Examen—Courbes Elliptiques—Corrigé

mardi 28 janvier 2014, 9h – 12h

Documents de cours autorisés

Exercice 1 Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$.

(1) Donner une estimation de $|E(\mathbb{F}_q)|$ en fonction de q.
(2) Donner la structure générale du groupe $E(\mathbb{F}_q)$.
(3) Montrer que si $q-1$ est premier et $q \geq 5$, alors $E(\mathbb{F}_q)$ est un groupe cyclique.
(4) Donner un exemple d'un corps fini $\mathbb{F}_q$ et d'une une courbe elliptique cyclique sur $\mathbb{F}_q$ de taille au moins 100. Justifier que la courbe est bien elliptique et cyclique, et de la bonne taille !
[Indication : Si $q-1$ est premier et au moins 4, alors q est pair.]
(5) Que peut-on dire si $\frac{q-1}{p-1}$ est premier, avec $q-3 \geq 3(p-1)^2$, où $p = \mathrm{car}(\mathbb{F}_q)$?

Solution.

(1) On a $|E(\mathbb{F}_q)| = q+1-t$ avec $|t| \leq 2\sqrt{q}$.
(2) On a $E(\mathbb{F}_q) = \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ avec $d_1 \mid d_2$ et $d_1 \mid q-1$.
(3) $E(\mathbb{F}_q)$ est cyclique si et seulement si $d_1 = 1$. Or, si $q-1$ est premier, alors soit $d_1 = 1$, soit $d_1 = q-1$. Dans le deuxième cas on aurait aussi $d_2 \geq d_1 = q-1$. Comme $q \geq 5$ on aurait alors
$$E(\mathbb{F}_q) = d_1 d_2 \geq (q-1)^2 = q(q-2)+1 \geq q+2q+1 > q+1+2\sqrt{q},$$
une contradiction. Donc $d_1 = 1$ et $E(\mathbb{F}_q)$ est cyclique.
(4) Comme q est une puissance de la caractéristique, qui est paire, on essaie $q = 2^7 = 128$. Alors $q-1 = 127$ est premier, et toute courbe elliptique sur $\mathbb{F}_{2^7}$ est cyclique. On pourrait prendre $E : y^2 + xy = x^3 + 1$, avec $\Delta(E) = a_6 = 1 \neq 0$, une courbe lisse et donc elliptique. On a
$$|E(\mathbb{F}_q)| \geq q+1-2\sqrt{q} = 2^7+1-2\sqrt{2^7} > 129 - 2\cdot 13 > 100.$$
(5) Si $\frac{q-1}{p-1}$ est premier et $q-3 \geq 3(p-1)^2$, alors soit $d_1 \leq p-1$ soit $d_2 \geq d_1 \geq \frac{q-1}{p-1}$, et
$$E(\mathbb{F}_q) = d_1 d_2 \geq \left(\frac{q-1}{p-1}\right)^2 = \frac{(q+1)(q-3)+4}{(p-1)^2} > 3(q+1) > q+1+2\sqrt{q},$$
ce qui donne aussi une contradiction. Donc $E(\mathbb{F}_q)$ a un sous-groupe cyclique d'indice au plus $p-1$.

Exercice 2

(1) On considère la courbe $E : y^2 = x^3 + 2x$ sur le corps fini $\mathbb{F}_{13}$. Calculer son discriminant Δ et son j-invariant. En déduire que E est une courbe elliptique.
(2) Énumérer les points de $E(\mathbb{F}_{13})$. Donner la structure de $E(\mathbb{F}_{13})$.
(3) Donner les points de $E(\mathbb{F}_{13})$ d'ordre 2.
(4) Soit $P = (1,4)$. Calculer $2P$ et $4P$, et donner un point d'ordre 5.
(5) On considère $\mathbb{F}_{13^2} = \mathbb{F}_{13}(\theta)$ avec $\theta^2 = -2$. Quels sont les points d'ordre 2 de $E(\mathbb{F}_{13^2})$? Le groupe $E(\mathbb{F}_{13^2})$, est-il cyclique ?
(6) Calculer $|E(\mathbb{F}_{13^2})|$.

Solution.

(1) D'après les formules du cours, on a
$$\Delta(E) = -16(4a_4^3 + 27a_6^2) = -3(4\cdot 2^3 + 0) = -3\cdot 6 = -18 = -5 = 8 \mod 13$$
$$j(E) = (-48a_4)^3/\Delta = (4\cdot 2)^3/8 = 8^2 = (-5)^2 = 25 = 1 \mod 13.$$
Ainsi $\Delta(E) \neq 0$, la courbe est lisse, et E est une courbe elliptique.

(2) On a

x	x^2	x^3	x^3+2x
0	0	0	0
± 1	1	± 1	± 3
± 2	4	∓ 5	∓ 1
± 3	-4	± 1	∓ 6
± 4	3	∓ 1	∓ 6
± 5	-1	∓ 5	± 5
± 6	-3	∓ 5	∓ 6

Ainsi

$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (0,0), (1,4), (1,-4), (-1,6), (-1,-6), (2,5), (2,-5), (-2,1), (-2,-1)\}.$$

Donc $|E(\mathbb{F}_{13})| = 10$; comme 10 n'a pas de facteur carré, $E(\mathbb{F}_{13}) \cong \mathbb{Z}/10\mathbb{Z}$ est cyclique.

(3) Les points d'ordre 2 sont ceux de deuxième coordonnée 0. Il n'y a qu'un seul, $(0,0)$.

(4) Si $Q = (x,y)$, alors $2Q = (x', y')$ avec

$$x' = \lambda^2 - 2x, \quad y' = \lambda(x - x') - y \quad \text{et} \quad \lambda = \frac{3x^2 + a_4}{2y}.$$

Ainsi

$$\lambda_1 = \frac{3 \cdot 1^2 + 2}{2 \cdot 4} = \frac{5}{8} = -1, \quad x_1 = (-1)^2 - 2 \cdot 1 = -1 \quad \text{et} \quad y_1 = (-1)(1 - (-1)) - 4 = -6$$

et $2P = (-1,-6)$. Ensuite,

$$\lambda_2 = \frac{3 \cdot (-1)^2 + 2}{2 \cdot (-6)} = \frac{5}{1} = 5, \quad x_2 = 5^2 - 2 \cdot (-1) = 1 \quad \text{et} \quad y_2 = 5(-1-1) - (-6) = -4$$

et $4P = (1,-4) = -P$. Donc $5P = \mathcal{O}$ et l'ordre de P est 5.

(5) Les points d'ordre deux sont ceux de la forme $(x,0)$ avec $0 = x^3 + 2x = x(x^2+2)$. Les trois points d'ordre deux sont donc $(0,0)$, $(\theta, 0)$ et $(-\theta, 0)$, où $\theta^2 = -2$. Ils sont tous les trois dans $E(\mathbb{F}_{13}(\theta)) = E(\mathbb{F}_{13^2})$. Donc $E(\mathbb{F}_{13^2})[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $E(\mathbb{F}_{13^2})$ n'est pas cyclique.

(6) La trace de l'endomorphisme de Frobenius de E sur $\mathbb{F}_{13}$ est

$$t = q + 1 - |E(\mathbb{F}_q)| = 14 - 10 = 4.$$

Le polynôme caractéristique du Frobenius est

$$\chi_E(T) = T^2 - tT + q = T^2 - 4T + 13.$$

Ses deux zéros sont

$$\tau_{1/2} = 2 \pm \sqrt{2^2 - 13} = 2 \pm 3i.$$

Alors

$$[E(\mathbb{F}_{13^2})| = 13^2 + 1 - \tau_1^2 - \tau_2^2 = 170 - 2(2^2 - 3^3) = 180.$$

Exercice 3 Soit E une courbe elliptique sur un corps fini k et n un entier tel que $\mathrm{car}(k)$ ne divise pas n. Soit μ_n le groupe multiplicatif des racines n-mes d'unité, et $e_n : E[n] \times E[n] \to \mu_n$ le couplage de Weil. Montrer que si $S, T \in E[n]$ alors l'ordre $o(e_n(S,T))$ divise $\mathrm{pgcd}(o(S), o(T))$. Est-ce qu'on a toujours égalité ?

Solution. Soit $o(S) = s$ et $o(T) = t$. Par bilinearité,

$$e_n(S,T)^s = e_n(sS,T) = e_n(\mathcal{O},T) = 1 \quad \text{et} \quad e_n(S,T)^t = e_n(S,tT) = e_n(S,\mathcal{O}) = 1.$$

Donc $o(e_n(S,T))$ divise $o(S)$ et $o(T)$, et aussi $\mathrm{pgcd}(o(S), o(T))$.

Enfin, si $\mathcal{O} \neq T \in E[n]$, alors $1 = e_n(T,T)$, et $o(e_n(T,T)) \neq 1$. On n'a pas toujours égalité.