CLASSES D'ISOMORPHISMES DES COURBES ELLIPTIQUES SUPERSINGULIÈRES EN CARACTÉRISTIQUE $\geqslant 3$

F. MORAIN

RÉSUMÉ. Nous donnons un représentant de chaque classe d'isomorphisme de courbes elliptiques supersingulières sur un corps fini de caractéristique $p = 3$ et indiquons les règles de classification en caractéristique > 3. Nous donnons la cardinalité de chacun des représentants en utilisant des sommes de caractères de Gauss et Jacobstahl.

1. INTRODUCTION

Une courbe elliptique définie sur un corps fini $\mathbb{K}$ de caractéristique p est dite supersingulière si son anneau d'endomorphismes est non commutatif. Deuring et Waterhouse ont dénombré les classes d'isomorphismes de telles courbes, comme nous le rappelons dans la section 3. Le but de cet article est de donner, dans le même esprit que [18] dans le cas de la caractéristique 2, des représentants explicites de chaque classe d'isomorphismes pour le cas $p = 3$ avec leur cardinalité. Quand $p > 3$, nous donnons des règles générales de classification et donnons une table numérique pour $p \leqslant 307$. Ces résultats sont utiles en cryptographie [19] car ils permettent d'avoir des courbes de cardinalité aisée à calculer. Une autre application est donnée dans [25] où l'auteur construit des courbes elliptiques ayant un nombre maximal de points en utilisant la forme de Legendre des courbes elliptiques. La motivation de ces travaux se trouve également dans l'implantation de l'algorithme de Schoof qui calcule le nombre de points d'une courbe elliptique dans un corps fini (voir par exemple [24, 22, 15, 14]).

La section 2 rappellent certaines propriétés des courbes elliptiques définies sur un corps fini. La section 3 reprend certains des résultats connus sur les courbes supersingulières et donne le programme de classification. Dans la section 4, nous rassemblons des résultats sur les sommes de caractères dans les corps finis et donnons en particulier les valeurs des sommes de Jacobsthal Φ_2 et Ψ_3 qui se basent sur des résultats connus. Dans la section 5, nous traitons le cas $p = 3$ et la section 6 contient les règles de classification pour $p > 3$.

Notations : dans le reste de l'article, p est un nombre premier impair. Le corps $\mathbb{K}$ considéré a pour cardinalité $q = p^n$. Si x est dans $\mathbb{K}$, on note $\mathrm{Tr}(x)$ la trace de x.

2. COURBES ELLIPTIQUES SUR UN CORPS FINI

La forme la plus générale d'une courbe elliptique E en caractéristique $p \geqslant 3$ est (voir par exemple [26, Appendix A])

$$E\ : Y^2 = X^3 + a_2X^2 + a_4X + a_6$$

où les a_i sont des éléments de $\mathbb{K}$ tels que le discriminant de E,

$$\Delta = -16a_2^2(4a_2a_6 - a_4^2) - 64a_4^3 - 432a_6^2 + 288a_2a_4a_6,$$

soit non nul. L'invariant de la courbe est $j(E) = (16a_2^2 - 48a_4)^3/\Delta$. On munit E d'une loi de groupe, appelée *loi de la tangente et de la corde*. Le groupe des points sur la courbe est noté $E(\mathbb{K})$.

Théorème 1 (Hasse). *Le cardinal de $E(\mathbb{K})$ s'écrit $\#E(\mathbb{K}) = q + 1 - t$ avec $|t| \leqslant 2\sqrt{q}$.*

Date: 29 avril 1996.

Mis à disposition du LIX par la Délégation Générale pour l'Armement.

Soit $\mathbb{K}_n$ une extension de degré n de $\mathbb{K}$. La fonction zeta de $E/\mathbb{K}$ est définie par

$$\log Z(E/\mathbb{K}, T) = \sum_{n=1}^{\infty} (\#(E/\mathbb{K}_n))T^n/n.$$

On a [26, Chapitre V]

Théorème 2 (Théorème de Weil)**.** *La fonction Z est donnée par :*

$$Z(E/\mathbb{K}, T) = \frac{1 - aT + qT^2}{(1-T)(1-qT)}$$

avec $1 - aT + qT^2 = (1 - \alpha T)(1 - \beta T)$ où α et β sont des nombres complexes de valeur absolue $\sqrt{q}$. Le nombre de points de $E/\mathbb{K}_n$ vaut donc $q^n + 1 - (\alpha^n + \beta^n)$.

Définition 1. *Deux courbes $E/\mathbb{K}$ et $E'/\mathbb{K}$ ayant même cardinal sont dites isogènes.*

Soit η le caractère quadratique de $\mathbb{K}$. D'un point de vue élémentaire, notons que

$$\#(E/\mathbb{K}) = q + 1 + \sum_{x \in \mathbb{K}} \eta(x^3 + a_2 x^2 + a_4 x + a_6) = q + 1 - t.$$

Il est facile de voir que la courbe $\tilde{E}$ d'équation :

$$Y^2 = X^3 + a_2 \gamma X^2 + a_4 \gamma^2 X + a_6 \gamma^3$$

où γ est un non carré dans $\mathbb{K}$ vérifie :

$$\#\tilde{E}(\mathbb{K}) = q + 1 + t.$$

Définition 2. *La courbe $\tilde{E}$ est appelée* tordue *de E.*

Pour finir, introduisons la notation $E_{a,b}$ pour désigner la courbe d'équation $y^2 = x^3 + ax + b$. On note $t_{a,b} = \#E_{a,b}(\mathbb{K}) - (q+1)$.

3. Propriétés des courbes supersingulières

Suivant les notations de [23], désignons par $h(-D)$ le nombre de classes de formes quadratiques primitives réduites de discriminant $-D < 0$ et par $H(-D)$ le nombre de classes de Kronecker :

$$H(-D) = \sum_{\substack{d>0 \\ d^2 \mid D \\ -D/d^2 \equiv 0 \text{ ou } 1 \bmod 4}} h(-D/d^2).$$

Notons que si $p \equiv 1 \bmod 4$, on a $H(-4p) = h(-p)$ et si $p \equiv 3 \bmod 4$, on a $H(-4p) = h(-p) + h(-4p)$.

3.1. Invariants supersinguliers.

Pour le théorème suivant, voir [26, Theorem 3.1].

Théorème 3. *Si $E/\mathbb{K}$ est supersingulière, alors $j(E) \in \mathbb{F}_{p^2}$.*

On appelle $S_p(J)$ le polynôme dont les racines dans $\overline{\mathbb{F}_p}$ (en fait $\mathbb{F}_{p^2}$) sont les invariants des courbes supersingulières. Le nombre de racines de S_p dans $\mathbb{F}_p$ est donné dans [21] :

Théorème 4. *Soit h le nombre de classes de $\mathbb{Q}(\sqrt{-p})$. Le nombre de racines de $S_p(J)$ dans $\mathbb{F}_p$ est $h/2$ si $p \equiv 1 \bmod 4$; $2h$ si $p \equiv 3 \bmod 8$ (et $p \neq 3$) ; h si $p \equiv 7 \bmod 8$.*

Le polynôme $S_p(J)$ peut se calculer à partir de l'invariant de Hasse ou bien par la méthode des graphes [20]. La méthode la plus rapide est due à Atkin [1, 2] (voir également [22]). Une table de ces polynômes pour $p \leqslant 97$ se trouve dans [6] (qui contient cependant quelques erreurs typographiques) et une table exacte pour $p \leqslant 307$ dans [4, pp. 143–144].

3.2. **Cardinalité et structure.** On note $\mathcal{Q}(p) = (p+6-4(-3/p)-3(-4/p))/12$ le nombre d'ordres maximaux dans l'algèbre de quaternion $\mathbb{Q}_{\infty,p}$, la seule algèbre définie sur $\mathbb{Q}$ et ramifiée seulement en p et ∞.

Les courbes elliptiques supersingulières sont caractérisées par le fait que $p \mid t$. On trouve dans la table 1 les valeurs possibles de t déterminées par Deuring [6] et Waterhouse [29, Theorem (4.1)] (voir aussi [23]). On indique aussi dans la table le nombre $N(t)$ de classes d'isomorphismes de courbes ayant $q+1-t$ points, ainsi que la structure du groupe $E(\mathbb{K})$ donnée dans [23]. Dans le cas $(*)$, si

n	t	p	$N(t)$	$E(\mathbb{K})$
impair	0		$H(-4p)$	$(*)$
	$\pm\sqrt{3q}$	3	1	cyclique
pair	0		$1-(-4/p)$	cyclique
	$\pm\sqrt{q}$		$1-(-3/p)$	cyclique
	$\pm 2\sqrt{q}$		$\mathcal{Q}(p)$	$\mathbb{Z}/(\sqrt{q}\mp 1)\mathbb{Z} \oplus \mathbb{Z}/(\sqrt{q}\mp 1)\mathbb{Z}$

TABLE 1. Nombre de classes d'isomorphismes de courbes supersingulières

$q \not\equiv -1 \bmod 4$, toutes les courbes ayant $t = 0$ sont cycliques ; si $q \equiv 1 \bmod 4$, $h(-4p)$ sont cycliques et $h(-p)$ sont isomorphes à $\mathbb{Z}/((q+1)/2)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

3.3. **Programme de classification.** La démarche est la suivante. On commence par calculer le polynôme $S_p(J)$. Pour chaque racine j_0, on construit les deux courbes elliptiques d'invariant j_0 (la courbe et sa tordue). Pour chacune des courbes, on précise alors le nombre de points. Comme dans la table 1, les deux cas n pair et n impair doivent être dissociés.

4. Sommes de caractères

4.1. **Sommes de Gauss.** Rappelons quelques propriétés des sommes de caractères. Soit ψ un caractère multiplicatif. Soit $\zeta_p = \exp(2i\pi/p)$. Introduisons la somme de Gauss :

$$G_n(\psi) = \sum_{x\in\mathbb{K}^*} \psi(x)\zeta_p^{\mathrm{Tr}(x)}.$$

Pour certains caractères, la valeur de G_n est connue. Le plus célèbre résultat est celui du calcul de $G_n(\eta)$ où η est le caractère quadratique. Le résultat suivant se trouve par exemple dans [16, Theorem 5.15] :

Théorème 5. *Avec $q = p^n$, alors*

$$G_n(\eta) = \begin{cases} (-1)^{n-1}\sqrt{q} & \text{si } p \equiv 1 \bmod 4. \\ (-1)^{n-1} i^n \sqrt{q} & \text{si } p \equiv 3 \bmod 4. \end{cases}$$

Nous serons amené à utiliser cette valeur en conjonction avec le résultat suivant [16, Theorem 5.30] :

Théorème 6. *On a*

$$\sum_{x\in\mathbb{K}} \zeta_p^{\mathrm{Tr}(x^2)} = G_n(\eta).$$

4.2. **Sommes de Jacobstahl.** Pour e entier, la somme de Jacobstahl est définie par

$$\Phi_{n,e}(a) = \sum_{x\in\mathbb{K}} \eta(x(x^e + a)).$$

On lui associe également la somme

$$\Psi_{n,e}(b) = \sum_{x\in\mathbb{K}} \eta(x^e + b).$$

Notons le lemme évident suivant.

Lemme 1. *Si -1 n'est pas un carré dans $\mathbb{K}$, alors $\Phi_{n,2e}(a) = 0$.*

4.2.1. *La somme $\Phi_{n,2}(a)$.* La somme $\Phi_{1,2}$ a été historiquement la première évaluée par Jacobstahl [9], mais avec une ambiguité sur les signes dans certains cas. On pourra consulter [5, 13, 8, 7, 10] pour la levée de cette ambiguité et des résultats connexes. Le cas $n > 1$ a été moins souvent abordé. Le cas $n = 2$ est traité dans [3, Theorems 6.1 and 6.2]. Le cas n quelconque et $a = 1$ est traité dans [27, p. 56]. Le cas général est donné par [5, §7], mais nous préférons citer [12, Theorem 2].

Théorème 7. *On suppose que $q = p^n \equiv 1 \bmod 4$. Soit a dans $\mathbb{F}_q$, $a \neq 0$. Si $p \equiv -1 \bmod 4$, on pose $s = (-p)^{n/2}$ and $t = 0$. Si $p \equiv 1 \bmod 4$, il existe s et t, $p \nmid s$, $s \equiv 1 \bmod 4$; dans le cas où a n'est pas un carré, on fixe le signe de t en imposant $a^{(q-1)/4} \equiv s/t \bmod p$. Alors*

$$\Phi_{n,2}(a) = \begin{cases} -2s & \text{si } a \text{ est une puissance quatrième dans } \mathbb{F}_q \\ 2s & \text{si } a \text{ est un carré mais une puissance quatrième dans } \mathbb{F}_q \\ 2t & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_q \end{cases}$$

4.2.2. *La somme $\Psi_{n,3}(a)$.* Cette somme a été évaluée complètement dans [5, §7] en utilisant la factorisation de q dans $\mathbb{Z}[\rho]$. Pour une version rationnelle, voir [11]. Nous nous contenterons de l'énoncé suivant.

Théorème 8. *On suppose que $q = p^n \equiv 1 \bmod 6$. Soit χ un caractère non trivial d'ordre 3. Si $p \equiv -1 \bmod 6$, alors $n = 2r$ et*

$$\Psi_{n,3}(b) = (-1)^{r+1}\eta(b)\sqrt{q}2\Re(\chi(b)).$$

5. Le cas $p = 3$

Les courbes supersingulières en caractéristique 3 sont caractérisées par $j(E) = 0$ (cf. [26, Appendix A]). Toute courbe est donc de la forme $E_{a,b}$ avec $a \neq 0$.

Théorème 9. *Soit γ un non carré dans $\mathbb{K}$ et δ un élément de trace 1. Les classes d'isomorphismes de courbes elliptiques supersingulières en caractéristique 3 ont pour représentants :*

n	a	b	$t_{a,b}$
$2r+1$	1	0	0
	-1	0	0
	-1	δ	$(-1)^{r+1}\sqrt{3q}$
	-1	$-\delta$	$(-1)^r\sqrt{3q}$
$2r$	-1	0	$2(-1)^r\sqrt{q}$
	$-\gamma^2$	0	$-2(-1)^r\sqrt{q}$
	$-\gamma$	0	0
	$-\gamma^3$	0	0
	-1	δ	$(-1)^{r+1}\sqrt{q}$
	$-\gamma^2$	$\gamma^3\delta$	$-(-1)^{r+1}\sqrt{q}$

Nous pouvons préciser la structure des courbes $E_{\pm 1,0}$ dans le cas $n = 2r+1$ (c'est le cas $(*)$ de la table 1). La courbe $E_{-1,0}$ a trois points de 2-torsion et donc $E_{-1,0}(\mathbb{K})$ est isomorphe à $\mathbb{Z}/((q+1)/2)\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, alors que la courbe $E_{1,0}$ a un seul point de 2-torsion et donc $E_{1,0}(\mathbb{K})$ est cyclique.

La démonstration du théorème 9 se fait en deux étapes. Dans la première, nous déterminons les représentants des classes d'isomorphisme en utilisant la 2-torsion des courbes elliptiques. Cela fait, nous calculons les cardinalités des courbes en utilisant des sommes de caractères.

5.1. **Préliminaires.** Rappelons la forme des isomorphismes entre courbes elliptiques [26, Appendix A].

Proposition 1. *Les deux courbes $E_{a,b}$ et $E_{a',b'}$ sont isomorphes si et seulement s'il existe u et v dans $\mathbb{K}$ tels que*

$$a' = au^4,$$
$$v^3 + av + b = u^6 b'.$$

Montrons maintenant :

Proposition 2. *La courbe $E_{a,b}$ admet un unique point de 2-torsion dans les cas suivants : n impair et a un carré ; n pair et a non carré.*

Démonstration : D'après [28, Corollary 1], on sait que $f(X) = X^3 + aX + b$ a un nombre pair de facteurs irréductibles (et donc une unique racine) si et seulement si son discriminant $\Delta = -a^3$ n'est pas un carré dans $\mathbb{K}$. Si n est impair, a carré équivaut à Δ non carré et si n est pair, les deux quantités sont des carrés ou des non carrés simultanément. La démonstration de la proposition en découle. □

5.2. **Classes d'isomorphismes.**

5.2.1. *Le cas où $E_{a,b}$ a un point de 2-torsion.*

Lemme 2. *Si $E_{a,b}$ a un point de torsion, alors $E_{a,b}$ est isomorphe à $E_{a,0}$.*

Démonstration : En effet, si x_0 est une racine de $X^3 + aX + b$, le changement de variable $(X, Y) \mapsto (X + x_0, Y)$ envoie $E_{a,b}$ sur $E_{a,0}$. □

Démontrons alors

Théorème 10. *Si n est impair, il y a deux classes d'isomorphismes dont les représentants sont $E_{1,0}$ et $E_{-1,0}$. Si n est pair, soit γ un non carré dans $\mathbb{K}$. Alors les quatre classes d'isomorphismes sont $E_{-\gamma^k,0}$ avec $0 \leqslant k \leqslant 3$.*

Démonstration : Supposons n impair. Si a est un carré, c'est aussi une puissance quatrième et alors $E_{a,0}$ est isomorphe à $E_{1,0}$. Si a n'est pas un carré, $-a$ est un carré et donc $E_{a,0}$ est isomorphe à $E_{-1,0}$.

Si n est pair, alors il existe λ dans $\mathbb{K}$ et k, $0 \leqslant k \leqslant 3$ tel que $a = -\lambda^4\gamma^k$. Utilisant la proposition 1, on voit que les courbes $E_{-\gamma^k,0}$ sont dans des classes d'isomorphismes différentes. □

5.2.2. *Le cas où $E_{a,b}$ n'a pas de 2-torsion.*

Théorème 11. *Quand n est impair, $E_{a,b}$ est isomorphe à $E_{-1,\beta}$, avec β dans $\mathbb{K}$. Si n est pair, $E_{a,b}$ est isomorphe à $E_{-1,\beta}$ ou $E_{-\gamma^2,\gamma^3\beta}$.*

Démonstration : Si n est impair, on remarque d'après la proposition 2 que a n'est pas un carré, donc est égal à l'opposé d'une puissance quatrième et en utilisant la proposition 1, on peut trouver β tel que $E_{a,b}$ soit isomorphe à $E_{-1,\beta}$.

Supposons maintenant n pair. D'après la proposition 2, a est un carré. Si a est une puissance quatrième, $E_{a,b}$ est isomorphe à $E_{-1,\beta}$ et si a n'est pas une puissance quatrième, $E_{a,b}$ est isomorphe à $E_{-\gamma^2,\gamma^3\beta}$. □

5.3. **Nombre de points.**

5.3.1. *Résultat fondamental.* Évaluons les quantités $N_k = \#\{x \in \mathbb{K}, \mathrm{Tr}(x^2) = k\}$ pour $k \in \{0, \pm 1\}$.

Proposition 3. *Soit $\zeta = \zeta_3$ une racine cubique de l'unité dans $\mathbb{C}$ et $\mathcal{G} = G_n(\eta)$. Alors*

$$N_0 = \frac{q + \mathcal{G} + \overline{\mathcal{G}}}{3}, \quad N_1 = \frac{q + \zeta^{-1}\mathcal{G} + \zeta\overline{\mathcal{G}}}{3}, \quad N_{-1} = \frac{q + \zeta\mathcal{G} + \zeta^{-1}\overline{\mathcal{G}}}{3}.$$

Démonstration : On a

$$\sum_{x \in \mathbb{K}} \zeta^{\mathrm{Tr}(x^2)} = N_0 + \zeta N_1 + \zeta^{-1} N_{-1} = \mathcal{G}$$

d'après le théorème 6. Conjugant cette relation et ajoutant l'équation $N_0 + N_1 + N_{-1} = q$, on en déduit les valeurs de N_k. □

5.3.2. *Le cas n impair.*

Théorème 12. *Soit $n = 2r + 1$ et soit β un élément de $\mathbb{K}$. Alors*

$$t_{-1,\beta} = (-1)^{r+1} \mathrm{Tr}(\beta) \sqrt{3q}.$$

Démonstration : On peut récrire l'équation de la courbe $E_{-1,\beta}$ sous la forme $X - X^3 = \beta - Y^2$. Pour Y fixé, cette équation a 3 solutions si et seulement si $\mathrm{Tr}(\beta - Y^2) = 0$ et 0 sinon, d'après le théorème de Hilbert (voir par exemple [17]). Posons $\tau = \mathrm{Tr}(\beta)$. On a ainsi $\#E_{-1,\beta}(\mathbb{K}) = 1 + 3N_\tau$ et on applique la proposition 3. □

5.3.3. *Le cas n pair.* Le théorème suivant se démontre de la même façon. On retrouve ainsi un cas particulier de [30].

Théorème 13. *Soient $n = 2r$ et β un élément de $\mathbb{K}$. Si $\mathrm{Tr}(\beta) = 0$, alors*

$$t_{-1,\beta} = 2(-1)^r \sqrt{q},$$

et si $\mathrm{Tr}(\beta) \neq 0$, alors

$$t_{-1,\beta} = (-1)^{r+1} \sqrt{q},$$

Le résultat qui suit est une application directe du théorème 7.

Théorème 14. *Soit γ un non carré dans $\mathbb{K}$. Alors $t_{-\gamma,0} = 0$.*

6. Le cas $p > 3$

Rappelons les propriétés suivantes.

Proposition 4. *Deux courbes $E_{a,b}$ et $E_{a',b'}$ sont isomorphes si et seulement s'il existe u dans $\mathbb{K}^*$ tel que $(a', b') = (u^4 a, u^6 b)$.*

Proposition 5. *Soit j_0 un élément de $\mathbb{K}$. Si $j_0 = 0$, les courbes ayant cet invariant sont les courbes $E_{0,b}$ avec $b \neq 0$; si $j_0 = 1728$, ce sont les courbes $E_{a,0}$ avec $a \neq 0$; si $j_0 \neq 0, 1728$, on pose $k = j_0/(1728 - j_0)$ et on prend $E_{3k,2k}$. Cette courbe sera désignée par $E(j_0)$.*

6.1. **Le cas n impair.**

Dans ce cas, le seul t possible est $t = 0$ et il y a $N(0) = H(-4p)$ classes. On peut regrouper les représentants des classes sur $\mathbb{F}_p$ en paires de courbes tordues l'une de l'autre. Il est facile de voir que ces courbes restent non isomorphes dans une extension de degré impair. De plus, deux courbes tordues sur $\mathbb{F}_p$ restent tordues sur toute extension de degré impair.

Une simple application du théorème de Weil donne :

Lemme 3. *Si $E/\mathbb{F}_p$ a $p + 1$ points, alors $E/\mathbb{F}_{p^n}$ a $p^n + 1$ points pour tout n impair.*

En conclusion, la classification des courbes sur $\mathbb{F}_p$ fournit immédiatement la classification sur $\mathbb{F}_{p^n}$.

6.2. **Le cas n pair.**

6.2.1. *Le cas $j(E) = 0$.* C'est le cas où $p \equiv 2 \bmod 3$. On sait qu'il y a deux classes de courbes pour chaque valeur de $t = \pm\sqrt{q}$. L'équation la plus générale d'une courbe d'invariant nul est $E\ : y^2 = x^3 + b$, $b \neq 0$. On utilise :

Proposition 6. *Écrivons $n = 2r$ comme dans la section 4.2.2. Si b n'est pas un cube, alors $t(E) = (-1)^{r+1}\eta(b)\sqrt{q}$.*

Démonstration : Si b n'est pas un cube, on a $\Re(\chi(b)) = -1/2$ et donc $t(E) = -\Psi_{n,3}(b) = (-1)^{r+1}\eta(b)\sqrt{q}$ d'après le théorème 8. □

De cela on déduit les deux représentants cherchés.

Théorème 15. *Soient b et μ des non cubes. Alors les deux courbes $E_{0,b}$ et $E_{0,\mu^2 b}$ sont non isomorphes et isogènes.*

Les représentants de la classe $-t_{0,b}$ sont bien sûr les tordues de ces courbes.

Notons que si on prend b un cube, alors la courbe $E_{0,b}$ fournit un représentant de la classe $\pm 2\sqrt{q}$.

6.2.2. *Le cas $j(E) = 1728$.* Dans ce cas, $p \equiv 3 \bmod 4$, $t = 0$ et il y a là encore deux classes de courbes. La forme la plus générale d'une courbe elliptique est $E_{a,0}$ avec $a \neq 0$. Il suffit de prendre a non carré et d'appliquer le théorème 7. Le second représentant est donné par une tordue de $E_{a,0}$.

Notons là aussi que prendre a puissance quatrième fournit une courbe dont le nombre de points est $\pm 2\sqrt{q}$.

6.2.3. *Les autres cas.* Ces cas sont ceux où $t = \pm 2\sqrt{q}$. On commence par chercher des représentants des $\mathcal{Q}(p)$ classes de courbes dans $\mathbb{F}_{p^2}$. Pour chaque invariant supersingulier j_0 dans $\mathbb{F}_{p^2}$, on appelle E la courbe ayant $t = 2\sqrt{p^2}$ et $\tilde{E}$ sa tordue, qui a $t = -2\sqrt{p^2}$. D'après le théorème de Weil, la courbe $E/\mathbb{F}_{(p^2)^r}$ a également $t = 2\sqrt{p^{2r}}$. Une tordue de E *sur* $\mathbb{F}_{p^{2r}}$, a alors $t = -2\sqrt{p^{2r}}$.

6.2.4. *Table numérique.* On représente $\mathbb{F}_{p^2}$ comme $\mathbb{F}_p[T]/(f(T))$ où $f(T) = T^2 - A$ et A le plus petit non résidu quadratique modulo p. Soit j_0 un invariant supersingulier dans $\mathbb{F}_{p^2}$. Il s'écrit $j_0 = a + bT$. Soit σ la conjugaison dans $\mathbb{F}_{p^2}$: $\sigma(u + vT) = u - vT$.

Lemme 4. *Les courbes $E(j_0)$ et $E(\sigma(j_0))$ ont même cardinalité.*

Démonstration : Écrivons

$$t(E(\sigma(j_0))) = -\sum_{x\in\mathbb{K}} \eta(x^3 + 3\sigma(k)x + 2\sigma(k)) = -\sum_{x\in\mathbb{K}} \eta(\sigma(x)^3 + 3\sigma(k)\sigma(x) + 2\sigma(k))$$

$$= -\sigma\left(\sum_{x\in\mathbb{K}} \eta(x^3 + 3kx + 2k)\right) = -t(E(j_0)).\square$$

On donne dans les tables 2 et 3 les valeurs des invariants supersinguliers de $\mathbb{F}_{p^2}$ pour $p \leqslant 307$. Pour chaque facteur $F(J)$ de degré 2 de $S_p(J)$, on indique le signe ε de $t(E(j_0))$ où j_0 est n'importe quelle racine de $F(J)$, ce qui est justifié par le lemme précédent.

Références

[1] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime. Draft, 1988.

[2] A. O. L. Atkin. The number of points on an elliptic curve modulo a prime (ii). Draft, 1992.

[3] B. C. Berndt and R. J. Evans. Sums of Gauss, Jacobi and Jacobsthal. *J. Number Theory 11* (1979), 349–398.

[4] B. J. Birch and W. Kuyk, Eds. *Modular functions of one variable IV* (1975), vol. 476 of *Lecture Notes in Math.*, Springer. Proceedings International Summer School University of Antwerp, RUCA, July 17-Agust 3, 1972.

[5] H. Davenport and H. Hasse. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *J. Reine Angew. Math. 172* (1935), 151–182.

p	A	j	ε	p	A	j	ε	p	A	j	ε
37	2	$27T+3$	$-$			$66T+43$	$+$			$34T+135$	$+$
43	2	$35T+12$	$-$			$10T+55$	$+$			$123T+130$	$+$
53	2	$44T+28$	$-$	163	2	$65T+22$	$+$	223	3	$129T+68$	$-$
61	2	$4T+42$	$-$			$14T+151$	$+$			$153T+124$	$+$
67	2	$32T+63$	$-$			$148T+87$	$-$			$103T+136$	$-$
		$30T+45$	$-$			$79T+127$	$+$			$111T+13$	$+$
73	5	$37T+8$	$-$			$120T+128$	$+$			$70T+217$	$-$
		$68T+39$	$-$			$2T+19$	$-$			$92T+43$	$-$
79	3	$41T+72$	$+$	167	5	$103T+79$	$+$	227	2	$84T+143$	$-$
83	2	$48T+38$	$+$			$114T+88$	$-$			$96T+2$	$-$
89	3	$50T+76$	$-$	173	2	$145T+31$	$-$			$188T+77$	$-$
97	5	$22T+81$	$-$			$65T+119$	$-$			$96T+73$	$-$
		$28T+45$	$+$			$50T+114$	$+$			$135T+176$	$-$
		$3T+76$	$+$			$60T+97$	$+$	229	2	$139T+213$	$-$
101	2	$100T+37$	$+$	179	2	$16T+109$	$-$			$7T+219$	$+$
103	3	$73T+20$	$-$			$10T+5$	$-$			$4T+83$	$-$
		$17T+61$	$+$			$77T+107$	$+$			$218T+89$	$+$
107	2	$68T+66$	$-$	181	2	$117T+54$	$-$			$28T+222$	$-$
		$26T+74$	$-$			$55T+107$	$+$			$160T+148$	$+$
109	2	$102T+98$	$+$			$140T+3$	$-$			$105T+87$	$+$
		$3T+70$	$-$			$18T+16$	$-$	233	3	$137T+32$	$-$
		$15T+24$	$+$			$72T+36$	$-$			$211T+152$	$-$
113	3	$74T+104$	$+$	191	7	$130T+23$	$+$			$213T+201$	$-$
		$34T+97$	$+$			$150T+126$	$+$			$65T+89$	$-$
		$99T+52$	$+$	193	5	$177T+148$	$+$			$127T+43$	$-$
127	3	$28T+55$	$-$			$55T+119$	$-$			$105T+104$	$-$
		$124T+16$	$-$			$68T+80$	$-$			$47T+76$	$+$
		$80T+83$	$+$			$58T+118$	$+$	239	7	$82T+141$	$-$
131	2	$36T+89$	$-$			$148T+114$	$-$			$100T+191$	$-$
137	3	$41T+19$	$-$			$97T+17$	$+$			$154T+94$	$+$
		$100T+122$	$-$			$35T+137$	$+$	241	7	$19T+227$	$+$
		$12T+73$	$+$	197	2	$174T+188$	$+$			$29T+65$	$+$
		$116T+49$	$-$			$115T+113$	$+$			$171T+107$	$-$
139	2	$73T+123$	$-$			$34T+59$	$+$			$116T+158$	$+$
		$37T+57$	$+$			$132T+61$	$+$			$89T+161$	$+$
		$137T+135$	$+$			$153T+24$	$+$			$105T+115$	$-$
149	2	$113T+140$	$-$			$84T+42$	$-$			$138T+138$	$+$
		$129T+85$	$+$	199	3	$36T+50$	$-$	251	2	$42T+166$	$+$
		$23T+92$	$+$			$156T+177$	$-$			$37T+30$	$-$
151	3	$68T+149$	$-$			$18T+189$	$+$			$125T+79$	$-$
		$6T+133$	$+$			$137T+191$	$+$			$67T+178$	$+$
		$67T+41$	$-$	211	2	$63T+45$	$-$	257	3	$254T+28$	$-$
157	2	$106T+22$	$-$			$203T+183$	$+$			$209T+34$	$-$
		$46T+143$	$+$			$181T+118$	$-$			$150T+52$	$-$
		$149T+75$	$+$			$179T+119$	$+$			$128T+135$	$-$

TABLE 2. Invariants supersinguliers de $\mathbb{F}_{p^2}$

p	A	j	ε	p	A	j	ε	p	A	j	ε
257	3	$31T+20$	$-$			$110T+41$	$+$			$66T+255$	$-$
		$162T+37$	$+$			$56T+163$	$+$			$193T+196$	$+$
		$167T+26$	$-$			$241T+53$	$+$	293	2	$271T+137$	$-$
263	5	$18T+53$	$+$			$24T+110$	$-$			$259T+233$	$-$
		$127T+55$	$-$			$198T+261$	$+$			$270T+62$	$+$
		$143T+23$	$-$			$6T+191$	$-$			$292T+292$	$-$
		$128T+162$	$+$			$113T+93$	$+$			$64T+241$	$+$
		$134T+84$	$-$			$130T+22$	$-$			$263T+266$	$+$
269	2	$188T+178$	$+$	281	3	$189T+116$	$-$			$47T+229$	$+$
		$T+82$	$+$			$173T+180$	$-$			$123T+25$	$+$
		$150T+193$	$+$			$29T+122$	$+$	307	2	$29T+253$	$-$
		$253T+253$	$-$			$159T+75$	$+$			$163T+132$	$+$
		$259T+153$	$+$			$82T+181$	$+$			$269T+225$	$+$
		$232T+258$	$-$			$250T+19$	$-$			$144T+177$	$+$
271	3	$118T+57$	$-$			$133T+132$	$+$			$37T+154$	$+$
		$125T+162$	$-$	283	2	$161T+119$	$-$			$249T+33$	$-$
		$116T+35$	$+$			$197T+208$	$+$			$4T+230$	$+$
		$63T+183$	$+$			$75T+86$	$+$			$174T+118$	$-$
		$226T+231$	$-$			$190T+183$	$-$			$271T+131$	$-$
		$182T+238$	$+$			$227T+29$	$+$			$79T+256$	$+$
277	2	$115T+2$	$-$			$52T+177$	$+$				
		$217T+169$	$-$			$222T$	$-$				

TABLE 3. Invariants supersinguliers de $\mathbb{F}_{p^2}$, suite

[6] M. DEURING. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. *Abh. Math. Sem. Hamburg 14* (1941), 197–272.

[7] R. J. EVANS. Determinations of Jacobsthal sums. *Pacific J. Math. 110*, 1 (1984), 49–58.

[8] R. H. HUDSON AND K. S. WILLIAMS. Resolution of ambiguities in the evaluation of cubic and quartic Jacobsthal sums. *Pacific J. Math. 99*, 2 (1982), 379–386.

[9] E. JACOBSTAHL. Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier quadrate. *J. Reine Angew. Math. 132* (1907), 238–245.

[10] S. A. KATRE. Jacobsthal sums in terms of quadratic partitions of a prime. In *Number Theory* (1985), K. Alladi, Ed., vol. 1122 of *Lecture Notes in Math.*, Springer-Verlag, pp. 153–162. Proceedings of the 4th Matscience Conference held at Ootacamund, India, January 5-10, 1984.

[11] S. A. KATRE AND A. R. RAJWADE. Jacobsthal sums of prime order. *Indian J. Pure Appl. Math. 17*, 12 (Dec. 1986), 1345–1362.

[12] S. A. KATRE AND A. R. RAJWADE. Resolution of sign ambiguity in the determination of the cyclotomic numbers of order 4 and the corresponding Jacobstahal sum. *Math. Scand. 60* (1987), 52–62.

[13] E. LEHMER. On the number of solutions of $u^k + d \equiv w^2 \bmod p$. *Pacific J. Math. 5* (1955), 103–18.

[14] R. LERCIER AND F. MORAIN. Counting points on elliptic curves over F_{p^n} using Couveignes's algorithm. Research Report LIX/RR/95/09, École Polytechnique–LIX, Sept. 1995. An improved version is being submitted.

[15] R. LERCIER AND F. MORAIN. Counting the number of points on elliptic curves over finite fields: strategies and performances. In *Advances in Cryptology – EUROCRYPT '95* (1995), L. C. Guillou and J.-J. Quisquater, Eds., vol. 921 of *Lecture Notes in Comput. Sci.*, pp. 79–94. International Conference on the Theory and Application of Cryptographic Techniques, Saint-Malo, France, May 1995, Proceedings.

[16] R. LIDL AND H. NIEDERREITER. *Finite fields.* No. 20 in Encyclopedia of mathematics and its applications. Reading : Addison-Wesley, 1983.

[17] R. MCELIECE. *Finite fields for computer scientists and engineers.* Kluwer international series in engineering and computer science. Kluwer Academic Publishers, 1988.

[18] A. MENEZES AND S. VANSTONE. Isomorphism classes of elliptic curves over finite fields of characteristic 2. *Utilitas Math. 38* (1990), 135–153.
[19] A. J. MENEZES. *Elliptic curve public key cryptosystems*. Kluwer Academic Publishers, 1993.
[20] J.-F. MESTRE. La méthode des graphes. Exemples et applications. In *Proc. of the International Conference on class numbers and fundamental units of algebraic number fields* (Nagoya, 1986), Nagoya Univ., pp. 217–242. Katata (Japan).
[21] J.-F. MESTRE AND J. OESTERLÉ. La méthode des graphes. Preprint, 19??
[22] F. MORAIN. Calcul du nombre de points sur une courbe elliptique dans un corps fini : aspects algorithmiques. *J. Théor. Nombres Bordeaux 7* (1995), 255–282.
[23] R. SCHOOF. Nonsingular plane cubic curves over finite fields. *J. Combin. Theory Ser. A 46* (1987), 183–211.
[24] R. SCHOOF. Counting points on elliptic curves over finite fields. *J. Théor. Nombres Bordeaux 7* (1995), 219–254.
[25] M. A. SHOKROLLAHI. Generation of optimal bilinear multiplication algorithms: theory and implementation. Tech. Rep. 8575-CS, Universität Bonn, Dec. 1992.
[26] J. H. SILVERMAN. *The arithmetic of elliptic curves*, vol. 106 of *Graduate Texts in Mathematics*. Springer, 1986.
[27] T. STORER. *Cyclotomy and difference sets*. Markham Publ. Co., Chicago, 1967.
[28] R. G. SWAN. Factorization of polynomials over finite fields. *Pacific J. Math. 12* (1962), 1099–1106.
[29] E. WATERHOUSE. Abelian varieties over finite fields. *Ann. Sci. École Norm. Sup. 2* (1969), 521–560.
[30] J. WOLFMANN. Nombre de points rationnels de courbes algébriques sur des corps finis associées à des codes cycliques. *C. R. Acad. Sci. Paris Sér. I Math. 305* (1987), 345–348.

LABORATOIRE D'INFORMATIQUE DE L'ÉCOLE POLYTECHNIQUE (LIX), F-91128 PALAISEAU CEDEX, FRANCE
E-mail address: `morain@polytechnique.fr`