N1MA8W04 – Courbes Elliptiques – Master CSI - année 2012/13
Examen: partie théorique - durée 1 heure
Aucun document ni l'ordinateur n'est autorisé

1. **Le morphisme de Frobenius**

   (a) Soit p un nombre premier. Montrer que pour $1 \leq k \leq p-1$ le coefficient binomial $\binom{p}{k}$ est divisible par p.

   (b) Soit K un corps de caractéristique p. Montrer que pour $x, y \in K$ on a $(x+y)^p = x^p + y^p$. Plus généralement, $(x+y)^{p^k} = x^{p^k} + y^{p^k}$ avec $k = 0, 1, 2 \ldots$

   (c) Soit $\mathbb{F}_q$ le corps de q éléments et $\bar{\mathbb{F}}_q$ sa clôture algébrique.

      i. Montrer que l'application $\bar{\mathbb{F}}_q \to \bar{\mathbb{F}}_q$ définie par $x \mapsto x^q$ est un automorphisme du corps $\bar{\mathbb{F}}_q$ (le *morphisme de Frobenius*).

      ii. Montrer que pour $x \in \bar{\mathbb{F}}_q$ on a $x^q = x$ si est seulement si $x \in \mathbb{F}_q$.

2. **Frobenius sur les courbes elliptique** On fixe une courbe elliptique E sur $\mathbb{F}_q$.

   (a) Rappeler la définition du morphisme de Frobenius $\phi_q : E \to E$.

   On admet (mais vous pouvez essayer de le démontrer) que l'application ϕ_q est un automorphisme du groupe abelien E.

   (b) Montrer que $\phi_q^k = \phi_{q^k}$ et que $\phi_q(P) = P$ si et seulement si $P \in E(\mathbb{F}_q)$.

   (c) Soit $m \in \mathbb{Z}$ un entier vérifiant $m\phi_q(P) = O$ pour tout $P \in E$. Montrer que $m = 0$. En déduire que l'égalité $m_1\phi_q = m_2\phi_q$ (avec $m_1, m_2 \in \mathbb{Z}$) implique $m_1 = m_2$.

3. **Le théorème de Weil** On fixe toujours une courbe elliptique E sur $\mathbb{F}_q$. On admet l'énoncé suivant.

   - *Posons $a_q = q + 1 - N_q$, où $N_q = |E(\mathbb{F}_q)|$. Alors le morphisme de Frobenius ϕ_q vérifie $\phi_q^2(P) - a_q\phi_q(P) + qP = O$ pour tout $P \in E$. Autrement dit, $\phi_q^2 - a_q\phi_q + q\,\mathrm{Id} = 0$.*

   On note par α et β les racines du polynôme $X^2 - a_qX + q$. (Le théorème de Hasse affirme que $\beta = \bar{\alpha}$, mais ceci ne joue aucun rôle dans la suite.)

   Notre objectif est de démontrer *le théorème de Weil*:

   $$a_{q^k} = \alpha^k + \beta^k \qquad (k = 1, 2, 3 \ldots).$$

   Dans la suite on note $a = a_q$, $b_k = \alpha^k + \beta^k$.

   (a) Montrer que $b_2 = a^2 - 2q$ et que $b_{k+1} = ab_k - qb_{k-1}$ pour $k \geq 2$. (Indication: vérifier que $\alpha^{k+1} = a\alpha^k - q\alpha^{k-1}$, et le même pour β.) En déduire que $b_k \in \mathbb{Z}$ pour tout $k \geq 1$.

   (b) Montrer que le polynôme $X^2 - aX + q$ divise le polynôme $X^{2k} - b_kX^k + q^k$. (Indication: montrer que $X^{2k} - b_kX^k + q^k = (X^k - \alpha^k)(X^k - \beta^k)$.)

   (c) Montrer que $\phi_{q^k}^2 - b_k\phi_{q^k} + q\,\mathrm{Id} = 0$. En déduire que $b_k\phi_{q^k} = a_{q^k}\phi_{q^k}$. Conclure, en utilisant la question 2c.

4. **Un exemple numérique** Dans la suite $q = 5$ et E est la courbe elliptique $y^2 = x^3 + 2x$ sur $\mathbb{F}_5$.

   (a) Sans utiliser l'ordinateur déterminer les nombres a_{5^k} et $N_{5^k} = |E(\mathbb{F}_{5^k})| = 5^k + 1 - a_{5^k}$ pour $k = 1, 2, 3, 4$.

   (b) Déterminer la structure des groupes $E(\mathbb{F}_5)$ et $E(\mathbb{F}_{5^3})$.

   (c) Montrer que le sous-groupe de 2-torsion $E[2]$ est contenu dans $E(\mathbb{F}_{5^2})$. (Indication: rappelons que les points de 2-torsion sont l'origine et les points avec $y = 0$.)

   (d) Déterminer la structure des groupes $E(\mathbb{F}_{5^2})$ et $E(\mathbb{F}_{5^4})$.

DS du 25 avril 2013
sujet sur machine 9h30 – 11h30

Durée : 2 heures. Les notes de cours et les programmes GP sont autorisés.

- Pour répondre aux questions, créer un seul fichier pour tout le sujet et séparer les exercices. Nommer le fichier `login.gp`, où login est votre identifiant informatique. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans le fichier `login.gp`.
- Pour rendre votre travail, envoyez le fichier par courriel à la fin de l'épreuve à l'adresse

  `jean.gillibert@math.u-bordeaux1.fr`

- Rappelons que la clarté des programmes et la pertinence des commentaires sont des éléments importants d'appréciation.

Exercice 1
Soit E la courbe elliptique définie sur $\mathbb{F}_{521}$ par les coefficients

$$E = [1, 1, 1, -3, 1]$$

1. Quelle est la structure de $E(\mathbb{F}_{521})$ en tant que groupe abélien fini ?
2. Le groupe $E(\mathbb{F}_{521})[5]$ est-il isomorphe à $(\mathbb{Z}/5\mathbb{Z}) \times (\mathbb{Z}/5\mathbb{Z})$?
3. On considère les points $P = (1, 0)$ et $Q = (21, 185)$ appartenant à $E(\mathbb{F}_{521})$. Vérifiez que P est d'ordre 5, et que Q est d'ordre 105.
4. Calculer le couplage de Weil $e_{105}(P, Q)$. En déduire que P n'appartient pas au sous-groupe cyclique engendré par Q.
5. Est-il vrai que le groupe $E(\mathbb{F}_{521})$ est engendré par P et Q ?

   On considère à présent le point $R = (0, 99)$ qui est d'ordre 3. On souhaite construire un autre point S d'ordre 3 tel que R et S engendrent le groupe $E(\overline{\mathbb{F}_{521}})[3]$. D'après les propriétés du couplage de Weil on sait que, pour construire un tel S, il faut aller dans une extension de $\mathbb{F}_{521}$ qui contient les racines 3-ièmes de l'unité.

6. Déterminer le plus petit entier k tel que $\mathbb{F}_{521^k}$ contienne les racines 3-ièmes de l'unité.
7. En utilisant les fonctions `elldivpol` et `factorff`, montrer que tous les points de 3-torsion de E sont définis sur $\mathbb{F}_{521^k}$, où k est l'entier de la question précédente.
8. Déterminer un point S tel que $E(\overline{\mathbb{F}_{521}})[3] = < R, S >$.

Exercice 2

Soit H la courbe elliptique définie sur $\mathbb{F}_{90000049}$ par les coefficients

$$H = [0, 0, 1, 1, 0]$$

On considère les points ci-dessous, à coordonnées dans $\mathbb{F}_{90000049}$

$$P = (36502070, 72583757)$$

$$Q = (74197837, 65666440)$$

On admet que Q appartient au groupe cyclique engendré par P.

1. Quel est l'ordre du groupe $H(\mathbb{F}_{90000049})$? Quel est l'ordre de P ? Que peut-on en déduire ?
2. En utilisant l'algorithme de Shanks, trouver un entier n tel que $[n]P = Q$.
3. Même question en utilisant la méthode rho de Pollard. Laquelle des deux méthodes est la plus rapide ?
4. Le point Q engendre-t-il le groupe $H(\mathbb{F}_{90000049})$?