Feuille d'exercices n° 6

Exercice 1. Soit E une courbe elliptique sur $\mathbb{F}_q$ avec $q = p^r$. Notons $a = \phi_q + \hat{\phi}_q \in \mathbb{Z}$.

1. Montrer que E est supersingulière si et seulement si $a \equiv 0$ modulo p.
2. Supposons $q = p \geq 5$. Montrer que E est supersingulière si et seulement si $\mathrm{Card}(E(\mathbb{F}_p)) = p + 1$.
3. Supposons $q = p \geq 5$. Montrer que $\mathrm{Card}(E(\mathbb{F}_{p^n}))$ est égal à $p^n + 1$ si n est impair et à $(p^{n/2} - (-1)^{n/2})^2$ si n est pair.

Exercice 2. Soit $p \geq 3$, $q = p^r$ et E la courbe elliptique sur $\mathbb{F}_q$ d'équation $y^2 = f(x)$ avec $f \in \mathbb{F}_q[X]$ de degré 3 à racines distinctes dans $\bar{\mathbb{F}}_p$. On note $\chi : \mathbb{F}_q^* \to \{\pm 1\}$ le caractère qui vérifie $\chi(x) = 1$ si et seulement si x est un carré dans $\mathbb{F}_q^*$. On l'étend en une application multiplicative $\chi : \mathbb{F}_q \to \mathbb{N}$ en posant $\chi(0) = 0$.

1. Montrer que $\mathrm{Card}(E(\mathbb{F}_q)) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x))$.
2. Vérifier que $\chi(x) = x^{(q-1)/2} \in \mathbb{F}_q$.
3. Montrer que $\sum_{x \in \mathbb{F}_q} x^i$ est égal à -1 si $(q-1)|i$ et à 0 sinon.
4. En déduire que si A_{p^s} est le coefficient de x^{p^s-1} dans $f(x)^{(p^s-1)/2}$ pour tout $s \geq 1$ on a
$$\mathrm{Card}(E(\mathbb{F}_q)) = 1 - A_q \in \mathbb{Z}/p\mathbb{Z}\,.$$
5. En déduire que E est supersingulière si et seulement si $A_q = 0$.
6. Montrer que $A_{p^{s+1}} = A_{p^s} \cdot A_p^{p^s}$.
7. En déduire finalement que E est supersingulière si et seulement $A_p = 0$.
8. Si $f(x) = x^3 - x$ que E est supersingulière si et seulement si $p \equiv 3 \bmod 4$.
9. Posons $m = (p-1)/2$ et
$$H_p(t) = \sum_{i=0}^{m} \left(C_m^i\right)^2 \cdot t^i \ \in \mathbb{F}_q[t]\,.$$
Posons $f(x) = x(x-1)(x-\lambda)$ avec $\lambda \in \mathbb{F}_q$. On considère donc les courbes elliptiques sous forme de Legendre. Montrer que $A_p = (-1)^m \cdot H_p(\lambda)$.
10. Soit $\mathcal{D}$ l'opérateur différentiel $4t(1-t) \cdot \partial^2 + 4(1-2t) \cdot \partial - 1$ agissant sur $\mathbb{F}_q[t]$. Montrer que $\mathcal{D}(H_p) = 0$.
11. En déduire que H_p a des racines distinctes dans $\bar{\mathbb{F}}_q$.
12. En déduire une estimation du nombre de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$.