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

Correction de l'examen du 12 mai 2022

Exercice 1

1.1) On vérifie que n est divisible par 17, d'où $n = 17 \times 89$. L'entier 89 est premier car il n'est pas divisible par un nombre premier plus petit que 10.

1.2) On a $\varphi(n) = 16 \times 88 = 1408$. Il s'agit alors de déterminer l'inverse de 37 modulo 1408. En utilisant l'algorithme d'Euclide, on obtient le tableau suivant.

	38	18	2	
1408	37	2	1	0
1	0	1	-18	
0	1	-38	685	

Il en résulte que l'on a

$$685 \times 37 - 18 \times 1408 = 1.$$

Par suite, l'inverse de 37 modulo 1408 est 685. Ainsi, la clé secrète est $(685, 1408)$.

2) On a $n = pq$ et $p + q = n - \varphi(n) + 1$ (cf. la démonstration du lemme 1.1). Par suite, p et q sont racines du polynôme $X^2 - 176X + 7663$. On obtient

$$p = 79 \quad \text{et} \quad q = 97.$$

3.1) On a $57 = 3 \times 19$. D'après le lemme 2.3 du cours, on a donc $|S| = 3$.

3.2) Il s'agit de déterminer l'ensemble des entiers a tels que l'on ait

$$1 < a < 57, \quad a^{56} \equiv 1 \text{ mod. } 3 \quad \text{et} \quad a^{56} \equiv 1 \text{ mod. } 19.$$

L'équation $x^{56} = 1$ possède deux solutions dans $\mathbb{F}_3$, à savoir 1 et -1. Par ailleurs, pour tout $x \in \mathbb{F}_{19}^*$, on a $x^{18} = 1$. Pour tout $x \in \mathbb{F}_{19}^*$, on a donc $x^{56} = 1$ si et seulement si $x^2 = 1$ i.e. $x = \pm 1$. Une solution particulière du système de congruences

$$\begin{cases} x \equiv -1 \text{ mod. } 3 \\ x \equiv 1 \text{ mod. } 19 \end{cases}$$

est $x = 20$. En tenant compte de la solution opposée, on en déduit que l'on a

$$S = \{20, 37, 56\}.$$

4) On a l'égalité du symbole de Jacobi $\left(\frac{7}{25}\right) = 1$. Par ailleurs, on a $7^2 = 49 \equiv -1$ mod. 25 d'où $7^{12} \equiv 1$ mod. 25 et le résultat (Définition 2.4).

Exercice 2

1) Le discriminant du polynôme $X^3 + 3X + 2 \in \mathbb{F}_5[X]$ est $-216 = -1$. Il est non nul, donc E est une courbe elliptique définie sur $\mathbb{F}_5$.

2) On vérifie que l'on a

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

où $O = [0,1,0]$ est le point à l'infini. Par suite, $E(\mathbb{F}_5)$ est cyclique d'ordre 5.

3) On en déduit que la trace du Frobenius de E vaut 1 et donc que le polynôme caractéristique du Frobenius de E est (voir page 27 du chapitre IV)

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

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

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

On a $\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta$ et $\alpha + \beta = 1$, $\alpha\beta = 5$. On obtient

$$|E(\mathbb{F}_{25})| = 35.$$

5) Parce que l'ordre de $E(\mathbb{F}_{25})$ est sans facteurs carrés, on en déduit que $E(\mathbb{F}_{25})$ est isomorphe à $\mathbb{Z}/35\mathbb{Z}$.

6) Avec les notations précédentes, on a

$$|E(\mathbb{F}_{125})| = 125 + 1 - (\alpha^3 + \beta^3).$$

On a $\alpha^3 + \beta^3 = (\alpha + \beta)^3 - 3\alpha\beta(\alpha + \beta)$. On obtient $\alpha^3 + \beta^3 = -14$, d'où

$$|E(\mathbb{F}_{125})| = 140.$$

7) Le groupe des points de 2-torsion de E est $\{O, (u,0), (v,0), (w,0)\}$ où u, v, w sont les racines dans $\overline{\mathbb{F}_5}$ (une clôture algébrique de $\mathbb{F}_5$) du polynôme $X^3 + 3X + 2 \in \mathbb{F}_5[X]$ (Lemme 4.5). Le corps $\mathbb{F}_5(E[2])$ des points de 2-torsion de E est $\mathbb{F}_5(u, v, w)$ (Lemme 4.7). Le polynôme $X^3 + 3X + 2$ est irréductible sur $\mathbb{F}_5$ car il est de degré 3 et n'a pas de racines dans $\mathbb{F}_5$. On a $v = u^5$ et $w = u^{25}$. Par suite, on a $\mathbb{F}_5(E[2]) = \mathbb{F}_{125}$.

8) On a $140 = 4 \times 35$. Il en résulte que $E(\mathbb{F}_{125})$ est isomorphe à l'un des groupes

$$\mathbb{Z}/140\mathbb{Z} \quad \text{et} \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/70\mathbb{Z}.$$

D'après la question précédente, $E(\mathbb{F}_{125})$ contient le sous-groupe des points de 2-torsion de E, qui est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Par suite, $E(\mathbb{F}_{125})$ est isomorphe au groupe produit $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/70\mathbb{Z}$.

Exercice 3

1) D'après la proposition 4.3, on a, avec ses notations,

$$|E(\mathbb{F}_5)| = 6 + \sum_{x \in \mathbb{F}_5} \chi(x^3 - x).$$

On en déduit directement que l'on a $|E(\mathbb{F}_5)| = 8$.

2) Soit t la trace du Frobenius de E. D'après la question précédente, on a $8 = 6 - t$, d'où $t = -2$. On a $t \neq 0$, donc E est ordinaire (Définition 4.6 et Corollaire 4.3). Le groupe $E[5]$ est donc d'ordre 5 (voir la page 30 du chapitre IV).

3) D'après la question 2 de l'exercice 4, l'entier r est l'ordre de t modulo 5. On a $t = -2$, d'où $r = 4$.

4.1) Le groupe $E[5]$ est cyclique d'ordre 5. Le point P étant non nul, c'est donc un générateur de $E[5]$. Par ailleurs, on a $5\phi_5(P) = \phi_5(5P) = O$, donc $\phi_5(P)$ est dans $E[5]$. Ainsi, il existe un entier k tel que l'on ait $\phi_5(P) = kP$.

4.2) On a l'égalité $\phi_5^2(P) - t\phi_5(P) + 5P = 0$ (Théorème 4.6) et $5P = O$. On en déduit que l'on a $\phi_5^2(P) + 2\phi_5(P) = O$. On obtient $\phi_5(\phi_5(P) + 2P) = O$. Parce que ϕ_5 est un morphisme de groupes injectif, on a donc

$$\phi_5(P) = 3P.$$

Par ailleurs, $\phi_5(P)$ est distinct de P et $2P$, sinon on aurait $3P = P$ i.e. $2P = O$ ou bien $3P = 2P$ i.e. $P = O$, ce qui n'est pas car P est d'ordre 5. On a ainsi $n = 3$. (On peut aussi évoquer directement le fait que P est un générateur de $E[5]$.)

Exercice 4

1) L'intervalle de Hasse pour le nombre premier 23 est $[24 - 2\sqrt{23}, 24 + 2\sqrt{23}]$. D'après le théorème de Hasse, l'ordre de $E(\mathbb{F}_{23})$ appartient donc à cet intervalle, autrement dit à $[15, 33]$ (Théorème 4.4).

2) Notons n l'ordre de $E(\mathbb{F}_{23})$. D'après la question précédente n appartient à $[15, 33]$. Les diviseurs premiers de l'exposant d'un groupe fini sont les mêmes que ceux de son ordre. D'après l'hypothèse faite, n est donc une puissance de 2. Il en résulte que l'on a $n = 16$ ou $n = 32$.

3) Rappelons que le sous-groupe des points de 2-torsion de $E(\mathbb{F}_{23})$ est d'ordre au plus 4. Si $n = 16$, le groupe $E(\mathbb{F}_{23})$ est donc isomorphe à

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

Seul le groupe $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ est d'exposant 8. Par ailleurs, si $n = 32$, $E(\mathbb{F}_{23})$ est isomorphe à

$$\mathbb{Z}/32\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/16\mathbb{Z} \quad \text{ou} \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Seul $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ est d'exposant 8. Dans ce cas, le groupe des points de 4-torsion de E, qui est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, est alors contenu dans $E(\mathbb{F}_{23})$. D'après le théorème 4.3, le groupe des racines 4-ièmes de l'unité dans une clôture algébrique de $\mathbb{F}_{23}$ est donc contenu dans $\mathbb{F}_{23}^*$, ce qui n'est pas car $23 \not\equiv 1 \bmod 4$. Par suite, $E(\mathbb{F}_{23})$ est d'ordre 16 isomorphe à

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$
