Sur les valeurs du polynôme de Deuring modulo p

Pierre Chrétien

Janvier 2026

1 Position du problème

Soit $p \geq 3$ premier. Soit

$$E_\lambda : y^2 = x(x-\lambda)(x-1), \qquad \lambda \in \mathbb{F}_p \setminus \{0,1\},$$

une courbe elliptique sous forme de Legendre. Il est bien connu (voir [Sil09], Theorem V.4.1) que E_λ est supersingulière si et seulement si λ est racine de

$$H_p(x) = \sum_{i=0}^{m} \binom{m}{i}^2 x^i = 0, \qquad \text{où } m = \frac{p-1}{2}.$$

Néanmoins, la répartition des valeurs de $H_p(x)$, $x \in \mathbb{F}_p$, est remarquable de symétrie. En effet, $H_p(\lambda)$ est intimement lié à la trace du Frobenius de $E_\lambda/\mathbb{F}_p$ d'une part et $|E_\lambda(\mathbb{F}_p)| \in 4\mathbb{Z}$ d'autre part (voir [AT02]).
Le but de ces notes personnelles est de clarifier en un seul document ces liens ainsi que d'expliquer certains arguments de [AT02]. En particulier on propose des versions complètes des preuves de [AT02] les plus élémentaires possibles, ne faisant pas référence à la 2-descente et en esquivant le plus possible la cohomologie galoisienne.

2 Comptage des points de E

Nous suivrons [Sil09] IV.4. Ici $q = p^r$, $p \geq 3$ et $r \geq 1$. Soit $E/\mathbb{F}_q : y^2 = f(x) = x^3 + ax^2 + bx + c$, avec

$$E(\mathbb{F}_q) = \{(x,y) \in \mathbb{F}_q^2 \mid y^2 = f(x)\} \cup \{\mathcal{O}\}.$$

Déterminons une expression de $|E(\mathbb{F}_q)|$. Soit

$$\begin{aligned} \chi : \ \mathbb{F}_q &\longrightarrow \{-1,0,1\} \\ y &\longmapsto \begin{cases} -1 & \text{si } y \notin (\mathbb{F}_q^\times)^2, \\ 0 & \text{si } y = 0, \\ 1 & \text{si } y \in (\mathbb{F}_q^\times)^2. \end{cases} \end{aligned}$$

On en déduit

$$|E(\mathbb{F}_q)| = \sum_{x \in \mathbb{F}_q} \big(1 + \chi(f(x))\big) + 1.$$

En effet

- $f(x) \notin (\mathbb{F}_q^\times)^2 \iff y^2 = f(x)$ n'a pas de solution sur $\mathbb{F}_q$;
- $f(x) = 0 \iff y^2 = f(x)$ a une solution sur $\mathbb{F}_q$;
- $f(x) \in (\mathbb{F}_q^\times)^2 \iff y^2 = f(x)$ a deux solutions distinctes sur $\mathbb{F}_q$.

De plus $\mathbb{F}_q^\times$ est cyclique et

$$\begin{aligned} \psi : \ \mathbb{F}_q^\times &\longrightarrow (\mathbb{F}_q^\times)^2 \\ x &\longmapsto x^2 \end{aligned}$$

a pour noyau $\mathrm{Ker}(\psi) = \{x \in \mathbb{F}_q^\times \mid x^2 = 1\} = \{\pm 1\}$ (car $q > 2$). Donc $\left|(\mathbb{F}_q^\times)^2\right| = \frac{q-1}{2}$ et $(\mathbb{F}_q^\times)^2$ est l'unique sous-groupe d'ordre $\frac{q-1}{2}$ de $\mathbb{F}_q^\times = \langle \alpha \rangle$, i.e. $(\mathbb{F}_q^\times)^2 = \langle \alpha^2 \rangle$.

Proposition 1. $\forall y \in \mathbb{F}_q,\ \chi(y) = y^{\frac{q-1}{2}}$ en tant qu'égalité dans $\mathbb{F}_q$.

Preuve. Tout d'abord, $\chi(0) = 0 = 0^{\frac{q-1}{2}}$.
Soit $y \in \mathbb{F}_q^\times$, $\chi(y) = 1 \iff y \in (\mathbb{F}_q^\times)^2 \iff y = (\alpha^2)^i,\ i \in \mathbb{Z} \iff y^{\frac{q-1}{2}} = 1$. Détaillons cette dernière équivalence.
Soit $y \in \mathbb{F}_q^\times$ tel que $y = (\alpha^2)^i$, alors $y^{\frac{q-1}{2}} = \alpha^{(q-1)i} = 1$ car $\langle \alpha \rangle = \mathbb{F}_q^\times$. Réciproquement,

$$y^{\frac{q-1}{2}} = 1 \Rightarrow o(y) \mid \frac{q-1}{2},$$

donc y est dans l'unique sous-groupe d'ordre $\frac{q-1}{2}$ du groupe cyclique $\mathbb{F}_q^\times$, c'est-à-dire $y \in (\mathbb{F}_q^\times)^2$.

□

Ainsi,

$$|E(\mathbb{F}_q)| = \sum_{x \in \mathbb{F}_q} (1 + \chi(f(x))) + 1 \qquad \text{dans } \mathbb{Z}.$$

$$\boxed{|E(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} f(x)^{\frac{q-1}{2}} \qquad (\dagger)} \qquad \text{dans } \mathbb{F}_q.$$

Proposition 2.

$$\sum_{x \in \mathbb{F}_q} x^i = \begin{cases} -1 & \text{si } q-1 \mid i, \\ 0 & \text{si } q-1 \nmid i. \end{cases}$$

Preuve. Vu que $\mathbb{F}_q^\times$ est cyclique d'ordre $q-1$, il suffit d'étudier les cas $0 \leq i < q-1$. Les polynômes de Newton sont $p_k = \sum_{j=1}^{q-1} x_j^k$ dans $\mathbb{F}_q[x_1, \ldots, x_{q-1}]$ et σ_k les polynômes symétriques élémentaires dans $\mathbb{F}_q[x_1, \ldots, x_{q-1}]$. Les relations de Newton donnent (voir [Fre01])

$$p_d = \sum_{k=1}^{d-1} (-1)^{k-1} \sigma_k p_{d-k} + (-1)^{d+1} d \sigma_d.$$

Puisque $\mathbb{F}_q = \{x \in \overline{\mathbb{F}_p} \mid x^q - x = 0\}$, $\mathbb{F}_q^\times = \{x \in \mathbb{F}_q \mid x^{q-1} - 1 = 0\}$, le polynôme $X^{q-1} - 1$ a pour fonctions symétriques élémentaires en ses racines $\sigma_1 = \cdots = \sigma_{q-2} = 0, \sigma_{q-1} = (-1)^q$.
Ici, $p_1 = p_2 = \cdots = p_{q-2} = 0$ et $p_{q-1} = \sum_{x \in \mathbb{F}_q} x^{q-1} = 0^{q-1} + \sum_{x \in \mathbb{F}_q^\times} x^{q-1} = 0 + \sum_{x \in \mathbb{F}_q^\times} 1 = q - 1 = -1$.

□

Donc dans la relation ($\dagger$) seuls les monômes de $f(x)^{\frac{q-1}{2}}$ de degré un multiple de $q-1$ contribuent à la somme. Or $\deg f(x) = 3$, donc

$$\deg f(x)^{\frac{q-1}{2}} = \frac{3}{2}(q-1)$$

et les seuls multiples entiers de $q-1$ dans $[0; \frac{3}{2}(q-1)]$ sont 0 et $q-1$. Si on note α le coefficient constant de $f(x)^{\frac{q-1}{2}}$ alors $\sum_{x \in \mathbb{F}_q} \alpha = q\alpha = 0$ donc seul le monôme de degré $q-1$ contribue dans la somme ($\dagger$). Soit A_q le coefficient de x^{q-1} dans $f(x)^{\frac{q-1}{2}}$. La discussion précédente fournit

$$\boxed{|E(\mathbb{F}_q)| = 1 - A_q \qquad \text{dans } \mathbb{F}_q}$$

Proposition 3. Pour tout $r \in \mathbb{N}$, en notant A_{p^r} le coefficient de $x^{p^r - 1}$ dans$f(x)^{\frac{p^r-1}{2}}$, on a

$$A_{p^{r+1}} = A_{p^r} \cdot A_p$$

Preuve. Soit

$$f(x) = x^3 + ax^2 + bx + c, \qquad a, b, c \in \mathbb{F}_q.$$

$$(*) \qquad f(x)^{\frac{p^{r+1}-1}{2}} = f(x)^{\frac{p^{r+1}-p^r+p^r-1}{2}} = f(x)^{\frac{p^r(p-1)}{2}} \cdot f(x)^{\frac{p^r-1}{2}} = \left(f(x)^{\frac{p-1}{2}}\right)^{p^r} \cdot f(x)^{\frac{p^r-1}{2}}$$

$$= \left[\sum_{i=0}^{\frac{3}{2}(p-1)} \alpha_i x^i\right]^{p^r} \cdot \left[\sum_{j=0}^{\frac{3}{2}(p^r-1)} \beta_j x^j\right] = \sum_{i=0}^{\frac{3}{2}(p-1)} \alpha_i^{p^r} x^{ip^r} \cdot \sum_{j=0}^{\frac{3}{2}(p^r-1)} \beta_j x^j$$

dont tout monôme est de la forme

$$\gamma_{ij} x^{ip^r + j}, \qquad i \in \left[\!\left[0, \tfrac{3}{2}(p-1)\right]\!\right],\ j \in \left[\!\left[0, \frac{3}{2}(p^r-1)\right]\!\right]$$

Étudions les solutions i, j d'une équation de la forme

$$(**) \qquad p^{r+1} - 1 = j + ip^r$$

On a

$$(**) \Rightarrow j = p^r(p-i) - 1 \ \Rightarrow \ j \equiv -1 \mod p^r$$

or

$$j = kp^r - 1 \leq \tfrac{3}{2}(p^r - 1) \Rightarrow 2kp^r - 2 \leq 3p^r - 3 \Rightarrow 1 \leq p^r(3-2k) \Rightarrow 3 - 2k \geq 0 \Rightarrow k \leq \tfrac{3}{2}.$$

De plus

$$0 \leq j = kp^r - 1 \Rightarrow kp^r \geq 1 \Rightarrow k > 0$$

Donc $k = 1$, i.e. $j = p^r - 1$. L'équation $(**)$ se lit alors

$$p^{r+1} - 1 = p^r - 1 + ip^r \Rightarrow p^{r+1} = p^r(i+1) \Rightarrow \quad i = p - 1.$$

En conclusion, dans le développement $(*)$, le coefficient $A_{p^{r+1}}$ du monôme de degré $p^{r+1} - 1$ de $f(x)^{\frac{p^{r+1}-1}{2}}$ ne provient que du produit des monômes de degré $p^r(p-1)$ (resp. $p^r - 1$) de $f(x)^{\frac{p^r(p-1)}{2}}$ (resp. $f(x)^{\frac{p^r-1}{2}}$). On a donc

$$A_{p^{r+1}} = A_{p^r} \cdot (A_p)^{p^r}.$$

$\square$

Proposition 4. Pour $q = p^n$

$$A_q = A_p^{\frac{q-1}{p-1}}.$$

3 Nombre de points rationnels d'une courbe sous forme de Legendre

3.1 Le polynôme de Deuring

Nous nous restreignons désormais au cas $q = p$ et

$$E_\lambda/\mathbb{F}_p : \quad y^2 = x(x-1)(x-\lambda), \qquad \lambda \in \mathbb{F}_p \setminus \{0, 1\}.$$

D'après le paragraphe précédent $|E_\lambda(\mathbb{F}_p)| = 1 - A_p \mod p$ où A_p est le coefficient de x^{p-1} de $(x(x-1)(x-\lambda))^{\frac{p-1}{2}}$. Posons $m = \frac{p-1}{2}$. Le coefficient de x^{p-1} de $[x(x-1)(x-\lambda)]^m$ est le coefficient de x^m de $(x-1)^m(x-\lambda)^m$. Or

$$(x-1)^m(x-\lambda)^m = \sum_{i=0}^{m} \binom{m}{i} (-1)^i x^{m-i} \cdot \sum_{j=0}^{m} \binom{m}{j} (-\lambda)^j x^{m-j}.$$

Les monômes de degré m de ce produit sont obtenus pour i et j tels que

$$m - i + m - j = m \iff m = i + j \iff j = m - i.$$

Le coefficient de x^m dans $(x-1)^m(x-\lambda)^m$ est donc

$$A_p = \sum_{j=0}^{m} \binom{m}{m-j} (-1)^{m-j} \binom{m}{j} (-\lambda)^j = (-1)^m \sum_{j=0}^{m} \binom{m}{j}^2 \lambda^j.$$

Donc

$$\boxed{|E_\lambda(\mathbb{F}_p)| = 1 - (-1)^m H_p(\lambda) \mod p}$$

où

$$H_p(X) = \sum_{i=0}^{m} \binom{m}{i}^2 X^i, \qquad m = \frac{p-1}{2}.$$

3.2 Cas $\lambda = 0$ et $\lambda = 1$

La courbe E_λ décrit une courbe elliptique si et seulement si $\lambda \notin \{0; 1\}$. Ces deux valeurs sont donc traitées de manière indépendante dans ce paragraphe. On a $\boxed{H_p(0) = 1}$. Déterminons

$$H_p(1) = \sum_{i=0}^{m} \binom{m}{i}^2 \qquad \mod p$$

Proposition 5.

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

Preuve. Soit $m \in \mathbb{N}$.

$$(1+x)^m (1+x)^m = (1+x)^{2m} \Longleftrightarrow \sum_{i=0}^{m} \binom{m}{i} x^i \cdot \sum_{j=0}^{m} \binom{m}{j} x^j = \sum_{k=0}^{2m} \binom{2m}{k} x^k.$$

Le coefficient de x^m de chaque membre vaut

$$\sum_{\substack{i+j=m \\ 0 \le i,j \le m}} \binom{m}{i}\binom{m}{j} = \binom{2m}{m} \Longleftrightarrow \sum_{i=0}^{m} \binom{m}{i}\binom{m}{m-i} = \binom{2m}{m} \Longleftrightarrow \sum_{i=0}^{m} \binom{m}{i}^2 = \binom{2m}{m}.$$

De plus

$$\binom{p-1}{i} \equiv (-1)^i \qquad \mod p, \qquad 0 \le i \le p-1.$$

En effet, $\binom{p-1}{0} = 1 \equiv (-1)^0 \mod p$ et $\binom{p-1}{p-1} = 1 \equiv (-1)^{p-1} \mod p$. De plus, pour $0 \le i \le p-2$,

$$\binom{p-1}{i} + \binom{p-1}{i+1} = \binom{p}{i+1} \equiv 0 \mod p$$

D'où $\binom{p-1}{i+1} \equiv -\binom{p-1}{i} \mod p$ qui donne $\binom{p-1}{i} \equiv (-1)^i \mod p$.

□

Proposition 6.

$$\boxed{H_p(1) = (-1)^{\frac{p-1}{2}} \quad \mod p}$$

On notera

$$H_p(1) \equiv 1 \quad \mod p \iff m \text{ est pair} \iff (-1)^{\frac{p-1}{2}} = 1 \iff -1 \in \mathbb{F}_p^2,$$

$$H_p(1) \equiv -1 \quad \mod p \iff m \text{ est impair} \iff (-1)^{\frac{p-1}{2}} = -1 \iff -1 \notin \mathbb{F}_p^2.$$

4 Courbes de Legendre et isogénies

On se limitera désormais au cas $p \ge 5$. Le comportement remarquable de $\{H_p(a),\ a \in \mathbb{F}_p \setminus \{0, 1\}\}$ et plus précisément de $(H_p(2), H_p(3), \ldots, H_p(p-1))$ provient de [AT02] et des résultats intermédiaires qui y sont exposés. On recopie le résultat principal de [AT02].

Théorème 1. Soit $E/\mathbb{F}_q$ une courbe elliptique. On note $q = r^2$, $r \in \mathbb{N}$, si q est un carré.

$$E \sim_{\mathbb{F}_q} E_\lambda, \quad \lambda \in \mathbb{F}_q \quad \iff \quad |E(\mathbb{F}_q)| \in 4\mathbb{Z} \setminus \{(r+1)^2\}$$

D'après le théorème d'isogénie de Tate,

$$E \sim_{\mathbb{F}_q} E_\lambda \quad \iff \quad |E(\mathbb{F}_q)| = |E_\lambda(\mathbb{F}_q)|$$

On a donc une description des ordres possibles pour $|E_\lambda(\mathbb{F}_q)|$ quand λ varie. Nous allons nous contenter de suivre la preuve de [AT02] et d'expliciter les points délicats dans le cas qui nous intéresse, à savoir $q = p$. Nous allons donc prouver le corollaire suivant.

Théorème 2. Soit $E/\mathbb{F}_p$ une courbe elliptique.

$$E \sim_{\mathbb{F}_p} E_\lambda, \quad \lambda \in \mathbb{F}_p \quad \iff \quad |E(\mathbb{F}_p)| \in 4\mathbb{Z}$$

4.1 Classes d'isomorphismes

Il est bien connu (voir [Sil09] III 1.7 et sa preuve)

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \quad \simeq_{\overline{\mathbb{F}}_p} \quad E_\gamma : y^2 = x(x-1)(x-\gamma)$$

$$\iff \quad \gamma \in \left\{\lambda,\ 1-\lambda,\ \frac{1}{\lambda},\ 1-\frac{1}{\lambda},\ \frac{1}{1-\lambda},\ 1-\frac{1}{1-\lambda}\right\}.$$

Ce qui donne une description complète des classes d'isomorphisme des courbes sous forme de Legendre. Néanmoins :

1. ce n'est une description que sur $\overline{\mathbb{F}}_p$,
2. la relation d'isomorphisme (même sur $\mathbb{F}_p$) n'est pas la bonne relation d'équivalence pour étudier $|E(\mathbb{F}_p)|$.

Théorème 3 (Tate)**.** Soient E_1, E_2 des courbes elliptiques sur $\mathbb{F}_q,\ q = p^n$. Il existe une isogénie $\mathbb{F}_q$-rationnelle $\varphi : E_1 \to E_2 \iff |E_1(\mathbb{F}_q)| = |E_2(\mathbb{F}_q)|$

La bonne relation d'équivalence à considérer pour le sujet qui nous intérese est donc $E_1 \sim_{\mathbb{F}_p} E_2$. Nous avons cependant besoin de comprendre un certain nombre de relations provenant d'isomorphismes sur $\mathbb{F}_p$. Nous collectons dans ce paragraphe des résultats sur ce sujet. À partir de maintenant, $E_1 \simeq E_2$ signifiera un isomorphisme $\mathbb{F}_p$-rationnel de courbes elliptiques $E_1/\mathbb{F}_p,\ E_2/\mathbb{F}_p$. De même, $E_1 \sim E_2$ signifiera une isogénie $\mathbb{F}_p$-rationnelle de courbes elliptiques $E_1/\mathbb{F}_p,\ E_2/\mathbb{F}_p$. La courbe

$$E_\lambda : y^2 = x(x-1)(x-\lambda), \qquad \lambda \in \mathbb{F}_p \setminus \{0;1\}$$

a toute sa 2-torsion $\mathbb{F}_p$-rationnelle

$$E_\lambda[2] = \{(0,0),(1,0),(\lambda,0),\mathcal{O}\} \subset E_\lambda(\mathbb{F}_p).$$

Proposition 7. Soit $E/\mathbb{F}_p : y^2 = x(x-\alpha)(x-\beta)$ une courbe elliptique.

$$\exists \lambda \in \mathbb{F}_p \quad / \quad E \simeq E_\lambda \iff \{\pm\alpha,\ \pm\beta,\ \pm(\alpha-\beta)\} \cap \mathbb{F}_p^2 \neq \emptyset$$

Dans ce cas on dit que E est *Legendre isomorphe.*

Preuve. Remarquons que $E/\mathbb{F}_p$ telle que $E[2] \subset E(\mathbb{F}_p)$ a un modèle $y^2 = (x-a)(x-b)(x-c),\ a,b,c \in \mathbb{F}_p$ et l'automorphisme

$$\begin{cases} x \mapsto x + a \\ y \mapsto y \end{cases}$$

ramène au modèle $E : y^2 = x(x-\alpha)(x-\beta),\ \alpha,\beta \in \mathbb{F}_p$. On traite donc dans cet énoncé des courbes elliptiques sur $\mathbb{F}_p$ ayant leur 2-torsion rationnelle. On étudie les isomorphismes de courbes elliptiques suivants

$$\begin{aligned} & y^2 = x(x-\alpha)(x-\beta) \ \simeq\ y^2 = x(x-1)(x-\lambda) \\ \iff \quad & y^2 = x^3 - (\alpha+\beta)x^2 + \alpha\beta x \ \simeq\ y^2 = x^3 - (1+\lambda)x^2 + \lambda x \end{aligned}$$

L'expression d'un isomorphisme de courbes elliptiques sous forme de Weiestrass est bien connue. Par exemple [Sil09] III, Table 3. fournit

$$\iff (S) : \begin{cases} u.0 = 2s \\ -u^2(\alpha+\beta) = -(1+\lambda) + 3R - \lambda s^2, \\ u^3 \cdot 0 = 2t, \\ u^4\alpha\beta = \lambda - 2R(1+\lambda) + 3R^2 - 2st, \\ u^6 \cdot 0 = R\lambda - R^2(1+\lambda) + R^3 - t^2. \end{cases} \qquad \iff (S) : \begin{cases} -u^2(\alpha+\beta) = -(1+\lambda) + 3R, \\ u^4\alpha\beta = \lambda - 2R(1+\lambda) + 3R^2, \\ 0 = R(\lambda - (1+\lambda)R + R^2). \end{cases}$$

Or $0 = R(\lambda - (1+\lambda)R + R^2) \iff R \in \{0, 1, \lambda\}$.

- Si $R = 0$:

$$(S) \iff \begin{cases} u^2(\alpha+\beta) = 1+\lambda, \\ u^4\alpha\beta = \lambda, \end{cases} \qquad \iff \qquad \begin{cases} \alpha+\beta = \dfrac{1}{u^2} + \dfrac{\lambda}{u^2}, \\ \alpha\beta = \dfrac{1}{u^2} \cdot \dfrac{\lambda}{u^2}. \end{cases} \quad \iff \{\alpha,\beta\} = \left\{\frac{1}{u^2}, \frac{\lambda}{u^2}\right\}.$$

- Si $R=\lambda$:

$$(S) \iff \begin{cases} u^2(\alpha+\beta) = 1-2\lambda, \\ u^4\alpha\beta = \lambda^2-\lambda, \end{cases} \iff \begin{cases} \alpha+\beta = \dfrac{-\lambda}{u^2} + \dfrac{1-\lambda}{u^2}, \\ \alpha\beta = \dfrac{-\lambda}{u^2}\cdot\dfrac{1-\lambda}{u^2}. \end{cases} \iff \{\alpha,\beta\} = \left\{\frac{-\lambda}{u^2}, \frac{1-\lambda}{u^2}\right\}.$$

Auquel cas $\alpha-\beta$ ou $\beta-\alpha$ vaut $\dfrac{1-\lambda}{u^2} - \dfrac{-\lambda}{u^2} = \dfrac{1}{u^2}$.

- Si $R=1$:

$$(S) \iff \begin{cases} u^2(\alpha+\beta) = \lambda-2, \\ u^4\alpha\beta = 1-\lambda, \end{cases} \iff \begin{cases} \alpha+\beta = \dfrac{-1}{u^2} + \dfrac{\lambda-1}{u^2}, \\ \alpha\beta = \dfrac{-1}{u^2}\cdot\dfrac{\lambda-1}{u^2}. \end{cases} \iff \{\alpha,\beta\} = \left\{\frac{-1}{u^2}, \frac{\lambda-1}{u^2}\right\}.$$

Auquel cas $-\alpha$ ou $-\beta$ vaut $\dfrac{1}{u^2}$.

□

Proposition 8. Soit $E/\mathbb{F}_p : y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ une courbe elliptique. Alors

$$(\gamma,0) \in 2E(\mathbb{F}_p) \iff \gamma-\alpha,\ \gamma-\beta \in (\mathbb{F}_p^\times)^2$$

Preuve. [AT02] renvoie à [Sil09] §X.1 qui traite de la 2-descente (dans le cas des corps de nombres donc) ou à [Sch95] qui n'énonce un résultat que pour les courbes hyperelliptiques. L'appendice A à la fin de cette note propose un exposé minimal des notions nécessaires, il s'agit encore de résultats bien connus.

□

4.2 Twists quadratiques

Définition 1. Soit $E/k : y^2 = f(x)$ une courbe elliptique. Soit $\alpha \in k^\times$ alors

$$E^{(\alpha)} : \alpha y^2 = f(x)$$

défini une courbe elliptique appelée *twist quadratique* de E par α.

Remarque 1.

1. Pour $\alpha \neq 1$, $\alpha y^2 = f(x) = x^3+ax^2+bx+c \simeq y^2 = x^3+\alpha a x^2+\alpha^2 bx+\alpha^3 c$ par

$$\varphi(x,y) = \left(\frac{x}{\alpha}, \frac{y}{\alpha^2}\right)$$

Notons que φ est un isomorphisme de courbes algébriques mais pas un isomorphisme de courbes elliptiques.

2. Le twist est trivial si et seulement si on a un isomorphisme k-rationnel de courbes elliptiques $E \simeq_k E^{(\alpha)}$.
3. Soit $E/\mathbb{F}_q$ et $\alpha \notin (\mathbb{F}_q^\times)^2$ alors $|E(\mathbb{F}_q)| + |E^{(\alpha)}(\mathbb{F}_q)| = q+2$.

Proposition 9. Soit E/k une courbe elliptique et $\alpha \in k^\times \setminus (k^\times)^2$.

$$E \simeq E^{(\alpha)} \implies j(E) = 1728 \quad \text{et} \quad k(\alpha) = k(\sqrt{-1})$$

Preuve. On suppose ici que $k=p \geq 5$ bien que le résultat reste vrai pour $p=3$. Cette restriction permet de donner un modèle de E/k sous forme de Weierstrass courte, ce qui simplifie l'expression de $j(E)$ et donc la preuve ci-dessous. Les formules pour $p=3$ sont disponibles dans [Sil09] Appendix A.
Soit

$$E/k : y^2 = x^3+Ax+B \quad \text{alors} \quad j(E) = 1728\,\frac{4A^3}{4A^3+27B^2}.$$

Si $E \simeq E^{(\alpha)}$, alors $E^{(\alpha)}$ a pour modèle $y^2 = x^3+\alpha^2 Ax+\alpha^3 B$. Un isomorphisme $\varphi : E \longrightarrow E^{(\alpha)}$ est de la forme $\varphi(x,y) = (u^2x, u^3y)$, $u \in (k^\times)$ et vérifie

$$\begin{cases} \dfrac{A}{u^4} = \alpha^2 A, \\ \dfrac{B}{u^6} = \alpha^3 B. \end{cases}$$

- Si $A \neq 0$ et $B \neq 0$, alors
$$\begin{cases} \alpha^2 = \dfrac{1}{u^4}, \\ \alpha^3 = \dfrac{1}{u^6}, \end{cases} \implies \alpha = \left(\frac{1}{u}\right)^2 \in (k^\times)^2.$$
ce qui est absurde.

- Si $A = 0$, alors $B \neq 0$ sinon E n'est pas lisse en $(0,0)$. On a
$$\alpha^3 = \frac{1}{u^6} \implies \alpha = \frac{1}{\alpha^2} \cdot \frac{1}{u^6} = \left(\frac{1}{\alpha u^3}\right)^2 \in (k^\times)^2.$$
ce qui est absurde.

- Donc $B = 0$, d'où $j(E) = 1728$. De plus $A \neq 0$, d'où $\alpha^2 = \frac{1}{u^4}$ donc $\alpha \in \{\frac{1}{u^2}; -\frac{1}{u^2}\}$. Or $\alpha \notin (k^\times)^2$ donc $\alpha = -\frac{1}{u^2}$. En particulier $k(\sqrt{\alpha}) = k(\sqrt{-1})$.

□

Proposition 10. $\forall \lambda \in \mathbb{F}_q \setminus \{0; 1\}$
$$E_\lambda^{(-1)} \simeq E_{1-\lambda} \qquad E_\lambda^{(\lambda)} \simeq E_{1/\lambda} \qquad E_\lambda^{(1-\lambda)} \simeq E_{\lambda/(\lambda-1)}$$

Preuve.
1. $E_\lambda : y^2 = x(x-1)(x-\lambda) = x^3 - (1+\lambda)x^2 + \lambda x$. Donc
$$E_\lambda^{(-1)} : y^2 = x^3 + (1+\lambda)x^2 + \lambda x = x(x+1)(x+\lambda).$$
Et $\varphi(x,y) = (x-1,\, y)$ fournit un isomorphisme $E_\lambda^{(-1)} \simeq E_{1-\lambda}$.
2. $E_\lambda^{(\lambda)} : y^2 = x^3 - (1+\lambda)\lambda x^2 + \lambda^3 x = x(x-\lambda)(x-\lambda^2)$ et $E_{1/\lambda} : y^2 = x(x-1)\left(x - \frac{1}{\lambda}\right)$. Donc $\varphi(x,y) = (\lambda^2 x,\, \lambda^3 y)$ fournit $E_\lambda^{(\lambda)} \simeq E_{1/\lambda}$.
3. $E_\lambda^{(1-\lambda)} : y^2 = x^3 - (1+\lambda)(1-\lambda)x^2 + \lambda(1-\lambda)^2 x = x(x-(1-\lambda))(x - \lambda(1-\lambda))$.
On vérifie que $\varphi(x,y) = \big((1-\lambda)^2 x + \lambda(1-\lambda),\ (1-\lambda)^3 y\big)$ fournit $E_\lambda^{(1-\lambda)} \simeq E_{\lambda/(\lambda-1)}$. En effet
$$\begin{aligned} & \varphi(y^2) = \varphi(x)\,\varphi(x-(1-\lambda))\,\varphi(x - \lambda(1-\lambda)) \\ \Leftrightarrow\ & (1-\lambda)^6 y^2 = \big[(1-\lambda)^2 x + \lambda(1-\lambda)\big]\big[(1-\lambda)^2 x + \lambda(1-\lambda) - (1-\lambda)\big]\big[(1-\lambda)^2 x\big] \\ \Leftrightarrow\ & y^2 = \left(x + \frac{\lambda}{1-\lambda}\right)\left(x + \frac{\lambda}{1-\lambda} - \frac{1}{1-\lambda}\right) x = x(x-1)\left(x - \frac{\lambda}{\lambda-1}\right). \end{aligned}$$

□

Proposition 11. Soit $\lambda \in \mathbb{F}_q \setminus \{0, 1, -1, 2, \frac{1}{2}\}$. Les assertions suivantes sont équivalentes :

(a) $E_\lambda \simeq E_\mu$ pour tout $\mu \in \left\{\lambda,\ 1-\lambda,\ \frac{1}{\lambda},\ 1 - \frac{1}{\lambda},\ \frac{1}{1-\lambda},\ \frac{\lambda}{\lambda-1}\right\}$.

(b) $-1,\ \lambda,\ 1-\lambda \in (\mathbb{F}_q^\times)^2$.

(c) $E_\lambda[4](\mathbb{F}_q) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Si $E_\lambda^{(\alpha)}/\mathbb{F}_q$ n'est pas Legendre isomorphe pour un $\alpha \in \mathbb{F}_q^\times$, alors les assertions précédentes sont satisfaites.

Preuve. L'hypothèse sur λ assure que $-1 \notin \left\{\lambda, \ldots, \frac{\lambda}{\lambda-1}\right\}$, donc $j(E_\lambda) \neq 1728$, (voir [Sil09] III 1.7).

(a) $\Rightarrow$ (b) Supposons que -1 ou λ ou $1-\lambda \notin (\mathbb{F}_q^\times)^2$. D'après la proposition 9, comme $j(E_\lambda) \neq 1728$
$$E_\lambda^{(-1)} \not\simeq E_\lambda \text{ ou } E_\lambda^{(\lambda)} \not\simeq E_\lambda \text{ ou } E_\lambda^{(1-\lambda)} \not\simeq E_\lambda.$$
Ce qui, avec la Proposition 10 contredit (a). Donc $-1,\ \lambda,\ 1-\lambda \in (\mathbb{F}_q^\times)^2$.

(b) $\Rightarrow$ (a) Si $\alpha \in (k^\times)^2$, alors $E^{(\alpha)} \simeq_k E$. Donc si $-1,\ \lambda,\ 1-\lambda \in (\mathbb{F}_q^\times)^2$

$$E_\lambda^{(-1)} \simeq E_\lambda, \qquad E_\lambda^{(\lambda)} \simeq E_\lambda, \qquad E_\lambda^{(1-\lambda)} \simeq E_\lambda.$$

Or

$$E_\lambda^{(-1)} \simeq E_{1-\lambda}, \qquad E_\lambda^{(\lambda)} \simeq E_{1/\lambda}, \qquad E_\lambda^{(1-\lambda)} \simeq E_{\lambda/(\lambda-1)}.$$

De plus $\frac{\lambda}{\lambda-1} = \frac{-\lambda}{1-\lambda} \in (\mathbb{F}_q^\times)^2$, donc

$$E_{\lambda/(\lambda-1)} \simeq E_{\lambda/(\lambda-1)}^{\lambda/(\lambda-1)} \simeq E_{(\lambda-1)/\lambda} \simeq E_{1-1/\lambda}.$$

Enfin, $1-\lambda \in (\mathbb{F}_q^\times)^2 \Rightarrow\ E_{1-\lambda} \simeq E_{1-\lambda}^{(1-\lambda)} \simeq E_{1/(1-\lambda)}$.

(b) $\Rightarrow$ (c) On a

$$0-1,\ 0-\lambda,\ 1-\lambda,\ 1-0,\ \lambda-0,\ \lambda-1 \in (\mathbb{F}_q^\times)^2.$$

D'après la Proposition 8, $(0,0),\ (1,0),\ (\lambda,0) \in 2E_\lambda(\mathbb{F}_q)$. Par exemple,

$$(0,0) = 2P_0, \qquad P_0 \in E_\lambda(\mathbb{F}_q),$$

et $-P_0 \in E_\lambda(\mathbb{F}_q)$. Or $P_0 \neq -P_0$, sinon $2P_0 = \mathcal{O}$, ce qui est absurde. Donc, $P_0 \in E_\lambda[4](\mathbb{F}_q)$ et $P_0, -P_0, 2P_0$ sont trois éléments distincts de $E_\lambda[4](\mathbb{F}_q)$. De même avec les points

$$(1,0) = 2P_1,\ \ (\lambda,0) = 2P_\lambda, \qquad P_1, P_\lambda \in E_\lambda[4](\mathbb{F}_q).$$

Donc $|E_\lambda[4](\mathbb{F}_q)| > 10$ et $E_\lambda[4](\mathbb{F}_q)$ est un sous-groupe de $E_\lambda[4](\overline{\mathbb{F}}_q) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Par conséquent

$$E_\lambda[4](\mathbb{F}_q) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

(c) $\Rightarrow$ (b) On a $E_\lambda[4](\mathbb{F}_q) = E_\lambda[4](\overline{\mathbb{F}}_q)$. De plus $[2] : E_\lambda(\overline{\mathbb{F}}_q) \to E_\lambda(\overline{\mathbb{F}}_q)$ est surjective. Ainsi,

$$\forall P \in E_\lambda[2](\overline{\mathbb{F}}_q), \quad \exists Q \in E_\lambda(\overline{\mathbb{F}}_q)\ /\ 2Q = P$$

Soit $P \in E_\lambda$ tel que $2P = \mathcal{O}$, et Q tel que $2Q = P$, en particulier $Q \in E_\lambda[4](\overline{\mathbb{F}}_q) = E_\lambda[4](\mathbb{F}_q)$ i.e. toute la 2-torsion est dans $2E_\lambda(\mathbb{F}_q)$. La proposition 8 assure

$$0-1,\ 0-\lambda,\ 1-0,\ 1-\lambda,\ \lambda-0,\ \lambda-1 \in (\mathbb{F}_q^\times)^2,$$

i.e.

$$-1,\ \lambda,\ 1-\lambda \in (\mathbb{F}_q^\times)^2.$$

Nous avons prouvé que les assertions (a), (b) et (c) sont équivalentes. Si $\alpha \in (\mathbb{F}_q^\times)^2$, alors $E_\lambda^{(\alpha)} \simeq E_\lambda$ donc $E_\lambda^{(\alpha)}$ est Legendre isomorphe. Supposons donc que $E_\lambda^{(\alpha)}$ ne soit pas Legendre isomorphe, en particulier $\alpha \notin (\mathbb{F}_q^\times)^2$. Supposons par l'absurde que $-1 \notin (\mathbb{F}_q^\times)^2$.

$$\left|\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^2\right| = 2\ \Rightarrow\ \frac{\alpha}{-1} \in (\mathbb{F}_q^\times)^2,$$

En notant $\delta^2 = -\alpha,\ \delta \in \mathbb{F}_q^\times$, on a un isomorphisme

$$\begin{aligned} \varphi : E_\lambda^{(-1)} &\xrightarrow{\sim} E_\lambda^{(\alpha)} \\ (x,y) &\mapsto \left(\frac{x}{\delta^2}, \frac{y}{\delta^3}\right), \end{aligned}$$

On en déduit $E_\lambda^{(\alpha)} \simeq E_\lambda^{(-1)} \simeq E_{1-\lambda}$, ce qui est absurde car $E_\lambda^{(\alpha)}$ n'est pas Legendre isomorphe. Donc $-1 \in (\mathbb{F}_q^\times)^2$. De même $\lambda, 1-\lambda \in (\mathbb{F}_q^\times)^2$.

$\square$

4.3 Preuve du résultat principal

Preuve. Supposons que $E/\mathbb{F}_p \sim E_\lambda/\mathbb{F}_p$, avec $\lambda \in \mathbb{F}_p$. Alors $|E(\mathbb{F}_p)| = |E_\lambda(\mathbb{F}_p)|$. Or $E_\lambda[2](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, donc

$$|E(\mathbb{F}_p)| \in 4\mathbb{Z}$$

Inversement, supposons que $|E(\mathbb{F}_p)| \in 4\mathbb{Z}$. Si $E[2](\mathbb{F}_p) \neq E[2](\overline{\mathbb{F}}_p)$, alors $E[2](\mathbb{F}_p)$ ne contient pas de sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Or

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}, \quad n_1 \mid n_2.$$

Si $2 \mid n_1$, alors $2 \mid n_2$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \subset E(\mathbb{F}_p)$, c'est absurde, d'où $2 \nmid n_1$ et $4 \mid n_2$. Ainsi, $E(\mathbb{F}_p)$ contient un élément P d'ordre 4, en particulier $2P \in E[2](\mathbb{F}_p) \subsetneq E[2](\overline{\mathbb{F}}_p)$. Soit $Q \in E[2](\overline{\mathbb{F}}_p) \setminus E[2](\mathbb{F}_p)$ et

$$\varphi : E \longrightarrow E/\langle 2P \rangle = \widetilde{E}$$

l'isogénie quotient. Notons pour plus tard que φ et $\widetilde{E}$ sont définies sur $\mathbb{F}_p$. Montrons que $\widetilde{E}[2](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

- D'abord
$$\begin{cases} 2\varphi(P) = \varphi(2P) = \mathcal{O} \\ \varphi(P) \neq \mathcal{O} \quad \text{car} \quad P \notin \langle 2P \rangle. \end{cases} \quad \Rightarrow \quad \circ(\varphi(P)) = 2.$$

- Ensuite
$$\begin{cases} 2\varphi(Q) = \varphi(2Q) = \varphi(\mathcal{O}) = \mathcal{O} \quad \text{car } Q \in E[2] \\ \varphi(Q) \neq \mathcal{O} \quad \text{car } Q \notin \langle 2P \rangle. \end{cases} \quad \Rightarrow \quad \circ(\varphi(Q)) = 2.$$

- Soit $n \in \mathbb{N}$ tel que $E[2](\mathbb{F}_{p^n}) = E[2](\overline{\mathbb{F}}_p)$, et soit σ un générateur de $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Puisque $Q \notin \langle 2P \rangle$ on a
$$E[2](\mathbb{F}_{p^n}) = \langle 2P, Q \rangle$$
En particulier, comme $\sigma(Q) \in E[2](\mathbb{F}_{p^n})$
$$\sigma(Q) = Q + 2P,$$
en effet si $\sigma(Q) = Q$, alors $Q \in E(\mathbb{F}_p)$, et si $\sigma(Q) = 2P$, alors $Q = \sigma^{-1}(2P) \in E(\mathbb{F}_p)$. D'où
$$\begin{aligned} \sigma(\varphi(Q)) &= \varphi(\sigma(Q)) && \text{car } \varphi \text{ est } \mathbb{F}_p\text{-rationnelle} \\ &= \varphi(Q + 2P) = \varphi(Q) + \varphi(2P) = \varphi(Q) + \mathcal{O} = \varphi(Q) \end{aligned}$$
Donc $\varphi(Q) \in \widetilde{E}(\mathbb{F}_p)$. Par conséquent,
$$\widetilde{E}[2](\mathbb{F}_p) = \langle \varphi(P), \varphi(Q) \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$
En effet,
$$\langle \varphi(P) \rangle = \langle \varphi(Q) \rangle \iff \varphi(P) = \varphi(Q) \iff P - Q \in \langle 2P \rangle \iff Q = P \text{ ou } Q = 3P,$$
ce qui est absurde.

Ainsi, l'isogénie $\varphi : E \longrightarrow \widetilde{E}$ permet de supposer qu'à $\mathbb{F}_p$-isogénie près

$$E[2](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

On peut écrire un modèle $E : y^2 = (x-a)(x-b)(x-c)$, $a, b, c \in \mathbb{F}_p$ puis appliquer l'isomorphisme $(x, y) \longmapsto (x+a,\ y)$ pour obtenir le modèle

$$E/\mathbb{F}_p : \quad y^2 = x(x-\alpha)(x-\beta), \qquad \alpha, \beta \in \mathbb{F}_p.$$

De plus,

$$E^{(\alpha)} : \quad y^2 = x^3 - \alpha(\alpha+\beta)x^2 + \alpha^3\beta x \ \simeq\ E_{\beta/\alpha} : \ y^2 = x^3 - \left(1 + \frac{\beta}{\alpha}\right)x^2 + \frac{\beta}{\alpha}x$$
$$(x, y) \longmapsto (\alpha^2 x,\ \alpha^3 y).$$

Donc $E^{(\alpha)} \simeq E_\lambda,\ \lambda = \frac{\beta}{\alpha} \in \mathbb{F}_p$. Si $\alpha \in (\mathbb{F}_p^\times)^2$ alors $E \simeq E^{(\alpha)} \simeq E_\lambda$ et la preuve est complète. On suppose à partir de maintenant que $\alpha \notin (\mathbb{F}_p^\times)^2$. On examine les cas supersinguliers et ordinaires séparément.

- Si E est supersingulière, alors
$$|E(\mathbb{F}_p)| = p+1-t \quad \text{et} \quad p \mid t.$$
Or
$$\begin{cases} |t| \le 2\sqrt{p} \\ t = kp, \end{cases} \Rightarrow k^2p^2 \le 4p \;\Rightarrow\; k^2p \le 4.$$
Si $p \ge 5$, alors $k=0$, i.e. $|E(\mathbb{F}_p)| = p+1$. Si $p=3$, alors $k \in \{-1,0,1\}$, cependant
$$\begin{cases} k = 1 \Rightarrow t = p \Rightarrow |E(\mathbb{F}_p)| = 1 \notin 4\mathbb{Z}, \\ k = -1 \Rightarrow |E(\mathbb{F}_p)| = 2p+1 \notin 4\mathbb{Z}. \end{cases}$$
Donc $k=0$ i.e. $|E(\mathbb{F}_p)| = p+1$. Or $\alpha \notin (\mathbb{F}_p^\times)^2$, d'où $|E^{(\alpha)}(\mathbb{F}_p)| + |E(\mathbb{F}_p)| = 2p+2$, i.e.
$$|E^{(\alpha)}(\mathbb{F}_p)| = p+1 = |E(\mathbb{F}_p)|.$$
D'après le théorème de Tate, $E \sim E^{(\alpha)}$. On a donc $E \sim E^{(\alpha)} \sim E_\lambda$, i.e. E est Legendre isogène sur $\mathbb{F}_p$.
- Si E est ordinaire. On distingue deux cas
  (a) Si $E_\lambda^{(\alpha)}$ est Legendre isogène, c'-à-d $E_\lambda^{(\alpha)} \sim E_\mu$, $\mu \in \mathbb{F}_p$. En notant $\operatorname{Tr}_{\mathbb{F}_p}(E)$ la trace du Frobenius de $E/\mathbb{F}_p$
  $$\operatorname{Tr}_{\mathbb{F}_p}(E) = -\operatorname{Tr}_{\mathbb{F}_p}(E^{(\alpha)}) = -\operatorname{Tr}_{\mathbb{F}_p}(E_\lambda) = +\operatorname{Tr}_{\mathbb{F}_p}(E_\lambda^{(\alpha)}),$$
  car $E^{(\alpha)} \simeq E_\lambda$ et $\alpha \notin (\mathbb{F}_p^\times)^2$. Donc, d'après le théorème de Tate $E \sim E_\lambda^{(\alpha)}$. D'où $E \sim E_\lambda^{(\alpha)} \sim E_\mu$ i.e. E est Legendre isogène sur $\mathbb{F}_p$.

  (b) Si $E_\lambda^{(\alpha)}$ n'est pas Legendre isogène, alors la proposition 11 assure que
  $$\begin{cases} E_\lambda[4](\mathbb{F}_p) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \\ -1 \in (\mathbb{F}_p^\times)^2. \end{cases}$$
  De plus,
  $$|E_\lambda(\mathbb{F}_p)| = 2^\alpha \cdot \prod_{p_i \text{ premier } \ge 3} p_i^{m_i}, \qquad \alpha \ge 4,$$
  Alors le théorème de Rück [Rü87] donne l'existence d'une courbe $E'/\mathbb{F}_p$ telle que
  $$\begin{cases} E_\lambda \sim E', \\ E'[4](\mathbb{F}_p) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}. \end{cases}$$
  En effet, $a=1$ vérifie $0 \le a \le \min\big(v_2(p-1), \lfloor \alpha/2 \rfloor\big)$, d'où l'existence de E' telle que
  $$E'[2^{\alpha-1}](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\alpha-1}\mathbb{Z}.$$
  Donc
  $$E'[4](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$
  Soit $P \in E'(\mathbb{F}_p)$ d'ordre 4 et $Q = 2P$, i.e. $Q \in E'[2](\mathbb{F}_p)$. Quitte à effectuer $(x,y) \mapsto (x - x_Q, y)$, on peut supposer qu'on a un modèle $E' : y^2 = x(x-\alpha')(x-\beta')$, $\alpha', \beta' \in \mathbb{F}_p$, avec $(0,0) \in 2E'(\mathbb{F}_p)$. La proposition 8 assure alors
  $$0 - \alpha' \in (\mathbb{F}_p^\times)^2.$$
  Donc
  $$\frac{-\alpha'}{-1} = \alpha' \in (\mathbb{F}_p^\times)^2, \quad \text{i.e.} \quad \alpha' = \delta^2,\ \delta \in \mathbb{F}_p.$$
  On a alors avec $\lambda' = \frac{\beta'}{\alpha'}$
  $$E' :\ y^2 = x^3 - (\alpha' + \beta')x^2 + \alpha'\beta' x \;\simeq\; E_{\lambda'} :\ y^2 = x^3 - \left(1 + \frac{\beta'}{\alpha'}\right)x^2 + \frac{\beta'}{\alpha'}x$$
  $$(x,y) \longmapsto (\delta^2 x,\ \delta^3 y).$$

Or

$$E_{\lambda'}[4](\mathbb{F}_p) \simeq E'[4](\mathbb{F}_p) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Donc la proposition 11 donne

$$\forall \gamma \in \mathbb{F}_p^\times, \quad E_{\lambda'}^{(\gamma)} \text{ est Legendre isomorphe.}$$

En particulier, $E_{\lambda'}^{(\alpha)}$ est Legendre isomorphe, i.e $E_{\lambda'}^{(\alpha)} \simeq E_\mu$. Enfin, on récapitule

$$E^{(\alpha)} \sim E_\lambda \sim E' \sim E_{\lambda'}, \qquad \alpha \notin (\mathbb{F}_p^\times)^2.$$

D'où

$$\operatorname{Tr}_{\mathbb{F}_p}(E) = -\operatorname{Tr}_{\mathbb{F}_p}(E^{(\alpha)}) = -\operatorname{Tr}_{\mathbb{F}_p}(E_{\lambda'}) = +\operatorname{Tr}_{\mathbb{F}_p}(E_{\lambda'}^{(\alpha)})$$

Donc $E \sim E_{\lambda'}^{(\alpha)} \sim E_\mu$, i.e. E est Legendre isogène sur $\mathbb{F}_p$.

□

5 Remarques finales

Les paragraphes précédents nous ont appris

$$\begin{cases} |E_\lambda(\mathbb{F}_p)| = 1 - (-1)^m H_p(\lambda) \mod p \\ |E_\lambda(\mathbb{F}_p)| \in 4\mathbb{Z}. \end{cases}$$

1. En notant t la trace du Frobenius de $E_\lambda/\mathbb{F}_p$, on a $|E_\lambda(\mathbb{F}_p)| = p + 1 - t$, d'où $t = p + 1 + 4k$. La borne de Hasse donne $|t| < 2\sqrt{p}$.

$$\begin{aligned} |t| < 2\sqrt{p} &\iff t^2 < 4p \iff (p+1+4k)^2 < (2\sqrt{p})^2 \\ &\iff (p+1+4k+2\sqrt{p})(p+1+4k-2\sqrt{p}) < 0 \\ &\iff (4k+(\sqrt{p}+1)^2)(4k+(\sqrt{p}-1)^2) < 0 \\ &\iff k \in \mathbb{Z} \cap \left[-\frac{(\sqrt{p}+1)^2}{4} \,;\, -\frac{(\sqrt{p}-1)^2}{4} \right] \\ &\iff k \in \left[\!\left[\left\lceil -\frac{(\sqrt{p}+1)^2}{4} \right\rceil \,;\, \left\lfloor -\frac{(\sqrt{p}-1)^2}{4} \right\rfloor \right]\!\right]. \end{aligned}$$

D'où

$$|E_\lambda(\mathbb{F}_p)| \in \left[\!\left[-4\left\lfloor -\frac{(\sqrt{p}-1)^2}{4} \right\rfloor \,;\, -4\left\lceil -\frac{(\sqrt{p}+1)^2}{4} \right\rceil \right]\!\right].$$

Tous les multiples de 4 de cet intervalle apparaissent comme ordre d'une courbe sous forme de Legendre sur $\mathbb{F}_p$.

2. De plus les valeurs apparaissant dans $\big(H_p(\lambda) \bmod p\,;\, \lambda \in \mathbb{F}_p^2 \setminus \{0,1\}\big)$ sont soumises aux conditions

$$m \text{ est pair} \iff \frac{p-1}{2} = 2\ell \iff p = 4\ell + 1 \iff p + 1 - t = 4\ell + 2 - t \iff t \equiv 2 \mod 4.$$

De même m est impair $\iff t \equiv 0 \mod 4$.

3. On remarque les symétries suivantes

$$\big(H_p(\lambda) \bmod p\,;\, \lambda \in \mathbb{F}_p^2 \setminus \{0,1\}\big) \text{ est un palyndrôme} \iff m \text{ est pair.}$$

En effet

$$m \text{ est pair} \iff (-1) \in (\mathbb{F}_p^\times)^2 \Rightarrow E_\lambda \simeq E_\lambda^{(-1)} \simeq E_{1-\lambda} \Rightarrow H_p(1-\lambda) = H_p(\lambda).$$

De même, on a le résultat

$$m \text{ est impair} \iff (-1) \notin (\mathbb{F}_p^\times)^2 \Rightarrow \operatorname{Tr}_{\mathbb{F}_p}(E_\lambda) = -\operatorname{Tr}_{\mathbb{F}_p}(E_\lambda^{(-1)}) = -\operatorname{Tr}_{\mathbb{F}_p}(E_{1-\lambda}) \Rightarrow H_p(\lambda) = -H_p(1-\lambda).$$

A Couplages de Weil, de Kummer et conséquences

Soit $m \in \mathbb{N}$, $m \geq 2$, $(m,p) = 1$ où $p = \operatorname{car} K$. Soit E/K une courbe elliptique, on a $E[m] = E[m](\overline{K}) \simeq (\mathbb{Z}/m\mathbb{Z})^2$.

Proposition 12. Le couplage de Weil

$$e_m : E[m] \times E[m] \longrightarrow \mu_m$$

est bilinéaire, alterné, non dégénéré et invariant sous l'action de Galois. En particulier

$$\begin{cases} \forall S \in E[m],\ e_m(S,T) = 1 \Rightarrow T = \mathcal{O}, \\ \forall \sigma \in \operatorname{Gal}(\overline{K}/K),\ e_m(S,T)^\sigma = e_m(S^\sigma, T^\sigma). \end{cases}$$

Proposition 13. Le couplage de Kummer

$$\begin{aligned} \kappa : E(K) \times \operatorname{Gal}(\overline{K}/K) &\longrightarrow E[m] \\ (P,\sigma) &\longmapsto Q^\sigma - Q, \qquad \text{où } Q \in E(\overline{K}) \ / \ [m]Q = P \end{aligned}$$

est bilinéaire, son noyau à gauche est $mE(K)$ et induit

$$\begin{aligned} \delta_E : E(K)/mE(K) &\longrightarrow \operatorname{Hom}(\operatorname{Gal}(\overline{K}/K), E[m]) \\ P &\longmapsto \delta_E(P) : \begin{cases} \operatorname{Gal}(\overline{K}/K) \longrightarrow E[m], \\ \sigma \longmapsto \kappa(P,\sigma). \end{cases} \end{aligned}$$

Théorème 4 (Hilbert 90)**.** Supposons que $\mu_m \subset K$. Alors

$$\begin{aligned} \delta_K : K^\times/(K^\times)^m &\xrightarrow{\sim} \operatorname{Hom}(\operatorname{Gal}(\overline{K}/K), \mu_m) \\ b &\longmapsto \delta_K(b) : \begin{cases} \operatorname{Gal}(\overline{K}/K) \longrightarrow \mu_m, \\ \sigma \longmapsto \dfrac{\sigma(\beta)}{\beta}, \quad \text{où } \beta^m = b. \end{cases} \end{aligned}$$

Des trois résultats précédents, on en déduit la construction suivante. Soient $P \in E(K)$ et $T \in E[m]$, alors

$$\begin{aligned} \operatorname{Gal}(\overline{K}/K) &\longrightarrow \mu_m \\ \sigma &\longmapsto e_m\big(\delta_E(P)(\sigma), T\big) \end{aligned}$$

définit un élément de $\operatorname{Hom}\big(\operatorname{Gal}(\overline{K}/K), \mu_m\big)$, le théorème 90 de Hilbert assure l'existence d'un unique $b = b(P,T)$ tel que $e_m\big(\delta_E(P)(\sigma), T\big) = \delta_K\big(b(P,T)\big)(\sigma)$.

Théorème 5. Il existe une application bilinéaire

$$b : \frac{E(K)}{mE(K)} \times E[m] \longrightarrow \frac{K^\times}{(K^\times)^m}$$

tel que $b(P,T)$ soit l'unique classe vérifiant

$$\forall \sigma \in \operatorname{Gal}(\overline{K}/K), \quad e_m\big(\delta_E(P)(\sigma), T\big) = \delta_K\big(b(P,T)\big)(\sigma)$$

Le noyau de b à gauche est trivial. Pour $T \in E[m]$, soient $f_T, g_T \in K(E)$ tels que

$$\begin{cases} \operatorname{div}(f_T) = m(T) - m(\mathcal{O}), \\ f_T \circ [m] = g_T^m. \end{cases}$$

Alors, pour tout $P \neq T$,

$$b(P,T) \equiv f_T(P) \mod (K^\times)^m$$

Remarque 2.

1. Si $\operatorname{Gal}(\overline{K}/K)$ agit trivialement sur le $\operatorname{Gal}(\overline{K}/K)$-module M, alors

$$\begin{cases} H^0\big(\operatorname{Gal}(\overline{K}/K), M\big) = M, \\ H^1\big(\operatorname{Gal}(\overline{K}/K), M\big) = \operatorname{Hom}_{\text{cont}}\big(\operatorname{Gal}(\overline{K}/K), M\big). \end{cases}$$

   L'hypothèse $\mu_m \subset K$ de la proposition provient de cette remarque.

2. Notons la mention de morphismes de groupes continus ci-dessus. Le groupe $\operatorname{Gal}(\overline{K}/K)$ est profini et les groupes $E[m]$, μ_m sont finis, donc

$$\begin{cases} \operatorname{Hom}\big(\operatorname{Gal}(\overline{K}/K), \mu_m\big) = \operatorname{Hom}_{\text{cont}}\big(\operatorname{Gal}(\overline{K}/K), \mu_m\big), \\ \operatorname{Hom}\big(\operatorname{Gal}(\overline{K}/K), E[m]\big) = \operatorname{Hom}_{\text{cont}}\big(\operatorname{Gal}(\overline{K}/K), E[m]\big). \end{cases}$$

Revenons à la preuve de la proposition 8. Soient $m = 2$, $p \geq 3$ premier et

$$E/\mathbb{F}_p : y^2 = (x-\alpha)(x-\beta)(x-\gamma), \quad \alpha, \beta, \gamma \in \mathbb{F}_p.$$

Alors $f_{P_\alpha} = x - \alpha \in \mathbb{F}_p(E)$ a pour diviseur $\mathrm{div}(f_{P_\alpha}) = 2(P_\alpha) - 2(\mathcal{O})$, où $P_\alpha = (\alpha, 0) \in E(\mathbb{F}_p)$. De plus, en notant

$$\begin{cases} S_1 & = \alpha + \beta + \gamma, \\ S_2 & = \alpha\beta + \alpha\gamma + \beta\gamma, \end{cases}$$

on a par un long calcul à partir des règles de calcul de l'addition sur E

$$f_{P_\alpha} \circ [2](x,y) = \left[\frac{x^2 - \alpha x - 2x^2 + 2S_1 x - S_2}{2y} \right]^2 = g_{P_\alpha}^2(x,y).$$

Donc, pour tout $Q \neq P_\alpha,\ b(Q, P_\alpha) \equiv f_{P_\alpha}(Q) \mod (\mathbb{F}_p^\times)^2$. De même pour P_β et P_γ. On a donc la caractérisation

$$Q \in 2E(\mathbb{F}_p) \Leftrightarrow \forall P \in E[2], \quad b(Q,P) \equiv 0$$

Ainsi,

$$P_\gamma = (\gamma, 0) \in 2E(\mathbb{F}_p) \iff \begin{cases} b(P_\gamma, P_\alpha) \equiv 0, \\ b(P_\gamma, P_\beta) \equiv 0, \\ b(P_\gamma, P_\gamma) \equiv 0. \end{cases}$$

Or :

- $b(P_\gamma, P_\alpha) = f_{P_\alpha}(P_\gamma) = \gamma - \alpha$.
- $b(P_\gamma, P_\beta) = f_{P_\beta}(P_\gamma) = \gamma - \beta$.
- $b(P_\gamma, P_\gamma) = b(P_\gamma, P_\gamma + P_\alpha - P_\alpha) = b(P_\gamma, P_\gamma + P_\alpha)\, b(P_\gamma, P_\alpha)^{-1} = b(P_\gamma, P_\beta)\, b(P_\gamma, P_\alpha)^{-1} = \frac{\gamma-\beta}{\gamma-\alpha}$

Ainsi

$$P_\gamma = (\gamma, 0) \in 2E(\mathbb{F}_p) \iff \gamma - \alpha,\ \gamma - \beta \in (\mathbb{F}_p^\times)^2.$$

References

[AT02] Roland Auer and Jaap Top. Legendre elliptic curves over finite fields. *Journal of Number Theory*, 95(2):303–312, 2002.

[Fre01] Jean Fresnel. *Anneaux*. Actualités scientifiques et industrielles. Hermann, 2001.

[Rü87] H.-G. Rück. A note on elliptic curves over finitefields. Math. Comp., 1987.

[Sch95] E. F. Schaefer. 2-descent on the jacobians of hyperelliptic curves. J. Number Th., 1995.

[Sil09] Joseph H Silverman. *The Arithmetic of Elliptic Curves*. Graduate texts in mathematics. Springer, Dordrecht, 2009.