Journal of Computational Mathematics, Vol.20, No.4, 2002, 337–348.

ISOGENOUS OF THE ELLIPTIC CURVES OVER THE RATIONALS[*1)]

Abderrahmane Nitaj
(*Mathematik, Universität des Saarlandes, Postfach 15 1150, D-66041, Saarbrücken, Germany*)

Abstract

An elliptic curve is a pair (E, O), where E is a smooth projective curve of genus 1 and O is a point of E, called the point at infinity. Every elliptic curve can be given by a Weierstrass equation

$$E: \qquad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Let $\mathbb{Q}$ be the set of rationals. E is said to be difined over $\mathbb{Q}$ if the coefficients a_i, $i = 1, 2, 3, 4, 6$ are rationals and O is defined over $\mathbb{Q}$.

Let $E/\mathbb{Q}$ be an elliptic curve and let $E(\mathbb{Q})_{\text{tors}}$ be the torsion group of points of E defined over $\mathbb{Q}$. The theorem of Mazur asserts that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 1, 2, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, 2, 3, 4. \end{cases}$$

We say that an elliptic curve $E'/\mathbb{Q}$ is isogenous to the elliptic curve E if there is an isogeny, i.e. a morphism $\phi : E \to E'$ such that $\phi(O) = O$, where O is the point at infinity.

We give an explicit model of all elliptic curves for which $E(\mathbb{Q})_{\text{tors}}$ is in the form $\mathbb{Z}/m\mathbb{Z}$ where $m = 9, 10, 12$ or $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ where $m = 4$, according to Mazur's theorem. Morever, for every family of such elliptic curves, we give an explicit model of all their isogenous curves with cyclic kernels consisting of rational points.

Key words: Courbe elliptique, Isogénie.

1. Introduction

Soit E une courbe elliptique définie sur $\mathbb{Q}$ par la forme de Weierstrass-Tate:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

avec $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. Soit $m \geq 1$ un entier. Si E admet un point de torsion d'ordre exactement m, alors E est paramétrisable par la courbe modulaire $X_1(m)$. D'après le théorème de Mazur [4], la structure du sous-groupe des points de torsion $E(\mathbb{Q})_{\text{tors}}$ est de la forme

$$E(\mathbb{Q})_{\text{tors}} = \begin{cases} \mathbb{Z}/m\mathbb{Z}, & m = 1, 2, \ldots, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, 2, 3, 4. \end{cases}$$

Ainsi, pour $m \in \{1, \ldots, 10, 12\}$, la courbe modulaire $X_1(m)$ est de genre nul, et on peut donc exprimer les quantités a_1, a_2, a_3, a_4, a_6 à l'aide des mêmes paramètres. Des paramétrisations de quelques courbes elliptiques définies sur $\mathbb{Q}$ et ayant un sous-groupe $E(\mathbb{Q})_{\text{tors}}$ donné ont été données (voir par exemple [1], [2], [6] et [7]). D'autre part, toutes les isogènes des courbes elliptiques de sous-groupe de torsion $E(\mathbb{Q})_{\text{tors}}$ de la forme $\mathbb{Z}/m\mathbb{Z}$, $m = 2, \ldots, 8$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$, $m = 1, 2, 3$, correspondant à des isogénies de noyaux formés par des points rationnels,

* Received May 17, 1999; Final revised July 7, 2000.
1) This research was supported by the TMR programme of the European Community under contract ERBFMBICT960848.

ont été explicitées dans [6]. Nous complétons ici ce formulaire dans le cas où $E(\mathbb{Q})_{\text{tors}}$ est de la forme $\mathbb{Z}/m\mathbb{Z}$ avec $m = 9, 10, 12$ ou de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ avec $m = 4$.

Si E admet un point de torsion d'ordre m, on peut, par translation, ramener ce point à $P_0 = (0,0)$. On peut ainsi écrire l'équation de E sous la forme (1) avec $a_6 = 0$. On peut d'autre part transformer E de telle sorte que la ligne $y = 0$ soit tangente en P_0. Ceci donne alors $a_4 = 0$. Finalement l'équation de E peut s'écrire sous la forme

$$E:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2.$$

Si P_0 est d'ordre $m \geq 4$, alors $a_2 \neq 0$ et $a_3 \neq 0$. Le changement de variables $(x, y) = (u^2x', u^3y')$ transforme l'équation de E en:

$$E:\ y'^2 + u^{-1}a_1x'y' + u^{-3}a_3y' = x'^3 + u^{-2}a_2x'^2.$$

Le choix $u = a_3/a_2$ permet d'avoir $u^{-3}a_3 = u^{-2}a_2$. En posant alors $u^{-1}a_1 = 1 - A/C$, $u^{-3}a_3 = -B/C$, où A, B et C sont des entiers, et en effectuant la transformation $(x', y') = (C^{-2}X, C^{-3}Y)$, l'équation de E devient:

$$E = E(A,B,C):\ Y^2 + (C - A)XY - BC^2Y = X^3 - BCX^2. \tag{2}$$

Pour $m \geq 4$, la structure de $X_1(m)$ peut être déterminée à l'aide de l'équation $\Psi_m(0,0) = 0$, où $\Psi_m(X,Y)$ est le polynôme de m-division (voir [6] ou [8]). Ceci permet d'exprimer A, B et C en fonction de deux paramètres s et t. On peut donc déterminer facilement tous les points de torsion rationnels de E, et déterminer la structure exacte du sous-groupe des points de torsion de E. Dans ce cas, les formules de Vélu [9] permettent alors de déterminer une expression de toutes les isogènes de E, en divisant E par les sous-groupes cycliques composés de points rationnels. Cette méthode a été utilisée dans [6] pour une partie des courbes elliptiques définies sur $\mathbb{Q}$ et ayant un point de torsion d'ordre m, avec $2 \leq m \leq 8$.

Nous donnons dans les parties 2, 3, 4 et 5 les différentes expressions obtenues de cette façon à partir des courbes elliptiques définies sur $\mathbb{Q}$ et ayant un sous-groupe de points de torsion de la forme $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ ou de la forme $\mathbb{Z}/m\mathbb{Z}$ avec $m = 9, 10, 12$. Dans ce travail, les courbes elliptiques sont indexées en poursuivant la numérotation commencée dans [6].

2. Courbes Elliptiques de Sous-groupe $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

L'expression des courbes elliptiques ayant $P_0 = (0,0)$ pour point de torsion d'ordre 8 a été déterminée dans [6]. Son équation est

$$\begin{aligned} E_{31}:\ y^2 - (2S^2 - 4ST + T^2)xy - S^3T(S-T)(2S-T)y \\ = x^3 - S^2(S-T)(2S-T)x^2, \end{aligned}$$

et a pour discriminant

$$\Delta_{31} = S^8T^2(S-T)^8(2S-T)^4(8S^2 - 8ST + T^2).$$

Le cas où $8S^2 - 8ST + T^2$ n'est pas un carré a été étudié dans [6] et donne lieu aux isogènes E_{32}, E_{33}, E_{34}, E_{35}, E_{36}.

2.1. Courbe Elliptique E_{37}

Supposons donc ici que $8S^2 - 8ST + T^2 = Z^2$ pour un rationnel Z. On écrit alors

$$8S^2 - 8ST + T^2 = (T - 4S)^2 - 8S^2 = Z^2,$$

ce qui donne la paramétrisation

$$S = st, \quad T = s^2 + 4st + 2t^2, \qquad Z = s^2 - 2t^2.$$

L'équation de E_{31} devient donc :

$$E_{37}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

avec

$$\begin{aligned}
a_1 &= -(s^4 + 4s^3t + 6s^2t^2 + 8st^3 + 4t^4),\\
a_2 &= -s^2t^2(s+t)(s+2t)(s^2+2st+2t^2),\\
a_3 &= -s^3t^3(s+t)(s+2t)(s^2+2st+2t^2)(s^2+4st+2t^2).
\end{aligned}$$

Le discriminant est alors :

$$\Delta_{37} = s^8t^8(s+t)^8(s+2t)^8(s^2-2t^2)^2(s^2+2st+2t^2)^4(s^2+4st+2t^2)^2.$$

La courbe E_{37} a trois points de torsion d'ordre 2, dont $R_1 = (x_1, -(a_1x_1+a_3)/2)$, avec $x_1 = -t^3(s+t)(s^2+2st+2t^2)(s^2+4st+2t^2)$. Les différents sous-groupes finis sont alors $< 4P_0 >$, $< R_1 >$, $< 4P_0 + R_1 >$, $< 2P_0 >$, $< 2P_0 + R_1 >$, $< P_0 >$ et $< P_0 + R_1 >$.

2.2. Courbe Elliptique E_{38}

En divisant E_{37} par le sous-groupe $< 4P_0 >$, on trouve la courbe

$$E_{38}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{aligned}
a_1 &= -(s^4 + 4s^3t + 6s^2t^2 + 8st^3 + 4t^4),\\
a_2 &= -s^2t^2(s+t)(s+2t)(s^2+2st+2t^2),\\
a_3 &= -s^3t^3(s+t)(s+2t)(s^2+2st+2t^2)(s^2+4st+2t^2),\\
a_4 &= -5s^4t^4(s+2t)^4(s+t)^4,\\
a_6 &= -s^4t^4(s+t)^4(s+2t)^4\\
&\quad \times (s^8 + 8s^7t + 24s^6t^2 + 37s^5t^3 + 47s^4t^4 + 74s^3t^5 + 96s^2t^6 + 64st^7 + 16t^8).
\end{aligned}$$

Le discriminant est alors

$$\Delta_{38} = s^4t^4(s+t)^4(s+2t)^4(s^2-2t^2)^4(s^2+2st+2t^2)^8(s^2+4st+2t^2)^4.$$

2.3. Courbe Elliptique E_{39}

En divisant E_{37} par le sous-groupe $< R_1 >$, on trouve la courbe

$$E_{39}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{aligned}
a_1 &= -(s^4 + 4s^3t + 6s^2t^2 + 8st^3 + 4t^4),\\
a_2 &= -s^2t^2(s+t)(s+2t)(s^2+2st+2t^2),\\
a_3 &= -s^3t^3(s+t)(s+2t)(s^2+2st+2t^2)(s^2+4st+2t^2),\\
a_4 &= 5t^4(s+t)^4(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2),\\
a_6 &= t^4(s+t)^4(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2)\\
&\quad \times (s^8 + 8s^7t + 24s^6t^2 + 37s^5t^3 + 19s^4t^4 - 38s^3t^5 - 72s^2t^6 - 48st^7 - 12t^8).
\end{aligned}$$

Le discriminant est alors

$$\Delta_{39} = -s^{16}t^4(s+t)^4(s+2t)^{16}(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2).$$

2.4. Courbe Elliptique E_{40}

En divisant E_{37} par le sous-groupe $< 4P_0 + R_1 >$, on trouve la courbe

$$E_{40}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec

$$\begin{aligned}
a_1 &= -\frac{1}{2}(s^4+4s^3t+6s^2t^2+8st^3+4t^4),\\
a_2 &= -\frac{1}{4}s^2t^2(s+t)(s+2t)(s^2+2st+2t^2),\\
a_3 &= -\frac{1}{8}s^3t^3(s+t)(s+2t)(s^2+2st+2t^2)(s^2+4st+2t^2),\\
a_4 &= -\frac{5}{256}s^4(s+2t)^4(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2),\\
a_6 &= \frac{1}{4096}s^4(s+2t)^4(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2)\\
&\quad \times (3s^8+24s^7t+72s^6t^2+76s^5t^3-76s^4t^4-296s^3t^5-384s^2t^6-256st^7-64t^8).
\end{aligned}$$

Le discriminant est alors

$$\Delta_{40} = s^4t^{16}(s+t)^{16}(s+2t)^4(s^2-2t^2)(s^2+2st+2t^2)^2(s^2+4st+2t^2).$$

2.5. Courbe elliptique E_{41}

En divisant E_{37} par le sous-groupe $< 2P_0 >$, on trouve la courbe

$$E_{41}:\ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

avec

$$\begin{aligned}
a_1 &= -(s^4+4s^3t+6s^2t^2+8st^3+4t^4),\\
a_2 &= -s^2t^2(s+t)(s+2t)(s^2+2st+2t^2),\\
a_3 &= -s^3t^3(s+t)(s+2t)(s^2+2st+2t^2)(s^2+4st+2t^2),\\
a_4 &= -5s^2t^2(s+t)^2(s+2t)^2\\
&\quad \times (s^8+8s^7t+33s^6t^2+86s^5t^3+149s^4t^4+172s^3t^5+132s^2t^6+64st^7+16t^8),\\
a_6 &= -s^2t^2(s+t)^2(s+2t)^2\\
&\qquad \times \big(s^{16}+16s^{15}t+135s^{14}t^2+775s^{13}t^3+3274s^{12}t^4+10531s^{11}t^5+26353s^{10}t^6\\
&\qquad\quad +52125s^9t^7+82339s^8t^8+104250s^7t^9+105412s^6t^{10}+84248s^5t^{11}\\
&\qquad\quad +52384s^4t^{12}+24800s^3t^{13}+8640s^2t^{14}+2048st^{15}+256t^{16}\big).
\end{aligned}$$

Le discriminant est alors

$$\Delta_{41} = s^2t^2(s+t)^2(s+2t)^2(s^2-2t^2)^8(s^2+2st+2t^2)^4(s^2+4st+2t^2)^8.$$

2.6. Courbe Elliptique E_{42}

En divisant E_{37} par le sous-groupe $< 2P_0 + R_1 >$, on peut écrire le résultat sous la forme:

$$E_{42}:\ y^2 = x^3+\frac{b_2}{4}x^2+\frac{b_4}{2}x+\frac{b_6}{4},$$

avec

$$\begin{aligned}
b_2 &= s^8 + 8s^7t + 24s^6t^2 + 44s^5t^3 + 68s^4t^4 + 88s^3t^5 + 96s^2t^6 + 64st^7 + 16t^8, \\
b_4 &= s^2t^2(s+2t)(s+t) \\
&\quad \times \Big(10s^{10} + 111s^9t + 420s^8t^2 + 432s^7t^3 - 1106s^6t^4 - 3254s^5t^5 - 2212s^4t^6 \\
&\quad + 1728s^3t^7 + 3360s^2t^8 + 1776st^9 + 320t^{10}\Big), \\
b_6 &= s^2t^2(s+2t)^2(s+t)^2 \\
&\quad \times \left(s^8 + 8s^7t + 8s^6t^2 - 60s^5t^3 - 164s^4t^4 - 120s^3t^5 + 32s^2t^6 + 64st^7 + 16t^8\right) \\
&\quad \times \Big(4s^8 + 32s^7t + 68s^6t^2 - 36s^5t^3 - 223s^4t^4 - 72s^3t^5 + 272s^2t^6 + 256st^7 \\
&\quad + 64t^8\Big).
\end{aligned}$$

Son discriminant est

$$\Delta_{42} = -s^2t^2(s+t)^2(s+2t)^2(s^2-2t^2)^2(s^2+2st+2t^2)^{16}(s^2+4st+2t^2)^2.$$

2.7. Courbe Elliptique E_{43}

En divisant E_{37} par le sous-groupe $< P_0 >$, on trouve une courbe dont l'équation peut être ramenée sous la forme :

$$E_{43}:\ y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

avec

$$\begin{aligned}
b_2 &= s^8 + 8s^7t + 24s^6t^2 + 44s^5t^3 + 68s^4t^4 + 88s^3t^5 + 96s^2t^6 + 64st^7 + 16t^8, \\
b_4 &= -st(s+2t)(s+t) \\
&\quad \times \Big(10s^{12} + 210s^{11}t + 1869s^{10}t^2 + 9620s^9t^3 + 32328s^8t^4 + 75346s^7t^5 \\
&\quad + 125494s^6t^6 + 150692s^5t^7 + 129312s^4t^8 + 76960s^3t^9 + 29904s^2t^{10} \\
&\quad + 6720st^{11} + 640t^{12}\Big), \\
b_6 &= -st(s+2t)(s+t) \\
&\quad \times \Big(s^8 + 24s^7t + 152s^6t^2 + 484s^5t^3 + 892s^4t^4 + 968s^3t^5 + 608s^2t^6 + 192st^7 \\
&\quad + 16t^8\Big) \\
&\quad \times \Big(4s^{12} + 76s^{11}t + 652s^{10}t^2 + 3304s^9t^3 + 11012s^8t^4 + 25547s^7t^5 + 42485s^6t^6 \\
&\quad + 51094s^5t^7 + 44048s^4t^8 + 26432s^3t^9 + 10432s^2t^{10} + 2432st^{11} + 256t^{12}\Big).
\end{aligned}$$

Le discriminant est

$$\Delta_{43} = st(s+t)(s+2t)(s^2-2t^2)^{16}(s^2+2st+2t^2)^2(s^2+4st+2t^2)^4.$$

2.8. Courbe Elliptique E_{44}

En divisant E_{37} par le sous-groupe $< P_0 + R_1 >$, on peut écrire le résultat sous la forme :

$$E_{44}:\ y^2 = x^3 + \frac{b_2}{4}x^2 + \frac{b_4}{2}x + \frac{b_6}{4},$$

avec

$$\begin{aligned}
b_2 &= s^8 + 8s^7t + 24s^6t^2 + 44s^5t^3 + 68s^4t^4 + 88s^3t^5 + 96s^2t^6 + 64st^7 + 16t^8,\\
b_4 &= st(s+t)(s+2t)\\
&\quad \times \Big(10s^{12} + 30s^{11}t - 109s^{10}t^2 - 820s^9t^3 - 2328s^8t^4 - 4306s^7t^5 - 6454s^6t^6\\
&\qquad - 8612s^5t^7 - 9312s^4t^8 - 6560s^3t^9 - 1744s^2t^{10} + 960st^{11} + 640t^{12}\Big),\\
b_6 &= st(s+t)(s+2t)\\
&\quad \times \Big(s^8 - 8s^7t - 72s^6t^2 - 220s^5t^3 - 388s^4t^4 - 440s^3t^5 - 288s^2t^6 - 64st^7\\
&\qquad + 16t^8\Big)\\
&\quad \times \Big(4s^{12} + 20s^{11}t + 36s^{10}t^2 + 64s^9t^3 + 324s^8t^4 + 1125s^7t^5 + 2123s^6t^6\\
&\qquad + 2250s^5t^7 + 1296s^4t^8 + 512s^3t^9 + 576s^2t^{10} + 640st^{11} + 256t^{12}\Big).
\end{aligned}$$

Le discriminant est

$$\Delta_{44} = -st(s+t)(s+2t)(s^2-2t^2)^4(s^2+2st+2t^2)^2(s^2+4st+2t^2)^{16}.$$

3. Courbes Elliptiques de Sous-groupe $E(\mathbb{Q})_{\mathbf{tors}} = \mathbb{Z}/9\mathbb{Z}$

3.1. Courbe Elliptique E_{45}

Pour que le point $P_0 = (0,0)$ soit d'ordre 9 sur la courbe elliptique E définie par (2), on doit avoir $\Psi_9(0,0) = 0$, et donc

$$A^5 + CA^4 + A^3C^2 - A^3BC - 3A^2BC^2 + 3AB^2C^2 - B^3C^2 = 0.$$

Ainsi $(A/C, B/C)$ est un point rationnel sur la courbe singulière d'équation :

$$X^5 + X^4 + X^3 - X^3Y - 3X^2Y + 3XY^2 - Y^3 = 0.$$

En posant $Y = dX$, on obtient $X^2 - dX + X = (d-1)^3$. En posant $X = (d-1)s/t$, avec s et t entiers, on en obtient $d = (s^2 - st + t^2)/t^2$. On peut alors prendre :

$$A = s^2t^2(s-t),\ B = s^2(s-t)(s^2-st+t^2),\ C = t^5.$$

Après réduction, l'équation de la courbe (2) devient :

$$E_{45}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

avec

$$\begin{aligned}
a_1 &= -(s^3 - s^2t - t^3),\\
a_2 &= -s^2t(s-t)(s^2-st+t^2),\\
a_3 &= -s^2t^4(s-t)(s^2-st+t^2).
\end{aligned}$$

Son discriminant est

$$\Delta_{45} = s^9t^9(s-t)^9(s^2-st+t^2)^3(s^3-6s^2t+3st^2+t^3).$$

Les sous-groupes finis nécessaires pour déterminer les isogènes de la courbe E_{45} sont $< 3P_0 >$ et $< P_0 >$.

3.2. Courbe Elliptique E_{46}

En divisant E_{45} par $< 3P_0 >$, on trouve la courbe

$$E_{46}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans E_{45} et avec

$$a_4 = -5s^3t^3(s-t)^3(s^3 - 3s^2t + t^3),$$
$$a_6 = -s^3t^3(s-t)^3 \times (s^9 - 9s^8t + 27s^7t^2 - 22s^6t^3 - 19s^5t^4 + 33s^4t^5 - 9s^3t^6 - 4s^2t^7 + t^9).$$

Le discriminant est alors

$$\Delta_{46} = s^3t^3(s-t)^3(s^2 - st + t^2)^9(s^3 - 6s^2t + 3st^2 + t^3)^3.$$

3.3. Courbe Elliptique E_{47}

En divisant E_{45} par $< P_0 >$, on trouve la courbe

$$E_{47}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans E_{45} et avec

$$a_4 = -5st(s-t) \times (s^9 - 8s^7t^2 + 25s^6t^3 - 47s^5t^4 + 61s^4t^5 - 53s^3t^6 + 28s^2t^7 - 9st^8 + t^9),$$
$$a_6 = -st(s-t) \times \Big(s^{15} + 8s^{14}t - 55s^{13}t^2 + 175s^{12}t^3 - 466s^{11}t^4 + 1173s^{10}t^5 - 2518s^9t^6 + 4189s^8t^7 - 5236s^7t^8 + 4938s^6t^9 - 3518s^5t^{10} + 1861s^4t^{11} - 698s^3t^{12} + 167s^2t^{13} - 23st^{14} + t^{15}\Big).$$

Le discriminant est alors

$$\Delta_{47} = st(s-t)(s^2 - st + t^2)^3(s^3 - 6s^2t + 3st^2 + t^3)^9.$$

4. Courbes Elliptiques de Sous-groupe $E(\mathbb{Q})_{\mathbf{tors}} = \mathbb{Z}/10\mathbb{Z}$

4.1. Courbe Elliptique E_{48}

Pour que le point $P_0 = (0,0)$ soit d'ordre 10 sur la courbe (2) avec $5P_0 \neq 0$, il faut avoir $A \neq B$ et $A^5 + A^4B + 3CA^3B + C^2A^2B - 3CA^2B^2 - 2C^2AB^2 + C^2B^3 = 0$. En posant $X = A/C$ et $Y = B/C$, on obtient la courbe singulière déquation:

$$X^5 + X^4Y + 3X^3Y + X^2Y - 3X^2Y^2 - 2XY^2 + Y^3 = 0.$$

Si on pose $Y = dX$ pù d est un rationnel, on obtient $X^2(d+1) + 3Xd(1-d) + d(1-d)^2 = 0$. Si on pose $X = (1-d)s/t$, où s et t sont des rationnels quelconques, on obtient alors

$$d = -\frac{s^2}{s^2 + 3st + t^2}, \ X = \frac{s(s+t)(2s+t)}{(s^2 + 3st + t^2)t}, \ Y = -\frac{s^3(s+t)(2s+t)}{t(s^2 + 3st + t^2)^2},$$

et donc

$$A = s(s+t)(2s+t)s^2 + 3st + t^2), \ B = -s^3(s+t)(2s+t), \ C = t(s^2 + 3st + t^2)^2.$$

Après réduction, on obtient la courbe d'équation :

$$E_{48}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

avec

$$a_1 = -(2s^3 + 2s^2t - 2st^2 - t^3),$$
$$a_2 = s^3t(s+t)(2s+t),$$
$$a_3 = s^3t^2(s+t)(2s+t)(s^2 + 3st + t^2).$$

Le discriminant est alors

$$\Delta_{48} = -s^{10}t^5(s+t)^{10}(2s+t)^5(s^2 + 3st + t^2)^2(4s^2 + 2st - t^2).$$

Les sous-groupes finis sont alors $< 5P_0 >$, $< 2P_0 >$ et $< P_0 >$.

4.2. Courbe elliptique E_{49}

En divisant E_{48} par $< 5P_0 >$, on trouve la courbe :

$$E_{49}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans E_{48} et avec

$$\begin{aligned} a_4 &= -5s^5(s+t)^5(s^2+3st+t^2), \\ a_6 &= -s^5(s+t)^5(s^2+3st+t^2)(-3s^6-12s^5t-20s^4t^2-15s^3t^3+4st^5+t^6). \end{aligned}$$

Le discriminant est alors

$$\Delta_{49} = s^5t^{10}(s+t)^5(2s+t)^{10}(s^2+3st+t^2)(4s^2+2st-t^2)^2.$$

4.3. Courbe Elliptique E_{50}

En divisant E_{48} par $< 2P_0 >$, on trouve la courbe :

$$E_{50}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans E_{48} et avec

$$\begin{aligned} a_4 &= 5s^2t(s+t)^2(2s+t)(4s^6-10s^4t^2-12s^3t^3-8s^2t^4-4st^5-t^6), \\ a_6 &= s^2t(s+t)^2(2s+t) \\ &\quad \times \Big(16s^{12}-48s^{11}t-316s^{10}t^2-562s^9t^3-570s^8t^4-578s^7t^5-683s^6t^6 \\ &\quad -626s^5t^7-370s^4t^8-141s^3t^9-38s^2t^{10}-8st^{11}-t^{12}\Big). \end{aligned}$$

Le discriminant est alors

$$\Delta_{50} = -s^2t(s+t)^2(2s+t)(s^2+3st+t^2)^{10}(4s^2+2st-t^2)^5.$$

4.4. Courbe Elliptique E_{51}

Enfin, en divisant E_{48} par $< P_0 >$, on trouve la courbe :

$$E_{51}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans E_{48} et avec

$$\begin{aligned} a_4 &= -5st(s+t) \\ &\quad \times \Big(s^{10}+7s^9t+83s^8t^2+346s^7t^3+739s^6t^4+935s^5t^5+729s^4t^6+352s^3t^7 \\ &\quad +102s^2t^8+16st^9+t^{10}\Big), \\ a_6 &= s(s+t) \\ &\quad \times \Big(3s^{16}+33s^{15}t-543s^{14}t^2-5875s^{13}t^3-27930s^{12}t^4-83206s^{11}t^5 \\ &\quad -170156s^{10}t^6-248030s^9t^7-263424s^8t^8-206431s^7t^9-119674s^6t^{10} \\ &\quad -50891s^5t^{11}-15541s^4t^{12}-3279s^3t^{13}-446s^2t^{14}-34t^{15}s-t^{16}\Big). \end{aligned}$$

Le discriminant est alors

$$\Delta_{51} = st^2(s+t)(2s+t)^2(s^2+3st+t^2)^5(4s^2+2st-t^2)^{10}.$$

5. Courbes Elliptiques de Sous-groupe $E(\mathbb{Q})_{\mathbf{tors}} = \mathbb{Z}/12\mathbb{Z}$

5.1. Courbe Elliptique E_{52}

Pour que $P_0 = (O, 0)$ soit d'ordre 12 sur la courbe (2), on doit avoir $A \neq 0$, $A^2 - BC + CA \neq 0$, et $A^6 + C^2A^4 + A^4BC - 5C^2A^3B - CA^2B^3 + 10A^2B^2C^2 - 9AC^2B^3 + 3C^2B^4 = 0$. Ainsi $(A/C, B/C)$ est un point rationnel sur la courbe singulière d'équation:

$$X^6 + X^4 + X^4Y - 5X^3Y - X^2Y^3 + 10X^2Y^2 - 9XY^3 + 3Y^4 = 0.$$

En posant $X = (1-d)q$ et $Y = dX$, avec $d \neq 1$ et $q \neq 0$, on obtient $(q+3)d^2 + (q-3)d + q^2 + 1 = 0$, et en posant

$$q = -\frac{s^2 + 3t^2}{4t^2},$$

on obtient alors

$$\begin{aligned} d &= -\frac{s^2 - 2st + 5t^2}{2t(s-3t)}, \\ X &= -\frac{(s^2 - t^2)(s^2 + 3t^2)}{8t^3(s-3t)}, \\ Y &= \frac{(s^2 - t^2)(s^2 + 3t^2)(s^2 - 2st + 5t^2)}{16t^4(s-3t)^2}, \end{aligned}$$

et on peut donc prendre

$$\begin{aligned} A &= -2t(s-3t)(s^2 - t^2)(s^2 + 3t^2), \\ B &= (s^2 - t^2)(s^2 + 3t^2)(s^2 - 2st + 5t^2), \\ C &= 16t^4(s-3t)^2. \end{aligned}$$

En remplaçant x par u^2x et y par u^3y dans (2), avec $u = -2t(s-3t)$, on obtient la courbe :

$$E_{52}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2,$$

avec

$$\begin{aligned} a_1 &= -(s^4 + 2s^2t^2 + 8st^3 - 27t^4), \\ a_2 &= -4t^2(s^2 - t^2)(s^2 + 3t^2)(s^2 - 2st + 5t^2), \\ a_3 &= 32t^5(s-3t)(s^2 - t^2)(s^2 + 3t^2)(s^2 - 2st + 5t^2). \end{aligned} \tag{3}$$

Son discriminant est alors

$$\Delta_{52} = 2^{12}t^{12}(s-t)^{12}(s+t)^6(s-3t)^2(s^2 + 3t^2)^4(s^2 + 6st - 3t^2)(s^2 - 2st + 5t^2)^3.$$

Les différents sous-groupes finis qui permettent de déterminer les expressions des isogènes de E_{52} sont $< 6P_0 >$, $< 4P_0 >$, $< 3P_0 >$, $< 2P_0 >$ et $< P_0 >$.

5.2. Courbe Elliptique E_{53}

En divisant E_{52} par $< 6P_0 >$, on obtient la courbe :

$$E_{53}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans (3) et

$$\begin{aligned} a_4 &= -320t^6(s-t)^6(s^2 + 3t^2)^2, \\ a_6 &= -64t^6(s-t)^6(s^2 + 3t^2) \\ &\quad \times (s^8 - 12s^6t^2 + 48s^5t^3 - 162s^4t^4 + 320s^3t^5 - 380s^2t^6 + 144st^7 + 297t^8). \end{aligned}$$

Son discriminant est alors

$$\Delta_{53} = 2^6t^6(s-t)^6(s+t)^{12}(s-3t)^4(s^2 + 3t^2)^2(s^2 + 6st - 3t^2)^2(s^2 - 2st + 5t^2)^6.$$

5.3. Courbe Elliptique E_{54}

En divisant E_{52} par $< 4P_0 >$, on obtient la courbe :

$$E_{54}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans (3) et

$$\begin{aligned}
a_4 &= -80t^4(s+t)^2(s-t)^4(s^2-2st+5t^2)(s^4-6s^2t^2+24st^3-3t^4),\\
a_6 &= -16t^4(s+t)^2(s-t)^4(s^2-2st+5t^2)\\
&\quad \times \Big(s^{12}-18s^{10}t^2+72s^9t^3+131s^8t^4-1152s^7t^5+2676s^6t^6\\
&\qquad -1328s^5t^7-5833s^4t^8+11456s^3t^9-10626s^2t^10+9384st^{11}-667t^{12}\Big).
\end{aligned}$$

Son discriminant est alors

$$\Delta_{54} = 2^4t^4(s-t)^4(s+t)^2(s-3t)^6(s^2+3t^2)^{12}(s^2+6st-3t^2)^3(s^2-2st+5t^2).$$

5.4. Courbe Elliptique E_{55}

En divisant E_{52} par $< 3P_0 >$, on obtient la courbe :

$$E_{55}: \ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans (3) et

$$\begin{aligned}
a_4 &= 40t^3(s-t)^3(s^2+3t^2)\\
&\quad \times (s^8-12s^6t^2-24s^5t^3+54s^4t^4+48s^3t^5+180s^2t^6-24st^7+33t^8),\\
a_6 &= 8t^3(s-t)^3(s^2+3t^2)\\
&\quad \times \Big(s^{16}-24s^{14}t^2-88s^{13}t^3+372s^{12}t^4+752s^{11}t^5-1176s^{10}t^6+504s^9t^7\\
&\qquad -14418s^8t^8+20896s^7t^9-33480s^6t^{10}+65304s^5t^{11}-62396s^4t^{12}\\
&\qquad +39024s^3t^{13}+32760s^2t^{14}+4680st^{15}+12825t^{16}\Big).
\end{aligned}$$

Son discriminant est alors

$$\Delta_{55} = -2^3t^3(s-t)^3(s+t)^6(s-3t)^2(s^2+3t^2)(s^2+6st-3t^2)^4(s^2-2st+5t^2)^{12}.$$

5.5. Courbe Elliptique E_{56}

En divisant E_{52} par $< 2P_0 >$, on obtient la courbe :

$$E_{56}: \ y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6,$$

où les expressions de a_1, a_2 et a_3 sont donnés dans (3) et

$$\begin{aligned}
a_4 &= -20(s-t)^2t^2\\
&\quad \times \Big(s^{12}+22s^{10}t^2-8s^9t^3+123s^8t^4+160s^7t^5+228s^6t^6+208s^5t^7+1799s^4t^8\\
&\qquad -864s^3t^9+1254s^2t^{10}+504st^{11}+669t^{12}\Big),\\
a_6 &= -4(s-t)^2t^2\\
&\quad \times \Big(s^{20}+66s^{18}t^2-72s^{17}t^3+873s^{16}t^4-160s^{15}t^5+5400s^{14}t^6\\
&\qquad -3904s^{13}t^7+33762s^{12}t^8-1440s^{11}t^9-55476s^{10}t^{10}+381552s^9t^{11}\\
&\qquad -637190s^8t^{12}+754976s^7t^{13}-469480s^6t^{14}+340992s^5t^{15}-267075s^4t^{16}\\
&\qquad +408864s^3t^{17}-66750s^2t^{18}+216344st^{19}+407293t^{20}\Big).
\end{aligned}$$

Son discriminant est alors

$$\Delta_{56} = 2^2t^2(s-t)^2(s+t)^4(s-3t)^{12}(s^2+3t^2)^6(s^2+6st-3t^2)^6(s^2-2st+5t^2)^2.$$

5.6. Courbe Elliptique E_{57}

En divisant E_{52} par $< P_0 >$, on obtient la courbe :

$$E_{57}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec a_1, a_2 et a_3 donnés dans (3) et

$$\begin{aligned} a_4 = {} & 10t(s-t) \\ & \times \Big(s^{14} - 18s^{13}t + 111s^{12}t^2 - 476s^{11}t^3 + 1257s^{10}t^4 - 2854s^9t^5 + 4111s^8t^6 \\ & - 4456s^7t^7 + 2011s^6t^8 + 706s^5t^9 - 7067s^4t^{10} + 7428s^3t^{11} - 5061s^2t^{12} \\ & - 330st^{13} + 21021t^{14}\Big), \\ a_6 = {} & 2t(s-t)^2 \\ & \times \Big(s^{22} - 46s^{21}t + 631s^{20}t^2 - 5084s^{19}t^3 + 26731s^{18}t^4 - 107886s^{17}t^5 \\ & + 332909s^{16}t^6 - 830736s^{15}t^7 + 1661306s^{14}t^8 - 2727580s^{13}t^9 \\ & + 3390262s^{12}t^{10} - 2988648s^{11}t^{11} + 1032774s^{10}t^{12} + 1630324s^9t^{13} \\ & - 2490518s^8t^{14} + 1924464s^7t^{15} - 2970539s^6t^{16} + 9049482s^5t^{17} \\ & - 20398461s^4t^{18} + 17076708s^3t^{19} - 11831425s^2t^{20} - 14632390st^{21} \\ & + 27052025t^{22}\Big). \end{aligned}$$

Son discriminant est alors

$$\Delta_{57} = -2t(s-t)(s+t)^2(s-3t)^6(s^2+3t^2)^3(s^2+6st-3t^2)^{12}(s^2-2st+5t^2)^4.$$

5.7. Courbe Elliptique E_{58}

La courbe E_{53} a trois points de torsion $R_i(x_i, y_i)$, $i = 1, 2, 3$, chacun d'ordre 2, avec $y_i = -(a_1x_i + a_3)/2$ et

$$\begin{aligned} x_1 &= -\frac{1}{4}\left(s^8 - 12s^6t^2 + 48s^5t^3 - 162s^4t^4 + 352s^3t^5 - 412s^2t^6 + 240st^7 + 201t^8\right), \\ x_2 &= -16t^3(s-t)(s^2+3t^2)(s^2-2st-t^2), \\ x_3 &= 16t^3(s-t)(s^2+3t^2)(s^2-2st+3t^2). \end{aligned}$$

En divisant E_{53} par le sous-groupe $< R_1 >$, on obtient la courbe E_{52} et en la divisant par $< R_2 >$ on obtient E_{55}. Enfin, en divisant E_{53} par $< R_3 >$, on obtient la courbe

$$E_{58}:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec a_1, a_2 et a_3 donnés dans (3) et

$$\begin{aligned} a_4 = {} & -40t^3(s^2+3t^2)(s-t)^3 \\ & \times \Big(s^8 - 12s^6t^2 - 120s^5t^3 + 378s^4t^4 + 912s^3t^5 - 1260s^2t^6 + 1272st^7 \\ & - 399t^8\Big) \\ a_6 = {} & -8t^3(s^2+3t^2)(s-t)^3 \\ & \times \Big(s^{16} - 24s^{14}t^2 + 280s^{13}t^3 - 732s^{12}t^4 - 1456s^{11}t^5 + 26056s^{10}t^6 \\ & - 135288s^9t^7 + 467070s^8t^8 - 1189664s^7t^9 + 2344056s^6t^{10} - 3594072s^5t^{11} \\ & + 4213396s^4t^{12} - 3597360s^3t^{13} + 1986648s^2t^{14} - 460872st^{15} + 7497t^{16}\Big). \end{aligned}$$

Le discriminant est alors

$$\Delta_{58} = -2^3t^3(s-t)^3(s+t)^{24}(s-3t)^8(s^2+3t^2)(s^2+6st-3t^2)(s^2-2st+5t^2)^3.$$

5.8. Courbe Elliptique E_{59}

La courbe E_{56} a aussi trois points de torsion $S_i(x_i, y_i)$, $i = 1, 2, 3$, d'ordre 2, avec $y_i = -(a_1x_i + a_3)/2$ et

$$x_1 = -4t(s-t)(s^6 - 2s^5t + 11s^4t^2 - 4s^3t^3 + 7s^2t^4 + 6st^5 + 13t^6),$$
$$x_2 = -\frac{1}{4}\left(s^8 + 52s^6t^2 - 80s^5t^3 + 30s^4t^4 + 608s^3t^5 - 988s^2t^6 + 112st^7 + 521t^8\right),$$
$$x_3 = 4t(s-t)(s^6 + 2s^5t + 7s^4t^2 + 4s^3t^3 + 47s^2t^4 - 6st^5 + 41t^6).$$

En divisant E_{56} par le sous-groupe $< S_1 >$, on obtient la courbe E_{57} et en la divisant par S_2 on obtient E_{54}. Enfin, en divisant E_{56} par S_3, on obtient la courbe

$$E_{59}: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

avec a_1, a_2 et a_3 donnés dans (3) et

$$\begin{aligned} a_4 = {} & -10t(-s+t) \\ & \times \Big(-s^{14} - 18s^{13}t - 75s^{12}t^2 - 188s^{11}t^3 - 561s^{10}t^4 - 1990s^9t^5 + 61s^8t^6 \\ & - 13096s^7t^7 + 15349s^6t^8 - 45950s^5t^9 + 56599s^4t^{10} - 62556s^3t^{11} \\ & + 54717s^2t^{12} - 23658st^{13} + 4983t^{14}\Big), \end{aligned}$$

$$\begin{aligned} a_6 = {} & -2t(-s+t)) \\ & \times \Big(-s^{22} - 46s^{21}t - 539s^{20}t^2 - 2876s^{19}t^3 - 8371s^{18}t^4 - 35150s^{17}t^5 \\ & - 83409s^{16}t^6 - 203920s^{15}t^7 - 572250s^{14}t^8 - 75292s^{13}t^9 - 4628222s^{12}t^{10} \\ & + 9413208s^{11}t^{11} - 31759734s^{10}t^{12} + 64303156s^9t^{13} - 117101522s^8t^{14} \\ & + 177706992s^7t^{15} - 215384885s^6t^{16} + 220525578s^5t^{17} - 174984855s^4t^{18} \\ & + 96321924s^3t^{19} - 34452295s^2t^{20} + 6666074st^{21} + 162131t^{22}\Big). \end{aligned}$$

Le discriminant est alors

$$\Delta_{59} = 2t(s-t)(s+t)^8(s-3t)^{24}(s^2+3t^2)^3(s^2+6st-3t^2)^3(s^2-2st+5t^2).$$

6. La Source des Courbes Elliptiques

Les calculs ont été effectués à l'aide du système de calcul `Maple` [3]. Les courbes elliptiques $E_i(s,t)$, $i = 1, \cdots, 59$ sont disponibles dans le fichier *elliptic.mws* (format `Maple`), à l'adresse suivante: http://www.math.unicaen.fr/~nitaj/.

References

[1] D. Husemöller, Elliptic Curves, Graduate Texts in Math., vol. 111, Springer-Verlag, Berlin, Heidelberg, New York, 1986.

[2] D.S. Kubert, Universal bounds on the torsion of elliptic curves, *Proc. London Math. Soc.,* **33** (1976), 193–237.

[3] Maple Home Page, http://www.maplesoft.com/index.html.

[4] B. Mazur, Modular curves and the Eisenstein ideal, *IHES Publ. Math.* **47** (1977), 33-186.

[5] T. Nagell, Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque, *Nova Acta Soc. Sci. Upsal, Ser. IV 15,* **6** (1952), 1–66.

[6] A. Nitaj, *Détermination de courbes elliptiques pour la conjecture de Szpiro, Acta Arith.,* **85** (1998), 351-376.

[7] M. Reichert, Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields *Math. Comput.,* **46** (1986), 637-658.

[8] J.H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math., vol. 106, Springer-Verlag, Berlin, Heidelberg, New York, Tokyo, 1986.

[9] J. Vélu, Isogénies entre courbes elliptiques, *C. R. Acad. Sci. Paris Sér. I Math.,* **273** (1971), 238–241.