Examen - Courbes Elliptiques

vendredi 6 janvier 2017, 9h – 12h

Documents non-autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^3 + X + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^3 + X + 1$. Construire le corps $\mathbb{F}_8$ à l'aide de θ.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_8 = \mathbb{F}(\theta)$.

(3) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique. La courbe E, est-elle supersingulière ?
(4) Pourquoi sait-on en avance que θ est un générateur multiplicatif de $\mathbb{F}_8^\times$? Écrire les éléments de $\mathbb{F}_8$ comme puissance de θ.
(5) Énumérer les points de $E(\mathbb{F}_8)$.
(6) Identifier les points de $E(\mathbb{F}_8)$ d'ordre 3, et identifier le groupe $E(\mathbb{F}_8)$.
(7) Calculer la trace t du Frobenius, et donner une formule pour $|E(\mathbb{F}_{8^n})|$.

Solution.

(1) Soit $P(X) = X^3 + X + 1$. On a $P(0) = P(1) = 1$. Donc P n'a pas de facteur linéaire sur $\mathbb{F}_2$; puisque son degré est trois, P est irréductible sur $\mathbb{F}_2$.
(2) On a $\mathbb{F}_8 = \mathbb{F}_{2^3} \cong \mathbb{F}[X]/(P) \cong \mathbb{F}(\theta) = \{a\theta^2 + b\theta + c : a, b, c \in \mathbb{F}_2\}$.
(3) On a $a_1 = a_2 = a_4 = 0$, $a_3 = a_6 = \theta$. Donc

$$b_2 = 0, \quad b_4 = 0, \quad b_6 = \theta^2, \quad b_8 = 0, \quad \Delta(E) = \theta^4, \quad \text{et} \quad j(E) = 0.$$

Comme $\Delta(E) \neq 0$, la courbe est lisse ; c'est donc une courbe elliptique. Puisqu'on est en caractéristique 2 et $j(E) = 0$, la courbe est supersingulière.
(4) $|\mathbb{F}_8^\times| = 8_1 = 7$ est premier. Donc tout élément différent de 0 et 1 est un générateur multiplicatif de $\mathbb{F}_8$. On a

$$1 = \theta^0, \quad \theta, \quad , \theta^2, \quad \theta^3 = \theta + 1, \quad \theta^4 = \theta^2 + \theta, \quad \theta^5 = \theta^2 + \theta + 1, \quad \theta^6 = \theta^2 + 1.$$

(5)

x	x^2	x^3	$x^2 + \theta x$	$x^3 + \theta$
0	0	0	0	θ
1	1	1	$\theta + 1$	$\theta + 1$
θ	θ^2	$\theta^3 = \theta + 1$	0	1
θ^2	$\theta^4 = \theta^2 + \theta$	$\theta^6 = \theta^2 + 1$	$\theta^2 + 1$	$\theta^2 + \theta + 1$
$\theta^3 = \theta + 1$	$\theta^6 = \theta^2 + 1$	θ^2	$\theta + 1$	$\theta^2 + \theta$
$\theta^4 = \theta^2 + \theta$	θ	$\theta^5 = \theta^2 + \theta + 1$	$\theta^2 + 1$	$\theta^2 + 1$
$\theta^5 = \theta^2 + \theta + 1$	$\theta^3 = \theta + 1$	θ	$\theta^2 + \theta$	0
$\theta^6 = \theta^2 + 1$	$\theta^5 = \theta^2 + \theta + 1$	$\theta^4 = \theta^2 + \theta$	$\theta^2 + \theta$	θ^2

Les valeurs communes sont 0, $\theta + 1$, $\theta^2 + 1$ et $\theta^2 + \theta$. Ainsi

$$\begin{aligned} E(\mathbb{F}_8) = \{&\mathcal{O}, (\theta^2 + \theta + 1, 0), (\theta^2 + \theta + 1, \theta), (1, 1), (1, \theta + 1), \\ &(\theta + 1, \theta^2 + \theta + 1), (\theta + 1, \theta^2 + 1), (\theta^2 + \theta, \theta^2), (\theta^2 + \theta, \theta^2 + \theta)\}. \end{aligned}$$

(6) Si $P = (x, y)$ est d'ordre 3, alors avec $\lambda = x^2/\theta$ on a

$$2P = (\lambda^2, \lambda(x + \lambda^2) + y + \theta) = -P = (x, y + \theta).$$

Ainsi $x^4/\theta^2 = x$ et $x^3 = \theta^2$, puisque $x \neq 0$. Donc $x = \theta^3 = \theta + 1$ et il y a deux points d'ordre 3 : $P_1 = (\theta + 1, \theta^2 + 1)$ et $P_2 = (\theta + 1, \theta^2 + \theta + 1)$. Comme $|E(\mathbb{F}_8)| = 9$, le groupe est cyclique : $E(\mathbb{F}_8) \cong \mathbb{Z}/9\mathbb{Z}$.

(7) La trace du Frobenius est $t = 8 + 1 - |E(\mathbb{F}_8)| = 9 - 9 = 0$. Le polynome caractéristique du Frobenius est donc $\chi_E(T) = T^2 - tT + q = T^2 + 8$, dont les racines sont $\tau_{1/2} = \pm i\,2\sqrt{2}$. Ainsi

$$|E(\mathbb{F}_{8^n}| = 8^n + 1 - \tau_1^n - \tau_2^n = \begin{cases} 8^n + 1 & \text{si } n \text{ est impair} \\ 8^n + 1 - 2\,(-8)^{n/2} & \text{si } n \text{ est pair.} \end{cases}$$

Exercice 2. On admet que 2017 est premier. On considère la courbe $E : y^2 = x^3 + 1$ sur le corps fini $\mathbb{F}_{2017}$.

(1) Calculer le discriminant $\Delta(E)$ et le j-invariant $j(E)$. En déduire que E est une courbe elliptique.
(2) Montrer que $\mathbb{F}_{2017}$ contient des racines 3^{mes} de l'unité.
(3) En déduire que $E(F_{2017})$ contient trois involutions.
(4) La courbe $E(\mathbb{F}_{2017})$, est-elle cyclique ? Est-elle supersingulière ?
(5) Donner une condition suffisante et nécessaire pour qu'un point (x, y) de E soit d'ordre 3.

Solution.

(1) On a $a_1 = a_2 = a_3 = a_4 = 0$ et $a_6 = 1$. Donc $b_2 = b_4 = b_8 = 0$ et $b_6 = 4$. Ainsi $\Delta(E) = -27 \cdot 4^2 = -432 \neq 0$ et $j(E) = 0$. Puisque $\Delta(E) \neq 0$, la courbe est lisse, et donc elliptique.
(2) On a $|\mathbb{F}_{2017}^\times| = 2016 = 3 \cdot 672$. Ainsi $\mathbb{F}_{2017}^\times$ contient des éléments d'ordre 3, c'est-à-dire des racines 3^{mes} de l'unité non-triviales. Si ω est un tel élément, alors ω^2 est l'autre racine 3^{me} de l'unité.
(3) Les involutions de E sont les points de la forme $(x, 0)$. Ainsi $x^3 = -1$, et soit $x = -1$, soit $-x$ est une racine 3^{me} de l'unité non-triviale. Alors $E(\mathbb{F}_{2017})[2] = \{\mathcal{O}, (-1, 0), (-\omega, 0), (-\omega^2, 0)\}$.
(4) Puisque $E(\mathbb{F}_{2017})$ contient plus qu'une seule involution, le groupe n'est pas cyclique. S'il était supersingulière, comme elle est sur un corps premier de cardinal ≥ 5, la trace du Frobenius serait 0, et $|E(\mathbb{F}_{2017})| = 2017+1-0 = 2018 = 2 \cdot 1009$. Mais $4 = |E(\mathbb{F}_{2017})[2]|$ divise $|E(\mathbb{F}_{2017})|$, une contradiction. Donc E n'est pas supersingulière.
(5) $P = (x, y)$ est d'ordre 3 si et seulement si pour $\lambda = 3x^2/2y$ on a

$$2P = (\lambda^2 - 2x, \lambda(3x - \lambda^2) - y) = -P = (x, -y),$$

et donc

$$3x = \frac{9x^4}{4y^2} = \frac{9}{4} x \frac{y^2 - 1}{y^2}.$$

Alors $x = 0$ et $y = \pm 1$, ou $12y^2 = 9(y^2 - 1)$ et $3y^2 = -9$, ce qui donne $y^2 = -3$ et $x^3 = -4$. Pour cela, il y a trois possibilités pour x et deux pour y, soit six points, ce qui fait au total $8 = 3^2 - 1$ points d'ordre 3.

Exercice 3. On admet que 2017 est premier. Est-ce que 1720 est un carré modulo 2017 ?

Solution. On a $\left(\frac{1720}{2017}\right) = \left(\frac{2^3}{2017}\right)\left(\frac{5}{2017}\right)\left(\frac{43}{2017}\right)$.

$$\left(\frac{2^3}{2017}\right) = \left(\frac{2^2}{2017}\right)\left(\frac{2}{2017}\right) = 1 \cdot (-1)^{\frac{2017^2-1}{8}} = (-1)^{\frac{1^2-1}{8}} = 1 \text{ puisque } 2017 \equiv 1 \bmod 8,$$

$$\left(\frac{5}{2017}\right) = \left(\frac{2017}{5}\right) \cdot (-1)^{\frac{2017-1}{2}\frac{5-1}{2}} = \left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = -1,$$

$$\left(\frac{43}{2017}\right) = \left(\frac{2017}{43}\right) \cdot (-1)^{\frac{2017-1}{2}\frac{43-1}{2}} = \left(\frac{-4}{43}\right) = \left(\frac{2^2}{43}\right) \cdot \left(\frac{-1}{43}\right) = 1 \cdot (-1)^{\frac{43-1}{2}} = -1.$$

Donc $\left(\frac{1720}{2017}\right) = 1$ et 1720 est un carré modulo 2017.

Exercice 4.

(1) Donner la définition du couplage de Weil, et ses propriétés principales.
(2) On suppose que E est une courbe elliptique sur un corps k, et que S et T dans $E(k)$ sont indépendants (c'est-à-dire si $mS+nT = \mathcal{O}$, alors $mS = \mathcal{O}$ et $nT = \mathcal{O}$). Donner l'ordre de $e_n(S,T)$ en fonction de $o(S)$ et $o(T)$.

Solution.

(1) Soit E une courbe elliptique défini sur un corps k, et n un entier tel que $\mathrm{car}(k)$ ne divise pas n. Soit μ_n le groupe de racines n^{mes} de l'unité. Alors le couplage de Weil est une application

$$e_n : E[n] \times E[n] \to \mu_n$$

telle que

- e_n est bilinéaire :
  $e_n(S+S',T) = e_n(S,T) \cdot e_n(S',T)$ et $e_n(S,T+T') = e_n(S,T) \cdot e_n(S,T')$.
- e_n est non-dégénéré : Si $e_n(S,T) = 1$ pour tout T, alors $S = \mathcal{O}$, et si $e_n(S,T) = 1$ pour tout S, alors $T = \mathcal{O}$.
- $e_n(S,S) = 1$ pour tout S.
- e_n est antisymétrique : $e_n(S,T) = e_n(T,S)^{-1}$.
- Si σ est un automorphisme de $\bar{k}$ qui stabilise E, alors $e_n(\sigma(S),\sigma(T)) = \sigma(e_n(S,T))$.
- Si φ est un endomorphisme de E de degré d, alors $e_n(\varphi(S),\varphi(T)) = e_n(S,T)^d$.

(2) Comme S et T sont indépendants, il y a une base (P,Q) de $E[n]$ tel que $S = sP$ et $T = tQ$. Alors $e_n(P,Q) = \zeta$ est une racine primitive n^{me} de l'unité, et

$$e_n(S,T) = e_n(sP,tQ) = e_n(P,Q)^{st} = \zeta^{st}.$$

Ainsi $o(e_n(S,T)) = n/\mathrm{pgcd}(n,st)$. Or, $o(S) = n/\mathrm{pgcd}(n,s)$ et $o(T) = n/\mathrm{pgcd}(n,t)$. Mais

$$\mathrm{pgcd}(n,st) = \mathrm{pgcd}(n, \mathrm{pgcd}(n,s) \cdot \mathrm{pgcd}(n,t)).$$

Donc $n/o(e_n(S,T)) = \mathrm{pgcd}(n, n/o(S) \cdot n/o(T))$.
Alors $o(e_n(S,T)) = n/\mathrm{pgcd}(n, n/o(S) \cdot n/o(T))$.