ACTA ARITHMETICA
144.1 (2010)

Structure de torsion des courbes elliptiques sur les corps quadratiques

par

F. Patrick Rabarison (Caen)

1. Introduction. Soit une courbe elliptique E définie par son modèle de Weierstrass :

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

On suppose que les a_i sont des éléments d'un corps K fixé, et on note $\mathcal{O}$ le point à l'infini. Mordell a démontré dans sa thèse que lorsque $K = \mathbb{Q}$, l'ensemble des points $E(\mathbb{Q})$ forme un groupe abélien de type fini. Son résultat fut ensuite généralisé par Weil dans le cas des corps de nombres algébriques en général.

Théorème 1.1 (Mordell–Weil, [17]). *Soit E une courbe elliptique définie sur un corps de nombres K. Alors il existe $n \in \mathbb{N}_0 = \mathbb{N} \cup 0$ et $\mathrm{Tors}(E, K)$, un groupe abélien fini, tels que*

$$E(K) \simeq \mathrm{Tors}(E, K) \times \mathbb{Z}^n.$$

Pour plus de détail sur la loi de groupe, voir par exemple [17, Chapitre III]. L'entier n est appelé le *rang* de la courbe sur K et on le notera par la suite $\mathrm{rang}(E, K)$. La partie $\mathrm{Tors}(E, K)$ est le sous-groupe des points d'ordre fini de $E(K)$. Pour bien comprendre l'arithmétique d'une courbe elliptique $E(K)$, il faut donc connaître d'une part le rang et d'autre part la partie de torsion. Dans le cas où le corps de base est $\mathbb{Q}$, Mazur a démontré que le cardinal de la partie de torsion d'une courbe elliptique est majoré par 16 et a donné la liste de tous les types de sous-groupes de torsion possibles :

Théorème 1.2 (Mazur, [15]). *Soit E une courbe elliptique définie sur $\mathbb{Q}$. Alors les seuls sous-groupes de torsion possibles de E sur $\mathbb{Q}$ sont donnés par*

$$\mathrm{Tors}(E, \mathbb{Q}) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{avec } 1 \le n \le 10 \text{ ou } n = 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & \text{avec } 1 \le n \le 4. \end{cases}$$

2010 *Mathematics Subject Classification*: Primary 11G05; Secondary 14H52.
Key words and phrases: elliptic curves, modular curves, torsion, quadratic field.

DOI: 10.4064/aa144-1-3

Lorsque l'on se donne une courbe elliptique E définie sur un corps K, la partie de torsion est relativement facile à trouver grâce, par exemple, aux polynômes de division associés à la courbe. Dans [14], Kubert a donné les paramétrisations des courbes elliptiques définies sur $\mathbb{Q}$, avec ces torsions. Le rang de la courbe reste cependant plus difficile à trouver.

1.1. Le cas des corps de nombres quadratiques

1.1.1. *Torsions admissibles.* Soit K une extension quadratique de $\mathbb{Q}$. Kamienny a montré dans [10] et [11] que le cardinal de $\mathrm{Tors}(E,K)$ est borné indépendamment de E et de K. Après Kamienny, Kenku et Momose ont donné la liste de tous les sous-groupes de torsion possibles :

Théorème 1.3 (Mazur–Kamienny–Kenku–Momose, [12]). *Soit E une courbe elliptique définie sur un corps de nombres quadratique K. Alors les seuls sous-groupes de torsion possibles de E sur K sont donnés par*

$$\mathrm{Tors}(E,K) \simeq \begin{cases} \mathbb{Z}/n\mathbb{Z} & \text{avec } 1 \le n \le 16 \text{ ou } n = 18, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & \text{avec } 1 \le n \le 6, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z} & \text{avec } n = 1, 2 \text{ si } K = \mathbb{Q}(\sqrt{-3}), \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{si } K = \mathbb{Q}(\sqrt{-1}). \end{cases}$$

Remarque 1. Notons que pour un corps quadratique fixé, il peut arriver que certains de ces groupes n'apparaissent pas comme la partie torsion.

1.1.2. *Paramétrisations connues.* Dans [16], Reichert a donné les paramétrisations des courbes elliptiques dont le sous-groupe de torsion est cyclique : $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, $\mathbb{Z}/15\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$. Nous retrouvons ici cettes paramétrisations avec plus ou moins de détails, en utilisant les algorithmes de van Hoeij [6]–[8], et avec des modèles des courbes modulaires plus simples.

1.1.3. *Nouvelles paramétrisations.* Dans cet article, nous donnons les paramétrisations des autres structures supplémentaires, c'est-à-dire, le cas où $\mathrm{Tors}(E,K)$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Nous donnons également quelques exemples explicites de courbes elliptiques avec des sous-groupes de torsion non triviaux, et de rang non nul. Nous montrons aussi la non existence de courbes elliptiques (définies sur certains corps) possédant des torsions spéciales.

1.1.4. *Sur le rang.* Soit K un corps de nombres et G un groupe abélien fini tel qu'il existe une courbe elliptique sur K dont le sous-groupe de torsion sur K est isomorphe à G, puis définissons

$$\mathrm{Sr}(G,K) = \sup_{E_G} \mathrm{rang}(E_G(K))$$

où E_G parcourt les courbes elliptiques sur K avec $\mathrm{Tors}(E,K) \simeq G$.

La recherche du rang d'une courbe est un peu délicate. La méthode la plus habituelle est celle de la 2-descente. Dans cet article, nous utilisons le programme de Simon [19] sur PARI/gp [2] pour calculer le rang des courbes, ou à défaut, trouver une bonne majoration pour celui-ci. Dans la pratique, conjuguer à la fois rang élevé et torsion non trivial est assez difficile. Par exemple, pour $K = \mathbb{Q}$ et pour $G = \mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, il est connu que $\mathrm{Sr}(G, \mathbb{Q}) \geq 3$ est la meilleure minoration que l'on connaît à ce jour pour cettes structures. Voir la page de Dujella [4] pour la liste des records actuels.

2. Paramétrisation des structures

2.1. Les courbes modulaires. Soient deux entiers positifs M et N tels que $M \mid N$ et soit $\Gamma_1(M, N)$ le sous-groupe de congruence de $\mathrm{SL}_2(\mathbb{Z})$ défini par

$$\Gamma_1(M,N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N,\ b \equiv 0 \bmod M \right\}.$$

Le groupe $\Gamma_1(M, N)$ agit sur le demi-plan de Poincaré

$$\mathbb{H} = \{z \in \mathbb{C} \mid \Im(z) > 0\},$$

et on note par $X_1(M, N)$ la courbe modulaire correspondant à $\Gamma_1(M, N)$. Notons que $Y_1(M, N) = X_1(M, N) \setminus \{\text{pointes}\}$ est l'espace des modules des classes d'isomorphismes des courbes elliptiques avec des points (P_M, P_N) tels que $\langle P_M \rangle \times \langle P_N \rangle$ est un sous-groupe isomorphe a $\mathbb{Z}/M\mathbb{Z} \times \mathbb{Z}/N\mathbb{Z}$ (voir [12]). Notons aussi que $X_1(N)$ et $X_1(1, N)$ représentent la même courbe modulaire.

Proposition 1 ([9]). *Soit $g \in \{0, 1, 2\}$ et soient les ensembles S_g suivants :*

$S_0 = \{(4), (5), (6), (7), (8), (9), (10), (12), (2, 4), (2, 6), (2, 8), (3, 6), (4, 4)\}$,
$S_1 = \{(11), (14), (15), (2, 10), (2, 12)\}$,
$S_2 = \{(13), (16), (18)\}$.

Alors $X_1(\lambda)$ est de genre g si $\lambda \in S_g$.

La dernière proposition signifie que si l'on se donne un corps de nombres K fixé, alors $\mathrm{Sr}(G, K)$ est borné pour $G = \mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ ou $\mathbb{Z}/18\mathbb{Z}$ puisqu'il n'existe qu'un nombre fini de courbes elliptiques avec cettes torsions. Ceci est une conséquence directe du théorème de Faltings (voir [5]).

2.2. Forme normale de Tate. Soit E une courbe elliptique définie sur le corps K de la forme

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

Supposons aussi que la courbe possède un point rationnel non trivial sur K. Une transformation birationnelle ramène ce point à l'origine et de plus l'équation de E devient

$$E_{b,c} : y^2 + (1-c)xy + by = x^3 + bx^2.$$

C'est la forme normale de Tate. Le discriminant de $E_{b,c}$ est donné par

$$\Delta_{E_{b,c}} = b^3(-c^4 + 3c^3 + (-8b-3)c^2 + (-20b+1)c + (-16b^2+b)) \neq 0.$$

Il est clair que le point $P_0 = (0,0)$ est sur la courbe $E_{b,c}$. Pour une discussion plus détaillée, voir par exemple [13, Chapitre V].

Remarque 2. Notons que dans l'équation de la courbe $E_{b,c}$, b doit être nécessairement non nul puisque dans le cas contraire, la courbe serait singulière.

2.3. Description générale

Les cas $\lambda = (N)$, $N \geq 4$. Partant de la forme normale de Tate $E_{b,c}$, on s'arrange à ce que le point $P_0 = (0,0)$ soit un point de torsion en utilisant la loi du groupe :

- Cas où N est pair : on utilise la relation $[N/2]P_0 = [-N/2]P_0$.
- Cas où N est impair : on utilise alors $[(N+1)/2]P_0 = [-(N-1)/2]P_0$.

Notons que nous utilisons PARI [2] pour les calculs :

1. Initialiser la courbe $E_{b,c} = [1-c, b, b, 0, 0]$.
2. Initialiser le point $P_0 = [0, 0]$.
3. Prendre le contenu du vecteur $M[P_0] - [N]P_0$.

On obtient ainsi une certaine équation $\mathcal{U}_{b,c} = 0$ en b et c. Cette équation ne définit pas forcément une courbe irréductible sur $\mathbb{Q}$. On regarde ensuite chacune des composantes irréductibles qui correspondent essentiellement aux diviseurs de N. L'équation obtenue est alors $X_1(\lambda)$, que l'on peut réduire en utilisant l'algorithme de van Hoeij [7].

Les cas $\lambda = (2, 2N)$. On commence par regarder la paramétrisation des courbes avec un point d'ordre $2N$, puis on remarque alors que le point $Q = [N]P_0$ est d'ordre 2. Cela suggère un changement de variable convenable, pour se ramener à une forme du type

$$E : y^2 = x(x^2 + fx + g).$$

Pour avoir la 2-torsion complète ($E[2] \subset E(K)$), nous imposons à ce que les trois racines de $x(x^2 + fx + g)$ soient dans K, c'est-à-dire $f^2 - 4g$ soit un carré dans K^*.

Les cas $\lambda = (3, 3N)$ *avec* $N \in \{1, 2\}$. Pour obtenir la 3-torsion complète ($E[3] \subset E(K)$), nous utilisons la paramétrisation des courbes correspondant

au type $\lambda = (3N)$ où $N = 1, 2$, ainsi que le 3ème polynôme de division correspondant.

Le cas $\lambda = (4, 4)$. Partant de la forme générale des courbes du type $(2, 4)$, on résout une équation de la forme $P = [2]Q$.

Pour les réductions et minimisation des courbes de genre 1 (resp. 2), on peut par exemple utiliser l'algorithme de van Hoeij [6] (resp. [8]).

3. Les torsions des courbes elliptiques dans $\mathbb{Q}$. Dans [14], Kubert a donné les paramétrisations des structures de torsion pour le cas $K = \mathbb{Q}$. Nous indiquons ici plus de détails sur ces paramétrisations.

3.1. Le cas $\mathrm{Tors}(E/K) \supseteq \mathbb{Z}/2\mathbb{Z}$**.** Prenons la forme de Weierstrass réduite

$$E : y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6.$$

Supposons que $P(x_P, y_P) \in E(K)[2]$. Le changement de variable $x \mapsto x - x_P$ ramène à la forme générale

$$\mathcal{E}^{(2)} : y^2 = x(x^2 + sx + t), \tag{3.1}$$

où $s, t \in K$ sont tels que

$$\Delta_{\mathcal{E}^{(2)}} = 16t^2(s^2 - 4t) \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 2.

3.2. Le cas $\mathrm{Tors}(E, K) \supseteq \mathbb{Z}/3\mathbb{Z}$**.** Nous connaissons par exemple depuis [13, p. 146] que les courbes elliptiques avec un point d'ordre 3 ont la forme générale

$$\mathcal{E}^{(3)} : y^2 + sxy + ty = x^3 \tag{3.2}$$

avec $s, t \in K$ tels que

$$\Delta_{\mathcal{E}^{(3)}} = t^3(s^3 - 27t) \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 3.

3.3. Le cas $\mathrm{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z}$**.** On sait que si E est donnée par son modèle de Tate $E_{b,c}$, alors $b \neq 0$ (voir remarque 2), et l'égalité $[2]P_0 = [-2]P_0$ équivaut alors à

$$\mathcal{U}_{b,c} : c = 0.$$

On en déduit alors la forme générale des courbes

$$\mathcal{E}^{(4)} : y^2 + xy + ty = x^3 + tx^2 \tag{3.3}$$

avec $t \in K$ tel que

$$\Delta_{\mathcal{E}^{(4)}} = (-16t + 1)t^4 \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 4.

3.4. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/5\mathbb{Z}$**.** L'égalité $[3]P_0 = [-2]P_0$ sur la forme normale de Tate $E_{b,c}$ est équivalente à

$$\mathcal{U}_{b,c} : b + c = 0.$$

On en déduit la forme générale des courbes

$$\mathcal{E}^{(5)} : y^2 + (1-t)xy - ty = x^3 - tx^2 \tag{3.4}$$

avec $t \in K$ tel que

$$\Delta_{\mathcal{E}^{(5)}} = t^5(t^2 - 11t - 1) \neq 0.$$

Le point $P_0 = (0,0)$ est d'ordre 5 sur $\mathcal{E}^{(5)}$.

3.5. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/6\mathbb{Z}$**.** L'égalité $[3]P_0 = [-3]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à

$$\mathcal{U}_{b,c} : b + c + c^2 = 0.$$

On en déduit la forme générale

$$\mathcal{E}^{(6)} : y^2 + (1-t)xy - t(t+1)y = x^3 - t(t+1)x^2 \tag{3.5}$$

avec $t \in K$ tel que

$$\Delta_{\mathcal{E}^{(6)}} = t^6(t+1)^3(9t+1) \neq 0.$$

Le point $P_0 = (0,0) \in \mathcal{E}^{(6)}$ est d'ordre 6.

3.6. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/7\mathbb{Z}$**.** L'égalité $[4]P_0 = [-3]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à

$$\mathcal{U}_{b,c} : -c^3 + bc + b^2 = 0.$$

Cela définit une courbe de genre 0, et donc paramétrisable. L'algorithme [7] donne ensuite

$$(b,c) = (t^2(1-t), t^2 - t).$$

On en déduit la forme générale des courbes

$$\mathcal{E}^{(7)} : y^2 - (t^2 - t - 1)xy - t^2(t-1)y = x^3 - t^2(t-1)x^2,$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(7)}} = t^7(t-1)^7(t^3 - 8t^2 + 5t + 1) \neq 0.$$

Le point $P_0 = (0,0)$ est d'ordre 7.

3.7. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/8\mathbb{Z}$**.** Pour que $P_0 = (0,0)$ soit d'ordre 8 sur la courbe elliptique $E_{b,c}$, il faut que $bc \neq 0$, puisque sinon $P_0 = (0,0)$ est d'ordre 4 d'après 2.2 et 3.3. L'égalité $[4]P = [-4]P$ équivaut alors à

$$\mathcal{U}_{b,c} : 2b^2 + bc^2 + 3bc + c^2 = 0,$$

que l'on peut parametrer grâce à [7] par

$$(b,c) = \left(-6 - 7u - 2u^2, -\frac{6 + 7u + 2u^2}{1+u}\right).$$

On obtient alors la forme

$$\mathcal{E} : y^2 - \frac{2t^2-4t+1}{t}\,xy - (2t-1)(t-1)y = x^3 - (2t-1)(t-1)x^2.$$

Puis en posant $t = u-1$, et en faisant le changement de variable

$$(x,y) \mapsto \left(\frac{x}{t^2}, \frac{y}{t^3}\right),$$

on obtient la forme générale plus simple

$$\mathcal{E}^{(8)} : y^2 - (2t^2-4t+1)xy - (2t-1)(t-1)t^3y = x^3 - (2t-1)(t-1)t^2x^2,$$

où $t \in K$ est tel que le discriminant de $\mathcal{E}^{(8)}$ est donné par

$$\Delta_{\mathcal{E}^{(8)}} = t^8(t-1)^8(2t-1)^4(8t^2-8t+1) \neq 0.$$

Le point $P_0 = (0,0)$ est d'ordre 8.

3.8. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/9\mathbb{Z}$**.** Soient $b \neq 0$ et $P_0 = (0,0)$ tel que $\mathrm{ord}(P_0) \neq 3$. L'égalité $[5]P_0 = [-4]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à

$$\mathcal{U}_{b,c} : b^3 + 3b^2c + bc^3 + 3bc^2 + c^5 + c^4 + c^3 = 0.$$

En utilisant l'algorithme [7], on trouve la paramétrisation suivante :

$$(b,c) = (-t^2(t-1)(t^2-t+1), t^2(t-1)).$$

On obtient alors la forme générale

$$\mathcal{E}^{(9)} : y^2 + (-t^3+t^2+1)xy - t^2(t-1)(t^2-t+1)y = x^3 - t^2(t-1)(t^2-t+1)x^2, \tag{3.6}$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(9)}} = t^9(t-1)^9(t^2-t+1)^3(t^3-6t^2+3t+1) \neq 0.$$

Le point $P_0 = (0,0)$ est d'ordre 9.

3.9. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/10\mathbb{Z}$**.** Soient $b \neq 0$ et $P_0 = (0,0)$ tel que $\mathrm{ord}(P_0) \notin \{2,5\}$. L'égalité $[5]P = [-5]P$ sur la forme normale de Tate $E_{b,c}$ est équivalente à

$$\mathcal{U}_{b,c} : b^3 + 3b^2c^2 + 2b^2c + bc^4 + 3bc^3 + bc^2 - c^5 = 0.$$

Cette équation définit une courbe de genre 0. L'algorithme [7] permet de trouver la paramétrisation

$$(b,c) = \left(\frac{-t^3(t-1)(t-2)}{(t^2-6t+4)^2}, \frac{-t(t-1)(t-2)}{t^2-6t+4}\right).$$

On obtient alors la forme

$$\mathcal{E}^{(10)} : y^2 + \frac{t^3-2t^2-4t+4}{t^2-6t+4}\,xy - \frac{(t-1)(t-2)t^3}{(t^2-6t+4)^2}\,y = x^3 - \frac{(t-1)(t-2)t^3}{(t^2-6t+4)^2}\,x^2,$$

et le changement de variable

$$(x,y)\mapsto\left(\frac{x}{(t^2-6t+4)^2},\frac{y}{(t^2-6t+4)^3}\right)$$

donne la forme générale plus simple

$$\begin{aligned}(3.7)\qquad \mathcal{E}^{(10)}: y^2+(t^3-2t^2-4t+4)xy-(t-1)(t-2)(t^2-6t+4)t^3y\\ =x^3-(t-1)(t-2)t^3x^2,\end{aligned}$$

où $t\in K$ est tel que

$$\Delta_{\mathcal{E}^{(10)}}=(t-1)^5(t-2)^{10}t^{10}(t^2-t-1)(t^2-6t+4)^2\neq 0.$$

Le point $P_0=(0,0)$ est d'ordre 10.

3.10. Le cas $\mathrm{Tors}(E,K)\supseteq\mathbb{Z}/12\mathbb{Z}$**.** On suppose que $b\neq 0$ et soit $P_0=(0,0)$ tel que $\mathrm{ord}(P_0)\notin\{2,3,4,6\}$. Alors l'égalité $[6]P_0=[-6]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à

$$\mathcal{U}_{b,c}: 3b^4+b^3c^2+9b^3c+10b^2c^2-bc^4+5bc^3+c^6+c^4=0.$$

Cette équation définit une courbe de genre 0. L'algorithme [7] permet de trouver la paramétrisation

$$(b,c)=\left(\frac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{(t-1)^4},\frac{-6t^4+9t^3-5t^2+t}{(t-1)^3}\right).$$

On obtient alors la forme

$$\begin{aligned}\mathcal{E}^{(12)}: y^2+\frac{6t^4-8t^3+2t^2+2t-1}{(t-1)^3}\,xy\\ +\frac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{(t-1)^4}\,y\\ =x^3+\frac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{(t-1)^4}\,x^2.\end{aligned}$$

Enfin, le changement de variable

$$(x,y)\mapsto\left(\frac{x}{(t-1)^6},\frac{y}{(t-1)^9}\right)$$

donne la forme générale, sans dénominateur

$$\begin{aligned}(3.8)\qquad \mathcal{E}^{(12)}: y^2+(6t^4-8t^3+2t^2+2t-1)xy\\ +(-12t^6+30t^5-34t^4+21t^3-7t^2+t)(t-1)^5y\\ =x^3+(-12t^6+30t^5-34t^4+21t^3-7t^2+t)(t-1)^2x^2,\end{aligned}$$

où $t\in K$ est tel que

$$\Delta_{\mathcal{E}^{(12)}}=t^{12}(t-1)^{12}(2t-1)^6(2t^2-2t+1)^3(3t^2-3t+1)^4(6t^2-6t+1)\neq 0.$$

Le point $P_0=(0,0)$ est d'ordre 12.

3.11. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$**.** La forme générale pour cette structure est bien connue :

$$\mathcal{E}^{(2,2)} : y^2 = x(x-s)(x-t)$$

avec $s,t \in K$ tels que

$$\Delta_{\mathcal{E}^{(2,2)}} = 16s^2t^2(s-t)^2 \neq 0.$$

Les points $(0,0),(s,0),(t,0)$ sont d'ordre 2.

3.12. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$**.** Considérons la forme de Tate des courbes avec un point d'ordre 4 :

$$\mathcal{E}^{(4)} : y^2 + xy + ty = x^3 + tx^2.$$

Cette courbe est birationnellement équivalente à

$$\mathcal{E}^{(4)} : y^2 = xf_t(x) = x\left(x^2 + \left(-2t + \frac{1}{4}\right)x + t^2\right).$$

Pour que cette courbe admette une 2-torsion complète, il faut et il suffit que le discriminant de $f_t(x)$ soit un carré dans K^* :

$$\Delta(f_t(x)) = -t + \frac{1}{16} = u^2, \quad \text{où } u \in K^*.$$

La forme générale des courbes elliptiques dont la partie de torsion contient cette structure s'ensuit :

$$\mathcal{E}^{(2,4)} : y^2 + xy - \left(t^2 - \frac{1}{16}\right)y = x^3 - \left(t^2 - \frac{1}{16}\right)x^2, \tag{3.9}$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(2,4)}} = \frac{1}{2^{12}}t^2(4t-1)^4(4t+1)^4 \neq 0.$$

Les points

$$P_0 = (0,0) \quad \text{et} \quad Q_2 = \left(\frac{1}{8}(4t-1), \frac{1}{32}(4t-1)^2\right)$$

sont d'ordre 4 et 2 respectivement et engendrent un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.

3.13. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$**.** Considérons la forme des courbes avec un point d'ordre 6 :

$$\mathcal{E}^{(6)} : y^2 + (1-t)xy - t(t+1)y = x^3 - t(t+1)x^2.$$

Cette courbe est birationnellement équivalente à

$$\mathcal{E}^{(6)} : y^2 = xf_t(x) = x\left(x^2 + \left(\frac{-3}{4}t^2 + \frac{3}{2}t + \frac{1}{4}\right)x - t^3\right).$$

Pour avoir la 2-torsion complète, nous imposons que le discriminant de $f_t(x)$,

$$\Delta(f_t(x)) = \frac{1}{16}(t+1)^3(9t+1),$$

soit un carré. On considère alors la courbe

$$X_1(2,6) : (t+1)(9t+1) - u^2 = 0.$$

Cette courbe est de genre 0. L'algorithme [7] permet de trouver la paramétrisation

$$(t,u) = \left(\frac{z^2-z}{3z+1}, \frac{3z^2+2z-1}{3z+1}\right);$$

puis le changement de variable

$$(x,y) \mapsto \left(\frac{x}{(3z+1)^2}, \frac{y}{(3z+1)^3}\right)$$

donne la forme générale simplifiée

$$\mathcal{E}^{(2,6)} : y^2 + (-t^2+4t+1)xy - t(t-1)(t+1)^2(3t+1)y = x^3 - t(t-1)(t+1)^2x^2, \tag{3.10}$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(2,6)}} = t^6(t-1)^6(t+1)^6(3t-1)^2(3t+1)^2 \neq 0.$$

Les points

$$P_0 = (0,0) \quad \text{et} \quad Q = \left(\frac{3}{4}(t-1)(3t+1)(t+1)^2, \frac{3}{8}(t-1)^2(3t+1)(t+1)^3\right),$$

sont d'ordre 6 et 2 respectivement et on a

$$\langle Q, P_0\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

3.14. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$**.** Considérons la forme des courbes avec un point d'ordre 8 :

$$\mathcal{E}^{(8)} : y^2 - \frac{2t^2-4t+1}{t}xy - (2t-1)(t-1)y = x^3 - (2t-1)(t-1)x^2.$$

Cette courbe est birationnellement équivalente à

$$\mathcal{E}^{(6)} : y^2 = xf_t(x) = x\left(x^2 + \frac{8t^4-16t^3+16t^2-8t+1}{4t^2}x + t^4 - 4t^3 + 6t^2 - 4t + 1\right).$$

Pour que la 2-torsion complète soit définie sur K, il faut et il suffit que le discriminant de $f_t(x)$,

$$\Delta(f_t(x)) = \frac{(2t-1)^4(8t^2-8t+1)}{16t^4},$$

soit un carré. Nous considérons alors la courbe

$$X_1(2,8) : 8t^2 - 8t - u^2 + 1 = 0.$$

Cette courbe est de genre 0 ; en utilisant l'algorithme [7], on obtient la paramétrisation

$$(t,u) = \left(\frac{2z+z^2}{-8+z^2}, \frac{-z^2-8-8z}{-8+z^2}\right).$$

La forme générale des courbes elliptiques avec cette structure est ainsi donnée par

$$\mathcal{E}^{(2,8)} : y^2 + \frac{z^4-24z^2-64z-64}{z(z+2)(z^2-8)}\,xy - 2\frac{(z^2+4z+8)(z+4)}{(z^2-8)^2}\,y = x^3 - 2\frac{(z^2+4z+8)(z+4)}{(z^2-8)^2}\,x^2.$$

Avec le changement de variable

$$(x,y) \mapsto \left(\frac{x}{(z(z+2)(z^2-8))^2}, \frac{y}{(z(z+2)(z^2-8))^3}\right)$$

puis en substituant z par t, on se ramène à la forme plus simple

$$\begin{aligned}(3.11)\qquad \mathcal{E}^{(2,8)} : y^2 &+ (t^4-24t^2-64t-64)xy \\ &- 2(t^2+4t+8)(t+4)(t^2-8)(t+2)^3t^3y \\ &= x^3 - 2(t^2+4t+8)(t+4)(t+2)^2t^2x^2,\end{aligned}$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(2,8)}} = 2^8t^8(t+2)^8(t+4)^8(t^2-8)^2(t^2+4t+8)^4(t^2+8t+8)^2 \neq 0.$$

Les points

$P_0 = (0,0)$,

$$Q = \left(\frac{-z^3(z+4)(z^2+8)(z^2+4z+8)}{4(z^2-8)}, \frac{z^4(z+4)^2(z^2+8)^3(z^2+4z+8)^2}{8(z^2-8)^2}\right),$$

sont d'ordre 8 et 2 respectivement, et on a

$$\langle Q, P_0\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

4. Les torsions supplémentaires pour $[K : \mathbb{Q}] = 2$. La paramétrisation des courbes avec un point d'ordre 11 est donc un peu différente des cas précédents puisque le genre de $X_1(11)$ est 1 et non plus 0. Nous reprenons ici la forme vue dans [18, p. 190] ou [16] pour plus détails des transformations utilisées. Soit maintenant la courbe modulaire $X_1(11)$ (ou courbe $11a3$ dans la table de Cremona [3]) définie par

$$X_1(11) : s^2 - s = t^3 - t^2.$$

Les expressions de b et $a = 1 - c$ deviennent

$$b = \frac{s(s-1)(s-t)}{t}, \quad a = 1 - c = \frac{st + t - s^2}{t}.$$

La forme générale des courbes avec un point d'ordre 11 est donnée par

$$\mathcal{E}^{(11)} : y^2 + (st + t - s^2)xy + s(s-1)(s-t)t^2 y = x^3 + s(s-1)(s-t)tx^2, \tag{4.1}$$

où $P = (t, s) \in X_1(11)$ est tel que

$$t(t-1)(t^5 - 18t^4 + 35t^3 - 16t^2 - 2t + 1) \neq 0.$$

Il est bien connu qu'il n'existe pas de courbes elliptiques définies sur $\mathbb{Q}$ avec un point d'ordre 11. En effet, la courbe modulaire $X_1(11)$ est de rang 0 sur $\mathbb{Q}$ et admet exactement cinq points rationnels sur $\mathbb{Q}$ (voir le rang de $11a3$ dans la table de Cremona [3]) :

$$X_1(11)(\mathbb{Q}) = \{\mathcal{O}, (0,0), (1,0), (0,1), (1,1)\}.$$

De plus, ces points induisent des courbes singulières dans la paramétrisation (4.1) ci-dessus.

LEMME 4.1. *Soit K un corps de nombres quadratique. Alors*

$$\mathrm{Tors}(X_1(11), K) = \mathrm{Tors}(X_1(11), \mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Preuve. Nous utilisons le modèle

$$C : y^2 = f(x) = x^3 - 432x + 8208$$

pour la courbe modulaire $X_1(11)$. On observe d'abord que

$$\mathrm{Tors}(X_1(11), K) \supseteq \mathrm{Tors}(X_1(11), \mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}.$$

Par le théorème 1.3, les seules structures possibles pour $\mathrm{Tors}(X_1(11), K)$ sont $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ ou $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Pour prouver le lemme, il suffit donc de voir que $X_1(11)$ n'a pas de point d'ordre 2, ni 3.

Le polynôme f est de degré 3 et est irréductible sur $\mathbb{Q}$, il est donc irréductible sur toutes les extensions quadratiques de $\mathbb{Q}$, d'où l'on tire que $X_1(11)$ ne possède pas de point de 2-torsion sur K.

Soit Ψ_3 le polynôme de 3-division de C :

$$\Psi_3(x) = x^4 - 864x^2 + 32832x - 62208.$$

Si $C(K)$ a un point d'ordre 3, alors Ψ_3 a un facteur linéaire sur K, donc Ψ_3 a un facteur quadratique sur $\mathbb{Q}$. Or Ψ_3 est irréductible sur $\mathbb{Q}$, il ne peut donc avoir de point d'ordre 3 dans $C(K)$. ∎

REMARQUE 3. Il est clair que si K est tel que $X_1(11)(K) = X_1(11)(\mathbb{Q})$, alors il n'existe pas de courbe elliptique sur K avec un point d'ordre 11. En revanche, si le rang de $X_1(11)$ sur K est non nul, cela permet d'affirmer

immédiatement qu'il existe une infinité de courbes elliptiques sur K avec un point d'ordre 11.

EXEMPLE 1. La courbe $C_d : y^2 = x^3 - 4dx^2 + 16d^3$ est isomorphe (sur $\mathbb{Q}(\sqrt{d})$) à la courbe $X_1(11)$, de plus si $P_3 = (a, b)$ est un point non trivial sur $C_d(\mathbb{Q})$, on trouvera que le point

$$P = (t, s) = \left(\frac{a}{4d}, \frac{b\sqrt{d}}{8d^2} + \frac{1}{2}\right)$$

est un point de $X_1(11)(\mathbb{Q}(\sqrt{d}))$. On peut utiliser cette méthode pour obtenir des points d'ordre infini sur $X_1(11)(K)$.

Nous utilisons ici le programme de Simon [19] pour trouver le rang et des points sur les courbes modulaires de genre 1.

Une liste des structure de groupe de la courbe elliptique $X_1(11)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$ est donnée dans la table ci-dessous.

Table 1. $X_1(11)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(11)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{241}{250}, -\frac{4961}{12500}\theta + \frac{1}{2})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{\theta+5}{8}, \frac{11-\theta}{16})$
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{25}{6}, \frac{18-139\theta}{36})$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/5\mathbb{Z}$	–
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/5\mathbb{Z}$	–
-2	$\theta^2 + 2 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{2}, \frac{2-\theta}{4})$
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/5\mathbb{Z}$	–
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{1}{2}, \frac{2-\theta}{4})$
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/5\mathbb{Z}$	–
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/5\mathbb{Z}$	–
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-7\theta + 18, -42\theta + 103)$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(-2\theta + 5, -6\theta + 16)$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$	$(\frac{9}{10}, \frac{50-13\theta}{50})$

Nous avons maintenant le théorème suivant :

THÉORÈME 4.2. *Soit* $d \in \{-3239, -599, -47, 6, 7, 22, 73, 193\}$. *Alors il existe au moins une courbe elliptique définie sur* $\mathbb{Q}(\sqrt{d})$ *de rang* 1 *et dont le groupe de torsion est isomorphe à* $\mathbb{Z}/11\mathbb{Z}$ *:*

$$\mathrm{Sr}(\mathbb{Z}/11\mathbb{Z}, \mathbb{Q}(\sqrt{d})) \geq 1.$$

Preuve. Pour $K = \mathbb{Q}(\sqrt{-3239})$, soit θ avec $\theta^2-\theta+810 = 0$. On considère la courbe

$$E_{-3239} : y^2 = x^3 + \left(3310\theta + \frac{823041}{4}\right)x^2 - (22996305\theta + 502211745)x + 204471924475\theta - 784526490225.$$

À noter que cette courbe est obtenue en faisant $t = -9$ dans l' expression de $\mathcal{E}^{(11)}$ ci-dessus. Puis un calcul de 2-descente en utilisant le programme [21] montre que $\mathrm{rang}(E_{-3239}, K) \leq 1$ et comme le point $P_1 = (-162\theta + 162, -100602\theta - 96228)$ n'est pas un point de 11-torsion, il est donc d'ordre infini d'après la liste des torsions possibles du théorème 1.3. Le rang vaut donc exactement 1.

Pour $K = \mathbb{Q}(\sqrt{-599})$, soit θ avec $\theta^2 - \theta + 150 = 0$, et soit la courbe

$$E_{-599} : y^2 = x^3 + \left(324\theta + \frac{30625}{4}\right)x^2 - (204375\theta + 3046875)x + 386718875\theta - 439453125.$$

Le rang de E_{-599} sur $\mathbb{Q}(\sqrt{-599})$ est 1. On peut vérifier facilement que $Q_2 = (0, -1875\theta - 9375)$ est d'ordre 11. Le point

$$P_2 = (-60\theta - 750, -7395\theta - 68250)$$

est d'ordre infini.

Pour $K = \mathbb{Q}(\sqrt{-47})$, soit θ avec $\theta^2 - \theta + 12 = 0$ et E_{-47} la courbe elliptique

$$E_{-47} : y^2 = x^3 + \left(\frac{45}{4}\,\theta + 46\right)x^2 - (24\theta + 1344)x + 2880\theta - 4608.$$

Le rang de E_3 sur $\mathbb{Q}(\sqrt{-47})$ est 1. Le point $Q_3 = (0, -24\theta - 48)$ est d'ordre 11 et le point

$$P_3 = (-3\theta + 15, -30\theta - 18)$$

est d'ordre infini.

Soit maintenant le corps $K = \mathbb{Q}(\sqrt{6})$, et soit θ avec $\theta^2 - 6 = 0$. Considérons alors la courbe

$$E_6 : y^2 = x^3 + (27257515 20\theta - 6998236812)x - 1251878646245 76\theta + 308865461210640.$$

Le rang de E_6 sur $\mathbb{Q}(\sqrt{6})$ est 1. Le point

$$Q_7 = (8328\theta - 3390, -64800 00\theta + 14580000)$$

est d'ordre 11 et le point

$$P_7 = (19128\theta - 46590, 6998400\theta - 15681600)$$

est d'ordre infini.

Pour $K=\mathbb{Q}(\sqrt{7})$, soit θ avec $\theta^2-7=0$, et soit la courbe :

$$E_7 : y^2 = x^3 - (4058899 20\theta + 1039492656)x + 70627371586556\theta + 18719722947456.$$

Le rang de E_7 sur $\mathbb{Q}(\sqrt{7})$ est 1. Le point

$$Q_8 = (8880\theta + 27420, -15759 36\theta - 3691008)$$

est d'ordre 11 et le point

$$P_6 = \left(\frac{27600}{7}\theta + \frac{115908}{7}, \frac{4852224}{49}\theta - \frac{2985984}{7}\right)$$

est d'ordre infini.

Pour $K=\mathbb{Q}(\sqrt{22})$, soit θ avec $\theta^2-4\theta-18=0$, et soit la courbe :

$$E_{22} : y^2 = x^3 + \left(\frac{59}{128}\theta - \frac{621}{256}\right)x^2 + \frac{81}{2048}\theta x - \frac{6561}{8192}\theta + \frac{177147}{32768}.$$

Le rang de E_{22} sur $\mathbb{Q}(\sqrt{22})$ est 1. Le point $Q_4 = \left(0, -\frac{81}{256}\theta + \frac{243}{128}\right)$ est d'ordre 11 et le point

$$P_4 = \left(\frac{81}{4}, -\frac{4779}{256}\theta + \frac{4131}{128}\right)$$

est d'ordre infini.

Pour $K=\mathbb{Q}(\sqrt{73})$, soit θ avec $\theta^2-\theta-18=0$, et soit la courbe :

$$E_{73} : y^2 = x^3 + \left(40\theta - \frac{351}{4}\right)x^2 + (-1539\theta + 6561)x - 32805\theta + 177147.$$

Le rang de E_{73} sur $\mathbb{Q}(\sqrt{73})$ est 1. Le point $Q_5 = (0, -81\theta + 243)$ est d'ordre 11 et le point

$$P_5 = (-22\theta + 90, -54\theta + 486)$$

est d'ordre infini.

Pour $K=\mathbb{Q}(\sqrt{193})$, soit θ avec $\theta^2-\theta-48=0$, et soit la courbe :

$$E_{193} : y^2 = x^3 + \left(\frac{513}{4}\theta - 176\right)x^2 + (-20352\theta + 122880)x - 1032192\theta + 9437184.$$

Le rang de E_{193} sur $\mathbb{Q}(\sqrt{193})$ est 1. Le point $Q_6 = (0, -384\theta + 1536)$ est d'ordre 11 et le point $P_6 = (8\theta, -156\theta - 576)$ est d'ordre infini. ∎

4.1. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/13\mathbb{Z}$**.** La condition $[7]P_0 = [-6]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut à

$$\begin{aligned}(4.2)\quad \mathcal{U}_{b,c} : {} & b^7 + 6cb^6 + (4c^3 + 15c^2)b^5 + (9c^5 + 15c^4 + 20c^3)b^4 \\ & + (5c^7 + 24c^6 + 21c^5 + 15c^4)b^3 + (c^9 + 6c^8 + 21c^7 + 13c^6 + 6c^5)b^2 \\ & + (6c^8 + 3c^7 + c^6)b - c^{10} = 0.\end{aligned}$$

Cette équation définit une courbe de genre 2. En utilisant l'algorithme de van Hoeij [8], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ par

$$X_1(13) : s^2 = t^6 - 2t^5 + t^4 - 2t^3 + 6t^2 - 4t + 1,$$

et où les b et c dans $E_{b,c}$ sont fonctions de s et t :

$$\begin{aligned} a &= 1 - c = \frac{(t-1)^2(t^2+t-1)s - t^7 + 2t^6 + 3t^5 - 2t^4 - 5t^3 + 9t^2 - 5t + 1}{2t^5}, \\ b &= \frac{(t-1)^2((t^5+2t^4-5t^2+4t-1)s - t^8 - t^7 + 4t^6 + 2t^5 + t^4 - 13t^3 + 14t^2 - 6t + 1)}{2t^9}. \end{aligned} \tag{4.3}$$

La forme générale des courbes elliptiques avec un point d'ordre 13 est ainsi donnée par

$$\mathcal{E}^{(13)} : y^2 + axy + by = x^3 + bx^2 \tag{4.4}$$

avec a, b donnés par (4.3), $P = (t, s) \in X_1(13)$ et

$$t(t-1)(t^3 - 4t^2 + t + 1) \neq 0.$$

Le point $P_0 = (0, 0)$ est d'ordre 13. Pour une forme sans dénominateur, on pourra faire le changement de variable $(x, y) \mapsto (4t^{10}x, 8t^{15}y)$.

THÉORÈME 4.3. *Soit $K = \mathbb{Q}(\sqrt{193})$. Alors il existe une courbe elliptique définie sur K de rang 2 et dont le groupe de torsion est isomorphe à $\mathbb{Z}/13\mathbb{Z}$:*

$$\mathrm{Sr}(\mathbb{Z}/13\mathbb{Z}, K) \geq 2.$$

Preuve. Soit θ tel que $\theta^2 - 193 = 0$ et soit la courbe

$$C : y^2 + \left(-\frac{9}{64}\theta - \frac{215}{64}\right)xy + \left(\frac{261}{1024}\theta - \frac{2277}{1024}\right)y = x^3 + \left(\frac{261}{1024}\theta - \frac{2277}{1024}\right)x^2.$$

Le point $P_0 = (0, 0)$ est sur la courbe C et il est d'ordre 13. Un calcul de 2-descente montre que l'ordre du 2-groupe de Selmer de la courbe C est 4 (car $\mathrm{Sel}^2(C/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), ce qui permet de majorer le rang :

$$\mathrm{rang}(C, K) \leq 2.$$

On vérifie alors que les points

$$\begin{aligned} P &= \left(-\frac{69}{196}\theta - \frac{87}{49}, -\frac{5361}{10976}\theta - \frac{17547}{10976}\right), \\ Q &= \left(-\frac{21}{64}\theta - \frac{267}{64}, -\frac{1623}{2048}\theta - \frac{22281}{2048}\right) \end{aligned}$$

sont d'ordre infini puisqu'ils ne sont pas de 13-torsion. De plus, P et Q sont indépendants. On conclut donc que $\mathrm{rang}(C, K) = 2$. ∎

4.2. Le cas $\mathrm{Tors}(E,K)\supseteq\mathbb{Z}/14\mathbb{Z}$**.** Soit $P=(0,0)$ tel que l'ordre de P n'est ni 2 ni 7, et $b\neq 0$. L'égalité $[7]P_0=[-7]P_0$ sur la forme normale de Tate $E_{b,c}$ est équivalente à

$$\begin{aligned}(4.5)\quad \mathcal{U}_{b,c}: {} & b^6+6b^5c^2+5b^5c+5b^4c^4+25b^4c^3+10b^4c^2+b^3c^6+16b^3c^5\\ & +40b^3c^4+10b^3c^3+4b^2c^7+17b^2c^6+30b^2c^5+5b^2c^4+bc^9\\ & +3bc^8+6bc^7+10bc^6+bc^5+c^7=0.\end{aligned}$$

En utilisant l'algorithme de van Hoeij [6], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ définie par (4.5) par

$$X_1(14): s^2+st+s=t^3-t$$

et on a

$$(4.6)\qquad \begin{aligned} a&=1-c=\tfrac{t^4-st^3+(2s-4)t^2-st+1}{(t+1)(t^3-2t^2-t+1)},\\ b&=\tfrac{-t^7+2t^6+(2s-1)t^5+(-2s-1)t^4+(-2s+2)t^3+(3s-1)t^2-st}{(t+1)^2(t^3-2t^2-t+1)^2}.\end{aligned}$$

À noter que cette courbe est la courbe $14a4$ dans la table de Cremona [3].

La forme générale des courbes elliptiques avec un point d'ordre 14 est ainsi donnée par

$$(4.7)\qquad \mathcal{E}_P^{(14)}: y^2+axy+by=x^3+bx^2$$

avec a,b donnés par (4.6), $P=(t,s)\in X_1(14)$ et

$$t(t-1)(t+1)(t^3-9t^2-t+1)(t^3-2t^2-t+1)\neq 0.$$

Le point $P_0=(0,0)$ est d'ordre 14.

La courbe modulaire $X_1(14)$ est de rang 0 sur $\mathbb{Q}$ et admet exactement six points rationnels sur $\mathbb{Q}$ (voir la table de Cremona [3] pour $14a4$). Clairement $X_1(14)(\mathbb{Q})=\mathrm{Tors}(X_1(14),\mathbb{Q})\simeq\mathbb{Z}/6\mathbb{Z}$, et de plus, ces points induisent des courbes singulières dans la paramétrisation (4.7) ci-dessus :

$$X_1(14)(\mathbb{Q})=\{\mathcal{O},(1,0),(0,0),(-1,0),(0,-1),(1,-2)\}.$$

Lemme 4.4. *Soit K une extension quadratique de $\mathbb{Q}$. Alors*

$$\mathrm{Tors}(X_1(14),K)\simeq\begin{cases}\mathbb{Z}/6\mathbb{Z} & \text{si } K\neq\mathbb{Q}(\sqrt{-7}),\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z} & \text{si } K=\mathbb{Q}(\sqrt{-7}).\end{cases}$$

Preuve. Soit K un corps quadratique. Nous utilisons alors le modèle de Weierstrass réduit de $X_1(14)$:

$$C: y^2=f(x)=x^3-675x+13662.$$

On observe d'abord que

$$\mathrm{Tors}(X_1(14),K)\supseteq\mathrm{Tors}(X_1(14),\mathbb{Q})\simeq\mathbb{Z}/6\mathbb{Z}.$$

Par le théorème 1.3, les seules structures possibles pour $\mathrm{Tors}(X_1(14),K)$ sont $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$. Il suffit donc de montrer

que $X_1(14)(K)$ n'a pas de 2-torsion complète sur K (sauf si $K = \mathbb{Q}(\sqrt{-7})$), ni de 4-torsion, ni de 9-torsion.

$C(K)$ possède une 2-torsion complète si et seulement si $\Psi_2 = f$ se scinde sur K. Or $f(x) = (x+3)(x^2 - 33x + 414)$ ne se scinde complètement que si $K = Q(\sqrt{-7})$. C'est donc le seul corps quadratique tel qu'on ait la 2-torsion complète.

La factorisation du polynôme de 4-division de C en facteurs irréductibles sur $\mathbb{Q}$ est donnée par

$$\Psi_4(x) = (x^2 + 66x - 1503)(x^4 - 66x^3 + 2484x^2 + 10098x + 788859).$$

Il en résulte que Ψ_4 n'a de zéros sur K que lorsque $K = Q(\sqrt{-7})$. Soit alors $K = Q(\sqrt{-7})$. Un calcul simple montre que si $x(P) = \theta$ est la première coordonnée d'un point P tel que $\theta^2 + 66\theta - 1503 = 0$, alors la deuxième coordonnée $y(P)$ n'est pas dans K puisque $f(\theta)$ n'est pas un carré dans $Q(\sqrt{-7})$.

Dans la factorisation sur $\mathbb{Q}$ du polynôme de 9-divisions sur $\mathbb{Q}$, il n'y apparaît pas de facteur de degré ≤ 2, il résulte donc que C ne possède pas de point de 9-torsion sur K. ∎

Exemple 2. La table 2 montre les structures de groupe de la courbe elliptique $X_1(14)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

Table 2. $X_1(14)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(14)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-\frac{2717}{405}, \frac{97648}{18225}\theta + \frac{1156}{405})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	–
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-\frac{35}{27}, \frac{92}{243}\theta + \frac{4}{27})$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-\frac{22}{81}\theta + \frac{35}{81}, \frac{308}{729}\theta - \frac{490}{729})$
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/6\mathbb{Z}$	–
-2	$\theta^2 + 2 = 0$	$\mathbb{Z}/6\mathbb{Z}$	–
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/6\mathbb{Z}$	–
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/6\mathbb{Z}$	–
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-2\theta + 3, 6\theta - 10)$
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/6\mathbb{Z}$	–
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(\frac{8}{25}\theta - \frac{3}{25}, -\frac{16}{125}\theta + \frac{6}{125})$
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{2}, -\frac{1}{4}\theta - \frac{1}{4})$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}$	$(\frac{4}{9}\theta + \frac{5}{9}, -\frac{20}{27}\theta - \frac{52}{27})$

Théorème 4.5. *Soit $K \in \{\mathbb{Q}(\sqrt{-23}), \mathbb{Q}(\sqrt{265})\}$. Alors il existe au moins une courbe elliptique définie sur K de rang 1 et dont le groupe de torsion*

est isomorphe à $\mathbb{Z}/14\mathbb{Z}$ *:*

$$\mathrm{Sr}(\mathbb{Z}/14\mathbb{Z}, K) \geq 1.$$

Preuve. Pour $K = \mathbb{Q}(\sqrt{-23})$ et θ tel que $\theta^2 + 368 = 0$, un calcul de 2-descente montre que la courbe d'équation

$$E_{-23} : y^2 + \left(\frac{5}{1872}\theta + \frac{539}{468}\right)xy + \left(\frac{47}{18252}\theta + \frac{527}{4563}\right)y = x^3 + \left(\frac{47}{18252}\theta + \frac{527}{4563}\right)x^2$$

est au plus de rang 1 et puisque le point

$$P = \left(\frac{1}{312}\theta - \frac{17}{78}, -\frac{17}{6084}\theta + \frac{133}{1521}\right)$$

n'est pas de 14-torsion, il est d'ordre infini et donc le rang de la courbe vaut exactement 1.

Soient maintenant $K = \mathbb{Q}(\sqrt{265})$ et θ tel que $\theta^2 + 5\theta - 60 = 0$. Alors calcul de 2-descente montre que la courbe d'équation

$$E_{265} : y^2 + \left(-\frac{36}{145}\theta + \frac{193}{145}\right)xy + \left(\frac{1452}{21025}\theta - \frac{1872}{4205}\right)y = x^3 + \left(\frac{1452}{21025}\theta - \frac{1872}{4205}\right)x^2$$

est au plus de rang 1. On vérifie facilement que le point

$$P = \left(\frac{10}{29}\theta + \frac{6}{29}, -\frac{202}{841}\theta + \frac{3846}{841}\right)$$

est d'ordre infini puisqu'il n'est pas de torsion (un calcul simple montre qu'il n'est pas d'ordre 14). Le point $P_0 = (0, 0)$ est d'ordre 14 et le rang vaut 1. ∎

4.3. Le cas $\mathrm{Tors}(E, K) \supseteq \mathbb{Z}/15\mathbb{Z}$**.** Soient $b \neq 0$ et $P_0 = (0, 0)$ tel que $\mathrm{ord}(P_0) \notin \{3, 5\}$. La condition $[8]P_0 = [-7]P_0$ sur $E_{b,c}$ équivaut alors à

$$\begin{aligned}(4.8)\quad \mathcal{U}_{b,c} : \; & -c^{13} + (b-1)c^{12} + (-b^2+3b-1)c^{11} + (-3b^2-2b-1)c^{10} \\ & + (-7b^3-19b^2-8b-1)c^9 + (-36b^3-37b^2-9b)c^8 \\ & + (-18b^4-73b^3-36b^2)c^7 + (-62b^4-74b^3)c^6 \\ & + (-19b^5-81b^4+b^3)c^5 + (-45b^5+5b^4)c^4 \\ & + (-10b^6+10b^5)c^3 + 10b^6c^2 + 5b^7c + b^8.\end{aligned}$$

En utilisant l'algorithme de van Hoeij [6], on montre qu'une transformation birationnelle permet de réécrire la courbe $\mathcal{U}_{b,c}$ défini par (4.8) par

$$X_1(15) : s^2 + st + s = t^3 + t^2$$

et on a

$$(4.9)\qquad \begin{aligned} a &= 1-c = \frac{(t^2-t)s+(t^5+5t^4+9t^3+7t^2+4t+1)}{(t+1)^3(t^2+t+1)},\\ b &= \frac{t(t^4-2t^2-t-1)s+t^3(t+1)(t^3+3t^2+t+1)}{(t+1)^6(t^2+t+1)}. \end{aligned}$$

La courbe $X_1(15)$ est la même que $15a8$ dans la table de Cremona [3].

La forme générale des courbes elliptiques avec un point d'ordre 15 est

$$(4.10)\qquad \mathcal{E}_P^{(15)} : y^2+axy+by = x^3+bx^2$$

avec a, b donnés par (4.9), $P=(t,s)\in X_1(15)$ et

$$t(t+1)(t^2+t+1)(t^4+3t^3+4t^2+2t+1)(t^4-7t^3-6t^2+2t+1)\neq 0.$$

Le point $P_0=(0,0)$ est d'ordre 15.

La courbe modulaire $X_1(15)$ est de rang 0 sur $\mathbb{Q}$ et admet exactement quatre points rationnels sur $\mathbb{Q}$. Clairement $X_1(15)(\mathbb{Q}) = \mathrm{Tors}(X_1(15),\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ et de plus ces points induisent des courbes singulières dans la paramétrisation (4.10) ci-dessus :

$$X_1(15)(\mathbb{Q}) = \{\mathcal{O}, (0,0), (-1,0), (0,-1)\}.$$

Lemme 4.6. *Soit K une extension quadratique de $\mathbb{Q}$. Alors*

$$\mathrm{Tors}(X_1(15),K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z} & \text{si } K=\mathbb{Q}(\sqrt{-15}),\\ \mathbb{Z}/8\mathbb{Z} & \text{si } K\in\{\mathbb{Q}(\sqrt{-3}),\mathbb{Q}(\sqrt{5})\},\\ \mathbb{Z}/4\mathbb{Z} & \text{sinon.}\end{cases}$$

Preuve. Soit K un corps quadratique. Nous utilisons alors le modèle de Weierstrass réduit de $X_1(15)$:

$$C : y^2 = f(x) = x^3-27x+8694.$$

On observe d'abord que

$$\mathrm{Tors}(X_1(15),K) \supseteq \mathrm{Tors}(X_1(15),\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Par le théorème 1.3, les seuls sous-groupes de torsion possibles sur K sont : $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$. Le polynôme de 3-division de C,

$$\Psi_3(x) = 3x^4-162x^2+104328x-729,$$

est irréductible sur $\mathbb{Q}$ et donc n'a pas de zéro sur K. Il en résulte que les cas $\mathbb{Z}/12\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$ sont à écarter puisque $C(K)$ ne peut avoir de point de 3-torsion.

La factorisation du polynôme de 8-division en facteurs irréductibles sur $\mathbb{Q}$ est donnée par

$$\Psi_8(x) = 8(x-15)(x+57)(x^2-66x-531)(x^2+6x+981)f_4^{(1)}f_4^{(2)}h_{16},$$

où $f_4^{(1)}$, $f_4^{(2)}$ et h_{16} sont des polynômes de degré $\deg(f_4^{(1)}) = \deg(f_4^{(2)}) = 4$ et $\deg(h_{16}) = 16$. Un calcul simple montre que les points d'abscisse $x(P) = 15$ sont d'ordre 4 sur $C(\mathbb{Q})$ et les points d'abscisse $x(P) = -57$ sont d'ordre 4 sur $C(\mathbb{Q}(\sqrt{-15}))$. Si $K = \mathbb{Q}(\sqrt{5})$ et θ_1 est tel que $\theta_1^2 - 66\theta_1 - 531 = 0$, alors les points tels que $x(P) = \theta_1$ sont d'ordre 8 sur $C(K)$. Si $K = \mathbb{Q}(\sqrt{-3})$ et θ_2 est tel que $\theta_2^2 + 6\theta_2 + 981 = 0$, alors les points tels que $x(P) = \theta_2$ sont d'ordre 8 sur $C(K)$.

La factorisation sur $\mathbb{Q}$ en facteurs irréductibles du polynôme

$$\frac{\Psi_{16}(x)}{\Psi_8(x)} = 2f_4^{(3)} f_4^{(4)} g_{16}^{(1)} g_{16}^{(2)} h_{64}^{(1)}$$

avec $f_i^{(j)}$, $g_i^{(k)}$ et $h_i^{(l)}$ de degré i implique qu'on ne peut pas obtenir des points d'ordre 16 si l'on se restreint à des extensions quadratiques. Maintenant, pour obtenir la 2-torsion complète, il faut et il suffit que f se scinde complètement dans K. Comme on a

$$\Psi_2(x) = f(x) = (x + 21)(x^2 - 21x + 414),$$

il en résulte que $C(K) \supset C[2]$ si et seulement si $K = \mathbb{Q}(\sqrt{-15})$. On montre de plus que si $K = \mathbb{Q}(\sqrt{-15})$ alors $\mathrm{Tors}(X_1(15), K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ puisque le polynôme de 4-division ne se scinde pas complètement sur K. ∎

Exemple 3. La table 3 montre les structures de groupe de la courbe elliptique $X_1(15)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

Table 3. $X_1(15)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(15)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2 + 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{13}{4}, -\frac{3}{2}\theta + \frac{9}{8})$
-7	$\theta^2 + 7 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{8}\theta - \frac{5}{8}, \frac{1}{16}\theta + \frac{5}{16})$
-6	$\theta^2 + 6 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{5}{4}, -\frac{1}{4}\theta + \frac{1}{8})$
-5	$\theta^2 + 5 = 0$	$\mathbb{Z}/4\mathbb{Z}$	–
-3	$\theta^2 + 3 = 0$	$\mathbb{Z}/8\mathbb{Z}$	–
-2	$\theta^2 + 2 = 0$	$\mathbb{Z}/4\mathbb{Z}$	–
-1	$\theta^2 + 1 = 0$	$\mathbb{Z}/4\mathbb{Z}$	–
2	$\theta^2 - 2 = 0$	$\mathbb{Z}/4\mathbb{Z}$	–
3	$\theta^2 - 3 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{1}{2}, -\frac{1}{4}\theta - \frac{1}{4})$
5	$\theta^2 - 5 = 0$	$\mathbb{Z}/8\mathbb{Z}$	–
6	$\theta^2 - 6 = 0$	$\mathbb{Z}/4\mathbb{Z}$	–
7	$\theta^2 - 7 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(\frac{3}{4}, \frac{1}{2}\theta - \frac{7}{8})$
10	$\theta^2 - 10 = 0$	$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}$	$(-\frac{3}{4}, \frac{1}{8}\theta - \frac{1}{8})$

4.4. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/16\mathbb{Z}$**.** Soient $P=(0,0)$ tel que $\mathrm{ord}(P) \notin \{2,4,8\}$ et $c \neq 0$. L'égalité $[8]P_0 = [-8]P_0$ sur la forme normale de Tate $E_{b,c}$ équivaut alors à

$$\begin{aligned}(4.11)\quad \mathcal{U}_{b,c} : {} & (b-1)c^{12} + 3bc^{11} + (4b^2+10b)c^{10} + (20b^2+6b)c^9 \\ & + (10b^3+15b^2+3b)c^8 + (10b^3+14b^2+b)c^7 \\ & + (30b^3+7b^2)c^6 + (40b^4+22b^3)c^5 + (b^6+35b^5+40b^4)c^4 \\ & + (18b^6+45b^5)c^3 + (4b^7+31b^6)c^2 + 12b^7c + 2b^8 = 0.\end{aligned}$$

Une transformation birationnelle ramène à la forme minimale

$$X_1(16) : s^2 = t(t^2+1)(t^2+2t-1),$$

où a et b sont fonctions de s et de t :

$$(4.12)\qquad \begin{aligned} a &= 1-c = \tfrac{(t-1)(t^4+2t^3+6t-1)}{(t+1)^5(t^2+2t-1)}\, s + \tfrac{t^5+t^4+14t^3+6t^2+9t+1}{(t+1)^5}, \\ b &= \tfrac{(t-1)^3(3t^4+8t^3-2t^2+8t-1)}{(t+1)^8(t^2+2t-1)}\, s + \tfrac{t(t-1)^3(t^2+1)(t^4+8t^3+10t^2-8t+5)}{(t+1)^8(t^2+2t-1)}. \end{aligned}$$

La forme générale des courbes elliptiques avec un point d'ordre 16 est

$$\mathcal{E}_P^{(16)} : y^2 + axy + by = x^3 + bx^2$$

avec a, b donnés par (4.12), $P=(t,s) \in X_1(16)$ et

$$t(t-1)(t+1)(t^2+1)(t^2-2t-1)(t^2+2t-1) \neq 0.$$

Le point $P_0=(0,0)$ est d'ordre 16.

Pour une forme sans dénominateur, on pourra faire le changement de variable

$$(x,y) \mapsto \left(\frac{x}{(t+1)^{10}(t^2+2t-1)^2}, \frac{y}{(t+1)^{15}(t^2+2t-1)^3} \right).$$

Théorème 4.7. *Soit $K=\mathbb{Q}(\sqrt{10})$. Alors il existe une courbe elliptique définie sur K de rang 1 et dont le groupe de torsion est isomorphe à $\mathbb{Z}/16\mathbb{Z}$:*

$$\mathrm{Sr}(\mathbb{Z}/16\mathbb{Z}, K) \geq 1.$$

Preuve. Soit θ tel que $\theta^2 - 10 = 0$ et soit la courbe elliptique

$$E : y^2 + (39\theta+121)xy - (1107\theta+3510)y = x^3 - (1107\theta+3510)x^2.$$

Un calcul de 2-descente permet d'obtenir que $\mathrm{rang}(E, \mathbb{Q}(\sqrt{10})) \leq 1$, et puisque le point

$$P = (-9\theta - 24, 2970\theta + 9402)$$

n'est pas de 16-torsion, il est d'ordre infini. Le rang vaut donc exactement 1. On vérifie facilement que le point $(0,0)$ est d'ordre 16. ∎

4.5. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/18\mathbb{Z}$**.** Soient $b \neq 0$ et $P = (0,0)$, supposons que $\mathrm{ord}(P) \notin \{2,3,6\}$ sur $E_{b,c}$. L'égalité $[9]P_0 = [-9]P_0$ dans la forme normale de Tate $E_{b,c}$ équivaut alors à

$$\begin{aligned}(4.13)\qquad \mathcal{U}_{b,c} : &- c^{13} + c^{12} + (-b^3 + 7b - 1)c^{11} + (-8b^3 - 11b)c^{10} \\ &+ (-7b^4 - 37b^3 - 55b^2)c^9 + (-50b^4 - 128b^3)c^8 \\ &+ (-18b^5 - 143b^4 + 8b^3)c^7 + (b^6 - 67b^5 + 41b^4 + b^3)c^6 \\ &+ (-b^6 + 84b^5 + 6b^4)c^5 + (6b^7 + 86b^6 + 15b^5)c^4 \\ &+ (44b^7 + 20b^6)c^3 + (9b^8 + 15b^7)c^2 + 6b^8c + b^9 = 0.\end{aligned}$$

En utilisant l'algorithme de van Hoeij [8], on montre qu'une transformation birationnelle permet de réécrire $\mathcal{U}_{b,c}$ donné par (4.13) par la forme plus simple

$$X_1(18) : s^2 = t^6 + 2t^5 + 5t^4 + 10t^3 + 10t^2 + 4t + 1$$

avec

$$\begin{aligned}a &= 1 - c \\ &= \frac{-t^2 - 3t - 2}{2t^3(t^3 - 3t - 1)}\, s - \frac{(-2t^5 + t^4 + 10t^3 + 11t^2 + 11t + 5)}{2t^2(t^3 - 3t - 1)}, \\ (4.14)\qquad b &= -\frac{(t+1)(t^2+t+1)(t^4+2t^3-t+1)}{2t^5(t^3-3t-1)^2}\, s \\ &\quad - \frac{(t+1)(t^2+t+1)(t^7+3t^6+4t^5+6t^4+4t^3-t^2-t-1)}{2t^5(t^3-3t-1)^2}.\end{aligned}$$

La forme générale des courbes elliptiques avec un point d'ordre 18 est finalement donnée par

$$\mathcal{E}_P^{(18)} : y^2 + axy + by = x^3 + bx^2$$

avec a, b donnés par (4.14), $P = (t,s) \in X_1(18)(K)$ et

$$t(t+1)(t^2+t+1)(t^3-3t-1) \neq 0.$$

Le point $P_0 = (0,0)$ est d'ordre 18. Pour une forme sans dénominateur, on pourra faire le changement de variable

$$(x,y) \mapsto \left(\frac{x}{4t^6(t^3-3t-1)^4}, \frac{y}{8t^9(t^3-3t-1)^6}\right).$$

4.6. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$**.** D'après la proposition 1, le genre de la courbe modulaire $X_1(2,10)$ est 1. Notre premier résultat est le suivant :

THÉORÈME 4.8. *La courbe modulaire* $X_1(2,10)$ *est donnée par l'équation*

$$X_1(2,10) : s^2 = t^3 + t^2 - t.$$

Preuve. Considérons la forme des courbes avec un point d'ordre 10 :

$$\mathcal{E}^{(10)} : y^2+\frac{t^3-2t^2-4t+4}{t^2-6t+4}\,xy-\frac{(t-1)(t-2)t^3}{(t^2-6t+4)^2}\,y=x^3-\frac{(t-1)(t-2)t^3}{(t^2-6t+4)^2}\,x^2.$$

Cette courbe est birationnellement équivalente à

$$\mathcal{E}^{(10)} : y^2 = xf_t(x) = x^3 + \frac{-t^6+8t^5-20t^4+20t^3-16t+8}{2(t^2-6t+4)^2}\,x^2 + \frac{t^5(t-2)^5}{16(t^2-6t+4)^3}\,x. \tag{4.15}$$

Le discriminant de $f_t(x)$ est donnée par

$$\Delta(f_t(x)) = \frac{2^4(t-1)^5(t^2-t-1)}{(t^2-6t+4)^4}$$

et doit être un carré. Pour que $E[2] \subset E(K)$, nous considérons la courbe

$$\mathcal{U}_{s,t} : s^2 - (t-1)(t^2-t-1) = 0.$$

Le genre de $\mathcal{U}_{s,t}$ est 1, et le changement de variable

$$(s,t) \mapsto (s, t+1)$$

donne la forme minimale de la courbe $X_1(2,10) : s^2 = t^3 + t^2 - t$. ∎

La courbe $X_1(2,10)$ est appelée $14a4$ dans la table de Cremona [3].

La forme des courbes elliptiques avec un sous-groupe de torsion isomorphe a $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ est donnée par

$$\mathcal{E}_P^{(2,10)} : y^2+\frac{t^3+t^2-4t+1}{t^2-4t-1}\,xy-\frac{t(t-1)(t+1)^3}{(t^2-4t-1)^2}\,y=x^3-\frac{t(t-1)(t+1)^3}{(t^2-4t-1)^2}\,x^2.$$

Pour obtenir une forme plus simple, faisons le changement de variable

$$(x,y) \mapsto \left(\frac{x}{(t^2-4t-1)^2}, \frac{y}{(t^2-4t-1)^3}\right).$$

On obtient alors la forme

$$\mathcal{E}_P^{(2,10)} : y^2 + (t^3+t^2-4t+1)xy - t(t-1)(t+1)^3(t^2-4t-1)y = x^3 - t(t-1)(t+1)^3x^2, \tag{4.16}$$

où $P = (t,s) \in X_1(2,10)$ est tel que

$$\Delta_{\mathcal{E}^{(2,10)}} = t^5(t^2-1)^{10}(t^2-4t-1)^2(t^2+t-1)^2 \neq 0.$$

Les points

$$P_0 = (0,0) \quad \text{et} \quad Q = ((-2t+s-1)(s+1)t, (s+1)^2((s+1)t^2-2t-2s^2)),$$

sont d'ordre 10 et 2 respectivement, et on a

$$\langle Q, P_0\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}.$$

La courbe modulaire $X_1(2,10)$ est de rang 0 sur $\mathbb{Q}$ et admet exactement six points rationnels sur $\mathbb{Q}$ (voir la table de Cremona pour la courbe $20a2$) :

$$X_1(2,10)(\mathbb{Q}) = \{\mathcal{O}, (-1,1), (1,-1), (0,0), (1,1), (-1,-1)\}.$$

Ces points induisent des courbes singulières dans la paramétrisation (4.16) ci-dessus.

LEMME 4.9. *Soit K une extension quadratique de $\mathbb{Q}$. Alors*

$$\mathrm{Tors}(X_1(2,10), K) \simeq \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} & \text{si } K = \mathbb{Q}(\sqrt{5}), \\ \mathbb{Z}/6\mathbb{Z} & \text{sinon.} \end{cases}$$

Preuve. Soit K un corps de nombres quadratique. Nous utilisons le modèle de Weierstrass réduit de $X_1(2,10)$:

$$C : y^2 = f(x) = x^3 - 1728x + 19008.$$

On observe d'abord que

$$\mathrm{Tors}(X_1(2,10), K) \supseteq \mathrm{Tors}(X_1(2,10), \mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}.$$

Par le théorème 1.3, les seules structures possibles pour $\mathrm{Tors}(X_1(2,10), K)$ sont $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

Pour obtenir la 2-torsion complète, il faut que f se scinde complètement sur K. Comme on a

$$\Psi_2(x) = f(x) = (x-12)(x^2 + 12x - 1584),$$

il faut donc que $K \supseteq \mathbb{Q}(\sqrt{5})$. On a ensuite la factorisation sur $\mathbb{Q}$ du polynôme

$$\frac{\Psi_4(x)}{\Psi_2(x)} = (x^2 - 24x + 1440) f_4^{(1)},$$

où $f_4^{(1)}$ est un polynôme irréductible de degré 4. Les points dont l'abscisse $x(P)$ est égale à θ avec $\theta^2 - 24\theta + 1440 = 0$ n'ont pas leurs ordonnées dans $K = \mathbb{Q}(\theta) = \mathbb{Q}(\sqrt{-1})$. Il ne peut donc y avoir de point d'ordre 4.

La factorisation du polynôme de 3-division de C en facteurs irréductibles sur $\mathbb{Q}$ est donnée par

$$\Psi_3(x) = (x-48)(x^3 + 48x^2 - 1152x + 20736).$$

Cela implique que quel que soit K, on ne peut avoir la 3-torsion complète.

Enfin, la factorisation du polynôme de 9-division est donnée par

$$\Psi_9(x) = f_9 f_{27} \Psi_3(x),$$

où f_9 et f_{27} sont des polynômes irréductibles sur $\mathbb{Q}$, de degré 9 et 27 respectivement. Il ne peut donc y avoir de point d'ordre 9 sur K. ∎

EXEMPLE 4. La table 4 montre les structures de groupe de la courbe elliptique $X_1(2,10)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

Table 4. $X_1(2,10)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(2,10)(\mathbb{Q}(\sqrt{d}))$	Point d'ordre infini
-10	$\theta^2+10=0$	$\mathbb{Z}/6\mathbb{Z}$	–
-7	$\theta^2+7=0$	$\mathbb{Z}/6\mathbb{Z}$	–
-6	$\theta^2+6=0$	$\mathbb{Z}/6\mathbb{Z}$	–
-5	$\theta^2+5=0$	$\mathbb{Z}/6\mathbb{Z}$	–
-3	$\theta^2+3=0$	$\mathbb{Z}/6\mathbb{Z}$	–
-2	$\theta^2+2=0$	$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}$	$(-2,-\theta)$
-1	$\theta^2+1=0$	$\mathbb{Z}/6\mathbb{Z}$	–
2	$\theta^2-2=0$	$\mathbb{Z}/6\mathbb{Z}$	–
3	$\theta^2-3=0$	$\mathbb{Z}/6\mathbb{Z}$	–
5	$\theta^2-5=0$	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$	–
6	$\theta^2-6=0$	$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}$	$(-2\theta+7, 8\theta-23)$
7	$\theta^2-7=0$	$\mathbb{Z}/6\mathbb{Z}$	–
10	$\theta^2-10=0$	$\mathbb{Z}/6\mathbb{Z}\times\mathbb{Z}$	$(2,-\theta)$

4.7. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$**.** Considérons la forme des courbes avec un point d'ordre 12 :

$$\begin{aligned}(4.17)\qquad \mathcal{E}^{(12)}: y^2 &+ \frac{6t^4-8t^3+2t^2+2t-1}{(t-1)^3}\,xy \\ &+ \frac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{(t-1)^4}\,y \\ &= x^3 + \frac{-12t^6+30t^5-34t^4+21t^3-7t^2+t}{(t-1)^4}\,x^2.\end{aligned}$$

Cette courbe est birationnellement équivalente à

$$\begin{aligned}(4.18)\qquad \mathcal{E}^{(12)}: y^2 &= x f_t(x) \\ &= x^3 + \frac{24t^8-96t^7+216t^6-312t^5+288t^4-168t^3+60t^2-12t+1}{4t^6-24t^5+60t^4-80t^3+60t^2-24t+4}\,x^2 \\ &\quad + \frac{9t^{10}-18t^9+15t^8-6t^7+t^6}{t^6-6t^5+15t^4-20t^3+15t^2-6t+1}\,x.\end{aligned}$$

Le discriminant de $f_t(x)$ est donné par

$$\Delta(f_t(x)) = \frac{(2t-1)^6(2t^2-2t+1)^3(6t^2-6t+1)}{16(t-1)^{12}}.$$

Pour que $E[2]\subset E(K)$, nous imposons que ce discriminant soit un carré dans K, ce qui nous amène à considérer la courbe

$$\Gamma : s^2 = (2t^2 - 2t + 1)(6t^2 - 6t + 1). \tag{4.19}$$

La courbe modulaire $X_1(2,12)$ est appelée $24a4$ dans la table de Cremona [3].

Nous trouvons la forme simplifiée en utilisant la même méthode que dans [1] :

$$\Gamma : s^2 = 12t^4 - 24t^3 + 20t^2 - 8t + 1.$$

Le point $(0,1)$ est sur Γ et, en posant

$$t = \left(T + \frac{1}{2}\right)^{-1} \quad \text{et} \quad s = St^2,$$

on trouve que Γ est birationnellement équivalente à

$$\Gamma' : S^2 = T^4 - 4T^2 - 8T - 4,$$

qui ensuite est birationnellement équivalente à

$$y^2 = x^3 + \frac{2}{3}x + \frac{7}{27},$$

par le changement de variable

$$T = \frac{y+1}{x - \frac{1}{3}} \quad \text{et} \quad S = -T^2 + 2x + \frac{2}{3}.$$

En faisant le changement de variable

$$(x,y) \mapsto \left(x - \frac{1}{3}, y\right)$$

on obtient efin la forme minimale $\Gamma'' : y^2 = x^3 - x^2 + x$.

THÉORÈME 4.10. *La courbe modulaire $X_1(2,12)$ est donnée par l'équation*

$$X_1(2,12) : s^2 = t^3 - t^2 + t.$$

Preuve. Voir la discussion ci-dessus. ∎

Bien qu'il y ait une correspondance entre les points rationnels de $X_1(2,12)$ et ceux de la courbe Γ, par souci de commodité, nous allons utiliser la paramétrisation des courbes elliptiques avec 2-torsion complète et un point d'ordre 12 par la courbe Γ.

La forme des courbes elliptiques avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ est donnée par

$$\begin{aligned} \mathcal{E}^{(2,12)} : y^2 &+ (6t^4 - 8t^3 + 2t^2 + 2t - 1)xy \\ &+ (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t-1)^5 y \\ &= x^3 + (-12t^6 + 30t^5 - 34t^4 + 21t^3 - 7t^2 + t)(t-1)^2 x^2 \end{aligned} \tag{4.20}$$

avec $P = (t,s) \in \Gamma(K)$ tel que

$$\Delta_{\mathcal{E}^{(2,12)}} = t^{12}(t-1)^{12}(2t-1)^6(2t^2-2t+1)^3(3t^2-3t+1)^4(6t^2-6t+1) \neq 0.$$

Les points $P_0 = (0,0)$ et

$$\begin{aligned} Q = \Bigg(& \frac{1}{72}((-36s^2 - 12s + 12)t^3 + (42s^2 + 18s - 22)t^2 \\ & + (-12s^3 - 12s^2 - 12s + 16)t + (6s^3 - 4s^2 + 3s - 5)), \\ & \frac{1}{864}((144s^4 - 108s^3 + 72s^2 - 12s + 16)t^3 \\ & + (-180s^4 + 210s^3 - 120s^2 + 26s - 28)t^2 \\ & + (36s^5 + 96s^4 - 132s^3 + 88s^2 - 20s + 20)t \\ & + (6s^5 - 21s^4 + 41s^3 - 27s^2 + 7s - 6)) \Bigg) \end{aligned}$$

sont d'ordre 12 et 2 respectivement, et on a

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}.$$

La courbe modulaire $X_1(2,12)$ est de rang 0 sur $\mathbb{Q}$ et admet exactement quatre points rationnels sur $\mathbb{Q}$. Clairement $X_1(2,12)(\mathbb{Q}) = \mathrm{Tors}(X_1(2,12),\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}$ et de plus ces points induisent des courbes singulières dans la paramétrisation (4.20) ci-dessus :

$$X_1(2,12)(\mathbb{Q}) = \{\mathcal{O}, (1,1), (0,0), (1,-1)\}.$$

LEMME 4.11. *Soit K une extension quadratique de $\mathbb{Q}$. Alors*

$$\mathrm{Tors}(X_1(2,12),K) \simeq \begin{cases} \mathbb{Z}/8\mathbb{Z} & \text{si } K \in \{\mathbb{Q}(\sqrt{-1}), \mathbb{Q}(\sqrt{3})\}, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} & \text{si } K = \mathbb{Q}(\sqrt{-3}), \\ \mathbb{Z}/4\mathbb{Z} & \text{sinon.} \end{cases}$$

Preuve. Soit K un corps de nombres quadratique. Nous utilisons le modèle de Weierstrass simplifié de $X_1(2,12)$:

$$C : y^2 = f(x) = x^3 + 864x + 12096.$$

On observe d'abord que

$$\mathrm{Tors}(X_1(2,12),K) \supseteq \mathrm{Tors}(X_1(2,12),\mathbb{Q}) \simeq \mathbb{Z}/4\mathbb{Z}.$$

Par le théorème 1.3, les seuls sous-groupes de torsion possibles sont $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

Pour obtenir la 2-torsion complète, il faut et il suffit que

$$\Psi_2(x) = f(x) = (x + 12)(x^2 - 12x + 1008)$$

se scinde complètement dans K, c'est-à-dire $K = \mathbb{Q}(\sqrt{-3})$.

La courbe C ne peut avoir un point d'ordre 3 puisque le polynôme de 3-division

$$\Psi_3(x) = x^4 + 1728x^2 + 48384x - 248832$$

est irréductible sur $\mathbb{Q}$ et donc ne peut posséder de racines sur K.

La factorisation du polynôme de 4-division en facteurs irréductibles sur $\mathbb{Q}$ est donnée par

$$\Psi_4(x) = (x-24)(x+48)f_4\Psi_2(x),$$

où f_4 est un polynôme irréductible de degré 4 sur $\mathbb{Q}$. Les points d'abscisse $x(P) = 24$ sont dans $C(\mathbb{Q})$ et les points d'abscisse $x(P) = -48$ appartiennent à $C(\mathbb{Q}(\sqrt{-3}))[4] \setminus C(\mathbb{Q})[4]$. Comme $\Psi_4(x)$ possède un facteur irréductible de degré 4, on ne peut donc avoir la 4-torsion complète sur K.

La factorisation du polynôme de 8-division est

$$\Psi_8(x) = (x^2-120x-288)(x^2+24x+1440)f_4^{(2)}f_{16}^{(2)}\Psi_4(C),$$

où les $f_i^{(j)}$ sont de degré i et sont irréductibles sur $\mathbb{Q}$. Soient $K = \mathbb{Q}(\sqrt{3})$ et θ_1 tel que $\theta_1^2 - 120\theta_1 - 288 = 0$. Alors les points d'abscisse $x(P) = \theta_1$ sont d'ordre 8 sur $C(K)$. De même, si $K = \mathbb{Q}(\sqrt{-1})$ et θ_2 est tel que $\theta^2 + 24\theta + 1440 = 0$, alors les points d'abscisse $x(P) = \theta_2$ sont d'ordre 8 sur $C(K)$.

La factorisation sur $\mathbb{Q}$ du polynôme de 16-division est donnée par

$$\Psi_{16}(x) = f_8^{(3)}f_8^{(4)}f_8^{(5)}f_8^{(6)}f_{64}^{(1)}\Psi_8(x),$$

où les $f_i^{(j)}$ sont des polynômes irréductibles de degré i. Ceci montre qu'il ne peut y avoir de point d'ordre 16 sur K. ∎

Exemple 5. La table 5 montre les structures de groupe de la courbe elliptique $X_1(2,12)$ sur $K = \mathbb{Q}(\sqrt{d})$ avec $|d| \leq 10$.

Table 5. $X_1(2,12)(\mathbb{Q}(\sqrt{d}))$, $-10 \leq d \leq 10$

d	$\mathbb{Q}(\sqrt{d})$	$X_1(2,12)/\mathbb{Q}(\sqrt{d})$	Point d'ordre infini
-10	$\theta^2+10=0$	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}$	$(\frac{1608\theta+3049}{5929}, \frac{20904\theta+39637}{456533})$
-7	$\theta^2+7=0$	$\mathbb{Z}/4\mathbb{Z}$	–
-6	$\theta^2+6=0$	$\mathbb{Z}/4\mathbb{Z}$	–
-5	$\theta^2+5=0$	$\mathbb{Z}/4\mathbb{Z}$	–
-3	$\theta^2+3=0$	$\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$	–
-2	$\theta^2+2=0$	$\mathbb{Z}/4\mathbb{Z}$	–
-1	$\theta^2+1=0$	$\mathbb{Z}/8\mathbb{Z}$	–
2	$\theta^2-2=0$	$\mathbb{Z}/4\mathbb{Z}$	–
3	$\theta^2-3=0$	$\mathbb{Z}/8\mathbb{Z}$	–
5	$\theta^2-5=0$	$\mathbb{Z}/4\mathbb{Z}$	–
6	$\theta^2-6=0$	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}$	$(2,-\theta)$
7	$\theta^2-7=0$	$\mathbb{Z}/4\mathbb{Z}$	–
10	$\theta^2-10=0$	$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}$	$(\frac{5}{8}, \frac{7}{32}\theta)$

4.8. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$**.** Dans [14], Kubert a proposé une paramétrisation pour cette structure comme suit :

$$C : y^2 = x^3 + ax^2 + bx + c, \quad \text{avec}$$
$$a = \frac{3}{4}(r+s),\ b = \frac{1}{2}(rs+t),\ c = \frac{1}{4}rt,\ r = \frac{2t}{s-v},\ t = \frac{v^2+3s^2}{12}.$$

Nous proposons ici une autre approche. Rappelons que la forme d'une courbe avec 3-torsion est donnée par

$$\mathcal{E}^{(3)} : y^2 + sxy + ty = x^3.$$

Grâce au changement de variable

$$(x,y) \mapsto \left(x - \frac{s^2}{12}, y - \frac{sx+t}{2}\right),$$

on obtient

$$C^{(3)} : y^2 = x^3 + \left(-\frac{1}{48}s^4 + 12ts\right)x + \frac{1}{864}s^6 - \frac{1}{24}ts^3 + \frac{1}{4}t^2.$$

On impose maintenant $E[3] \in E[K]$. En factorisant complètement le polynôme de 3-division associé

$$\Psi_3(x) = \frac{3}{576}\left(x - \frac{s^2}{12}\right)\Phi_{3,s}(x,t) = 0,$$

on est ramené à résoudre

$$C_3 : \Phi_{3,s}(x,t) = 576x^3 + 48s^2x^2 + (576st - 20s^4)x + (576t^2 - 48s^3t + s^6).$$

En considérant s comme un paramètre, l'algorithme de van Hoeij [7] permet de trouver

$$t = \frac{4v(144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)}{(vs^2-12)^3},$$
$$x = -\frac{-48v^2s^3 + 576v^2 + v^2s^6 - 24vs^4 + 576vs + 144s^2}{4(vs^2-12)^2},$$

où $v \in K$ est tel que $vs^2 - 12 \neq 0$. Avec le changement de variable

$$(x,y) \mapsto \left(\frac{x}{(vs^2-12)^2}, \frac{y}{(vs^2-12)^3}\right),$$

on obtient la forme générale

$$\mathcal{E}^{(3,3)} : y^2 + s(vs^2-12)xy + 4v(144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)y = x^3, \tag{4.21}$$

où $v, s \in K$ sont tels que

$$\Delta_{\mathcal{E}^{(3,3)}} = 2^6v^3(vs^3 - 36v - 12s)^3 \times (144s^2 - 24vs^4 + 432vs + 432v^2 + v^2s^6 - 36v^2s^3)^3 \neq 0.$$

Les points

$$P_0 = (0,0),$$
$$Q = \left(-\frac{-48v^2s^3 + 576v^2 + v^2s^6 - 24vs^4 + 576vs + 144s^2}{4}, \right.$$
$$\left. \frac{(\sqrt{-3}+3)(vs^3 + (-6\sqrt{-3}-18)v - 12s)^2(vs^3 + (6\sqrt{-3}-18)v - 12s)}{18v^3} \right)$$

sont d'ordre 3, et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

THÉORÈME 4.12. *Soit $K = \mathbb{Q}(\sqrt{-3})$, alors il existe une courbe elliptique définie sur K de rang 2 et avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$:*

$$\mathrm{Sr}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}, K) \geq 2.$$

Preuve. En substituant v par -3 et s par 1 dans l'équation (4.21), nous obtenons la courbe elliptique

$$E : y^2 - 15xy - 29916y = x^3.$$

En utilisant le programme [19], nous trouvons que le rang vaut 2. Les points

$$P_1 = (-180, -13392) \quad \text{et} \quad P_2 = \left(-\frac{14958}{49}, \frac{3941433}{343} \right)$$

sont d'ordre infini et indépendants. De plus,

$$(0,0) \quad \text{et} \quad \left(-831, \frac{25761}{2}\sqrt{-3} + \frac{17451}{2} \right)$$

sont d'ordre 3 et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. ∎

4.9. Le cas $\mathrm{Tors}(E,K) \supseteq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$**.** Le principe pour le cas $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ est le même que précédemment. Rappelons que la forme des courbes elliptiques avec un point d'ordre 6 est

$$\mathcal{E}^{(6)} : y^2 + (1-t)xy - t(t+1)y = x^3 - t(t+1)x^2.$$

Cherchons d'abord une forme du type $y^2 = x^3 + A(t)x + B(t)$. Cela s'obtient en faisant le changement de variable

$$(x,y) \mapsto \left(x + \frac{3}{4}t^2 + \frac{3}{2}t - \frac{1}{4}, y - \frac{(1-t)x - t(t+1)}{2} \right).$$

On obtient alors l'équation

$$C^{(6)} : y^2 = x^3 + \left(-\frac{3}{16}t^4 - \frac{1}{4}t^3 - \frac{5}{8}t^2 - \frac{1}{4}t - \frac{1}{48} \right)x + \left(-\frac{1}{32}t^6 - \frac{1}{16}t^5 + \frac{5}{32}t^4 + \frac{5}{24}t^3 + \frac{11}{96}t^2 + \frac{1}{48}t + \frac{1}{864} \right). \tag{4.22}$$

Le polynôme de 3-division de cette courbe est donné par

$$\Psi_3(x,t) = \frac{3}{576}\left(x - \frac{3}{4}t^2 - \frac{1}{2}t - \frac{1}{12}\right)\Phi_3(x,t)$$

avec

$$\begin{aligned}(4.23)\qquad \Phi_3(x,t) &= 576x^3 + (432t^2 + 288t + 48)x^2 \\ &\quad + (108t^4 + 144t^3 - 504t^2 - 240t - 20)x \\ &\quad + (9t^6 + 18t^5 + 63t^4 + 60t^3 + 87t^2 + 18t + 1).\end{aligned}$$

La courbe $C : \Phi_3(x,t) = 0$ est de genre 0 et la paramétrisation de cette courbe, donnée par l'algorithme [7], induit que t doit être de la forme

$$t = -\frac{(3v-2)(3v^2+4)}{9(v-2)^3} \quad \text{où } v \in K \setminus \{2\}.$$

On obtient alors la forme générale

$$\begin{aligned}\mathcal{E}^{(3,6)} : y^2 + \frac{2(9v^3 - 30v^2 + 60v - 40)}{9(v-2)^3}\,xy \\ - \frac{16(3v-2)(3v^2+4)(3v^2-6v+4)}{81(v-2)^6}\,y \\ = x^3 - \frac{16(3v-2)(3v^2+4)(3v^2-6v+4)}{81(v-2)^6}\,x^2.\end{aligned}$$

Le changement de variable

$$(x,y) \mapsto \left(\frac{x}{81(v-2)^6}, \frac{y}{729(v-2)^9}\right)$$

nous ramène à la forme plus simple

$$\begin{aligned}(4.24)\qquad \mathcal{E}^{(3,6)} : y^2 + 2(9v^3 - 30v^2 + 60v - 40)xy \\ - 144(3v-2)(3v^2+4)(3v^2-6v+4)(v-2)^3 y \\ = x^3 - 16(3v-2)(3v^2+4)(3v^2-6v+4)x^2,\end{aligned}$$

où $v \in K$ est tel que le discriminant de $\mathcal{E}^{(3,6)}$, donné par

$$\Delta_{\mathcal{E}^{(3,6)}} = 2^{15}3^6v^3(v-2)^6(3v-2)^6(3v^2+4)^6(3v^2-6v+4)^3,$$

est non nul. Les points $P_0 = (0,0)$ et

$$\begin{aligned}Q = \Bigg(&-12(v-2)^2(3v^2-16v+4)(3v^2+4), \\ &(324\sqrt{-3}+972)(v-2)^2\left(v - \frac{2}{3}\sqrt{-3}\right)^2\left(v - \frac{1}{3}\sqrt{-3} - 1\right) \\ &\times \left(v + \frac{1}{3}\sqrt{-3} - 1\right)^2\left(v + \frac{2}{3}\sqrt{-3}\right)^2\Bigg)\end{aligned}$$

sont d'ordre 6 et 3 respectivement, et engendrent un sous-groupe isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

THÉORÈME 4.13. *Soit $K = \mathbb{Q}(\sqrt{-3})$. Alors il existe une courbe elliptique définie sur K de rang 3 et avec un sous-groupe de torsion isomorphe à $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$:*

$$\mathrm{Sr}(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, K) \geq 3.$$

Preuve. En substituant v par $-\frac{3}{2}$ dans l'équation (4.24), nous obtenons la courbe elliptique

$$E : y^2 - \frac{1823}{4}xy - \frac{136325007}{16}y = x^3 + \frac{44161}{2}x^2.$$

En utilisant le programme de Simon [20], on trouve

$$\mathrm{rang}(E, \mathbb{Q}) = 1 \quad \text{et} \quad \mathrm{rang}(E^{(-3)}, \mathbb{Q}) = 1.$$

Les points

$$\left(\frac{7927256701}{6400}, \frac{873716268258379}{512000}\right),$$
$$\left(-\frac{112359}{4}, \frac{3677661}{16}\theta - \frac{34252725}{16}\right),$$
$$\left(-\frac{2570841}{16}, \frac{3718175643}{128}\theta - \frac{4141343115}{128}\right)$$

sont d'ordre infini et indépendants. De plus, les points

$$P_0 = (0, 0),$$
$$Q = \left(-\frac{499359}{16}, -\frac{64417311}{128}\sqrt{-3} - \frac{365031429}{128}\right)$$

sont d'ordre 6 et 3 respectivement, et on a

$$\langle Q, P_0 \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}.$$

4.10. Le cas $\mathrm{Tors}(E, K) \supseteq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$**.** On commence par considérer la forme générale des courbes elliptiques dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$\mathcal{E}^{(2,4)} : y^2 + xy - \left(t^2 - \frac{1}{16}\right)y = x^3 - \left(t^2 - \frac{1}{16}\right)x^2. \tag{4.25}$$

Notons

$$P_4 = (0, 0) \quad \text{et} \quad P_2 = \left(\frac{1}{4}(4t - 1), \frac{1}{32}(4t - 1)^2\right).$$

Nous avons vu (section 3.12) que les points P_4 et P_2 sont d'ordre 4 et 2 respectivement, et de plus

$$\langle P_2, P_4 \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

Pour obtenir la 4-torsion complète, il nous faut alors résoudre l'équation

$$P_2 = [2]Q.$$

LEMME 4.14. *Soit E une courbe elliptique sur un corps K, définie par l'équation*

$$E : y^2 = (x-\alpha)(x-\beta)(x-\gamma),$$

où $\alpha, \beta, \gamma \in K$, et soit $P = (x_P, y_P) \in E(K)$. Alors il existe un point $Q \in E(K)$ tel que $P = [2]Q$ si et seulement s'il existe $u, v, z \in K$ avec

$$x_P - \alpha = u^2, \quad x_P - \beta = v^2, \quad x_P - \gamma = z^2.$$

Preuve. Voir [13, page 85]. ∎

Nous utilisons maintenant le modèle

$$C : y^2 = \left(x - t^2 + \frac{1}{16}\right)\left(x - \frac{1}{2}t + \frac{1}{8}\right)\left(x + \frac{1}{2}t + \frac{1}{8}\right)$$

pour la surface elliptique $\mathcal{E}^{(2,4)}$. Le point $P_2 = \left(\frac{1}{2}t - \frac{1}{8}, 0\right)$ est d'ordre 2 sur la courbe C. Grâce au lemme 4.14, une condition nécessaire et suffisante pour que ce point soit le double d'un autre point Q est que $t = z^2$ et $\left(t - \frac{1}{4}\right)^2 = -v^2$ avec $v, z \in K$.

REMARQUE 4. La dernière condition signifie que -1 doit être nécessairement un carré dans le corps K. Cela veut dire que le seul corps quadratique tel qu'il existe une courbe elliptique dont le sous-groupe de torsion est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ est $\mathbb{Q}(\sqrt{-1})$ (voir le théorème 1.3).

La discussion ci-dessus permet de trouver la forme générale des courbes elliptiques avec une torsion isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$:

$$\mathcal{E}^{(4,4)} : y^2 + xy - \left(t^4 - \frac{1}{16}\right)y = x^3 - \left(t^4 - \frac{1}{16}\right)x^2, \tag{4.26}$$

où $t \in K$ est tel que

$$\Delta_{\mathcal{E}^{(4,4)}} = \frac{1}{2^{12}} t^4 (2t-1)^4 (2t+1)^4 (4t^2+1)^4 \neq 0.$$

Les points

$$P = (0,0),$$

$$Q = \left(-\frac{1}{8}(2t+1)(4t^2+1), \sqrt{-1}\left(t + \frac{1}{2}\right)^2 \left(t - \frac{\sqrt{-1}}{2}\right)^2 \left(t + \frac{\sqrt{-1}}{2}\right)\right)$$

sont générateurs de la 4-torsion complète :

$$\langle P, Q \rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

THÉORÈME 4.15. *Soit $K = \mathbb{Q}(\sqrt{-1})$. Alors il existe une courbe elliptique E définie sur K de rang 3 et telle que* $\mathrm{Tors}(E, K) \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *:*

$$\mathrm{Sr}(\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, K) \geq 3.$$

Preuve. En substituant t par 11 dans l'équation (4.26), nous obtenons la courbe elliptique

$$E : y^2 + xy - \frac{234255}{16}y = x^3 - \frac{234255}{16}x^2.$$

En utilisant le programme de Simon [20], nous trouvons que $\mathrm{rang}(E, \mathbb{Q}) = 1$ et $\mathrm{rang}(E^{(-1)}, \mathbb{Q}) = 2$. Les points

$$\left(\frac{1699800809}{73984}, \frac{42124907328091}{20123648}\right),$$
$$\left(-\frac{424005}{784}, \frac{726647625\sqrt{-1}}{10976} + \frac{2975625}{392}\right),$$
$$\left(-\frac{203021}{72}, \frac{10057348\sqrt{-1}}{27} + \frac{2514337}{288}\right),$$

sont indépendants sur $E(K)$ et de plus

$$\langle (0,0) \rangle \left\langle \left(-\frac{11155}{8}, \frac{2822215\sqrt{-1}}{16} + \frac{256565}{32}\right) \right\rangle \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}. \ \blacksquare$$

Remerciements. Je remercie Denis Simon pour l'aide précieuse lors de la préparation de ce manuscrit tant dans la forme que dans le contenu. Je remercie aussi Oswaldo Velásquez pour les premières remarques sur ce document.

Références

[1] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. 60 (1993), 399–405.

[2] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *The computer algebra system pari-gp*, http://pari.math.u-bordeaux.fr/.

[3] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, seconde éd., Cambridge Univ. Press, Cambridge, 1997.

[4] A. Dujella, *High rank elliptic curves with prescribed torsion*, http://web.math.hr/~duje/tors/tors.html.

[5] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. 73 (1983), 349–366.

[6] M. van Hoeij, *An algorithm for computing the Weierstrass normal form*, dans : International Symposium on Symbolic and Algebraic Computation ISSAC '95, ACM Press, New York, 1995, 90–95.

[7] —, *Rational parametrizations of algebraic curves using a canonical divisor*, J. Symbolic Comput. 23 (1997), 209–227.

[8] —, *An algorithm for computing the Weierstrass normal form of hyperelliptic curves*, http://www.citebase.org/abstract?id=oai:arXiv.org:math/0203130, 2002.

[9] D. Jeon and C. H. Kim, *Bielliptic modular curves* $X_1(M, N)$, Manuscripta Math. 118 (2005), 455–466.

[10] S. Kamienny, *Torsion points on elliptic curves over all quadratic fields*, Duke Math. J. 53 (1986), 157–162.
[11] —, *Torsion points on elliptic curves over all quadratic fields. II*, Bull. Soc. Math. France 114 (1986), 119–122.
[12] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.
[13] A. W. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, NJ, 1992.
[14] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Compos. Math. 38 (1979), 121–128.
[15] B. Mazur, *Rational isogenies of prime degree* (with an appendix by D. Goldfeld), Invent. Math. 44 (1978), 129–162.
[16] M. A. Reichert, *Explicit determination of nontrivial torsion structures of elliptic curves over quadratic number fields*, dans : EUROCAL '85, Lecture Notes in Comput. Sci. 204, Springer, Berlin, 1985, 489–490.
[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.
[18] —, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.
[19] D. Simon, Le fichier gp, http://www.math.unicaen.fr/~simon/ell.gp.
[20] —, Le fichier gp, http://www.math.unicaen.fr/~simon/ellQ.gp.
[21] —, *Computing the rank of elliptic curves over number fields*, LMS J. Comput. Math. 5 (2002), 7–17.

F. Patrick Rabarison
LMNO–UMR 6139
Université de Caen
Campus II
Bd Maréchal Juin
BP 5186, 14032 Caen, France
E-mail: rabarison@math.unicaen.fr

Reçu le 19.5.2009
et révisé le 16.12.2009 (6033)