

Courbes elliptiques et cryptographie

Examen du 11 janvier 2011 - Durée 2 heures

L'usage de tout document est interdit. La calculatrice n'est pas autorisée. La rigueur du raisonnement et la clarté de la rédaction seront prises en compte dans la notation.

Document recto/verso.

Exercice 1 On considère un corps fini \mathbb{F}_q de caractéristique $p > 3$ et une courbe elliptique E définie sur \mathbb{F}_q :

$$E : y^2 = x^3 + ax + b$$

- 1- Donnez la définition de $E(\mathbb{F}_q)$.
- 2- On suppose dans cette question que $b = 0$. Montrez que $|E(\mathbb{F}_q)|$ est pair.
- 3- Énoncez le théorème de Hasse-Weil.
- 4- Soit $m \in \mathbb{N}$ un nombre premier. Qu'est-ce qu'un point de m -torsion ? Montrez rapidement que l'ensemble, $E[m]$, des points de m -torsion est un sous-groupe de $E(\overline{\mathbb{F}_q})$. Que pouvez-vous dire sur la structure de ce groupe ? (on pourra distinguer 2 cas.)

On suppose que m est premier avec p et que $E[m] \subset E(\mathbb{F}_q)$.

- 5- Expliquer brièvement pourquoi il existe $G_1 \in E(\mathbb{F}_q)$ et $G_2 \in E(\mathbb{F}_q)$ tels que tout point $P \in E[m]$ de m -torsion s'écrit $P = aG_1 + bG_2$ avec $a, b \in \mathbb{Z}$.
- 6- Montrez que l'on a $m|q - 1$.
- 7- On considère $e_m : E[m] \times E[m] \rightarrow \overline{\mathbb{F}_q}$ le pairing de Weil associé à E et à m . Quelles sont les propriétés de e_m ?
- 8- Soient $P = aG_1 + bG_2$ et $Q = cG_1 + dG_2$ deux points de m -torsion. Montrez que l'on a :

$$e_m(P, Q) = e_m(G_1, G_2)^D \text{ où } D = \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Exercice 2

Soit G un groupe abélien fini tel que $G \simeq \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ avec m et n deux entiers premiers entre eux. Quel théorème permet d'affirmer que G est un groupe cyclique d'ordre mn ?

On considère un corps fini \mathbb{F}_q de caractéristique $p > 3$ et une courbe elliptique E définie sur \mathbb{F}_q .

- 2- On suppose que $|E(\mathbb{F}_q)|$ est sans facteur carré. Montrez que $E(\mathbb{F}_q)$ est un groupe cyclique.
- 3- Si $|E(\mathbb{F}_q)|$ est premier avec $q - 1$, le groupe $E(\mathbb{F}_q)$ est-il forcément cyclique ?

On suppose maintenant que $|E(\mathbb{F}_q)| = 3\ell$ où $\ell > 3$ est un "grand" nombre premier.

- 4- Expliquez pourquoi il existe $G \in E(\mathbb{F}_q)$ d'ordre 3ℓ .
- 5- Montrez que l'ensemble des solutions de $3P = \mathcal{O}$, $P \in E(\mathbb{F}_q)$, est $\{\mathcal{O}, G, 2G\}$.
- 6- Soit P un point pris au hasard dans $E(\mathbb{F}_q)$. Quelle est la probabilité pour que $3P = \mathcal{O}$?
- 7- Proposez une stratégie efficace pour construire un point $P \in E(\mathbb{F}_q)$ d'ordre ℓ .

Exercice 3 Soit E la courbe elliptique définie sur \mathbb{F}_7 par :

$$E : y^2 = x^3 + x + 4$$

- 1- Énumérez tous les points de $E(\mathbb{F}_7)$.
- 2- Donnez la valeur, t , de la trace du Frobenius pour E . La courbe est-elle super-singulière ?
- 3- Soit $G = (0, 2) \in E(\mathbb{F}_7)$. Calculez $2G$ puis $4G$.
- 4- En déduire que G est d'ordre 10 puis que $E(\mathbb{F}_7)$ est cyclique.
- 5- Que vaut $5G$?
- 6- Construisez le corps \mathbb{F}_{49} . Que vaut $|E(\mathbb{F}_{49})|$?

Formulaire

Soit une courbe elliptique, E , définie sur un corps k (de caractéristique $\neq 2$) par :

$$E : y^2 = x^3 + ax + b$$

Pour $P_1 = (x_1, y_1) \in E(k)$ et $P_2 = (x_2, y_2) \in E(k)$, on a :

- $-P_1 = (x_1, -y_1)$.
- $P_1 + P_2 = (x_3, y_3)$ avec $x_3 = \lambda^2 - x_1 - x_2$, $y_3 = \lambda(x_1 - x_3) - y_1$ où :

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{si } P_1 \neq P_2, -P_2 \\ (3x_1^2 + a)(2y_1)^{-1} & \text{si } P_1 = P_2 \text{ et } 2P_1 \neq \mathcal{O} \end{cases}$$