left(x^{7^n}, y^{7^n}\right)$. Par ailleurs, x appartient à $\mathbb{F}_{7^n}$ si et seulement si on a l'égalité $x^{7^n} = x$ et il en est de même pour y. Ainsi R appartient à $E(\mathbb{F}_{7^n})$ si et seulement si $x^{7^n} = x$ et $y^{7^n} = y$ i.e. si on a $\phi_7^n(R) = R$.

10) On a $\phi_7(P) = P$ car P est dans $E(\mathbb{F}_7)$. Il existe a et b dans $\mathbb{Z}/3\mathbb{Z}$ tels que l'on ait $\Phi_7(Q) = aP + bQ$. On a donc

$$M = \begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}.$$

D'après le théorème 4.7, on a $\det(M) = 7 + 3\mathbb{Z}$ i.e. $\det(M) = 1 + 3\mathbb{Z}$. On a donc $b = 1$, d'où l'assertion.

11) On a $3a = 0$. Par suite, M^3 est la matrice identité.

12) La matrice de ϕ_7^3 dans la base (P, Q) est M^3. On a donc $\phi_7^3(P) = P$ et $\phi_7^3(Q) = Q$. D'après les questions 9 et 10, on en déduit que P et Q appartiennent à $E(\mathbb{F}_{7^3})$. Par suite, $\mathbb{F}_7(E[3])$ est contenu dans $\mathbb{F}_{7^3}$. D'après la question 1, Q n'est pas rationnel sur $\mathbb{F}_7$, car les seuls points d'ordre 3 de $E(\mathbb{F}_7)$ sont $\pm P$. Il en résulte que M est d'ordre 3, et donc que l'on a $\mathbb{F}_7(E[3]) = \mathbb{F}_{7^3}$.

13) Avec les notations déjà utilisées, on a

$$|E(\mathbb{F}_{7^3})| = 7^3 + 1 - (\alpha^3 + \beta^3).$$

On a $\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)$. On obtient $\alpha^3 + \beta^3 = -34$, d'où

$$|E(\mathbb{F}_{7^3})| = 378.$$

14) On a $378 = 3^3 \times 14$. On en déduit que $E(\mathbb{F}_{7^3})$ est isomorphe à $\mathbb{Z}/378\mathbb{Z}$ ou bien à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}$. D'après la question 12, $E(\mathbb{F}_{7^3})$ contient un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, donc $E(\mathbb{F}_{7^3})$ est isomorphe à

$$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}.$$