Examen - Courbes Elliptiques

vendredi 22 janvier 2016, 8h45 – 11h45

Documents non-autorisés

Toutes les réponses devront être soigneusement justifiées

Exercice 1.

(1) Montrer que $X^2 + X + 1$ est irréductible dans $\mathbb{F}_2$.
(2) Soit θ une racine de $X^2 + X + 1$. Construire le corps $\mathbb{F}_4$ à l'aide de θ.

On considère la courbe $E : y^2 + \theta y = x^3 + \theta$ sur $\mathbb{F}_4$, où $\theta \in \mathbb{F}_4$ satisfait $\theta^2 + \theta + 1 = 0$.

(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) Énumérer les points de $E(\mathbb{F}_4)$. La courbe $E(\mathbb{F}_4)$, est-elle cyclique ?
(5) Donner la table d'addition de $E(\mathbb{F}_4)$.
[Indication : Identifier d'abord les couples $(P, -P)$.]
(6) Calculer $|E(\mathbb{F}_{1024}|$.

Solution.

(1) Soit $P(X) = X^2 + X + 1$. Alors $P(0) = P(1) = 1$. Donc P n'a pas de facteur linéaire ; comme $\deg(P) = 2$, le polynôme P est irréductible.
(2) On a $\mathbb{F}_4 = \mathbb{F}_2(\theta) \cong \mathbb{F}_2[X]/(P) \cong \{a + b\theta : a, b \in \mathbb{F}_2\}$.
(3) On a $a_1 = a_2 = a_4 = 0$ et $a_3 = a_6 = \theta$. Donc $b_2 = 0$, $b_4 = 0$, $b_6 = \theta^2$ et $b_8 = 0$. Ainsi $\Delta(E) = b_6^2 = \theta^4 = \theta$ et $j(E) = 0$. Puisque $\Delta(E) \neq 0$, la courbe est lisse et donc elliptique ; comme la caractéristique est 2 et $j(E) = 0$, la courbe est supersingulière.
(4)

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

Ainsi $E(\mathbb{F}_8) = \{O, (1,1), (1,\theta+1), (\theta,1), (\theta,\theta+1), (\theta+1,1), (\theta+1,\theta+1)\}$ et $|E(\mathbb{F}_4)| = 7$. Comme 7 est premier, le groupe $E(\mathbb{F}_4)$ est cyclique.
(5) Soit $P = (x, y) = (1, 1)$. On calcule $2P = (x', y')$:

$$\lambda = \frac{x^2}{\theta} = \theta^{-1} = \theta + 1, \quad x' = \lambda^2 = \theta, \quad y' = \lambda(x + x') + y + \theta = (\theta + 1)^2 + \theta + 1 = 1.$$

Donc $2P = (\theta, 1)$. On calcule $3P = P + 2P = (x'', y'')$:

$$\lambda = \frac{1+1}{\theta+1} = 0, \quad x'' = \lambda^2 + x + x' = \theta + 1, \quad y'' = \lambda(x + x'') + y + \theta = \theta + 1.$$

Donc $3P = (\theta + 1, \theta + 1)$. Alors $4P = -3P = (\theta + 1, 1)$, $5P = -2P = (\theta, \theta + 1)$ et $6P = -P = (1, \theta + 1)$. Ainsi

$+$	O	P	$2P$	$3P$	$4P$	$5P$	$6P$
O	O	P	$2P$	$3P$	$4P$	$5P$	$6P$
P	P	$2P$	$3P$	$4P$	$5P$	$6P$	O
$2P$	$2P$	$3P$	$4P$	$5P$	$6P$	O	P
$3P$	$3P$	$4P$	$5P$	$6P$	O	P	$2P$
$4P$	$4P$	$5P$	$6P$	O	P	$2P$	$3P$
$5P$	$5P$	$6P$	O	P	$2P$	$3P$	$4P$
$6P$	$6P$	O	P	$2P$	$3P$	$4P$	$5P$

soit

2 $+$	O	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$
O	O	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$
$(1,1)$	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$	O
$(\theta,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$	O	$(1,1)$
$(\theta+1,\theta+1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$	O	$(1,1)$	$(\theta,1)$
$(\theta+1,1)$	$(\theta+1,1)$	$(\theta,\theta+1)$	$(1,\theta+1)$	O	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$
$(\theta,\theta+1)$	$(\theta,\theta+1)$	$(1,\theta+1)$	O	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$
$(1,\theta+1)$	$(1,\theta+1)$	O	$(1,1)$	$(\theta,1)$	$(\theta+1,\theta+1)$	$(\theta+1,1)$	$(\theta,\theta+1)$

(6) La trace t du Frobenius vaut $t = 4 + 1 - |E(\mathbb{F}_4)| = -2$. Le polynôme caractéristique du Frobenius est donc $\chi_E(T) = T^2 - tT + q = T^2 + 2T + 4$; ses racines sont $\tau_{1/2} = -1 \pm i\sqrt{3} = 2e^{\pm i\frac{2}{3}\pi}$.
On a

$$\begin{aligned}|E(\mathbb{F}_{1024})| = |E(\mathbb{F}_{2^{10}})| = |E(\mathbb{F}_{4^5})| &= 4^5 + 1 - 2\,\mathrm{Re}(\tau^5)\\ &= 1024 + 1 - 2\cdot 2^5\cos(\frac{10}{3}\pi)\\ &= 1025 - 64\cos(-\frac{2}{3}\pi) = 1025 - 64(-\frac{1}{2}) = 1057.\end{aligned}$$

Exercice 2. On admet que 2017 et 1009 sont premiers. 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 supersingulière.
(2) Donner $|E(\mathbb{F}_{2017})|$. En déduire que $E(\mathbb{F}_{2017})$ est cyclique.
(3) Quels sont les ordres possibles des éléments de $E(\mathbb{F}_{2017})$?
(4) Donner tous les éléments d'ordre au plus 100.

Solution.

(1) On a $a_1 = a_2 = a_3 = a_4 = 0$ et $a_6 = 1$. Donc $b_2 = b_4 = 0$, $b_6 = 4$ et $b_8 = 0$. Donc $\Delta(E) = -27b_6^2 = -27 \cdot 16 = -432$ et la courbe est lisse et elliptique ; de plus $j(E) = 0$.
Comme la caractéristique n'est ni 2 ni 3, on ne peut pas en déduire que la courbe est supersingulière (il y a une erreur dans l'énoncé). Pour les parties suivantes, on supposera donc qu'elle le soit.
(2) Si la courbe est supersingulère, comme le corps de base est premier et la caractéristique est supérieure à 5, la trace t du Frobenius vaut 0. Ainsi

$$|E(\mathbb{F}_{2017})| = 2017 + 1 - t = 2018 = 2 \cdot 1009.$$

Puisque l'ordre ne contient pas de carré, le groupe est cyclique.
(3) Les ordres possibles sont les diviseurs de $|E(\mathbb{F}_{2017})| = 2018$, soit 1, 2, 1009 et 2018.
(4) Le seul point d'ordre 1 est O. Puisque $2 \mid 2018$ mais $4 \nmid 2018$, il n'y a qu'un seul élément d'ordre 2. Comme $a_1 = a_3 = 0$, il est de la forme $(x, 0)$, où x doit satisfaire $x^3 + 1 = 0$. Donc $(-1, 0) \in E(\mathbb{F}_{2017})$ est un point d'ordre 2.
Bonus : En fait, 3 divise $2016 = |\mathbb{F}_{2017}^\times|$. Il y a donc des racines 3^{mes} de l'unité j et j^2 dans $\mathbb{F}_{2017}$, ce qui implique que l'équation $x^3 + 1 = 0$ a deux autres solutions, $-j$ et $-j^2$. Ceci donne que les deux autres involutions de E sont $(-j, 0)$ et $-j^2, 0)$, qui sont ainsi $\mathbb{F}_{2017}$-rationnels. Mais alors $4 \mid |E(\mathbb{F}_{2017})|$, ce qui est une contradiction. On en déduit que E n'est pas supersingulière.

Exercice 3. On rappelle que le couplage de Tate-Lichtenbaum est une application bilinéaire non-dégénérée

$$\tau_n : E(\mathbb{F}_q)[n] \times E(\mathbb{F}_q)/nE(\mathbb{F}_q) \to \mu_n,$$

où μ_n est le groupe de racines n-mes de l'unité. En supposant que $P \in E(\mathbb{F}_q)$ est d'ordre n premier avec $\text{pgcd}(n, q) = 1$ et $\mu_n \subseteq \mathbb{F}_q$, donner un algorithme pour transformer le problème du logarithme discrèt dans $E(\mathbb{F}_q)$ avec point de base P en problème du logarithme discrèt dans $\mathbb{F}_q^\times$. Justifier l'algorithme.
[Indication : S'inspirer de l'attaque MOV.]

Solution. Étant donne un point Q, le problème du logarithme discrèt à base P consiste à trouver k, s'il existe, tel que $kP = Q$.
On choisit un point $R \in E(\mathbb{F}_q)$ au hasard, et on calcule $\zeta = \tau_n(P, R)$. Si $\zeta = 1$, on recommence. Sinon, puisque n est premier, ζ est un générateur de μ_n. On calcule alors $\tau_n(Q, R) = \zeta'$. On résout dans μ_n le problème du logarithme discrèt pour trouver ℓ avec $\zeta^\ell = \zeta'$. On calcule ℓP; si $\ell P = Q$, on pose $k = \ell$; sinon il n'y a pas de solution.
Justification. Si $Q = kP$, alors par linéarité de τ_n à gauche on a

$$\zeta^\ell = \zeta' = \tau_n(Q, R) = \tau_n(kP, Q) = \tau_n(P, Q)^k = \zeta^k.$$

Comme l'ordre de ζ est n, on a $\ell \equiv k \mod n$, et l'algorithme donne la bonne solution.
En général, l'algorithme va sortir k si $\tau_n(Q - kP, Q) = 1$, c'est-à-dire si $Q - kP \in \ker \tau_n(., R)$. Il est donc nécessaire de bien vérifier que $kP = Q$.
On a $\tau_n(P, R) = 1$ si $R \in \ker \tau_n(P, .)$. Puisque τ_n est non-dégénérée et n est premier, on a $\text{im}\, \tau_n(P, .) = \mu_n$ et $\ker \tau_n(P, .)$ est un sous-groupe de $E(\mathbb{F}_q)$ d'indice n. Si on choisit $R \in E(\mathbb{F}_q)$ au hasard, on obtient donc $\tau_n(P, R) \neq 1$ avec probabilité $\frac{n-1}{n} = 1 - \frac{1}{n}$.