N1MA8W04 – Courbes Elliptiques – Master CSI - année 2012/13
Examen: partie théorique
Corrigé

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 $x \in \mathbb{F}_q$.*

   (a) Puisque $\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{Z}$, le produit $k!(p-k)!$ divise $p! = p \cdot (p-1)!$. Pour $1 \leq k \leq p-1$ on a $\mathrm{pgcd}(p, k!(p-k)!) = 1$, ce qui implique que $k!(p-k)!$ divise $(p-1)!$, et donc

   $$\binom{p}{k} = \frac{p!}{k!(p-k)!} = p\frac{(p-1)!}{k!(p-k)!}$$

   est divisible par p.

   (b) On a

   $$(x+y)^p = x^p + y^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k}.$$

   La question précédente implique qu'en caractéristique p la dernière somme est nulle, ce qui montre $(x+y)^p = x^p + y^p$. On déduit de ceci que $(x+y)^{p^k} = x^{p^k} + y^{p^k}$ par récurrence simple sur k:

   $$(x+y)^{p^k} = \left((x+y)^{p^{k-1}}\right)^p = \left(x^{p^{k-1}} + y^{p^{k-1}}\right)^p = x^{p^k} + y^{p^k}.$$

   (c) i. On a $(xy)^q = x^q y^q$ et $(x+y)^q = x^q + y^q$ par la question précédente. Ceci démontre que notre application est morphisme de corps.
   Si $x^q = 0$ alors $x = 0$ ce qui montre que le noyau de notre morphisme est nul, donc il est injectif.
   Puisque $\bar{\mathbb{F}}_q$ est algébriquement clos, pour tout $y \in \bar{\mathbb{F}}_q$ on trouve $x \in \bar{\mathbb{F}}_q$ tel que $x^q = y$; il est donc surjectif. Nous avons donc un isomorphisme.

   ii. Le groupe multiplicatif $\mathbb{F}_q^\times$ est d'ordre $q-1$ ce qui montre que pour tout $x \in \mathbb{F}_q^\times$ on a $x^{q-1} = 1$. Ceci implique que $\mathbb{F}_q \subset \{\text{racines de } x^q - x\}$. Puisque le polynôme $x^q - x$ ne peut pas avoir plus de q racines, on a en fait $\mathbb{F}_q = \{\text{racines de } x^q - x\}$.

2. **Frobenius sur les courbes elliptiques** *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 $m_1 = m_2$.*

   (a) Pour $P = (x, y)$ on a $\phi_q(P) = (x^q, y^q)$.

   (b) Le premier énoncé est démontré par récurrence simple sur k:

   $$\phi_q^k(P) = \phi_q(\phi_q^{k-1}(P)) = \phi_q(\phi_{q^{k-1}}(P)) = \phi_q(x^{q^{k-1}}, y^{q^{k-1}}) = (x^{q^k}, y^{q^k}) = \phi_{q^k}(P).$$

   Le deuxième énoncé est une conséquence immédiate de la question 1c:ii.

   (c) Supposons $m \neq 0$. Puisque ϕ_q est surjectif, « $m\phi_q(P) = O$ pour tout $P \in E$ » implique que $mP = O$ pour tout $P \in E$; autrement dit, $E = E[m]$. Mais E est un ensemble infini, tandis que $E[m]$ est fini, contradiction.
   Si $m_1\phi_q = m_2\phi_q$ alors $(m_1 - m_2)\phi_q = 0$, et donc $m_1 - m_2 = 0$ comme on a vu tout à l'heure.

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.*

   (a) On a $a = \alpha + \beta$ et $q = \alpha\beta$, ce qui montre que $b_2 = \alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = a^2 - 2q$.
   Puis, en multipliant les relations $\alpha^2 = a\alpha - q$ et $\beta^2 = a\beta - q$ respectivement par α^{k-1} et β^{k-1}, on obtient $\alpha^{k+1} = a\alpha^k - q\alpha^{k-1}$ et $\beta^{k+1} = a\beta^k - q\beta^{k-1}$. La somme des deux dernières identités nous donne $b_{k+1} = ab_k - qb_{k-1}$.
   Finalement, on montre par récurrence sur k que $b_k \in \mathbb{Z}$. On a $b_1 = a \in \mathbb{Z}$ et $b_2 = a^2 - 2q \in \mathbb{Z}$; puis, si $b_{k-1}, b_k \in \mathbb{Z}$, alors $b_{k+1} = ab_k - qb_{k-1} \in \mathbb{Z}$.

   (b) On a
   $$(X^k - \alpha^k)(X^k - \beta^k) = X^{2k} - (\alpha^k + \beta^k)X^k + (\alpha\beta)^k = X^{2k} - b_kX^k + q^k,$$
   ce qui implique que α et β sont des racines de $X^{2k} - b_kX^k + q^k$. Ceci montre que le polynôme $X^2 - aX + q = (X - \alpha)(X - \beta)$ divise $X^{2k} - b_kX^k + q^k$.

   (c) Écrivons $X^{2k} - b_kX^k + q^k = (X^2 - a_qX + q)(X^{2k-2} + c_{2k-3}X^{2k-3} + \cdots + c_1X + c_0)$. Alors
   $$\begin{aligned}\phi_{q^k}^2 - b_k\phi_{q^k} + q\,\mathrm{Id} &= \phi_q^{2k} - b_k\phi_q^k + q\,\mathrm{Id} \qquad (\text{parce que } \phi_{q^k} = \phi_q^k)\\ &= (\phi_q^2 - a_q\phi_q + q\,\mathrm{Id})(\phi_q^{2k-2} + c_{2k-3}\phi_q^{2k-3} + \cdots + c_1\phi_q + c_0\,\mathrm{Id})\\ &= 0 \qquad (\text{parce que } \phi_q^2 - a_q\phi_q + q\,\mathrm{Id} = 0).\end{aligned}$$
   De $\phi_{q^k}^2 - b_k\phi_{q^k} + q\,\mathrm{Id} = 0$ et $\phi_{q^k}^2 - a_{q^k}\phi_{q^k} + q\,\mathrm{Id} = 0$ on déduit que $b_k\phi_{q^k} = a_{q^k}\phi_{q^k}$, ce qui implique $a_{q^k} = b_k = \alpha^k + \beta^k$. Ceci démontre le théorème de Weil.

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 $E(\mathbb{F}_{5^4})$~~[1].*

[1] C'est une erreur dans le sujet: il est trop difficile de déterminer la structure du groupe $E(\mathbb{F}_{5^4})$ sans ordinateur. Tout étudiant aura 1 point de bonus pour compenser cette faute.

(a) Pour $x = 0$ on trouve $y^2 = 0^2 + 2 \cdot 0 = 0$, et on obtient le point $(0, 0) \in E(\mathbb{F}_5)$. Pour $x = 1$ on trouve $y^2 = 3$ et donc il n'y a pas de point dans $E(\mathbb{F}_5)$ avec $x = 1$. De la même façon on vérifie qu'il n'y a pas de points avec $x = 2, 3, 4$. On conclut que $(0, 0)$ est le seul point fini dans $E(\mathbb{F}_5)$, et donc

$$N_5 = |E(\mathbb{F}_5)| = 2, \qquad a_5 = 5 + 1 - 2 = 4.$$

Les racines du polynôme $X^2 - 4X + 5$ sont $2 \pm i$. Par le théorème de Weil $a_{5^k} = (2 - i)^k + (2 + i)^k$. En particulier,

$$\begin{aligned} a_{5^2} &= (2-i)^2 + (2+i)^2 = 6, & N_{5^2} &= 5^2 + 1 - 6 = 20, \\ a_{5^3} &= (2-i)^3 + (2+i)^3 = 4, & N_{5^3} &= 5^3 + 1 - 4 = 122, \\ a_{5^4} &= (2-i)^4 + (2+i)^4 = -14, & N_{5^2} &= 5^4 + 1 + 14 = 640. \end{aligned}$$

(b) Le groupe $E(\mathbb{F}_5)$ est le groupe à 2 éléments: $E(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z}$.

En général on sait d'après le cours que $E(\mathbb{F}_q) \cong \mathbb{Z}/m1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$ avec $m_1 \mid m_2$. En particulier, m_1^2 divise $N_q = |E(\mathbb{F}_q)|$.

Dans le cas $q = 5^3$ on a $m_1^2 \mid 122 = 2 \cdot 61$, ce qui implique que $m_1 = 1$ et $m_2 = 122$. On a donc $E(\mathbb{F}_{5^3}) \cong \mathbb{Z}/122\mathbb{Z}$, un groupe cyclique.

(c) Les racines du polynôme $x^3 + 2x$ appartiennent au corps $\mathbb{F}_5(\sqrt{-2}) = \mathbb{F}_{5^2}$, ce qui implique que $E[2] \subset E(\mathbb{F}_{5^2})$.

(d) En utilisant les notations ci-dessus, on a $m_1^2 \mid 20$, d'où $m_1 = 1$ ou $m_1 = 2$. Si $m_1 = 1$ alors le groupe $E(\mathbb{F}_{5^2})$ est cyclique. Mais il contient le sous groupe $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, un groupe non cyclique. Puisque tout sous groupe d'un groupe cyclique est forcément cyclique, on ne peut pas avoir $m_1 = 1$. On obtient $m_1 = 2$ et $m_2 = 10$, et donc $E(\mathbb{F}_{5^2}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$.