Examen - Courbes Elliptiques

Lundi 28 janvier 2013, 9h – 11h

Corrigé

Exercice 1.

(1) Montrer que $X^3 + X^2 + 1$ est irréductible dans $\mathbb{F}_2$. En déduire que $\mathbb{F}_8 = \mathbb{F}_2(\theta)$ où θ est un zéro de $X^3 + X^2 + 1$.
(2) Calculer θ^i pour $0 \leq i < 7$. En déduire que θ est un générateur pour le groupe multiplicatif $\mathbb{F}_8^\times$.
(3) On considère la courbe $E : y^2 + xy = x^3 + \theta$ sur $\mathbb{F}_2(\theta)$. Montrer que E est une courbe elliptique, et calculer son discriminant Δ et son j-invariant.
(4) Énumérer les points de $E(\mathbb{F}_8)$.
[Indication : Pour $x \neq 0$ on pourra se servir de l'équation $z^2 + z = x + \theta x^{-2}$ avec $z = yx^{-1}$; pour le calcul de x^{-2} il sera utile de transformer x en puissance de θ.]
(5) Le groupe $E(\mathbb{F}_8)$, est-il cyclique ?
(6) Calculer la valeur t de la trace du Frobenius. La courbe, est-elle supersingulière ? Est-elle anormale ?
(7) Donner une formule pour $|E(\mathbb{F}_{8^k})|$.
(8) Quelle est la plus petite extension k de $\mathbb{F}_8$ tel que $E(k)$ soit anormale ?

Solution.

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

$$\mathbb{F}_8 = \mathbb{F}_{2^3} \cong \mathbb{F}_2[X]/(X^3 + X^2 + 1) \cong \mathbb{F}(\theta),$$

où $\theta = X + (X^3 + X^2 + 1) \in \mathbb{F}_2[X]/(X^3 + X^2 + 1)$ satisfait $\theta^3 + \theta^2 + 1 = 0$.
(2)

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

Donc les puissances de θ forment le groupe $\mathbb{F}_8^\times$ qui a $8 - 1 = 7$ éléments.
(3) D'après le cours, $\Delta = a_6 = \theta$ et $j(E) = 1/a_6 = \theta^{-1} = \theta^6 = \theta^2 + \theta$. Comme $\Delta \neq 0$, la courbe est lisse et E est une courbe elliptique.
(4) Pour $x = 0$ on cherche y avec $y^2 = \theta$; il y a une unique solution $y = \theta^4 = \theta^2+\theta+1$. On calcule :

x	$x^2 + x$	$x + \theta x^{-2}$
0	0	
1	0	$\theta + 1$
θ	$\theta^2 + \theta$	θ^2
$\theta + 1$	$\theta^2 + \theta$	0
θ^2	$\theta + 1$	$\theta + 1$
$\theta^2 + 1$	$\theta + 1$	1
$\theta^2 + \theta$	$\theta^2 + 1$	$\theta + 1$
$\theta^2 + \theta + 1$	$\theta^2 + 1$	$\theta^2 + \theta$

Les points sont donc O, $(0, \theta^2 + \theta + 1)$ et les points (x, y) avec

x	1	1	$\theta+1$	$\theta+1$	θ^2	θ^2	θ^2+1	θ^2+1	$\theta^2+\theta+1$	$\theta^2+\theta+1$
z	θ^2	θ^2+1	0	1	θ^2	θ^2+1	θ^2	θ^2+1	θ	$\theta+1$
$y = zx$	θ^2	θ^2+1	0	$\theta+1$	$\theta^2+\theta+1$	$\theta+1$	$\theta+1$	$\theta^2+\theta$	$\theta+1$	θ^2

(5) On a $|E(\mathbb{F}_8)| = 12 = 3 \cdot 4$. Comme en caractéristique 2 il ne peut y avoir qu'un seul élément d'ordre 2, le groupe est cyclique.
(6) La trace du Frobenius est $t = q + 1 - |E(\mathbb{F}_8)| = 9 - 12 = -3$. La caractéristique ne divise pas t ; la courbe n'est pas supersingulière. Elle n'est pas anormale car $t \neq 1$.
(7) Le polynôme caractéristique est

$$\chi_E(T) = T^2 - tT + q = T^2 + 3T + 8.$$

Ses zéros sont $\tau_1 = \frac{-3+i\sqrt{23}}{2}$ et $\tau_2 = \frac{-3-i\sqrt{23}}{2}$. On a

$$|E(\mathbb{F}_{8^k}| = 8^k + 1 - \tau_1^k - \tau_2^k = 8^k + 1 - 2^{1-k} \sum_{j=0}^{\lfloor \frac{k}{2} \rfloor} \binom{k}{2j} (-3)^{k-2j} (-23)^j.$$

(8) Si $E(\mathbb{F}_{8^k})$ etait anormale, alors $|E(\mathbb{F}_{8^k})| = 8^k + 1 - 1 = 8^k$. Or, $|E(\mathbb{F}_8)| = 12$ divise $|E(\mathbb{F}_{8^k})|$. C'est donc impossible.

Exercice 2. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$, telle que la trace t du Frobenius soit 0. Supposons que $E(\mathbb{F}_q)$ contiennne un point d'ordre n. Soit $\phi_q : x \mapsto x^q$ l'endormorphisme de Frobenius.

(1) Montrer que $\phi_q^2(S) = -qS$ pour tout point $S \in E$.
[Indication : ϕ_q satisfait le polynôme caractéristique χ_T.]
(2) Montrer que n divise $q + 1$. En déduire que $\phi_q^2(S) = S$ pour tout $S \in E[n]$.
(3) En déduire que $E[n] \subseteq E(\mathbb{F}_{q^2})$.
(4) En déduire que si $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ où d_1 divise d_2, alors $d_1 d_2$ divise $q^2 - 1$. Quel est donc le degré MOV de E ?

[Rappel : On a $x \in \mathbb{F}_q$ si et seulement si $x^q = x$.]

Solution.

(1) Puisque $t = 0$, on a pour tout point $S \in E$

$$0 = \chi_T(\phi_q)(S) = (\phi_q^2 - t\phi_q + q)(S) = \phi_q^2(S) + qS.$$

Donc $\phi_q^2(S) = -qS$.
(2) Puisque $E(\mathbb{F}_q)$ contient un point d'ordre n,

$$n \mid |E(\mathbb{F}_q)| = q + 1 - t = q + 1.$$

Ainsi si $S \in E[n]$, alors $(q+1)S = 0$ et $\phi_q^2(S) = -qS = S$.
(3) Soit $s = (x, y) \in E[n]$. Alors

$$(x, y) = S = \phi_q^2(S) = (x^{q^2}, y^{q^2}).$$

Donc $x^{q^2} = x$ et $y^{q^2} = y$. Ainsi $x, y \in \mathbb{F}_{q^2}$ et $S \in E(\mathbb{F}_{q^2})$.
(4) Puisque $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$, la courbe E contient un point d'ordre d_2. Par (2) on a $d_2 \mid q + 1$. Par ailleurs, $d_1 \mid q - 1$. Ainsi $d_1 d_2 \mid (q-1)(q+1) = q^2 - 1$. Comme $d_1 d_2 = |E(\mathbb{F}_q)|$, le degré MOV de E est au plus 2.

Exercice 3. On considere le groupe $G = \mathbb{F}_{2011}^{\times}$. On cherche k tel que $2^k \equiv 206 \mod 2010$. Donner en détail deux algorithmes rapides pour trouver k et expliquer pourquoi ils marchent.

Solution. *1. Algorithme de Pohlig-Hellman*

On a $|\mathbb{F}_{2011}^{\times}| = 2010 = 2 \cdot 3 \cdot 5 \cdot 67$. Pour $n \in \{2, 3, 5, 67\}$, en essayant $k_n = 0, 1, 2, \ldots, n-1$ on détermine $k_n \mod n$ tel que

$$206^{2010/n} \equiv (2^{2010/n})^{k_n} \mod n.$$

Alors on aura $k_n \equiv k \mod n$, ce qui nous donne $k \mod 2010$ avec le théorème des restes chinois.

2. Algorithe Pas de bébé, pas de géant

On prend $m = \lceil \sqrt{2010} \rceil = 45$. Alors $k = 45i + j$ avec $0 \leq i, j < 45$, et $206 \cdot (2^{-45})^i \equiv 2^j \mod 2010$. On calcule $2^\ell \mod 2010$ pour $0 \leq \ell < 45$. Ensuite, on calcule $2^{-45} \mod 2010$, et pour $0 \leq n < 45$ on calcule $206 \cdot (2^{-45})^n \mod 2010$ et compare avec les valeurs de 2^ℓ ; quand on trouve la même valeur, on recupère les exposants ℓ et n et pose $k = 45n + \ell$.

Exercice 4. Soit E une courbe elliptique sur un corps fini $\mathbb{F}_q$ et n un entier non divisible par $\mathrm{car}(\mathbb{F}_q)$. Soit μ_n le groupe des racines $n$mes de 1.

(1) Montrer que le couplage de Weil $e_n : E[n] \times E[n] \to \mu_n$ est surjectif. [On peut utiliser le fait qu'il est non dégénéré.]
(2) En déduire que si $E[n] \subseteq E(\mathbb{F}_q)$ alors $\mu_n \leq \mathbb{F}_q^{\times}$, et n divise $q - 1$.
(3) En déduire que si $E(\mathbb{F}_q) \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$ où d_1 divise d_2, alors d_1 divise $q - 1$.

Solution

(1) Soit (S, T) une base de $E[n]$ et $\omega = e_n(S, T) \in \mu_n$. Si ω n'est pas une racine primitive $n$me, alors $d = o(\omega) < n$ et $dS \neq 0$. Or, tout point $P \in E[n]$ est de la forme $P = iS + jT$ pour $0 \leq i, j < n$. Alors

$$e_n(dS, P) = e_n(dS, iS + jT) = e_n(S, S)^{di}\, e_n(S, T)^{dj} = 1^{di}\, \omega^{dj} = 1,$$

ce qui contredit le fait que e_n est non-dégénéré. Alors ω est une racine primitive $n$me, et

$$e_n(S, iT) = e_n(S, T)^i = \omega^i$$

parcourt μ_n pour $i \in \{0, 1, \ldots, n-1\}$.

(2) Si $E[n] \subseteq E(\mathbb{F}_q)$ on a une base (S, T) dans $E(\mathbb{F}_q)$. Soit $\phi_q : x \mapsto x^q$ l'automorphisme de Frobenius. Alors $\phi_q(S) = S$ et $\phi_q(T) = T$. Or,

$$\omega = e_n(S, T) = e_n(\phi_q(S), \phi_q(T)) = \phi_q(e_n(S, T)) = \phi_q(\omega) = \omega^q.$$

Donc $\omega \in \mathbb{F}_q$; comme $\mu_n = \langle \omega \rangle$, on a $\mu_n \leq \mathbb{F}_q^{\times}$. Alors $n = |\mu_n|$ divise $q - 1 = |\mathbb{F}_q^{\times}|$.

(3) Puisque $d_1 \mid d_2$, on a $E[d_1] \subseteq \mathbb{F}_q$. Alors $d_1 \mid q - 1$ d'après (2).