INTRODUCTION À L'ARITHMÉTIQUE DES COURBES ELLIPTIQUES
MASTER 2 – SORBONNE UNIVERSITÉ (2024)
FEUILLE DE TD 4

On fixe un nombre premier $p \geq 3$, K un corps parfait de caractéristique p. Soit E une courbe elliptique sur K.

Rappelons que

$$|\mathrm{E}[p](\bar{\mathrm{K}})| = \deg_s[p] = \deg_s(\hat{\phi} \circ \phi) = \deg_s(\hat{\phi}) \tag{1}$$

où $\phi : \mathrm{E} \to \mathrm{E}$ désigne le p-Frobenius (une isogénie purement inséparable de degré p) et $\hat{\phi}$ l'isogénie duale. Alors $\deg_s(\hat{\phi})$ divise $\deg(\hat{\phi}) = \deg(\phi) = p$ et donc $\deg_s(\hat{\phi}) \in \{1, p\}$. En conséquence

$$\mathrm{E}[p](\bar{\mathrm{K}}) \in \{(0), \mathbb{Z}/p\mathbb{Z}\}.$$

Definition. On dit que E est *supersingulière* si E n'a pas de point de p-torsion, autrement dit si $\mathrm{E}[p](\bar{\mathrm{K}}) = (0)$; ou, de manière équivalente, si $\hat{\phi}$ est inséparable. Sinon, on dit que E est *ordinaire*.

Exercice 1. On suppose ici que $\mathrm{K} = \mathbb{F}_q$ est un corps fini et que la partie affine de E est représentée par l'équation $y^2 = f(x)$ où $f(x) \in \mathbb{F}_q[x]$ est un polynôme de degré 3 à racines distinctes.

(1) Soit $\chi : \mathbb{F}_q \to \mathbb{Z}$ l'unique application valant 0 sur 0, 1 sur les carrés non nuls et -1 ailleurs. Montrer que
$$|\mathrm{E}(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(f(x)).$$
En déduire que $|\sum_{x \in \mathbb{F}_q} \chi(f(x))| \leq 2\sqrt{q}$.

(2) Déduire de la formule précédente que $|\mathrm{E}(\mathbb{F}_q)| \equiv 1 - \mathrm{A}_q$ dans $\mathbb{F}_q$, où $\mathrm{A}_q \in \mathbb{F}_q$ est le coefficient du monôme x^{q-1} dans l'écriture canonique du polynôme $f(x)^{\frac{q-1}{2}}$.

(3) Soit $\mathrm{A}_p \in \mathbb{F}_q$ le coefficient du monôme x^{p-1} dans l'écriture canonique du polynôme $f(x)^{\frac{p-1}{2}}$. Montrer que $\mathrm{A}_p = 0$ si, et seulement si $\mathrm{A}_q = 0$.

(4) En déduire que E est supersingulière si, et seulement si le polynôme $f(x)^{\frac{p-1}{2}}$ n'a pas de terme en x^{p-1}.

Solution: (1) Il s'agit de compter les points sur E : on compte le point O à l'infini et, pour $x \in \mathbb{F}_q$, les points sur la partie affine d'abscisse x :

- si $f(x) = 0$ alors $(x, 0)$ est un $\mathbb{F}_q$-point de E,
- si $f(x)$ est un carré non nul, e.g. $f(x) = y^2$ alors (x, y) et $(x, -y)$ sont deux points distincts de E,
- si $f(x)$ n'est un carré non nul, alors il n'y a pas de points d'abscisse x.

En formule :
$$|\mathrm{E}(\mathbb{F}_q)| = 1 + \sum_{x \in \mathbb{F}_q} (1 + \chi(x)) = 1 + q + \sum_{x \in \mathbb{F}_q} \chi(x).$$
D'après la borne de Hasse, on a donc
$$\left| \sum_{x \in \mathbb{F}_q} \chi(x) \right| = ||\mathrm{E}(\mathbb{F}_q)| - 1 - q| \leq 2\sqrt{q}.$$
(2) On considère le polynôme $\mathrm{P}(\mathrm{Z}) = \mathrm{Z}^{\frac{q-1}{2}} - 1$ dans $\mathbb{F}_q$, où il a au plus $\frac{q-1}{2}$ racines. Si $z \neq 0$ admet une racine carrée dans $\mathbb{F}_q$, alors $\mathrm{P}(z) = 0$ par le petit théorème de Fermat. Comme il y au moins $\frac{p-1}{2}$ carré dans $\mathbb{F}_q^\times$, on trouve
$$\{\text{racines de } \mathrm{P}(\mathrm{Z}) \text{ dans } \mathbb{F}_q\} = (\mathbb{F}_q^\times)^2.$$
On en déduit $\chi(z) \equiv z^{\frac{q-1}{2}}$ dans $\mathbb{F}_q$. En particulier,
$$|\mathrm{E}(\mathbb{F}_q)| \equiv 1 + \sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}}.$$
Comme $\mathrm{S}_i := \sum_{x \in \mathbb{F}_q} x^i = 0$ si $q - 1 \nmid i$ et -1 sinon, et que $f(x)^{\frac{q-1}{2}}$ est de degré $\leq \frac{3}{2}(q-1)$, on trouve bien $|\mathrm{E}(\mathbb{F}_q)| \equiv 1 - \mathrm{A}_q$.

(3) Comme $f(x)^{\frac{p^{r+1}-1}{2}} = f(x)^{\frac{p^r-1}{2}} f(x)^{p^r\left(\frac{p-1}{2}\right)}$, en se rappelant que f est de degré 3, on trouve $\mathrm{A}_{p^{r+1}} = \mathrm{A}_{p^r}\mathrm{A}_p^{p^r}$. Le résultat se déduit alors par récurrence sur r.
(4) Soit a l'entier $|\mathrm{E}(\mathbb{F}_q)| - 1 - q$. Alors $a = 1 + \deg(\phi) - \deg(1-\phi)$ et alors

$$[a] = 1 + [\deg(\phi)] - [\deg(1-\phi)] = 1 + \phi\circ\hat{\phi} - (1-\phi)\circ(1-\hat{\phi}) = \phi + \hat{\phi}.$$

Comme $a \equiv \mathrm{A}_q$ dans $\mathbb{F}_q$, on a $p \nmid a$ si, et seulement si $\mathrm{A}_p \equiv 0$ dans $\mathbb{F}_q$. Ainsi, E est supersingulière si, et seulement si $\hat{\phi} = a - \phi$ est inséparable si, et seulement si $p \nmid a$ si, et seulement si, $\mathrm{A}_p \equiv 0$.

Exercice 2. On considère le *polynôme de Hasse* (ou *invariant de Hasse*)

$$\mathrm{H}_p(t) := \sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}^2 t^i.$$

(1) En utilisant l'Exercice 1, montrer qu'une courbe elliptique sous la *forme de Legendre* $\mathrm{E}_\lambda : y^2 = x(x-1)(x-\lambda)$ (où $\lambda \in \bar{\mathbb{F}}_p \setminus \{0,1\}$) est supersingulière si, et seulement si $\mathrm{H}_p(\lambda) = 0$.
(2) Soit D l'opérateur différentiel $\mathrm{D}(f) := 4t(1-t)\partial_t^2(f) + 4(1-2t)\partial_t(f) - f$. Montrer que $\mathrm{D}(\mathrm{H}_p) \equiv 0$ modulo p. En déduire que H_p est à racines simples dans $\mathbb{F}_p$.

Si $p \geq 5$, on pourra admettre que E_λ a pour j-invariant

$$j(\mathrm{E}_\lambda) := j(\lambda) := 256 \cdot \frac{\lambda^2 - \lambda + 1}{\lambda^2(1-\lambda)^2}$$

et qu'un point générique de $\bar{\mathbb{F}}_p$ admet six antécédants par l'application $\lambda \mapsto j(\lambda)$ sauf 0 et 1728 qui en admettent respectivement 2 et 3.

(3) On suppose $p \geq 5$. Montrer que le nombre de courbes supersingulières sur $\mathbb{F}_p$ correspond à

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(0)\right) + \varepsilon_p(0) + \varepsilon_p(1728)$$

où $\varepsilon_p(j)$ est égal à 1 si la courbe elliptique de j-invariant j est supersingulière et 0 si elle est ordinaire.
(4) En déduire que le nombre de courbes elliptiques supersingulières sur $\bar{\mathbb{F}}_p$ est égal à

$$\begin{cases} 1 & \text{si } p = 3, \\ \lfloor \frac{p}{12} \rfloor & \text{si } p \equiv 1 \pmod{12}, \\ \lfloor \frac{p}{12} \rfloor + 1 & \text{si } p \equiv 5, 7 \pmod{12}, \\ \lfloor \frac{p}{12} \rfloor + 2 & \text{si } p \equiv 11 \pmod{12}. \end{cases}$$

On pourra utiliser que les équations $y^2 = x^3 + 1$ et $y^2 = x^3 + x$ définissent des courbes elliptiques de j-invariant 0 et 1728 respectivement.

Solution: (1) Le coefficient de x^{p-1} du polynôme $(x(x-1)(x-\lambda))^{\frac{p-1}{2}}$ correspond au coefficient de $x^{\frac{p-1}{2}}$ du polynôme $((x-1)(x-\lambda))^{\frac{p-1}{2}}$, c'est-à-dire

$$\sum_{i=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{i}(-t)^i \binom{\frac{p-1}{2}}{\frac{p-1}{2} - i}(-1)^{\frac{p-1}{2}-i}$$

qui ne diffère de $\mathrm{H}_p(t)$ que d'un facteur $(-1)^{\frac{p-1}{2}}$.
(2) On vérifie que

$$(\mathrm{DH}_p)(t) = p\sum_{i=0}^{\frac{p-1}{2}} (p-2-4i)\binom{\frac{p-1}{2}}{i}^2 t^i \equiv 0 \pmod{p}.$$

On en déduit que si λ est racine double de H_p, alors soit $\lambda = 0$ ou 1, ou bien λ est racine triple. Le dernier cas est impossible car, en dériviant successivement la relation $\mathrm{DH}_p(t) = 0$ on trouverait que λ est racine d'odre arbitraire. Les deux premiers cas sont également impossibles car

$$\mathrm{H}_p(0) = 1, \quad \text{et} \quad \mathrm{H}_p(1) = \binom{p-1}{\frac{p-1}{2}} \neq 0 \pmod{p},$$

Donc H_p n'a pas de racines doubles.
(3) Le nombre de courbes elliptiques sur $\bar{\mathbb{F}}_p$ supersingulières à isomorphisme près est donné par

$$\#\{j(\lambda) \mid \mathrm{E}_\lambda \text{ supersingulière}\} = \#\{j(\lambda) \neq 0, 1728 \mid \mathrm{E}_\lambda \text{ supersingulière}\} + \varepsilon_p(0) + \varepsilon_p(1728).$$

Comme $p \geq 5$, on a

$$\begin{aligned}\#\{j(\lambda) \neq 0, 1728 \mid \mathrm{E}_\lambda \text{ supersingulière}\} &= \frac{1}{6}\#\left(\{\lambda \mid \mathrm{E}_\lambda \text{ supersinglière}\} \setminus j^{-1}(0) \sqcup j^{-1}(1728)\right) \\ &= \frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right).\end{aligned}$$

(4) On suppose $p \geq 5$. Il suffit de déterminer, en utilisant le critère de l'Exercice 1, les premiers $p \geq 5$ pour lesquels on a $\varepsilon_p(0) = 1$ et ceux tels que $\varepsilon_p(1728) = 1$. Pour la première courbe, d'équation $y^2 = x^3 + 1$, on a que $(x^3+1)^{\frac{p-1}{2}}$ n'a pas de coefficient en x^{p-1}, a moins que $p \equiv 1 \pmod 3$ auquel cas ce coefficient est

$$\binom{\frac{p-1}{2}}{\frac{p-1}{3}}.$$

Ce coefficient n'est pas nul modulo p. On en déduit que la courbe de j-invariant nul est supersingulière si, et seulement si $p \equiv 1 \pmod 3$.
De même, pour la courbe $y^2 = x^3 + x$ de j-invariant 1728, le coefficient de x^{p-1} dans $(x^3+x)^{\frac{p-1}{2}}$ est égal au coefficient de $x^{\frac{p-1}{2}}$ dans $(x^2+1)^{\frac{p-1}{2}}$, ce coefficient n'étant non nul que si $p \equiv 1 \pmod 4$ auquel cas il correspond à

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}}$$

qui est non nul modulo p, toujours par Lucas.
Si $p = 3$, $\mathrm{H}_p(t) = 1 + t$ et alors il n'y a q'une seule courbe elliptique supersingulière, de j-invariant est $j(-1) = 1728$.