ACTA ARITHMETICA
108.4 (2003)

Families of elliptic curves of high rank with nontrivial torsion group over $\mathbb{Q}$

by

LEOPOLDO KULESZ (Buenos Aires)

Introduction. In 1976, B. Mazur [Maz] proved Beppo Levi's conjecture which asserts that if E is an elliptic curve defined over $\mathbb{Q}$, the only possible torsion groups over $\mathbb{Q}$ are

$$\begin{cases} \mathbb{Z}/k\mathbb{Z}, & k = 2, \ldots, 10 \text{ and } 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}, & m = 1, \ldots, 4. \end{cases}$$

For a finite group G and a number field $\mathbf{K}$, let

$$\mathrm{Br}(G, \mathbf{K}) = \limsup_{E_G} \operatorname{rank}(E_G(\mathbf{K})),$$

where E_G runs through the elliptic curves defined over $\mathbf{K}$ for which $E(\mathbf{K})_{\mathrm{tors}}$ is isomorphic to G.

In order to accelerate the factorisation algorithm of H. W. Lenstra [Len], P. L. Montgomery [Mon], H. Suyama [Suy] and A. O. L. Atkin–F. Morain [A-M] obtain the following result:

PROPOSITION. $\mathrm{Br}(G, \mathbb{Q}) \geq 1$ *for all* G.

More precisely, for each torsion case they construct an infinite family of elliptic curves over $\mathbb{Q}$ of rank ≥ 1 parametrised either by the projective line or by another elliptic curve of rank ≥ 1.

It is natural to ask, for each torsion case, if there exist families of elliptic curves of higher rank.

The case $G = \mathbb{Z}/2\mathbb{Z}$ was studied by K. Nagao [Nag] and S. Fermigier [Fer]. Nagao shows that $\mathrm{Br}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) \geq 6$ using a family of elliptic curves defined over $\mathbb{Q}$ of rank at least 6 with a rational point of order 2, parametrised by another elliptic curve of rank ≥ 1. This result was improved by Fermigier, who showed that $\mathrm{Br}(\mathbb{Z}/2\mathbb{Z}, \mathbb{Q}) \geq 8$. He constructed a family of elliptic curves

2000 *Mathematics Subject Classification*: 11G05, 14H52.

This work was supported by ECOS A99E06.

defined over $\mathbb{Q}$ of rank at least 8 with a rational of order 2, parametrised by $\mathbb{Q}(t_1, \ldots, t_5)$. He also found in this family a single curve of rank 14.

Both Nagao and Fermigier obtain their results by applying the method used by J.-F. Mestre in order to find an infinite family of elliptic curves of rank ≥ 12 [Mes1], [Mes2].

In this paper, we will improve the lower bound of $\mathrm{Br}(G, \mathbb{Q})$ for the other cases of torsion and sharpen the corresponding parametrisations.

1. PRELIMINARIES

1.1. Parametrisation of the elliptic curves with a fixed torsion group. In this section we will recall and sometimes reformulate some classic results [Kna], [Kub] and [Na].

Let E be an elliptic curve defined over $\mathbb{Q}$ passing through a $\mathbb{Q}$-rational point P. Without loss of generality we can assume $P = (0, 0)$; then E admits the following equation on the affine plane:

$$p(x, y) = y^2 + a_1xy + a_3y - (x^3 + a_2x^2 + a_4x) = 0.$$

Moreover, since $(\partial p/\partial x)(0, 0) = -a_4$ and $(\partial p/\partial y)(0, 0) = a_3$, E is not singular at P if and only if $a_3 \neq 0$ or $a_4 \neq 0$. We will suppose from now on that E is nonsingular at P.

The point P is of order 2 if and only if the tangent to E at P is vertical, hence, if and only if $a_3 = 0$, i.e., if and only if E has the equation

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x. \tag{1.1.1}$$

Suppose now that $a_3 \neq 0$. Under the change of coordinates

$$(x, y) \mapsto (X, Y + a_3^{-1}a_4X),$$

the point P remains invariant and the curve becomes

$$Y^2 + (a_1 + 2a_3^{-1}a_4)XY + a_3Y = X^3 + (a_2 - a_1a_3^{-1}a_4 - a_3^{-2}a_4^2)X^2.$$

We can rewrite this by changing the notation:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2. \tag{$*$}$$

Using the chord-tangent method we obtain

$$-P = (0, -a_3), \quad [2]P = (-a_2, a_1a_2 - a_3).$$

As $[3]P = 0$ if and only if $-P = [2]P$, we conclude that P is of order 3 if and only if $a_2 = 0$, i.e. E has the equation

$$y^2 + a_1xy + a_3y = x^3. \tag{1.1.2}$$

For other cyclic cases of torsion we start directly from Tate's normal form

$$y^2 + (1 - c)xy - by = (x^3 - bx^2),$$

which can be obtained by the change of coordinates

$$(x, y) \mapsto (X/u^2, Y/u^3) \quad \text{with } u = a_3^{-1} a_2,$$

and letting $b = -a_3^{-2} a_2^3$ and $c = 1 - a_3^{-1} a_1 a_2$. The chord-tangent method from the point $P = (0, 0)$ yields

$$-P = (0, b), \qquad [2]P = (b, bc), \qquad [-2]P = (b, 0),$$
$$[3]P = (c, b - c), \qquad [-3]P = (c, c^2),$$
$$[4]P = \left(\frac{b(b-c)}{c^2}, \frac{-b^2(b-c-c^2)}{c^3}\right), \qquad [-4]P = \left(\frac{b(b-c)}{c^2}, \frac{(b-c)^2 b}{c^3}\right),$$
$$[5]P = \left(\frac{-bc(-c^2+b-c)}{(b-c)^2}, \frac{bc^2(b^2-bc-c^3)}{(b-c)^3}\right),$$
$$[-5]P = \left(\frac{-bc(-c^2+b-c)}{(b-c)^2}, \frac{b^2(-c^2+b-c)^2}{(b-c)^3}\right),$$
$$[6]P = \left(\frac{(-b+c)(c^3+bc-b^2)}{(-b+c+c^2)^2}, \frac{c(bc^2-c^2+3bc-2b^2)(-b+c)^2}{(-bc+c^2)^3}\right),$$
$$[-6]P = \left(\frac{(-b+c)(c^3+bc-b^2)}{(-b+c+c^2)^2}, \frac{c(c^3+bc-b^2)^2}{(-b+c+c^2)^3}\right),$$

and therefore:

(1.1.3) P is of order 4 if and only if $c = 0$ ($[2]P = [-2]P$).

(1.1.4) P is of order 5 if and only if $b = c$ ($[3]P = [-2]P$).

(1.1.5) P is of order 6 if and only if $b = c + c^2$ ($[3]P = [-3]P$).

(1.1.6) P is of order 7 if and only if $b = d^3 - d^2$ and $c = d^2 - d$.

(1.1.7) P is of order 8 if and only if

$$b = (2d-1)(d-1), \qquad c = \frac{(2d-1)(d-1)}{d}.$$

(1.1.8) P is of order 9 if and only if

$$b = cd, \qquad c = fd - f, \qquad d = f(f-1) + 1.$$

(1.1.9) P is of order 10 if and only if

$$b = cd, \qquad c = fd - f, \qquad d = \frac{f^2}{f - (f-1)^2}.$$

(1.1.10) P is of order 12 if and only if

$$b = cd, \qquad c = fd - f, \qquad d = m + t,$$
$$f = \frac{m}{1-t}, \qquad m = \frac{3t - 3t^2 - 1}{t - 1}.$$

The cases (1.1.6)–(1.1.10) were obtained from the equalities $[4]P = [-3]P$, $[4]P = [-4]P$, $[5]P = [-4]P$, $[5]P = [-5]P$, $[5]P = [-6]P$, respectively, which give curves of genus 0 in b and c, hence parametrisable.

We suggest a different parametrisation for the cases $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$, which will be useful later. Instead of considering the conditions that the point $P=(0,0)$ should verify in order to have $[9]P=0$ (resp. $[10]P=0$ and $[12]P=0$), we start from the simpler case $[3]P=0$ (resp. $[5]P=0$ and $[6]P=0$) and look for a point Q such that $[3]Q=P$ (resp. $[2]Q=P$ and $[2]Q=P$). In this manner we obtain the following results:

- On the elliptic curve defined by the equation

$$(1.1.8') \quad E_t: \quad (32t^2-8t)y^2 + (-48t^2+64t^3+1)xy + t(4t-1)y - 8tx^3(4t-1) = 0,$$

the point $Q=(t, 2t^2/(4t-1))$ is of order 9.

- On the elliptic curve defined by the equation

$$(1.1.9') \quad E_t: \quad (t+1)^2y^2 + (2t^2+2t+1+2t^3)xy + t^2(2t+1)y - (t+1)^2x^3 - t^2(2t+1)x^2 = 0,$$

the point $Q=(-t^2(2t+1)/(t+1)^3, -t^3(2t+1)^2/(t+1)^5)$ is of order 10.

- On the elliptic curve defined by the equation

$$(1.1.10') \quad E_t: \quad y_1(x_1+1)y^2 + (-y_1^2+2y_1+x_1^3)xy + (-y_1^2+x_1^3-2x_1y_1)y - y_1(x_1+1)x^3 = 0$$

with $x_1 = -(t+1)(t^2-2t+5)/8$ and $y_1 = t(1-t^2)x_1/4$, the point $Q = (x_1, y_1)$ is of order 12.

In order to treat the torsion cases of the form $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2n\mathbb{Z}$ we start from the elliptic curve in Weierstrass form:

$$(1.1.11) \qquad E: \quad y^2 = (x-\alpha)(x-\beta)(x-\gamma).$$

We know that if α, β and γ are in $\mathbb{Q}$ then $E(\mathbb{Q})_{\text{tors}}$ contains one torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

In order to study the torsion case $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ we consider the following result (cf. [Kna, Chapter IV]):

THEOREM 1.1. *Let E be an elliptic curve defined over a field $\mathbf{k}$ of characteristic $\neq 2$ or 3. Suppose that E is given by*

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

with $\alpha,\beta,\gamma\in\mathbf{k}$. For (x_2,y_2) in $E(\mathbf{k})$ there exists $(x_1,y_1)\in E(\mathbf{k})$ with $[2](x_1,y_1)=(x_2,y_2)$ if and only if $x_2-\alpha$, $x_2-\beta$ and $x_2-\gamma$ are perfect squares in $\mathbf{k}$.

It follows that the curves E with a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ have the equation

$$y^2 = x(x + x_1^2)(x + x_2^2), \qquad x_1, x_2 \in \mathbb{Q}. \tag{1.1.12}$$

Indeed, by applying the theorem, we verify that the point $(0, 0)$ is of order 4.

If we look for x_1 and x_2 in the equation (1.1.12) such that the point $(x_1x_2, x_1x_2(x_1 + x_2))$ is a double point (cf. Theorem 1.1), we find that the elliptic curves E with a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ have the equation

$$y^2 = x(x + x_1^2)(x + x_2^2) \tag{1.1.13}$$

with $x_1 = (t^2 - 1)/(2t)$, $x_2 = 1/x_1$ and $t \in \mathbb{Q}$. For this last case, it is also possible to start from (1.1.7) and find the parameter d such that this curve has another point of order 2. It is sufficient to set

$$d = \frac{-2(4 + t)}{-8 + t^2}. \tag{1.1.13$'$}$$

Finally, in order to obtain a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, it is sufficient to set $\alpha = x_1^2$, $\beta = x_2^2$ and $\gamma = x_3^2$ in (1.1.11) and find x_1, x_2 and x_3 such that the point $(0, x_1x_2x_3)$ is of order 3 (using (1.1.2)).

Thus, the curves with a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ have the equation

$$y^2 = (x - x_1^2)(x - x_2^2)\left(x - \frac{x_1^2x_2^2}{(x_1 - x_2)^2}\right). \tag{1.1.14}$$

1.2. Transforming a quartic into a cubic. We recall some results about quartics [Cas], [A-M]. Let E be the elliptic curve satisfying the equation

$$y^2 = a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 = f(x),$$

and passing through the rational point (x_0, y_0). If we set

$$x = x_0 + y_0\left(X - \frac{f'(x_0)}{4y_0}\right)^{-1}, \qquad y = \frac{Y}{y_0}\,(x - x_0)^2,$$

we see that E is birationally equivalent to

$$E' : \quad Y^2 = X^4 - 6A_2X^2 + 4A_1X + A_0 = F(X).$$

This last curve is also birationally equivalent to

$$E'' : \quad T^2 = S^3 - \frac{3A_2^2 + A_0}{4}\,S + \frac{A_1^2 - A_2(A_2^2 - A_0)}{4},$$

after the following change of coordinates:

$$X = \frac{T - A_1/2}{S - A_2}, \qquad Y = -X^2 + 2S + A_2.$$

1.3. Independence of a system of points. We consider elliptic curves $E_{x_1,\dots,x_r}$ defined over the field $\mathbb{Q}(x_1,\dots,x_r)$; we will have to show that certain points $P_1(x_1,\dots,x_r),\dots,P_n(x_1,\dots,x_r)$ are independent on the curve $E_{x_1,\dots,x_r}(\mathbb{Q}(x_1,\dots,x_r))$. It will be sufficient to find a suitable specialisation $y_1,\dots,y_r$ of $x_1,\dots,x_r$ in rational values and to show that the points $P_1(y_1,\dots,y_r),\dots,P_n(y_1,\dots,y_r)$ are independent on $E_{y_1,\dots,y_r}(\mathbb{Q})$ ([Sil]). For this, we will compute the matrix of the Néron–Tate heights with gp-PARI [Fer].

2. RESULTS

Let us recall some results obtained by Montgomery [Mon], Suyama [Suy] and Atkin–Morain [A-M]:

• For $E(\mathbb{Q})_{\text{tors}}$ isomorphic to $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$, they obtain families of elliptic curves of rank ≥ 1, parametrised by $\mathbb{Q}(t)$.

• For $E(\mathbb{Q})_{\text{tors}}$ isomorphic to $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, they obtain families of elliptic curves of rank ≥ 1, parametrised by an elliptic curve of rank ≥ 1.

In what follows we improve these results for $E(\mathbb{Q})_{\text{tors}}$ isomorphic to $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, either by constructing infinite families of elliptic curves of higher rank or by sharpening the corresponding parametrisation. For $E(\mathbb{Q})_{\text{tors}}$ isomorphic to $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$, we will find parametrisations by other elliptic curves of rank ≥ 1.

2.1. The case $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$

THEOREM 2.1. $\mathrm{Br}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z},\mathbb{Q}) \geq 4$. *More precisely, there is an infinite family of elliptic curves of rank at least four, with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ and parametrised by $\mathbb{Q}(x_1,x_2,x_3,x_4)$.*

Proof. We know that E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ if and only if E has a cubic model of the form

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) \quad \text{with } \alpha,\beta,\gamma \in \mathbf{K}$$

(cf. (1.1.8)). Consider the curves

$$E_{a,b}: \quad y^2 = a(x^2+1)^2 + bx^2 \quad \text{with } a,b \in \mathbb{Q},$$

passing through a $\mathbb{Q}$-rational point (x_0,y_0). It is easy to verify (cf. 1.2) that these curves have a cubic model of the form

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

with

$$\alpha = -\frac{(ax_0^4 + 2ax_0^2 + a - y_0^2)(ax_0^4 - 2ax_0^2 - y_0^2 + a)}{x_0^2 y_0^4},$$
$$\beta = -\frac{a(x_0 - 1)^2(x_0 + 1)^2(ax_0^4 + 2ax_0^2 + a - y_0^2)}{x_0^2 y_0^4},$$
$$\gamma = -\frac{a(x_0^2 + 1)^2(ax_0^4 - 2ax_0^2 - y_0^2 + a)}{x_0^2 y_0^4},$$

and thus, the curves $E_{a,b}$ have a torsion subgroup defined over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In order to obtain such curves we will apply the following method due to J.-F. Mestre [Mes1].

Let X, X_1, X_2, X_3, X_4 be five indeterminates and $\mathbf{K} = \mathbb{Q}(X_1, X_2, X_3, X_4)$. Let $P \in \mathbf{K}[X]$ be the polynomial $P(X) = \prod_{i=1}^4 (X - X_i) = X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$. It may be written in a unique form as $P = Q^2 - R$ with Q and R in $\mathbf{K}[X]$ such that $Q(X) = X^2 + d_1X + d_0$ and $R(X) = r_1X + r_2$, where $d_1, d_0, r_1, r_2 \in \mathbb{Q}$. Indeed, we obtain the equality by setting $d_1 = c_3/2$, $d_0 = (c_2 - d_1^2)/2$, $r_1 = 2d_1d_0 - c_1$ and $r_2 = d_0^2 - c_0$.

The rational fraction $F_1(x) = (x^2 + 1)^2/x^2$ is invariant under the action of the group G_1 of four homographies generated by $x \mapsto -x$ and $x \mapsto 1/x$. Let x_1, x_2, x_3 and x_4 be four indeterminates. If we set $X_i = F_1(x_i)$ the numerator of $P(F_1(x))$ splits completely over $\mathbb{Q}(x_1, x_2, x_3, x_4)$. In this way, we obtain the curve E_{r_1,r_2} satisfying the equation

$$y^2 = r_1(x^2 + 1)^2 + r_2x^2$$

and passing through the points of abscissae x_1, x_2, x_3 and x_4 (and by their conjugates) under the action of G_1.

When we apply this method to the case where $x_1 = 2$, $x_2 = 3$, $x_3 = 4$ and $x_4 = 5$, we obtain the elliptic curve E satisfying the minimal equation

$$E: \quad y^2 + xy = x^3 + ax + b$$

with

$$a = -33266039859280269453163159675,$$
$$b = 1266432590907122115122625450016203315594257.$$

It has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ generated by the points

$$P_1 = (159074830970654, -79537415485327),$$
$$P_2 = (-199067488994146, 99533744497073),$$

and passes through the following four independent points (images of the points on E_{r_1,r_2} of x-coordinate $x_1 = 2$, $x_2 = 3$, $x_3 = 4$ and $x_4 = 5$):

$$Q_1 = (-20566252547452, 1393517661684992475371),$$
$$Q_2 = (360529885950854, 6011268744207477259073),$$

$$Q_3 = (34589314411754, 396442222829819164073),$$
$$Q_4 = (32245757889364, 476731254985118349883).$$

The determinant of the Néron–Tate matrix is 1803.84 (computed with gp-PARI), which completes the proof of Theorem 2.1.

2.2. The case $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/3\mathbb{Z}$

THEOREM 2.2. $\mathrm{Br}(\mathbb{Z}/3\mathbb{Z}, \mathbb{Q}) \geq 6$. *More precisely, there is an infinite family of elliptic curves of rank at least six, with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/3\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(x_1, x_2, x_3)$.

Proof. By (1.1.2), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/3\mathbb{Z}$ if and only if E has a cubic model of the form

$$y^2 + a_1xy + a_3y = x^3 \quad \text{with } a_1, a_3 \in \mathbf{K}.$$

Let X, X_1, X_2, X_3 be four indeterminates and $\mathbf{K} = \mathbb{Q}(X_1, X_2, X_3)$. Let $P(X) = X\prod_{i=1}^3 (X - X_i) = X^4 + c_3X^3 + c_2X^2 + c_1X \in \mathbf{K}[X]$. Then $P = Q^2 - R$ for unique Q and R in $\mathbf{K}[X]$ such that $Q(X) = X^2 + d_1X + d_0$ and $R(X) = r_1X + r_2^2$, where $d_1, d_0, r_1, r_2 \in \mathbb{Q}$. Indeed, set $d_1 = c_3/2$, $d_0 = (c_2 - d_1^2)/2$, $r_1 = 2d_1d_0 - c_1$ and $r_2 = d_0$.

Consider the rational fractions

$$F_2(x) = \frac{x^3}{(x+1)^2}, \qquad g_2(x) = -\frac{1}{4}\,\frac{(x^2+3)^3}{(x-1)^2(x+1)^2},$$

and three indeterminates x_1, x_2 and x_3. By setting $X_i = g_2(x_i)$, the numerator of $P(F_2(x))$ splits completely over $\mathbb{Q}(x_1, x_2, x_3)$. In this way, we obtain the curves

$$E_{r_1,r_2}: \quad y^2 = r_1x^3 + r_2^2(x+1)^2$$

with a torsion subgroup defined over $\mathbb{Q}(x_1, x_2, x_3)$ isomorphic to $\mathbb{Z}/3\mathbb{Z}$. They have a cubic model of the form (cf. 1.2)

$$E'_{r_1,r_2}: \quad y^2 - 2r_2xy - 2r_1r_2y = x^3,$$

via

$$E_{r_1,r_2} \to E'_{r_1,r_2}, \qquad (x, y) \mapsto (r_1x, r_1(r_2(x + r_1) + y)).$$

Moreover, they pass through the points whose x-coordinates are the roots of $F_2(x)\prod_{i=1}^3 (F_2(x) - g_2(x_i))$.

If we apply this method in the case where $x_1 = 2$, $x_2 = 4$, and $x_3 = 6$, then we obtain the points $P_1, \ldots, P_6$ of x-coordinates $-7, -7/9, -19/9, -19/25, -39/4, -39/49$ (6 of the 9 roots of $\prod_{i=1}^3 (F_2(x) - g_2(x_i))$).

We obtain the elliptic curve E of minimal equation

$$y^2 + xy = x^3 + ax + b$$

with

$$a = -782035204274190398414114 67,$$
$$b = 2593140502228536612763037647323129955 69.$$

It has a torsion subgroup isomorphic to $\mathbb{Z}/3\mathbb{Z}$ generated by the point

$$P = (7167424811990, 818540968662700 9297),$$

and passes through the following six independent points (images of the points $P_1, \ldots, P_6$):

$$\begin{aligned}
Q_1 &= (30967676391166/9, 1502449681391012593 55/27),\\
Q_2 &= (-5189102999442, 2292148348481771526 5),\\
Q_3 &= (7167424811990, -818541685405182128 7),\\
Q_4 &= (52150295496478/9, 2292140266482297082 7/27),\\
Q_5 &= (145646473383006/25, 1502446504744323885 89/125),\\
Q_6 &= (5762455177454, 131221750961285185).
\end{aligned}$$

The determinant of the Néron–Tate matrix is 648532.73, which completes the proof of Theorem 2.2.

2.3. The case $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/4\mathbb{Z}$

THEOREM 2.3. $\mathrm{Br}(\mathbb{Z}/4\mathbb{Z}, \mathbb{Q}) \geq 3$. *More precisely, there is an infinite family of elliptic curves of rank at least three, with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/4\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(x_1, x_2, x_3)$.

Proof. By (1.1.3), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/4\mathbb{Z}$ if and only if E has a cubic model of the form

$$y^2 + xy - by = x^3 - bx^2 \quad \text{with } b \in \mathbf{K}.$$

We proceed as in Theorem 2.2, this time with the rational fraction $F_3(x) = x^2/(x-1)$. If we set $X_i = F_3(x_i)$, the numerator of $P(F_3(x))$ splits completely over $\mathbb{Q}(x_1, x_2, x_3)$. In this way, we obtain the curves

$$E_{r_1,r_2}: \quad y^2 = r_1 x^2(x-1) + r_2^2(x-1)^2$$

with a torsion subgroup defined over $\mathbb{Q}(x_1, x_2, x_3)$ isomorphic to $\mathbb{Z}/4\mathbb{Z}$. Indeed, they have a cubic model of the form (cf. 1.2)

$$E'_{r_1,r_2}: \quad y^2 - 2(x-b)y = x^3 - bx^2 \quad \text{with } b = r_1/r_2^2,$$

via

$$E_{r_1,r_2} \to E'_{r_1,r_2}, \qquad (x, y) \mapsto (bx, b(x - 1 + y/r_2)).$$

Moreover, they pass through the points whose x-coordinates are the roots of $F_2(x)\prod_{i=1}^{3}(F_2(x) - g_2(x_i))$.

Applying this method to the case where $x_1 = 3$, $x_2 = 4$, and $x_3 = 5$, we obtain the elliptic curve E of minimal equation

$$y^2 + xy = x^3 + ax + b$$

with

$$a = -266721356141, \qquad b = 52307554376730321.$$

It has a torsion group isomorphic to $\mathbb{Z}/4\mathbb{Z}$ generated by the point

$$P = (554026, 272839207),$$

and passes through the following three independent points (images of the points on E_{r_1,r_2} of x-coordinates x_1, x_2 and x_3):

$$Q_1 = (249930, 35340231),$$
$$Q_2 = (268936, 5139697),$$
$$Q_3 = (211918, 72706027).$$

The determinant of the Néron–Tate matrix is 43.88, which completes the proof of Theorem 2.3.

2.4. The case $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/5\mathbb{Z}$

THEOREM 2.4. $\mathrm{Br}(\mathbb{Z}/5\mathbb{Z}, \mathbb{Q}) \geq 2$. *More precisely*, *there is an infinite family of elliptic curves of rank at least two*, *with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/5\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(t)$.

Proof. By (1.1.4), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/5\mathbb{Z}$ if and only if E has a cubic model of the form

$$E_b: \quad y^2 + (1-b)xy - by = x^3 - bx^2 \quad \text{with } b \in \mathbf{K}.$$

Set

$$b = \frac{-(3t^2+6t+4)(t^2+6t+12)}{(t-2)^2(t+2)^2},$$
$$u = \frac{-(8+8t+t^2)}{(t-2)(t+2)},$$
$$v = \frac{-(t^2+6t+12)}{(t-2)(t+2)}.$$

We will show that the points $P_1 = (-1, u)$ and $P_2 = (v, v)$ are independent in $E_b(\mathbb{Q}(t))$. If $t = 4$, we obtain the elliptic curve E of minimal equation

$$y^2 + y = x^3 + x^2 + ax + b$$

with

$$a = -112845920, \qquad b = 461373286640.$$

It has a torsion subgroup isomorphic to $\mathbb{Z}/5\mathbb{Z}$ generated by the point

$$P = (6202, 10003),$$

and passes through the following two independent points (images of P_1 and P_2):

$$Q_1 = (6121, 3766), \qquad Q_2 = (5851, 38083).$$

The determinant of the Néron–Tate matrix is 11.74, which completes the proof of Theorem 2.4.

2.5. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/6\mathbb{Z}$

THEOREM 2.5. $\mathrm{Br}(\mathbb{Z}/6\mathbb{Z}, \mathbb{Q}) \geq 2$. *More precisely*, *there is an infinite family of elliptic curves of rank at least two*, *with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/6\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(t)$.

Proof. By (1.1.5), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/6\mathbb{Z}$ if and only if E has a cubic model of the form

$$E_c: \quad y^2 + (1-c)xy - (c+c^2)y = x^3 - (c+c^2)x^2 \quad \text{with } c \in \mathbf{K}.$$

Set

$$c = \frac{4(t-1)(-2t+1+2t^2)}{5-8t+4t^4}.$$

We will show that the points P_1 and P_2 of x-coordinate $-c$ and ct respectively are independent in $E_c(\mathbb{Q}(t))$. If $t = 2$, we obtain the elliptic curve E of minimal equation

$$y^2 + xy = x^3 + ax + b$$

with

$$a = -1747020, \qquad b = 867156112.$$

It has a torsion subgroup isomorphic to $\mathbb{Z}/6\mathbb{Z}$ generated by the point

$$P = (-396, 38888),$$

and passes through the following two independent points (images of P_1 and P_2):

$$Q_1 = (-1456, 18748), \qquad Q_2 = (1724, 53728).$$

The determinant of the Néron–Tate matrix is 6.47, which completes the proof of Theorem 2.5.

2.6. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/7\mathbb{Z}$

THEOREM 2.6. $\mathrm{Br}(\mathbb{Z}/7\mathbb{Z}, \mathbb{Q}) \geq 1$. *More precisely*, *there is an infinite family of elliptic curves of rank at least one*, *with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/7\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(t)$.

Proof. By (1.1.6), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/7\mathbb{Z}$, if and only if E has a cubic model of the form

$$E_d : \quad y^2 + (1-c)xy - by = x^3 - bx^2$$

with $b = d^3 - d^2$, $c = d^2 - d$ and $d \in \mathbf{K}$. Set

$$d = \frac{-2(-3+t)}{3+t^2}.$$

The point of abscissa

$$\frac{-2(t-1)(t+3)(t+1)(-3+t)^2}{(3+t^2)^3}$$

is of infinite order in $E_d(\mathbb{Q}(t))$ since it is not in $E_d(\mathbb{Q}(t))_{\mathrm{tors}}$, except for a finite set of rational values of t, which completes the proof of Theorem 2.6.

2.7. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/8\mathbb{Z}$

THEOREM 2.7. $\mathrm{Br}(\mathbb{Z}/8\mathbb{Z}, \mathbb{Q}) \geq 1$. *More precisely, there is an infinite family of elliptic curves of rank at least one, with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/8\mathbb{Z}$ and parametrised by $\mathbb{Q}(t)$.*

Proof. By (1.1.7), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/8\mathbb{Z}$ if and only if E has a cubic model of the form

$$E_d : \quad y^2 + (1-c)xy - by = x^3 - bx^2$$

with $b = (2d-1)(d-1)$, $c = (2d-1)(d-1)/d$ and $d \in \mathbf{K}$. Set $d = (2-2t+t^2)/(2+t^2)$.

The point of abscissa

$$\frac{-2t(2-4t+t^2)(t^2-2)}{(2+t^2)^2(2-2t+t^2)}$$

is of infinite order in $E_d(\mathbb{Q}(t))$ since it is not in $E_d(\mathbb{Q}(t))_{\mathrm{tors}}$, and $E_d(\mathbb{Q}(t))_{\mathrm{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ only for a finite number of values of t, which completes the proof of Theorem 2.7.

2.8. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

THEOREM 2.8. $\mathrm{Br}(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Q}) \geq 2$. *More precisely, there is an infinite family of elliptic curves of rank at least two, with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and parametrised by $\mathbb{Q}(t_1, t_2, t_3)$.*

Proof. By (1.1.9), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ if and only if E has a cubic model of the form

$$E_{u_1,u_2}: \quad y^2 = x(x+u_1^2)(x+u_2^2) \quad \text{with } u_1, u_2 \in \mathbf{K}.$$

Let $x_1, x_2 \in \mathbb{Q}$. How could we find u_1, u_2, y_1 and y_2 in $\mathbb{Q}$ such that $(x_i^2+u_1^2)(x_i^2+u_2^2) = y_i^2$ $(i=1,2)$?

If we consider E_{u_1,u_2} as a conic in y and u_2, it is easy to see that we can answer this question by setting

$$u_2 = \frac{s^2u_1 - 2su_1^2 - 2x_1^2s + u_1x_1^2 + u_1^3}{s^2 - x_1^2 - u_1^2},$$
$$s = \frac{1}{2}\,\frac{x_2^2x_1^2 + u_1^4 + 2x_2^2u_1^2}{u_1(x_2^2+u_1^2)}.$$

In this manner, we construct an infinite family of elliptic curves

$$E_{u_1,u_2}: \quad y^2 = x(x+u_1^2)(x+u_2^2)$$

with $u_2 \in \mathbb{Q}(x_1, x_2, u_1)$, and passing through the points with the x-coordinate given by x_1^2 and x_2^2.

The points P_1 and P_2 with x-coordinates 4 and t^2 are independent in $E_t(\mathbb{Q}(t))$. If $t=5$, we obtain the elliptic curve E satisfying the minimal equation

$$y^2 = x^3 + ax^2 + bx$$

with

$$a = 1866892562, \qquad b = 153388875753868561.$$

It has a torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ generated by the points

$$R_1 = (-86136961, 0), \qquad R_2 = (391648919, 20162086350120)$$

and passes through the following two independent points (images of P_1 and P_2):

$$Q_1 = (344547844, 17758857249370),$$
$$Q_2 = (2153424025, 137744198443930).$$

The determinant of the Néron–Tate matrix is 112.65, which completes the proof of Theorem 2.8.

2.9. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$

THEOREM 2.9. $\mathrm{Br}(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}, \mathbb{Q}) \ge 1$. *More precisely, there is an infinite family of elliptic curves of rank at least one, with a torsion subgroup over* $\mathbb{Q}$ *isomorphic to* $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ *and parametrised by* $\mathbb{Q}(t)$.

Proof. By (1.1.10), E is an elliptic curve defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ if and only if E has a cubic model of the form

$$E_{x_1,x_2}: \quad y^2 = (x + x_1^2)(x + x_2^2)\left(x + \frac{x_1^2 x_2^2}{(x_1 - x_2)^2}\right) \quad \text{with } x_1, x_2 \in \mathbf{K}.$$

Set

$$x_1 = -\frac{1+2t}{(t-1)(t+1)}, \qquad x_2 = x_1^2.$$

The point whose x-coordinate is x_1^3 is of infinite order in $E_{x_1,x_2}(\mathbb{Q}(t))$ since it is not in $E_{x_1,x_2}(\mathbb{Q}(t))_{\text{tors}}$, except for a finite number of rational values of t, which completes the proof of Theorem 2.9.

2.10. The case $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/9\mathbb{Z}$. In the first section we found two different parametrisations of elliptic curves defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/9\mathbb{Z}$:

$$E_f: \quad y^2 + (1-c)xy - by = (x^3 - bx^2)$$

with $b = cd$, $c = fd - f$ and $d = f(f-1)+1$ (cf. (1.1.8)) and

$$E_t: \quad (32t^2 - 8t)y^2 + (-48t^2 + 64t^3 + 1)xy + t(4t-1)y - 8tx^3(4t-1) = 0$$

(cf. (1.1.8′)). We consider the following elliptic curves:

$$\begin{aligned} E_1: &\quad y^2 = (x-2)(x^3 - 4x^2 + x - 2),\\ E_2: &\quad y^2 = x(4x+1)(4x^2 - 7x + 1),\\ E_3: &\quad y^2 = -(2x-1)(32x^2 - 2x - 1),\\ E_4: &\quad y^2 = -(8x-1)(4x-1)(32x^2 - 20x - 1). \end{aligned}$$

The point $(0,2)$ (resp. $(-1/4,0)$, $(1/4,1/2)$, $(1/8,0)$) is of infinite order in $E_1(\mathbb{Q})$ (resp. $E_2(\mathbb{Q})$, $E_3(\mathbb{Q})$, $E_4(\mathbb{Q})$) and hence E_1 (resp. E_2, E_3, E_4) has rank ≥ 1 over $\mathbb{Q}$.

Theorem 2.10. *$E_1(\mathbb{Q})$, $E_2(\mathbb{Q})$, $E_3(\mathbb{Q})$ and $E_4(\mathbb{Q})$ parametrise elliptic curves with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/9\mathbb{Z}$, of rank ≥ 1.*

Proof. On E_f, $[6](0,0) = (u(f), v(f))$ with

$$u(f) = f^2(f-1), \qquad v(f) = f^4(f-1)^2.$$

Hence, if we set

$$p(x,y) = y^2 + (1-c)xy - by - (x^3 - bx^2)$$

with $b = cd$, $c = fd - f$ and $d = f(f-1)+1$, then the polynomial $p(x, v(f))$ vanishes at $x = u(f)$. In this way, $p(x, v(f))/(x - u(f))$ is a polynomial of degree 2 in x and splits in $\mathbb{Q}$ if and only if $(f-2)(f^3 - fx^2 + f - 2)$ is a square in $\mathbb{Q}$, i.e. if and only if f is the abscissa of a point of $E_1(\mathbb{Q})$. The roots of this polynomial are the x-coordinates of points of infinite order of $E_f(\mathbb{Q})$.

For E_2, E_3 and E_4 we apply the same idea to E_t with $P=(t, 2t^2/(4t-1))$,

$$[4]P = \left(\frac{-1}{4(4t-1)}, \frac{-1}{32t(4t-1)}\right) \quad \text{and} \quad [5]P = \left(\frac{-1}{4(4t-1)}, \frac{-1}{2t(4t-1)^2}\right)$$

respectively.

2.11. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/10\mathbb{Z}$. In the first section we found two different parametrisations of elliptic curves defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/10\mathbb{Z}$:

$$E_f: \quad y^2 + (1-c)xy - by = (x^3 - bx^2)$$

with $b = cd$, $c = fd - f$ and $d = f^2/(f - (f-1)^2)$ (cf. (1.1.9)), and

$$E_t: \quad (t+1)^2y^2 + (2t^2 + 2t + 1 + 2t^3)xy + t^2(2t+1)y \\ - (t+1)^2x^3 - t^2(2t+1)x^2 = 0$$

(cf. (1.1.9′)). We consider the following elliptic curves:

$$\begin{aligned} E_1: &\quad y^2 = (x-2)(x+1)(x^2 - 5x + 2), \\ E_2: &\quad y^2 = 2x^3 + 2x^2 + 2x + 1, \\ E_3: &\quad y^2 = (1 - 3x - 4x^2 + 4x^3)(x+1), \\ E_4: &\quad y^2 = 5x^4 + 8x^3 + 12x^2 + 12x + 4. \end{aligned}$$

The point $(-1, 0)$ (resp. $(0, 1)$, $(-1, 0)$, $(-1, 1)$) is of infinite order in $E_1(\mathbb{Q})$ (resp. $E_2(\mathbb{Q})$, $E_3(\mathbb{Q})$, $E_4(\mathbb{Q})$) and thus E_1 (resp. E_2, E_3, E_4) has rank ≥ 1 over $\mathbb{Q}$.

THEOREM 2.11. *$E_1(\mathbb{Q})$, $E_2(\mathbb{Q})$, $E_3(\mathbb{Q})$ and $E_4(\mathbb{Q})$ parametrise elliptic curves with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/10\mathbb{Z}$, of rank ≥ 1.*

Proof. On E_f, $[6](0,0) = (u(f), v(f))$ with

$$u(f) = \frac{f^2(2f-1)(f-1)}{(-3f + f^2 + 1)^2}, \qquad v(f) = \frac{-f^2(2f-1)^2(f-1)^2}{(-3f + f^2 + 1)^3}.$$

Hence, if we set

$$p(x, y) = y^2 + (1-c)xy - by - (x^3 - bx^2)$$

with $b = cd$, $c = fd - f$ and $d = f^2/(f - (f-1)^2)$, then the polynomial $p(x, v(f))$ vanishes at $x = u(f)$. In this way, $p(x, v(f))/(x - u(f))$ is a polynomial of degree 2 in x and splits in $\mathbb{Q}$ if and only if $(f-2)(f+1)(f^2-5f+2)$ is a square in $\mathbb{Q}$, i.e. if and only if f is the x-coordinate of a point of $E_1(\mathbb{Q})$. The roots of this polynomial are the x-coordinates of points of infinite order of $E_f(\mathbb{Q})$.

For E_2, E_3 and E_4 we apply the same idea to E_t with

$$[2]P = \left(\frac{-t^2(2t+1)}{(t+1)^2}, \frac{t^4(2t+1)^2}{(t+1)^4}\right),$$

$$[3]P = \left(\frac{t(2t+1)}{t+1}, \frac{t^2(2t+1)^2}{(t+1)^3}\right),$$
$$[5]P = \left(-t^2, \frac{t^4}{t+1}\right)$$

respectively, where

$$P = \left(\frac{-t^2(2t+1)}{(t+1)^3}, \frac{-t^3(2t+1)^2}{(t+1)^5}\right).$$

2.12. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/12\mathbb{Z}$. In the first section we parametrised the elliptic curves defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/12\mathbb{Z}$, in the following way (cf. (1.1.10′)):

$$\begin{aligned} E_t: \quad & x_1y_1(x_1+1)y^2 + (-y_1^2x_1 - 2x_1y_1 + x_1^2x_1^2)xy \\ & + x_1(-y_1^2 + x_1x_1^2 + 2x_1y_1)y - x_1y_1(x_1+1)x^3 = 0 \end{aligned}$$

with $x_1 = -(t+1)(t^2-2t+5)/8$ and $y_1 = t(1-t^2)/4$.

We consider the following elliptic curve:

$$E_1: \quad y^2 = (x^4 + 6x^3 - 24x^2 + 90x - 9).$$

The point $(1,8)$ is of infinite order in $E_1(\mathbb{Q})$ and thus E_1 has rank ≥ 1 over $\mathbb{Q}$.

THEOREM 2.12. *$E_1(\mathbb{Q})$ parametrises elliptic curves with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/12\mathbb{Z}$, of rank ≥ 1.*

Proof. On E_t, $[9](x_1,y_1) = (u(t),v(t))$ with

$$u(t) = \frac{\frac{1}{4}(t^2-2t+5)(t+1)^2}{(t-1)^2}, \qquad v(t) = \frac{\frac{1}{16}(t^2-2t+5)^2(t+1)^4}{(t-1)^4}.$$

Thus, if we set

$$\begin{aligned} p(x,y) = {} & x_1y_1(x_1+1)y^2 + (-y_1^2x_1 - 2x_1y_1 + x_1^2x_1^2)xy \\ & + x_1(-y_1^2 + x_1x_1^2 + 2x_1y_1)y - x_1y_1(x_1+1)x^3, \end{aligned}$$

with

$$b = (2d-1)(d-1), \qquad c = \frac{(2d-1)(d-1)}{d}, \quad d = \frac{-2(4+t)}{-8+t^2},$$

the polynomial $p(x,v(t))$ vanishes at $x = u(t)$. Hence, $p(x,v(t))/(x-v(t))$ is a polynomial of degree 2 in x and splits in $\mathbb{Q}$ if and only if $t^4 + 6t^3 - 24t^2 + 90t - 9$ is a square in $\mathbb{Q}$, i.e. if and only if t is the x-coordinate of a point of $E_1(\mathbb{Q})$. The roots of this polynomial are the x-coordinates of points of infinite order of $E_t(\mathbb{Q})$.

2.13. The case $E(\mathbb{Q})_{\mathrm{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. In the first section we parametrised the elliptic curves defined over a field $\mathbf{K}$ with a torsion subgroup over $\mathbf{K}$ isomorphic to $\mathbb{Z}/12\mathbb{Z}$ in the following way (cf. (1.1.13′)):

$$E_t: \quad y^2 + (1-c)xy - by = x^3 - bx^2$$

with

$$b = (2d-1)(d-1), \qquad c = \frac{(2d-1)(d-1)}{d}, \quad d = \frac{-2(4+t)}{-8+t^2}.$$

Define the elliptic curve

$$E_1: \quad y^2 = -(x^4 + 8x^3 + 24x^2 - 64).$$

The point $(-2,4)$ is of infinite order in the curve $E_1(\mathbb{Q})$ and hence E_1 has rank ≥ 1 over $\mathbb{Q}$.

THEOREM 2.13. *$E_t(\mathbb{Q})$ parametrises elliptic curves with a torsion subgroup over $\mathbb{Q}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, of rank ≥ 1.*

Proof. On E_t, $[3](0,0) = (u(t), v(t))$ with

$$u(t) = \frac{(8+4t+t^2)t(2+t)}{(-8+t^2)^2}, \qquad v(t) = \frac{-\frac{1}{2}t^2(2+t)^2(8+4t+t^2)^2}{(4+t)(-8+t^2)^3}.$$

Thus, if we let

$$p(x,y) = y^2 + (1-c)xy - by - (x^3 - bx^2)$$

with

$$b = (2d-1)(d-1), \qquad c = \frac{(2d-1)(d-1)}{d}, \qquad d = \frac{-2(4+t)}{-8+t^2},$$

the polynomial $p(x, v(t))$ vanishes at $x = u(t)$. It follows that the polynomial $p(x, v(t))/(x - u(t))$ is of degree 2 in x and it splits in $\mathbb{Q}$ if and only if $-(t^4 + 8t^3 + 24t^2 - 64)$ is a square in $\mathbb{Q}$, i.e. if and only if t is the x-coordinate of a point of $E_1(\mathbb{Q})$. The roots of this polynomial are the x-coordinates of points of infinite order of $E_t(\mathbb{Q})$.

References

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

[Cas] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts 24, 1991.

[Fer] S. Fermigier, *Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possédant des points d'ordre 2*, C. R. Acad. Sci. Paris Sér. I 322 (1996), 949–952.

[Kna] A. Knapp, *Elliptic Curves*, Math. Notes, Princeton Univ. Press, 1992.

[Kub] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) 33 (1976), 193–237.

[Len] H. W. Lenstra, Jr., *Factoring integers with elliptic curves*, Ann. of Math. (2) 126 (1987), 649–673.

[Maz] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–169.

[Mes1] J.-F. Mestre, *Courbes elliptiques de rang* ≥ 11 *sur* $\mathbb{Q}(t)$, C. R. Acad. Sci. Paris Sér. I 313 (1991), 139–142.

[Mes2] —, *Courbes elliptiques de rang* ≥ 12 *sur* $\mathbb{Q}(t)$, ibid. 313 (1991), 171–174.

[Mon] P. L. Montgomery, *Speeding the Pollard and elliptic curve m and hods of factorization*, Math. Comp. 48 (1987), 243–264.

[Nag] K. Nagao, *Construction of high-rank elliptic curves with a non-trivial torsion point*, ibid. 66 (1997), 411–415.

[Na] T. Nagell, *Recherches sur l'arithmétique des cubiques planes du premier genre dans un domaine de rationalité quelconque*, Nova Acta Soc. Sci. Upsal. (4) 15 (1952), no. 6.

[Sil] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Grad. Texts in Math. 151, Springer, New York, 1994.

[Suy] H. Suyama, informal preliminary report, 1985.

Universidad Nacional de General Sarmiento
Arenales 3675 9P
1425 Capital Federal, Argentina
E-mail: lkulesz@ungs.edu.ar
kulesz@math.jussieu.fr

Received on 20.7.2001
and in revised form on 7.5.2002 (4079)