Examen Partiel - Courbes Elliptiques

mardi 18 décembre 2012, 9h – 11h

Documents de cours autorisés

Toutes les réponses devront être soigneusement justifiées

Corrigé

Exercice 1.

(1) Montrer que le polynôme $P(X) = X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_5[X]$. En déduire que $\mathbb{F}_{125} = \mathbb{F}_5(\theta)$ où $\theta^3 + \theta^2 + 1 = 0$.
(2) Calculer θ^{-1} en fonction de θ.
(3) Calculer θ^{30}, puis θ^{31}. En déduire que θ et $-\theta$ sont des carrés dans $\mathbb{F}_{125}$.

On considère la courbe E définie sur $\mathbb{F}_{125}$ d'équation

$$y^2 = x^3 + \theta x.$$

(4) Calculer le discriminant et le j-invariant de E. En déduire que E est une courbe elliptique.
(5) Montrer qu'il existent trois points dans $E(\mathbb{F}_{125})$ de la forme $(x, 0)$. En déduire que $E(\mathbb{F}_{125})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
(6) Montrer que les points $P_1 = (\theta, 3)$, $P_2 = (1, 2\theta + 2\theta^2)$ et $P_3 = (-1, \theta + \theta^2)$ sont sur E. Calculer $P_2 + P_3$.

Solution.

(1) $P(X) \neq 0 \mod 5$ pour $X = 0, 1, 2, 3, 4$. Donc P n'a pas de facteur linéaire ; comme il est de degré trois, il est irréductible. Ainsi

$$\mathbb{F}_{125} = \mathbb{F}_{5^3} \cong \mathbb{F}_5[X]/(P) \cong \mathbb{F}(\theta),$$

où $\theta = X + (P) \in \mathbb{F}_5[X]/(P)$ satisfait de $0 = P(\theta) = \theta^3 + \theta^2 + 1$.
(2) On a $\theta(\theta^2 + \theta) = -1$. Donc $\theta^{-1} = -\theta^2 - \theta$.
(3) $\theta^3 = -\theta^2 - 1$, d'où

$$\begin{aligned}\theta^6 = (-\theta^2 - 1)^2 = \theta^4 + 2\theta^2 + 1 = \theta(-\theta^2 - 1) + 2\theta^2 + 1 = -\theta^3 - \theta + 2\theta^2 + 1 \\ = \theta^2 + 1 - \theta + 2\theta^2 + 1 = -2\theta^2 - \theta + 2.\end{aligned}$$

Donc

$$\begin{aligned}\theta^{30} = (\theta^6)^5 = (-2\theta^2 - \theta + 2)^5 = -2(\theta^2)^5 - \theta^5 + 2 = \theta^4(-2\theta^6 - \theta) + 2 \\ = \theta^4(-2(-2\theta^2 - \theta + 2) - \theta) + 2 = -\theta^2 + \theta^5 + \theta^4 + 2 \\ = 2\theta^2 + \theta - 2 + \theta^2(\theta^3 + \theta^2) + 2 = 2\theta^2 + \theta - \theta^2 = \theta^2 + \theta = -\theta^{-1}.\end{aligned}$$

Ainsi $\theta^{31} = -1$. Comme $\mathbb{F}_{125}$ est cyclique d'ordre 124 et $\theta^{62} = 1$, il suit que θ est un carré. Or, $-\theta = 2^2\theta$, donc $-\theta$ est également un carré.
(4) D'après le cours,

$$\Delta(E) = -16(4a_4^3 + 27a_6^2) = \theta^3 \quad \text{et} \quad j(E) = -(48a_4)^3/\Delta = -2.$$

Comme $\Delta(E) \neq 0$, la courbe est lisse et E est une courbe elliptique.
(5) On a $Q_0 = (0, 0) =\in E(\mathbb{F}_{125})$. Si $\alpha \in \mathbb{F}_{125}$ satisfait $\alpha^2 = -\theta$, alors $Q_1 = (\alpha, 0) \in \mathbb{F}_{125}$ et $Q_2 = (-\alpha, 0) \in \mathbb{F}_{125}$, car

$$(\pm\alpha)^3 + (\pm\alpha)\theta = \pm\theta(\alpha^2 + \theta) = 0.$$

Or, $Q_i = -Q_i$ pour $i = 0, 1, 2$. On a donc trois points d'ordre 2 ; comme $|E[2]| = 4$, ce sont tous les points d'ordre deux, et $E(\mathbb{F}_{125})[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

(6) On a $\theta^3+\theta^2=-1=3^2$; comme $\theta^2(\theta+1)=-1$ on a

$$(2\theta+2\theta^2)^2=4(-\theta^{-1})^2=-\theta^{-2}=\theta+1.$$

Enfin, $(\theta+\theta^2)^2=(-\theta^{-1})^2=-\theta-1$. Ainsi, P_1, P_2 et P_3 sont sur la courbe.

Pour calculer $P_2+P_3=(x,y)$, calculons

$$\lambda=\frac{(2\theta^2+2\theta)-(\theta+\theta^2)}{1-(-1)}=3(\theta+\theta^2)=2\theta^{-1}.$$

Donc $x=\lambda^2-1-(-1)=-\theta^{-2}=\theta+1$ et

$$y=\lambda(1-\theta-1)-(2\theta+2\theta^2)=2\theta^{-1}(-\theta)-2\theta-2\theta^2=-2-2\theta-2\theta^2.$$

Exercice 2. On considère la courbe

$$E: y^2=x^3+\theta x^2+\theta$$

sur le corps $\mathbb{F}_9=\mathbb{F}_3(\theta)$, où $\theta^2=-1$.

(1) Montrer que E est une courbe elliptique; calculer son discriminant et son j-invariant.
(2) Déterminer les points de $E(\mathbb{F}_9)$.
(3) En déduire la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ?
(4) Le groupe $E(\mathbb{F}_9)$, est-il cyclique ?
(5) Quelle est la plus petite extension k de $\mathbb{F}_9$ tel que $E(k)$ ait un point d'ordre 2 ?

Solution.

(1) D'après le cours,

$$\Delta(E)=-a_2^3a_6=-\theta^4=-1 \quad \text{et} \quad j(E)=-a_2^3/a_6=-\theta^2=1.$$

Comme $\Delta(E)\neq 0$, la courbe est lisse et E est une courbe elliptique.

(2)

x	x^2	x^3	$x^3+\theta x^2+\theta$
0	0	0	θ
1	1	1	$1-\theta$
-1	1	-1	$-1-\theta$
θ	-1	$-\theta$	$-\theta$
$-\theta$	-1	θ	θ
$\theta+1$	$-\theta$	$1-\theta$	-1
$-\theta-1$	$-\theta$	$\theta-1$	$-\theta$
$\theta-1$	θ	$-1-\theta$	1
$1-\theta$	θ	$1+\theta$	$-\theta$

On a donc

$$\begin{aligned}E(\mathbb{F}_9)=\{&O,(0,\theta-1),(0,1-\theta),(\theta,\theta+1),(\theta,-1-\theta),(-\theta,\theta-1),(-\theta,1-\theta),\\&(\theta+1,\theta),(\theta+1,-\theta),(-1-\theta,\theta+1),(-1-\theta,-1-\theta),\\&(\theta-1,1),(\theta-1,-1),(1-\theta,\theta+1),(1-\theta,-1-\theta)\}\end{aligned}$$

et $|E(\mathbb{F}_9)|=15$.

(3) On a $t=9+1-|E(\mathbb{F}_9)|=-5$. Comme $3\nmid -5$, la courbe n'est pas supersingulière.
(4) Comme $15=3\cdot 5$ n'a pas de facteur carré, $E(\mathbb{F}_9)$ est un groupe cyclique.
(5) Un point d'ordre deux est un point de la forme $(x,0)$. Il convient donc de ressoudre $P(x)=x^3+\theta x+\theta=0$. Or, P n'a pas de zéro dans $\mathbb{F}_9$, et donc pas de facteur linéaire. Il est donc irréductible, et la plus petite extension de $\mathbb{F}_9$ tel que P y ait un zéro est $k=\mathbb{F}_{9^3}=\mathbb{F}_9[X]/(P)$.

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

2

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.