TD3 - Courbes elliptiques sur les corps finis

Exercice 1. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$. On pose $\chi_E = T^2 - t_E T + q \in \mathbb{Z}[T]$ le polynôme caractéristique de E, α et β ses racines, $t_E = \alpha + \beta$ la trace de E et ϕ_q le morphisme de Frobenius. On considère la suite $s_n = \alpha^n + \beta^n$.

1. Justifier que $\beta = \overline{\alpha}$.
2. Montrer que $|\alpha| = |\beta| = \sqrt{q}$.
3. Montrer que pour tout $n \geq 1$ on a
$$s_{n+1} = t_E s_n - q s_{n-1}.$$
4. Montrer que pour tout $n \geq 1$ le polynôme $T^{2n} - s_n T^n + q^n$ est divisible par $T^2 - t_E T + q$. En déduire que la trace de $\phi_{q^n} = \phi_q^n$ est égale à s_n et que
$$\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n).$$
5. On considère la série formelle définie par
$$\zeta(T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right).$$
Montrer que $\zeta(T) = \dfrac{1 - t_E T + qT^2}{(1-T)(1-qT)}$.

Note d'ouverture : Plus généralement, pour une courbe C lisse de genre g définie sur un corps fini $\mathbb{F}_q$ on peut poser $\zeta(T) = \exp\left(\sum_{n=1}^{\infty} \#E(\mathbb{F}_{q^n}) \frac{T^n}{n}\right)$ et il existe un polynôme f de degré $2g$ dont les racines dans $\mathbb{C}$ sont de module $\sqrt{q}$ tel que
$$\zeta(T) = \frac{f(T)}{(1-T)(1-qT)}.$$
Il s'agit des conjectures de Weil et de l'hypothèse de Riemann sur les corps finis (qui malgré leurs noms sont des résultats démontrés). À l'instar des courbes elliptiques, la connaissance de f permet donc de déterminer le nombre de points rationnels de C sur toutes les extensions finies de $\mathbb{F}_q$.

Exercice 2. Soit E une courbe elliptique de trace t_E définie sur un corps fini $\mathbb{F}_q$ avec $q = p^r$. On considère la suite s_n de l'Exercice 1.

1. Montrer que pour $n \geq 1$ on a $s_n = t_E^n \mod p$. En déduire que pour tout $n \geq 1$ on a $\#E(\mathbb{F}_{q^n}) = 1 - t_E^n \mod p$.
2. Montrer que si $t_E = 0 \mod p$ alors E est supersingulière.
3. On suppose que $t_E \neq 0 \mod p$.
   (a) À l'aide du petit théorème de Fermat, montrer que $E(\mathbb{F}_{q^{p-1}})$ contient un élément d'ordre p.
   (b) En déduire que E n'est pas supersingulière.
4. On suppose que $q = p$ (i.e. $r = 1$) et $p \geq 5$.
   (a) Montrer que E est supersingulière si, et seulement si $t_E = 0$.
   (b) Montrer que :
   Si n est impair : $\#E(\mathbb{F}_{p^n}) = p^n + 1$.
   Si n est pair : $\#E(\mathbb{F}_{p^n}) = \left(p^{n/2} - (-1)^{n/2}\right)^2$.

Exercice 3. Soit $K = \mathbb{F}_{49} = \mathbb{F}_7[i] \simeq \mathbb{F}_7[X]/\langle X^2 + 1\rangle$. On considère la courbe elliptique $E\colon y^2 = x^3 - (1+i)x$.

1. Montrer que $(4+i)^2 = 1 + i$. En déduire que $X^3 - (1+i)X \in K[X]$ est scindé dans K et que $E(K)$ contient toute la 2-torsion.

2. Montrer que le polynôme de 3 division de E est $\psi_3 = 3(X^4 + 2(1+i)X^2 + 4i)$.
3. Montrer que
$$\psi_3 = 3(X + (1-i))(X - (1-i))(X - 3i)(X + 3i).$$
4. En déduire que tous les points de 3-torsion ont leur abscisse dans K. On admet qu'il en est de même pour les ordonnées.
5. Montrer que $E(K)$ contient un sous-groupe isomorphe à $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
6. Montrer que $E(K) \simeq \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.
7. Montrer que $\chi_E = (T-7)^2$. En déduire que ϕ_{49}, le morphisme de Frobenius de E, satisfait $\phi_{49} = [7]$ (c'est la multiplication par 7 dans E).
8. Montrer que
$$\begin{array}{rccc} \phi\colon & E & \longrightarrow & E \\ & (x,y) & \longmapsto & (-x, iy) \end{array}$$
est un inversible de $\mathrm{End}(E)$ d'ordre 4 dans $\mathrm{End}(E)^\times = \mathrm{Aut}(E)$. En déduire que $\mathrm{End}(E) \not\simeq \mathbb{Z}$.
9. On souhaite déterminer s'il existe une courbe E_0 sur $\mathbb{F}_7$ telle que E et E_0 sont isomorphes sur K.
   (a) Montrer que si E_0 existe elle doit être supersingulière. Que vaut alors $\#E_0(\mathbb{F}_7)$?
   (b) Montrer qu'on doit alors avoir $\#E_0(K) = 64$.
   (c) Conclure.

Exercice 4. Soit r une puissance d'un nombre premier et $q = r^2$. Soit E une courbe elliptique sur $\mathbb{F}_q$ telle que $\#E(\mathbb{F}_q) = (r-1)^2$ et ϕ_q l'endomorphisme de Frobenius de E.

1. Montrer que $(\phi - [r])^2 = 0$.
2. En déduire que $\phi = [r]$.
3. Montrer que pour tout $P \in E(\mathbb{F}_q)$ on a $(r-1)P = O = [0\colon 1\colon 0]$.
4. En déduire que $E(\mathbb{F}_q) \simeq \mathbb{Z}/(r-1)\mathbb{Z} \times \mathbb{Z}/(r-1)\mathbb{Z}$.