RAD HRVATSKE AKADEMIJE ZNANOSTI I UMJETNOSTI
MATEMATIČKE ZNANOSTI

L. Halbeisen, N. Hungerbühler, A. Shamsi Zargar and M. Voznyy
A geometric approach to elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, *and* $\mathbb{Z}/16\mathbb{Z}$

Manuscript accepted for publication

A GEOMETRIC APPROACH TO ELLIPTIC CURVES WITH TORSION GROUPS $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$, AND $\mathbb{Z}/16\mathbb{Z}$

Lorenz Halbeisen, Norbert Hungerbühler,
Arman Shamsi Zargar, Maksym Voznyy

Abstract. We give new parametrisations of elliptic curves in Weierstrass normal form $y^2 = x^3 + ax^2 + bx$ with torsion groups $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}$, and with $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields. Even though the parametrisations are equivalent to those given by Kubert and Rabarison, respectively, with the new parametrisations we found three infinite families of elliptic curves with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank. Furthermore, we found elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$ and rank 3 – which is a new record for such curves – as well as some new elliptic curves with torsion group $\mathbb{Z}/16\mathbb{Z}$ and rank 3.

1. Introduction

An elliptic curve E over a field K is a smooth projective curve of genus 1 equipped with a K-rational point. When embedded in the affine plane, E is described by the Weierstrass model $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, where the coefficients belong to K. Elliptic curves can be represented by several other equations. The interested reader may consult [14, Ch. 2]. In the few past decades, many alternative equations describing E have been introduced in the context of cryptographic applications.

Given an elliptic curve E defined over a field K, the Mordell–Weil theorem shows that as an abelian group $E(K)$ is finitely generated over a number field. In particular, $E(K) \cong \mathcal{T} \times \mathbb{Z}^r$, where the torsion group $\mathcal{T}$ is finite. The non-negative integer r is called the rank.

2010 *Mathematics Subject Classification.* 11G05, 14H52.

Key words and phrases. elliptic curve, parametrisation, quadratic field, rank, torsion group.

Many number theorists have tried to construct families of elliptic curves with rank as high as possible. The rank of an elliptic curve measures, in some sense, the number of rational points on the curve. Despite this, there is no known algorithm guaranteed to compute the rank.

With a geometric approach developed in [5], we investigate the rank of elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ over $\mathbb{Q}$, and with torsion groups $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields. In particular, we give new parametrisations of elliptic curves in Weierstrass normal form for these curves. Even though the parametrisations are equivalent to those given by Kubert [6] and Rabarison [12], respectively, especially the parametrisation of elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$ and $\mathbb{Z}/16\mathbb{Z}$ over quadratic fields are novel (see [3]). By our approach, we are able to find parametrisations of elliptic curves with torsion groups $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$, and we provide three infinite families of curves with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank. Furthermore, we find elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$ and rank 3 – which is a new record for such curves, as well as some new elliptic curves with torsion group $\mathbb{Z}/16\mathbb{Z}$ and rank 3. Consult [2,3] for the current records on the rank of elliptic curves (with prescribed torsion groups) over the rational and quadratic fields.

2. A geometric approach to elliptic curves

In this section we present a geometric approach to elliptic curves with torsion groups $\mathbb{Z}/2n\mathbb{Z}$ over arbitrary fields. The approach is bases on a ruler construction of cubic curves due to Schroeter [13], which was further developed and applied to elliptic curves in [5].

Let $\mathbb{F}$ be a finite field extension of $\mathbb{Q}$ and let

$$\Gamma_{a,b}:\ y^2 = x^3 + ax^2 + bx$$

with $a, b \in \mathbb{F}$ be a cubic curve. Furthermore, let $T := (0, 0)$. Then T belongs to $\Gamma_{a,b}$ and $T + T = \mathscr{O}$, where $\mathscr{O}$ denotes the neutral element of the Mordell–Weil group of $\Gamma_{a,b}$ and "+" is the group operation. If A is a point on $\Gamma_{a,b}$, then we call the point $\bar{A} := T + A$ the *conjugate of* A. Since $T + T = \mathscr{O}$, we have

$$\bar{\bar{A}} = T + \bar{A} = T + T + A = \mathscr{O} + A = A.$$

Furthermore, for points A, B on an elliptic curve Γ (over $\mathbb{F}$), let

$$A \# B := -(A + B).$$

In particular, if $C = A \# A$, then the line through C and A is tangent to $\Gamma_{a,b}$ with contact point A.

The following fact gives a connection between conjugate points and tangents (see Figure 1):

Fact 2.1. *If $A, \bar{A}, B$ are three points on $\Gamma_{a,b}$ which lie on a straight line, then $A \# A = \bar{B}$.*

PROOF. If $A, \bar{A}, B$ are three points on $\Gamma_{a,b}$ lying on a straight line, then $A + \bar{A} = -B$ (see Figure 1). Thus, $A + T + A = T + A + A = -B$, which implies

$$\begin{aligned} A + A &= T + (T + A + A) = T + (-B) \\ &= (-T) + (-B) = -(T + B) = -\bar{B}. \end{aligned}$$

Therefore, the line $A\bar{B}$ is tangent to $\Gamma_{a,b}$ with contact point A, *i.e.*, $A \# A = \bar{B}$. □

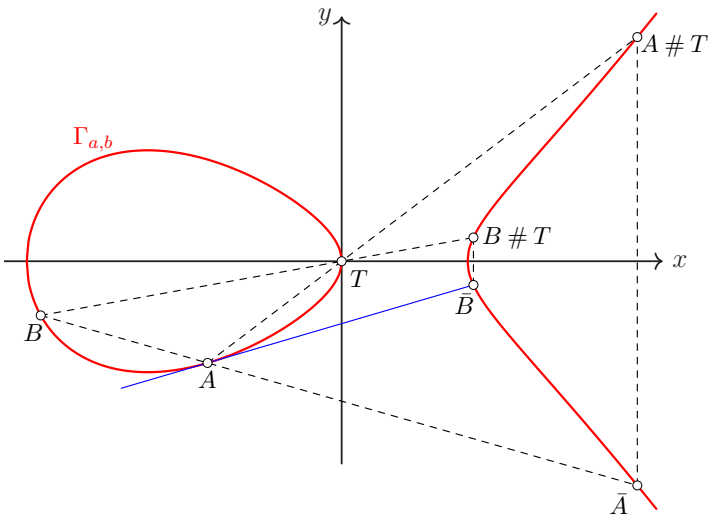

FIGURE 1. Conjugate points and tangents.

In homogeneous coordinates, the curve $y^2 = x^3 + ax^2 + bx$ becomes

$$\Gamma : \; Y^2 Z = X^3 + aX^2 Z + bXZ^2.$$

Assume now that $\tilde{A} = (x_0, y_0, 1)$ is a point on the cubic Γ, where $x_0, y_0 \in \mathbb{F}$ and $y_0 \neq 0$. Then the point $(1, 1, 1)$ is on the curve

$$y_0^2 \, Y^2 Z = x_0^3 \, X^3 + a \, x_0^2 \, X^2 Z + b \, x_0 \, XZ^2.$$

Now, by exchanging X and Z (*i.e.*, $(X, Y, Z) \mapsto (Z, Y, X)$), dehomogenising with respect to the third coordinate (*i.e.*, $(Z, Y, X) \mapsto (Z/X, \, Y/X, \, 1)$), and multiplying with $1/y_0^2$, we obtain that the point $A = (1, 1)$ is on the curve

$$\Gamma_{\alpha,\beta,\gamma} : \; y^2 x = \alpha + \beta x + \gamma x^2,$$

where $\alpha, \beta, \gamma \in \mathbb{F}$. Notice that since $A = (1,1)$ is on $\Gamma_{\alpha,\beta,\gamma}$, we have $\alpha+\beta+\gamma = 1$. We denote this projective transformation which maps $\Gamma_{a,b}$ to $\Gamma_{\alpha,\beta,\gamma}$ and $\tilde{A}$ to A by Φ.

In homogeneous coordinates, the neutral element of $\Gamma_{\alpha,\beta,\gamma}$ is $\mathscr{O} = (0,1,0)$, and the image under Φ of the point $(0,0,1)$ on $\Gamma_{a,b}$ is $T = (1,0,0)$. With respect to the curve $\Gamma_{\alpha,\beta,\gamma}$, we obtain that the conjugate $\bar{P}$ of a point $P = (x_0, y_0)$ on $\Gamma_{\alpha,\beta,\gamma}$ is of the form $\bar{P} = (x_1, -y_0)$ for some $x_1 \in \mathbb{F}$.

A generalisation of these observations is given by the following:

LEMMA 2.2. *Let $\tilde{A}_0 = (x_0, y_0)$ be a point on the cubic $\Gamma_{a,b} : y^2 = x^3 + ax^2 + bx$, where $x_0, y_0, a, b \in \mathbb{F}$ and $y_0 \neq 0$. Then there exists an $\mathbb{F}$-projective transformation Φ which maps the curve $\Gamma_{a,b}$ to the curve*

$$\Gamma_{\alpha,\beta,\gamma,\delta} : \; y^2(x-\delta) = \alpha + \beta x + \gamma x^2 \quad \textit{(with } \alpha, \beta, \gamma, \delta \in \mathbb{F}\textit{)},$$

and the point $\tilde{A}_0$ to $A_0 = (1,1)$. Moreover, we can require that $\bar{A}_0 = (-1,-1)$.

PROOF. By the above observations there exists an $\mathbb{F}$-projective transformation Φ which maps the curve $\Gamma_{a,b}$ to the curve

$$\tilde{\Gamma} : \; y^2 x = \tilde{\alpha} + \tilde{\beta} x + \tilde{\gamma} x^2 \quad (\text{with } \tilde{\alpha}, \tilde{\beta}, \tilde{\gamma} \in \mathbb{F}),$$

and the point $\tilde{A}_0$ to $A_0 = (1,1)$. The conjugate $\bar{A}_0$ of A_0 is of the form $\bar{A}_0 = (x_1, -1)$, and by shifting and stretching the x-axis, we obtain the curve

$$\Gamma_{\alpha,\beta,\gamma,\delta} : \; y^2(x-\delta) = \alpha + \beta x + \gamma x^2 \quad (\text{with } \alpha, \beta, \gamma, \delta \in \mathbb{F}),$$

which contains the points $A_0 = (1,1)$ and $\bar{A}_0 = (-1,1)$. □

With respect to the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$, we can compute the conjugate of a point by the following:

FACT 2.3. *Let $P = (x_0, y_0)$ be a point on $\Gamma_{\alpha,\beta,\gamma,\delta}$. Then*

$$\bar{P} = \left(\frac{\alpha + \delta(x_0\gamma + \beta)}{\gamma(x_0 - \delta)}, -y_0 \right).$$

PROOF. Let $P = (x_0, y_0)$ be a point on $\Gamma_{\alpha,\beta,\gamma,\delta}$. Then

$$y_0^2(x_0 - \delta) = \alpha + \beta x_0 + \gamma x_0^2,$$

which implies that x_0 is a root of

$$x^2\gamma + x(\beta - y_0^2) + (\alpha - \delta y_0^2),$$

and since the other root is $\frac{\alpha+\delta(x_0\gamma+\beta)}{\gamma(x_0-\delta)}$, we obtain $\bar{P} = \left(\frac{\alpha+\delta(x_0\gamma+\beta)}{\gamma(x_0-\delta)}, -y_0 \right)$. □

Let $\Gamma_{a,b} : \; y^2 = x^3 + ax^2 + bx$ be a regular curve over some field $\mathbb{F}$ with torsion group $\mathbb{Z}/2n\mathbb{Z}$ (for some $n \geq 5$). Each element of the group $\mathbb{Z}/2n\mathbb{Z} = \{0, 1, \ldots, 2n-1\}$ corresponds to a point on $\Gamma_{a,b}$. Let $\tilde{T}$ be the unique point of order 2. Then $\tilde{T}$ corresponds to n. Furthermore, let A' be

a point on $\Gamma_{a,b}$ which corresponds to 1. Then A' is of order $2n$. Finally, let B' be the point on $\Gamma_{a,b}$ which corresponds to 2. Then $A' + A' = B'$. Now, by Lemma 2.2, there is a projective transformation Φ which maps the curve $\Gamma_{a,b}$ to the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$, the point A' to the point $A = (1, 1)$, and the point $\bar{A}'$ to the point $\bar{A} = (-1, -1)$. Moreover, since $A + \bar{A}$ corresponds to $1+(n+1) = n+2$, we obtain that $A+\bar{A} = \bar{B}$. In other words, $A\#\bar{A} = -\bar{B}$, which implies that $-\bar{B}$ is on the line $A\bar{A}$. Hence, $-\bar{B} = (u, u)$ for some $u \in \mathbb{F}$, and therefore $B = (v, u)$ for some $v \in \mathbb{F}$.

Since the points $A, \bar{A}, B, \bar{B}$ belong to the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$, we obtain

$$\alpha = -u, \quad \beta = 1, \quad \gamma = \frac{u^2-1}{u+v}, \quad \delta = u - \gamma, \quad v = \frac{u^2 - u\gamma - 1}{\gamma}.$$

For $u, v \in \mathbb{F}$, let

$$\Gamma_{u,v} : \; y^2 \left(x - u + \frac{u^2-1}{u+v} \right) = -u + x + \frac{u^2-1}{u+v}\, x^2.$$

By applying Φ^{-1} to the curve $\Gamma_{u,v}$, we obtain the curve $\Gamma_{a,b}$ with

$$a = -2 + 3u^2 + 2u^3 v + v^2 \quad \text{and} \quad b = (u^2-1)^3(v^2-1).$$

In the following sections we shall apply this approach to elliptic curves with torsion groups $\mathbb{Z}/2n\mathbb{Z}$ for $n = 5, 6, 7, 8$.

3. Elliptic curves with torsion group $\mathbb{Z}/\mathbf{10}\mathbb{Z}$

To warm up, we give a parametrisation of elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$.

Let $\Gamma_{a,b} : \; y^2 = x^3 + ax^2 + bx$ be a regular curve with torsion group $\mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}$. Each element of the group $\mathbb{Z}/10\mathbb{Z} = \{0, 1, \ldots, 9\}$ corresponds to a rational point on $\Gamma_{a,b}$. Let $\tilde{T}$ be the unique point of order 2. Then $\tilde{T}$ correspond to 5. Furthermore, let $\tilde{A}$ and $\tilde{B}$ be the rational points on $\Gamma_{a,b}$ which correspond to 1 and 2, respectively. Then $\tilde{A}$ is of order 10 and $\tilde{B}$ is of order 5. Finally, let Φ be a projective transformation Φ which maps the curve $\Gamma_{a,b}$ to the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$, the point $\tilde{A}$ to the point $A = (1, 1)$, and the conjugate of $\tilde{A}$ to the point $\bar{A} = (-1, -1)$. Let $B := \Phi(\tilde{B})$ and $T := \Phi(\tilde{T})$. Then, for $A, -A, \bar{A}, \ldots$ we obtain the following correspondence between these points on $\Gamma_{\alpha,\beta,\gamma,\delta}$ and the elements of the group $\mathbb{Z}/10\mathbb{Z}$:

Elements of $\mathbb{Z}/10\mathbb{Z}$	0	1	2	3	4	5	6	7	8	9
Points on $\Gamma_{\alpha,\beta,\gamma,\delta}$	$\mathscr{O}$	A	B	$-\bar{B}$	$-\bar{A}$	T	$\bar{A}$	$\bar{B}$	$-B$	$-A$

By definition, we have:

(i) The points $A, \bar{A}, -\bar{B}$ are collinear.
(ii) The points $A, B, \bar{B}$ are collinear.

Since $A = (1,1)$ and $\bar{A} = (-1,-1)$, by (i) we have $-\bar{B} = (u,u)$ for some $u \in \mathbb{Q}$, *i.e.*, $\bar{B} = (u,-u)$ and $B = (v,u)$. So, by (ii), we have

$$v = \frac{3u - u^2}{u+1},$$

and since $v = \frac{u^2 - u\gamma - 1}{\gamma}$, we have

$$\gamma = \frac{(u+1)^2(u-1)}{4u}.$$

Now, by applying the formulae $a = -2 + 3u^2 + 2u^3 v + v^2$ and $b = (u^2 - 1)^3(v^2 - 1)$ for the parameters of the curve $\Gamma_{a,b}$, we obtain the following result:

THEOREM 3.1. *Let* $u \in \mathbb{Q} \setminus \{0, \pm 1\}$ *and let*

$$a_1 = -2(1 + 2u - 5u^2 - 5u^4 - 2u^5 + u^6),$$
$$b_1 = (u^2 - 1)^5(-1 - 4u + u^2).$$

Then, the curve

$$\Gamma_{a_1,b_1} : y^2 = x^3 + a_1 x^2 + b_1 x$$

is an elliptic curve with torsion group $\mathbb{Z}/10\mathbb{Z}$. *Conversely, if* $\Gamma_{a,b}$ *is a regular elliptic curve with torsion group* $\mathbb{Z}/10\mathbb{Z}$, *then there exists a* $u \in \mathbb{Q}$ *such that* $\Gamma_{a,b}$ *is isomorphic to* Γ_{a_1,b_1}.

Remarks.

- In [6, Table 3, p. 217], Kubert gives the following parametrisation of curves of the form

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

  with torsion group $\mathbb{Z}/10\mathbb{Z}$ (see also Kulesz [8, p. 341,(1.1.9)], who found Kubert's parametrisation in a different way):

  $$\tau = \frac{p}{q}, \quad d = \frac{\tau^2}{\tau - (\tau-1)^2}, \quad c = \tau(d-1), \quad b = cd.$$

  After transforming Kubert's curve into the form

  $$y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x,$$

  we find

  $$\tilde{a} = -(2p^2 - 2pq + q^2)(4p^4 - 12p^3 q + 6p^2 q^2 + 2pq^3 - q^4),$$
  $$\tilde{b} = 16p^5(p-q)^5(p^2 - 3pq + q^2).$$

Now, by substituting in $\tilde{a}$ and $\tilde{b}$ the values p and q with $p+q$ and $2q$, respectively, and setting $u = p/q$, we obtain $4a_1$ and $16b_1$, respectively, which shows that the two parametrisations are equivalent.

- Recall that the Calkin–Wilf sequence
$$s_1 = 1, \quad s_{n+1} = \frac{1}{2\lfloor s_n \rfloor - s_n + 1}$$
lists every positive rational number exactly once. By checking the first 22 000 fractions in this sequence we found, with the help of `MAGMA`, 46 elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$ and rank 3.
- The following table gives the fractions p/q and their indices in the Calkin–Wilf sequence of six of the 25 known elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$ and rank 4 (see [2]):

p	q	Calkin–Wilf index	Discovered by
2244	1271	307 485	Fisher (2016)
3051	2164	623 897	Fisher (2016)
4777	7725	1 629 610	Fisher (2016)
1333	475	3 137 659	Dujella (2005)
2407	308	67 161 983	Dujella (2008)
1564	1991	532 575 944 622	Elkies (2006)

- For $p/q = 13360/9499$ (Calkin–Wilf index 15 352 857), we identified a new $\mathbb{Z}/10\mathbb{Z}$ curve of conditional rank 4:
$$\begin{aligned} y^2 + xy = x^3 & \\ & - 377271759465005133444077928672396475004284950623 95\, x \\ & + 8919228755111936535268573001459752244770998391496121\backslash \\ & \quad 1487019041502289387025 \end{aligned}$$
`MAGMA` computations reveal three generators on the curve and confirm that its root number is 1, therefore the rank should be even. The point search up to height 2^{38} on each of the 256 4-coverings for each of the 4 curves in the isogeny class did not uncover the missing last generator. We leave it as an open challenge to test new descent methods.

4. Elliptic curves with torsion group $\mathbb{Z}/12\mathbb{Z}$

Let us now consider parametrisations of elliptic curves with torsion group $\mathbb{Z}/12\mathbb{Z}$. By similar arguments as above, one can show the following result:

Theorem 4.1. *Let $t \in \mathbb{Q} \setminus \{1\}$ be a positive rational and let*
$$a_1 = 2(3t^8 + 24t^6 + 6t^4 - 1), \qquad b_1 = (t^2-1)^6(1+3t^2)^2.$$
Then the curve
$$\Gamma_{a_1,b_1} : y^2 = x^3 + a_1x^2 + b_1x$$

is an elliptic curve with torsion group $\mathbb{Z}/12\mathbb{Z}$*. Conversely, if* $\Gamma_{a,b}$ *is a regular elliptic curve with torsion group* $\mathbb{Z}/12\mathbb{Z}$*, then there exists a positive rational* t *such that* $\Gamma_{a,b}$ *is isomorphic to* Γ_{a_1,b_1}*.*

In [6, Table 3, p. 217], Kubert gives the following parametrisation of elliptic curves of the form

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

with torsion group $\mathbb{Z}/12\mathbb{Z}$ (see also Kulesz [8, p. 341,(1.1.10)], who found Kubert's parametrisation in a different way):

(4.1)

$$\tau = \frac{r}{s}, \quad m = \frac{3\tau - 3\tau^2 - 1}{\tau - 1}, \quad f = \frac{m}{1-\tau}, \quad d = m + \tau, \quad c = f(d-1), \quad b = cd.$$

After transforming Kubert's curve into the form

$$y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x,$$

we find

$$\tilde{a} = s^8 + 12r(r-s)\big(s^6 + 2r(r-s)(r^2 - rs + s^2)(r^2 - rs + 2s^2)\big),$$

$$\tilde{b} = 16r^6(r-s)^6\big(3r(r-s) + s^2\big)^2.$$

Now, for $t = r/s$ we obtain

$$a_1 := 6r^8 + 48r^6s^2 + 12r^4s^4 - 2s^8 \quad \text{and} \quad b_1 := (r^2 - s^2)^6\,(3r^2 + s^2)^2.$$

Then, by substituting in $\tilde{a}$ and $\tilde{b}$, r with $r + s$ and s with $2s$, we obtain $4a$ and $16b$, respectively. This shows that the two elliptic curves

$$\Gamma_{\tilde{a},\tilde{b}}: \; y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x$$

and

$$\Gamma_{a,b}: \; y^2 = x^3 + ax^2 + bx$$

are equivalent.

4.1. *Elliptic curves of rank at least* 2. By checking the first 3441 fractions r/s of the Calkin–Wilf sequence we found, with the help of `MAGMA`, 125 fractions which lead to elliptic curves with torsion group $\mathbb{Z}/12\mathbb{Z}$ and rank 2, and among these 3441 fractions, we even found some which lead to curves with rank 3.

As a matter of fact, we would like to mention that until today (April 2022), up to isomorphisms only one elliptic curve of rank 4 is known, namely

$$\begin{aligned} y^2 + xy = x^3 &- 4422329901784763147754792226039053294186858800\,x \\ &+ 98943710602886706347390586357680210847183616798\backslash \\ &\quad 063680624530387016000 \end{aligned}$$

discovered by Fisher in 2008 (see [2]). This curve is isomorphic to

$$y^2 = x^3 + 588436986469809874425598\,x^2 + 44662083920000859376188675997725867856489478401\,x$$

which is of type $\Gamma_{a,b}$, where $r = 726$ and $s = 133$ (Calkin–Wilf index of $726/133$ is 274 335).

4.2. *Families of elliptic curves with positive rank.* In this section, we construct three infinite families of elliptic curves $\Gamma_{a,b}$ with positive rank. Other such families were found, for example, by Rabarison [11, Thm. 12], Kulesz [8, Thm. 2.12] (see also [7, Sec. 2.12]), and by Suyama (see [9, p. 262 f]). Although the parametric families of positive rank and torsion group $\mathbb{Z}/12\mathbb{Z}$ are not explicitly given in the work of Rabarison, they are mentioned on page 17, line 3 of his manuscript and on page 90, line 1 of his thesis. In fact, the elliptic curves which correspond to our three families are, in Cremona's notation, the curves 368d1, 226a1 and 720e2.

Let $t \in \mathbb{Q} \setminus \{-1, 0, 1\}$. Instead of $\Gamma_{a,b}$ we consider the equivalent elliptic curve

$$\Gamma_t : \; y^2 = x^3 + 2(3t^8 + 24t^6 + 6t^4 - 1)x^2 + (t^2 - 1)^6(1 + 3t^2)^2 x.$$

The finite torsion points of Γ_t are given in the following table:

Order	x-coordinate	y-coordinate
2	0	0
3	$(t^2-1)^4$	$\pm 4t^2(t^2-1)^4(t^2+1)$
4	$-(t^2-1)^3(1+3t^2)$	$\pm 8t^3(t^2-1)^3(1+3t^2)$
6	$(t^2-1)^2(1+3t^2)^2$	$\pm 4t^2(t^2-1)^2(t^2+1)(1+3t^2)^2$
12	$(t^2-1)(t+1)^4(1+3t^2)^2$	$\pm 4t(t^2-1)(t+1)^4(1+t^2)(1+3t^2)$
12	$-(t^2-1)(t+1)^4(1+3t^2)^2$	$\pm 4t(t^2-1)(t-1)^4(1+t^2)(1+3t^2)$

Now, if we find any additional rational point P on Γ_t, then the order of P is infinite which implies that the rank of Γ_t is positive. On the other hand, if we find an infinite family $\mathscr{T}$ of values for t such that for every $t \in \mathscr{T}$, the curve Γ_t has an additional point, then $\{\Gamma_t : t \in \mathscr{T}\}$ is an infinite family of elliptic curves with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank.

4.2.1. *First family.* Let $P_1 = (x_1, y_1)$ with

$$x_1 = -(t+1)^2(t-1)^6.$$

Then P_1 is a rational point on Γ_t if and only if

$$v^2 = -(t^4 + 8t^3 + 2t^2 + 1) \quad \text{for some rational } v.$$

This quartic curve has a rational solution $(t, v) = (-1, 2)$, hence, by [4, Prop. 15.1, p. 477], it is equivalent to the elliptic curve

$$y^2 = x^3 + x^2 - 1,$$

which is a rank-1 elliptic curve, where $G_1 := (1, 1)$ is a point of infinite order. In particular, for all but finitely many $k \in \mathbb{Z}$, for $[k]G_1 = (x_k, y_k)$ and $t_k := (y_k - 1)/(2x_k - y_k - 1)$, Γ_{t_k} is a non-singular curve with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank.

Examples. For $k = 2$ we obtain $[2]G_1 = (13/4, -53/8)$ and $t_2 = -61/97$. So, the parameters a and b of $\Gamma_{a,b}$ are

$$a = \frac{23452774585480768}{7837433594376961} \quad \text{and} \quad b = \frac{1433212402140932302965493569945 6}{614253653462685704461977675955 21},$$

where $\Gamma_{a,b}$ has rank 2. In order to compute the rank of $\Gamma_{a,b}$, it seems to be faster to use Kubert's form (4.1) with $\tau = (r + s)/(2s)$ where $t_2 = r/s$, which gives us

$$1 - c = \frac{53471797}{47824783} \quad \text{and} \quad b = -\frac{37072646910}{366481312129}.$$

The following table summarises what we have found with the help of `MAGMA`:

k	t_k	$1 - c$	b	Rank
-2	-5	$-\frac{163}{27}$	$\frac{2470}{81}$	1
-1	-1	1	0	Γ_{-1} is singular
2	$-\frac{61}{97}$	$\frac{53471797}{47824783}$	$-\frac{37072646910}{366481312129}$	2
3	$-\frac{5737}{1921}$	$-\frac{172463134332983}{107840890126669}$	$\frac{5130041565973335306660}{793224637894724969521}$	2
4	$-\frac{1500953}{1090945}$	$\frac{p}{q}$	$\frac{r}{s}$	1

with $\frac{p}{q} = \frac{176300986438386243254744 9}{237446946417216233521480 5}$ and $\frac{r}{s} = \frac{105263409116564664324521726781595865 2}{335704649291525517559144807449212302 5}$. `MAGMA` calculations also confirm the rank to be at least 1 for both $k = 5$ and $k = 6$.

4.2.2. *Second family.* Let $P_2 = (x_2, y_2)$ with

$$x_2 = (t + 1)^8.$$

Then P_2 is a rational point on Γ_t if and only if

$$v^2 = t^4 - 2t^3 + 13t^2 + 4t + 4 \quad \text{for some rational } v.$$

This quartic curve has a solution $(t, v) = (0, 2)$ and, by [14, Thm. 2.17], is birationally equivalent to

$$y^2 + xy = x^3 - 5x + 1,$$

which is, according to MAGMA, a rank-1 elliptic curve, where $G_2 := (0,1)$ is a point of infinite order. In particular, for all but finitely many $k \in \mathbb{Z}$, for $[k]G_2 = (x_k, y_k)$ and $t_k := 2(x_k+2)/(y_k+1)$, Γ_{t_k} is a non-singular curve with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank.

Examples. With the help of MAGMA, we computed the rank of the curve Γ_{t_k} for $k = 1, \ldots, 8, 10$:

k	t_k	$1-c$	b	Rank
1	2	79	390	1
2	$\frac{4}{3}$	533	$\frac{13300}{3}$	1
3	$\frac{3}{14}$	$\frac{7261}{18634}$	$\frac{2331465}{2869636}$	1
4	$\frac{175}{17}$	$\frac{395470463}{8381663}$	$\frac{5983231581600}{11256573409}$	1
5	$-\frac{799}{1200}$	$\frac{3553536961599}{3195202399600}$	$-\frac{744762911993283599}{7664651516160480000}$	1
6	$-\frac{43872}{18847}$	$-\frac{2079664621920150527}{4649857101108754273}$	$\frac{153430524136694311178634306400}{54964333016731199119524650 89}$	1

MAGMA calculations also confirm that the rank is exactly 1 for $k = 7$ and $k = 10$, and the rank is at least 1 for $k = 8$.

4.2.3. *Third family.* Let $P_3 = (x_3, y_3)$ with

$$x_3 = \tfrac{3}{4}(t+1)^4(t-1)^4.$$

Then P_3 is a rational point on Γ_t if and only if

$$v^2 = 75t^4 + 66t^2 + 3 \quad \text{for some rational } v.$$

This quartic curve has a solution $(t, v) = (1, 12)$, hence it is equivalent to an elliptic curve

$$y^2 = x^3 - 147x - 286$$

of rank 1, generated by the point $G_3 = (-5, -18)$ of infinite order, as determined by MAGMA. For all but finitely many $k \in \mathbb{Z}$, for $[k]G_3 = (x_k, y_k)$ and $t_k := (y_k - 3x_k + 3)/(y_k + 9x_k + 63)$, Γ_{t_k} is a non-singular curve with torsion group $\mathbb{Z}/12\mathbb{Z}$ and positive rank.
We have computed the rank of the curve Γ_{t_k} for $k = -2, 2, 3, 4$:

k	t_k	$1-c$	b	Rank
-2	$-\frac{1}{11}$	$\frac{2531}{2376}$	$-\frac{9455}{156816}$	2
2	$-\frac{59}{169}$	$\frac{282022931}{250380936}$	$-\frac{506936401895}{4823839112976}$	2
3	$-\frac{9059}{61}$	$-\frac{2502776666788081}{5783947776000}$	$\frac{102937783902951852766681}{1608862913372160000}$	≥ 1
4	$\frac{2086379}{6069899}$	$-\frac{581881542681690082605213 61}{47961469780361881818624000}$	$\frac{r}{s}$	≥ 1

with $\frac{r}{s} = \frac{2186504518566993279256742865370434477481}{5798437155904408180157947698004377600 00}$.

5. Elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$

For an elliptic curve over some field $\mathbb{F}$ with torsion group $\mathbb{Z}/14\mathbb{Z}$, starting with a value for $u \in \mathbb{F}$, we compute a value for v, which will lead to a parametrisation of elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$.

Theorem 5.1. *Let $\mathbb{F}$ be a field containing $\mathbb{Q}$. Then there exists an elliptic curve $\Gamma_{a,b}$ over $\mathbb{F}$ with torsion group $\mathbb{Z}/14\mathbb{Z}$ if and only if for some $u \in \mathbb{F} \setminus \{-1, 0, 1\}$,*

$$\sqrt{1 - 2u + u^2 + 4u^3}$$

belongs to $\mathbb{F}$.

Proof. Assume that the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$ over $\mathbb{F}$ has torsion group $\mathbb{Z}/14\mathbb{Z}$ and that the points $A = (1, 1)$, $\bar{A} = (-1, -1)$, $B = (v, u)$, $-\bar{B} = (u, u)$ belong to $\Gamma_{\alpha,\beta,\gamma,\delta}$, where A, $\bar{A}$, B, $-\bar{B}$ correspond to 1, 8, 2, 5, respectively. Finally, let $C := A + B$. Then C corresponds to 3. The complete group table is given as follows:

Elements of $\mathbb{Z}/14\mathbb{Z}$	0	1	2	3	4	5	6	7
Points on $\Gamma_{\alpha,\beta,\gamma,\delta}$	$\mathscr{O}$	A	B	C	$-\bar{C}$	$-\bar{B}$	$-\bar{A}$	T
Points on $\Gamma_{\alpha,\beta,\gamma,\delta}$	$\mathscr{O}$	$-A$	$-B$	$-C$	$\bar{C}$	$\bar{B}$	$\bar{A}$	T
Elements of $\mathbb{Z}/14\mathbb{Z}$	14	13	12	11	10	9	8	7

Since $B \# \bar{B} = C$, the point C is on the line g passing through B and $\bar{B}$. Furthermore, we have $A \# B = -C = \bar{A} \# \bar{B}$. In other words, $-C$ is the intersection point of the lines AB and $\bar{A}\bar{B}$, denoted $-C = AB \wedge \bar{A}\bar{B}$. Furthermore, we have $-\bar{C} = A\bar{B} \wedge \bar{A}B$. Notice that the points C and $-\bar{C}$ have the same y-coordinate.

In homogeneous coordinates, we obtain

$$g : \ B \times \bar{B} = (v, u, 1) \times (u, -u, 1) = (2u,\, u - v,\, -u^2 - uv)$$

and

$$-C = (A \times B) \times (\bar{A} \times \bar{B}) = \big(-3u - u^2 + v + 3uv,\, (u-1)(3u-v),\, (1-u)(u+v)\big),$$

and therefore

$$C = \big(-3u - u^2 + v + 3uv,\, (1-u)(3u-v),\, (1-u)(u+v)\big).$$

Since the point C belongs to g, we must have the scalar product $\langle g, C \rangle = 0$, *i.e.*,

$$u^2(-3 - 6u + u^2) + 2u(-1 + 4u + u^2)\, v + (u-1)^2\, v^2 = 0.$$

Now, for $u \in \mathbb{F}$, this implies that also

$$v_{1,2} = \frac{u\big(1 - 4u - u^2 \pm 2\sqrt{1 - 2u + u^2 + 4u^3}\big)}{(u-1)^2}$$

belong to $\mathbb{F}$, and hence $\sqrt{1 - 2u + u^2 + 4u^3}$ belongs to $\mathbb{F}$.

On the other hand, if $\Gamma_{a,b}$ is an elliptic curve over $\mathbb{F}$ with torsion group $\mathbb{Z}/14\mathbb{Z}$, then we can transform this curve (over $\mathbb{F}$) to the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$ which contains the points $A = (1,1)$, $B = (v,u)$, and $-\bar{B} = (u,u)$ with the above properties. In particular, we have that $u, v \in \mathbb{F}$ which implies that $\sqrt{1-2u+u^2+4u^3}$ belongs to $\mathbb{F}$. □

As an immediate consequence we obtain:

COROLLARY 5.2. *Let $u \in \mathbb{Q}\backslash\{-1,0,1\}$ and let $d = 1-2u+u^2+4u^3$. Then there exists an elliptic curve $\Gamma_{a,b}$ over $\mathbb{Q}(\sqrt{d})$ with torsion group $\mathbb{Z}/14\mathbb{Z}$.*

5.1. *High rank elliptic curves with torsion group $\mathbb{Z}/\mathbf{14}\mathbb{Z}$.* By some further calculations, we can slightly simplify the formulae for the parameters a and b of the curve $\Gamma_{a,b}$. For $z = \sqrt{1-2u+u^2+4u^3}$ we have:

$$\begin{aligned} a &= -2(1-4u+2u^2+10u^3-18u^4-10u^6+2u^7+u^8) \\ &\quad + 4u^2(1-4u-2u^3+u^4)z \\ b &= (1-u)^7(1+u)^3\big((1+u)(1-5u+6u^2+6u^3-23u^4-u^5) \\ &\quad - 4u^2(1-4u-u^2)z\big) \end{aligned}$$

With the help of `MAGMA` we found that for each

$$u = 4,\ \frac{4}{7},\ \frac{4}{9},\ \frac{8}{5},\ -\frac{4}{11},\ \frac{5}{17},\ \frac{\sqrt{2081}+39}{8},\ \frac{\sqrt{2713}+37}{32},\ \frac{\sqrt{12121}+121}{18},\ \frac{\sqrt{23641}+109}{98},\ \frac{\sqrt{55441}+169}{128},$$

the corresponding curve has rank 2. We would like to mention that different values of $u \in \mathbb{Q}$ may not necessarily lead to different quadratic fields $\mathbb{Q}(\sqrt{d})$. For example, for $u_1 = 4/9$ and $u_2 = 5/13$, both curves have torsion group $\mathbb{Z}/14\mathbb{Z}$ over the same quadratic field $\mathbb{Q}(\sqrt{481})$. Moreover, for u_1 and u_2, the corresponding curves have the same rank, which follows from the following result (see Rabarison [12, Lem. 4.4]):

FACT 5.3. *Let d be a square-free integer and let $\mathbb{F}_d = \mathbb{Q}(\sqrt{d})$. Furthermore, let $u_0 \in \mathbb{F}_d$ be such that $\mathbb{F}_d = \mathbb{Q}(\sqrt{z})$ where $z = 1-2u_0+u_0^2+4u_0^3$. Then the elliptic curve*

$$\Gamma_0 :\ y^2 = 4x^3 + x^2 - 2x + 1$$

has torsion group $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{F}_d$ for $d \neq -7$ and has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ over $\mathbb{F}_{-7}$.

Now, since (u_0, z) is a non-torsion point on Γ_0, the curve Γ_0 has rank ≥ 1 over $\mathbb{F}_d$, and by adding (in the case $d \neq -7$) the 6 torsion points of Γ_0 to (u_0, z), we obtain the following 6 values for u, which all lead to essentially the

same curve with torsion group $\mathbb{Z}/14\mathbb{Z}$ over $\mathbb{F}_d$:

$$u_1 = u_0, \quad u_2 = \frac{1-u_0}{1+u_0}, \quad u_{3,4} = \frac{u_0(u_0+1) \pm z}{(u_0-1)^2}, \quad u_{5,6} = \frac{(1-u_0) \pm z}{2u_0^2}.$$

For example, if $u_1 = 4/9$, then $u_2 = 5/13$ and the corresponding curves are essentially the same.

In order to obtain different curves with torsion group $\mathbb{Z}/14\mathbb{Z}$, we can, for example, start with an arbitrary $u_0 \in \mathbb{Q} \setminus \{-1, 0, 1\}$ and double the point (u_0, z) on Γ_0 (over the corresponding field $\mathbb{F}_d$). This way, we get the following value for u:

$$u = \frac{u_0(u_0-1)(u_0^2+u_0+2)}{z^2} = \frac{u_0(u_0-1)(u_0^2+u_0+2)}{(u_0+1)(4u_0^2-3u_0+1)}.$$

For example, taking $u_0 = 1/2$ (curve of rank 0) we produce a different $\mathbb{Z}/14\mathbb{Z}$ curve with $u = -11/12$ (rank 1) over the same field $\mathbb{Q}(\sqrt{3})$. Similarly, taking $u_0 = 2/3$ (curve of rank 1) we produce a different $\mathbb{Z}/14\mathbb{Z}$ curve with $u = -8/15$ (rank 0) over the same field $\mathbb{Q}(\sqrt{105})$.

Another approach to find independent values for u would be to search for values d, such that Γ_0 has high rank over $\mathbb{F}_d$. With the help of `MAGMA` we found an abundance of quadratic fields $\mathbb{F}_d$ over which the $\mathbb{Z}/6\mathbb{Z}$ curve Γ_0 has rank $2, 3, 4, 5$. The fields $\mathbb{F}_d$ with the smallest absolute d-values for the curve Γ_0 of rank $2, 3, 4, 5$ are $\mathbb{F}_{22}, \mathbb{F}_{874}, \mathbb{F}_{-5069}, \mathbb{F}_{1578610}$, respectively. Two essentially different $\mathbb{Z}/14\mathbb{Z}$ curves over $\mathbb{Q}(\sqrt{22})$ we found this way are produced by $u_1 = 1/8$ and $u_2 = 7/4$. The former curve has rank 0, whereas the latter has rank 1. The mentioned u-values correspond to the two generators of Γ_0, which has rank 2 over $\mathbb{F}_{22}$. Similarly, the four $\mathbb{Z}/14\mathbb{Z}$ curves over $\mathbb{Q}(\sqrt{2233})$ produced by $u_1 = 4/7$ (curve of rank 2), $u_2 = 13$ (rank 1), $u_3 = 1/28$ (rank 0), and $u_4 = -2/11$ (rank 1) are all essentially different, as all the u-values correspond to pairwise linearly independent combinations of the three generators of the curve Γ_0 over $\mathbb{F}_{2233}$.

Let us now turn back to the search of high rank elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$. With the help of `MAGMA` we first found that for $u = 11/5$ (or equivalently for $u = -3/8$), the produced curve has rank 3 – the current record for torsion group $\mathbb{Z}/14\mathbb{Z}$ (see Dujella [3]). The curve in Weierstrass normal form is

$$y^2 = x^3 - \frac{64\left(214412\sqrt{430} - 4876337\right)}{390625}\, x^2 - \frac{146767085568\left(9559\sqrt{430} - 198202\right)}{152587890625}\, x,$$

and is isomorphic to the curve

$$y^2 = x^3 - (214412\sqrt{430} - 4876337)\, x^2 - 12^7(9559\sqrt{430} - 198202)\, x$$

with the three independent points of infinite order

$$P_1 = (85536\sqrt{430} - 1844856, 117398160\sqrt{430} - 2391265800),$$

$$P_2 = (-45684\sqrt{430} + 945999, 197481240\sqrt{430} - 4096319040),$$

$$P_3 = (150336\sqrt{430} + 5895504, 389901600\sqrt{430} + 19611195120).$$

Later, we found that also $u = \frac{\sqrt{-2759}-11}{32}$ produces a $\mathbb{Z}/14\mathbb{Z}$ curve of rank 3:

$$\begin{aligned} y^2 = x^3 &- (5327056844923892\sqrt{-2759} + 151212615362621956)\, x^2 \\ &+ 6525845768\,(236459153187683150165981\sqrt{-2759} \\ &- 271862776771967684826119 99)\, x \end{aligned}$$

with the three generators

$$\begin{aligned} P_1 = (&3390432200076922\sqrt{-2759} + 362094129708044162, \\ &407419421343476192247168 0\sqrt{-2759} \\ &+ 346721377875091153164172 80), \end{aligned}$$

$$\begin{aligned} P_2 = (&2744055515797882\sqrt{-2759} + 421484961222088322, \\ &334461704243056525848960 0\sqrt{-2759} \\ &+ 573359924912883988890816 00), \end{aligned}$$

$$\begin{aligned} P_3 = (&29793656566415482\sqrt{-2759} - 1346439443735230078, \\ &- 179125012373434156396224 00\sqrt{-2759} \\ &- 271401316258614487548819 8400). \end{aligned}$$

Another parametrisation of elliptic curves over a quadratic field with torsion group $\mathbb{Z}/14\mathbb{Z}$ is given by Rabarison [12, Sec. 4.2]. The defining polynomial of the quadratic field is $w^2 + wu + w = u^3 - u$, which leads to

$$w_{1,2} = \frac{-(u+1) \pm \sqrt{1 - 2u + u^2 + 4u^3}}{2}.$$

The parametrised curve is

$$E_{\tilde{a},\tilde{b}} : \; y^2 + \tilde{a}xy + \tilde{b}y = x^3 + \tilde{b}x^2$$

with

$$\tilde{a} = \frac{u^4 - u^3w + u^2(2w-4) - uw + 1}{(u+1)(u^3 - 2u^2 - u + 1)},$$

$$\tilde{b} = \frac{u(1-u)\big(u^5 - u^4 - 2u^3w + u^2 + u(2w-1) - w\big)}{(u+1)^2(u^3 - 2u^2 - u + 1)^2},$$

where the point $(0, 0)$ is a point of order 14.

Like Kubert's parametrisation for elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$ or $\mathbb{Z}/12\mathbb{Z}$, Rabarison's parametrisation for elliptic curves with torsion group $\mathbb{Z}/14\mathbb{Z}$ can be transformed to our parametrisation. For this, notice first that a and b depend on u and v. Now, for

$$v = \frac{u(1-4u-u^2+2z)}{(u-1)^2}$$

we obtain expressions for a and b which just depend on u and z. On the other hand, if we set

$$v = -\frac{u(u^2+2u-3-4w)}{(u-1)^2},$$

then, for

$$w = \frac{-(u+1)+z}{2},$$

we obtain exactly the same expressions for a and b (also depending just on u and z). A similar result we get for $\tilde{a}$ and $\tilde{b}$ by setting

$$w = \frac{u(u^2+2u-3)+v(u-1)^2}{4u}.$$

With respect to Rabarison's parametrisation, the curve given above with rank 3 obtained by $u = 11/5$ is

$$y^2 + \frac{-15835+792\sqrt{430}}{1160}\,xy + \frac{165(-46394+2\,237\sqrt{430})}{26912}\,y = x^3 + \frac{165(-46394+2237\sqrt{430})}{26912}\,x^2,$$

where three independent points of infinite order are:

$$P_1 = \left(\frac{85983835575-4146565170\sqrt{430}}{39891856}, \frac{27225(2574034836965503-124130941794256\sqrt{430})}{423791610918272}\right),$$

$$P_2 = \left(\frac{2298171927997-110831541546\sqrt{430}}{1777510688}, \frac{121(69150183657283025-3334717851516528\sqrt{430})}{105982297261312}\right),$$

$$P_3 = \left(\frac{-36778174426785+1824475255680\sqrt{430}}{15921363350048}, \frac{1089(1274259861468796925-61481356412574002\sqrt{430})}{89843234417066460928}\right).$$

5.2. *A normal form for elliptic curves with torsion group* $\mathbb{Z}/\mathbf{14}\mathbb{Z}$. For $u \in \mathbb{Q}$, $d := 1 - 2u + u^2 + 4u^3$, $z := \sqrt{d}$, and

$$v := \frac{u\big(1 - 4u - u^2 \pm 2\sqrt{1 - 2u + u^2 + 4u^3}\big)}{(u-1)^2},$$

the elliptic curve

$$\Gamma_{u,v}:\ y^2 = (u^2-1)^2(v^2-1)\cdot\frac{1}{x} + (3u^2 + 2u^3v + v^2 - 2) + (u^2-1)x$$

over the quadratic field $\mathbb{Q}(\sqrt{d})$ has torsion group $\mathbb{Z}/14\mathbb{Z}$. Notice that $\Gamma_{u,v}$ has two points at infinity, namely $(0,1,0)$, which is the point of order 1, and $(1,0,0)$, which is the point of order 2. The finite torsion points of $\Gamma_{u,v}$ are given in the following table:

Order	x-coordinate	y-coordinate
14	$u^2 - 1$	$\pm u(u+v)$
7	$v^2 - 1$	$\pm u(u+v)$
14	$-(u-1)(v-1)$	$\pm(u+v)$
7	$-(u+1)(v+1)$	$\pm(u+v)$
14	$-\dfrac{(u+1)^2(v-1)}{(u-1)}$	$\pm(3u-v)$
7	$-\dfrac{(u-1)^2(v+1)}{(u+1)}$	$\pm(3u-v)$

As a matter of fact we would like to mention that for

$$a := (u^2-1)^2(v^2-1), \quad b := 3u^2 + 2u^3v + v^2 - 2, \quad c := (u^2-1),$$

if (x_0, y_0) is a point on $\Gamma_{u,v}$, then $(a/x_0,\ ay_0/x_0)$ is a point on

$$\Gamma_{b,\,ac}:\ y^2 = x^3 + bx^2 + acx,$$

where the point at infinity $(1,0,0)$ is moved to $(0,0)$.

6. Elliptic curves with torsion group $\mathbb{Z}/\mathbf{16}\mathbb{Z}$

In this section we use our geometric approach to construct a parametrisation of elliptic curves with torsion group $\mathbb{Z}/16\mathbb{Z}$.

Theorem 6.1. *Let* $\mathbb{F}$ *be a field containing* $\mathbb{Q}$. *Then there exists an elliptic curve* $\Gamma_{a,b}$ *over* $\mathbb{F}$ *with torsion group* $\mathbb{Z}/16\mathbb{Z}$ *if and only if for some* $\alpha \in$

$\mathbb{F} \setminus \{-1, 0, 1\}$,

$$\alpha\sqrt{1-\alpha^2} \pm \sqrt{\alpha(\alpha^2-1)\Big(1+\sqrt{1-\alpha^2}-\alpha\big(1+\alpha+\sqrt{1-\alpha^2}\,\big)\Big)}$$

or

$$\alpha\sqrt{1-\alpha^2} \pm \sqrt{\alpha(\alpha^2-1)\Big(1-\sqrt{1-\alpha^2}-\alpha\big(1+\alpha-\sqrt{1-\alpha^2}\,\big)\Big)}$$

belongs to $\mathbb{F}$.

PROOF. Assume that the curve $\Gamma_{\alpha,\beta,\gamma,\delta}$ over $\mathbb{F}$ has torsion group $\mathbb{Z}/16\mathbb{Z}$ and that for the points A and $\bar{A}$, which correspond to 2 and 10, respectively, we have $A = (1, 1)$ and $\bar{A} = (-1, -1)$. Furthermore, let B and D be points on $\Gamma_{\alpha,\beta,\gamma,\delta}$ which correspond to 7 and 4, respectively. Then, the group table with respect to these points, their inverses and their conjugates, is given as follows:

Elements of $\mathbb{Z}/16\mathbb{Z}$	0	1	2	3	4	5	6	7	8
Points on $\Gamma_{\alpha,\beta,\gamma,\delta}$	$\mathscr{O}$	$-\bar{B}$	A		D		$-\bar{A}$	B	T
Points on $\Gamma_{\alpha,\beta,\gamma,\delta}$	$\mathscr{O}$	$\bar{B}$	$-A$		$\bar{D}$		$\bar{A}$	$-B$	T
Elements of $\mathbb{Z}/16\mathbb{Z}$	16	15	14	13	12	11	10	9	8

Because A and $\bar{A}$ are on $\Gamma_{\alpha,\beta,\gamma,\delta}$, we have $\beta = 1$ and $\delta = -(\alpha + \gamma)$. Now, since $A \# \bar{A} = D$, the point D is on the line passing through A and $\bar{A}$, and therefore, $D = (x_0, x_0)$ for some $x_0 \in \mathbb{F}$. Since D is on $\Gamma_{\alpha,\beta,\gamma,\delta}$ and D is different from A and $\bar{A}$, we obtain

$$x_0 = -\alpha. \tag{6.2}$$

Furthermore, we have $-D = \bar{D}$, which implies that for $\bar{D} = (\bar{x}_0, -x_0)$ we have $x_0 = \bar{x}_0$, where by Fact 2.3,

$$\bar{x}_0 = \frac{\alpha + \delta(x_0\gamma + \beta)}{\gamma(x_0 - \delta)}.$$

Thus, by (6.2) we obtain

$$\gamma = \frac{1-\alpha^2}{2\alpha},$$

and for a point $P = (x, y)$ on $\Gamma_{\alpha,\beta,\gamma,\delta}$, the x-coordinate of $\bar{P}$ is

$$\bar{x} = -\frac{x + 2\alpha + x\alpha^2}{1 + 2x\alpha + \alpha^2}.$$

Now, let us consider the points B and $\bar{B}$. Since $B \# \bar{B} = \bar{A}$, the point $\bar{A}$ is on the line g passing through B and $\bar{B}$. Let λ be the slope of g, then

$$g(x) = \lambda x + (\lambda - 1).$$

Because the line g passes through the the points $B = (x_1, y_1)$ and $\bar{B} = (\bar{x}_1, -y_1)$, we must have $g(x_1) = -g(\bar{x}_1)$, and solving this equation for λ gives

$$\lambda_0 = \frac{1 + 2x_1\alpha + \alpha^2}{1 + 2x_1\alpha + \alpha^2 + \alpha(x_1^2 - 1)}.$$

Furthermore, we must have that the points B and $\bar{B}$ are on $\Gamma_{\alpha,\beta,\gamma,\delta}$, *i.e.*,

$$g_{\lambda_0}(x_1)^2 = \big(\lambda_0 x_1 + (\lambda_0 - 1)\big)^2 = \frac{\alpha + \beta x_1 + \gamma x_1^2}{x_1 - \delta} = \frac{x_1^2 + 2x_1\alpha - \alpha^2(x_1^2 - 2)}{1 + 2x_1\alpha + \alpha^2},$$

which finally gives us the following four values for x_1:

$$-1 - \frac{\sqrt{1-\alpha^2}}{1+\alpha} \pm \frac{\sqrt{\alpha(\alpha^2-1)\Big(1 + \sqrt{1-\alpha^2} - \alpha\big(1 + \alpha + \sqrt{1-\alpha^2}\,\big)\Big)}}{\alpha(1+\alpha)}$$

$$-1 + \frac{\sqrt{1-\alpha^2}}{1+\alpha} \pm \frac{\sqrt{\alpha(\alpha^2-1)\Big(1 - \sqrt{1-\alpha^2} - \alpha\big(1 + \alpha - \sqrt{1-\alpha^2}\,\big)\Big)}}{\alpha(1+\alpha)}$$

Since x_1 and α belong to $\mathbb{F}$, this implies that at least one of

$$z_{1,3} = \alpha\sqrt{1-\alpha^2} \pm \sqrt{\alpha(\alpha^2-1)\Big(1 + \sqrt{1-\alpha^2} - \alpha\big(1 + \alpha + \sqrt{1-\alpha^2}\,\big)\Big)}$$

and

$$z_{2,4} = \alpha\sqrt{1-\alpha^2} \pm \sqrt{\alpha(\alpha^2-1)\Big(1 - \sqrt{1-\alpha^2} - \alpha\big(1 + \alpha - \sqrt{1-\alpha^2}\,\big)\Big)}$$

belongs to $\mathbb{F}$. On the other hand, if at least one of z_1, z_2, z_3, z_4 belongs to $\mathbb{F}$, then also the corresponding x_1 belongs to $\mathbb{F}$, which shows that there exists an elliptic curve $\Gamma_{a,b}$ with torsion group $\mathbb{Z}/16\mathbb{Z}$ over $\mathbb{F}$. □

As a consequence of Theorem 6.1 we obtain:

COROLLARY 6.2. *Let* $m \in \mathbb{Q} \setminus \{-1, 0, 1\}$ *and let*

$$d_1 = (m^4 - 1)(m^2 - 2m - 1), \quad d_2 = m(m^2 + 1)(m^2 + 2m - 1).$$

Then for each $i \in \{1, 2\}$ *there is an elliptic curve over* $\mathbb{Q}(\sqrt{d_i})$ *with torsion group* $\mathbb{Z}/16\mathbb{Z}$.

PROOF. If $\alpha \in \mathbb{Q}$ is such that $\sqrt{1-\alpha^2} \in \mathbb{Q}$, then $\alpha = \alpha_1$ or $\alpha = \alpha_2$, where

$$\alpha_1 = \frac{m^2 - 1}{m^2 + 1} \quad \text{or} \quad \alpha_2 = \frac{2m}{m^2 + 1}.$$

Let z_1, z_2 be as above. If we substitute α by α_1 into z_1, then $z_1 \in \mathbb{Q}(\sqrt{d_1})$, and if we substitute α by α_2 into z_2, then $z_2 \in \mathbb{Q}(\sqrt{d_2})$. □

For each $m_1 \neq \pm 1$, let $m_2 := 1/m_1$, $m_3 := (m_1 - 1)/(m_1 + 1)$, $m_4 := 1/m_3$, and for $j \in \{1, 2, 3, 4\}$ let $m_{-j} := -m_j$. Furthermore, for $i \in \{1, 2\}$ and $k \in \{\pm 1, \pm 2, \pm 3, \pm 4\}$ let $d_{i,k}$ be the value of d_i obtained from m_k. Now, for each value $m_1 \neq \pm 1$ we obtain four groups of four pairwise isomorphic elliptic curves with torsion group $\mathbb{Z}/16\mathbb{Z}$ over the same quadratic field $\mathbb{Q}(\sqrt{d})$. The four groups are given by the following pairs $(m_k, d_{i,k})$ over the respective quadratic fields:

over $\mathbb{Q}(\sqrt{d_{1,1}})$:	$(m_1,\, d_{1,1})$	$(m_{-2},\, d_{1,-2})$	$(m_3,\, d_{2,3})$	$(m_{-4},\, d_{2,-4})$
over $\mathbb{Q}(\sqrt{d_{2,1}})$:	$(m_1,\, d_{2,1})$	$(m_{-2},\, d_{2,-2})$	$(m_3,\, d_{1,3})$	$(m_{-4},\, d_{1,-4})$
over $\mathbb{Q}(\sqrt{d_{1,-1}})$:	$(m_{-1},\, d_{1,-1})$	$(m_2,\, d_{1,2})$	$(m_{-3},\, d_{2,-3})$	$(m_4,\, d_{2,4})$
over $\mathbb{Q}(\sqrt{d_{2,-1}})$:	$(m_{-1},\, d_{2,-1})$	$(m_2,\, d_{2,2})$	$(m_{-3},\, d_{1,-3})$	$(m_4,\, d_{1,4})$

For example, over $\mathbb{Q}(\sqrt{d_1})$ we obtain the parametrisation

$$y^2 = x^3 + \big((m^4 - 1)^2 - 4m^2(m^4 + 1)\big)x^2 + 16m^8 x, \tag{6.3}$$

or equivalently

$$y^2 + \left(\frac{m^4 + 2m^2 - 1}{m^2}\right) xy + (m^4 - 1)\, y = x^3 + (m^2 - 1)\, x^2,$$

and over $\mathbb{Q}(\sqrt{d_2})$, with respect to another normal form, we obtain the parametrisation

$$y^2 + (1 - c)\, xy - b\, y = x^3 - b\, x^2$$

where

$$b = -\frac{m(m-1)^2}{(m^2+1)^2} \quad \text{and} \quad c = -\frac{2m(m-1)^2}{(m^2+1)(m+1)^2}.$$

6.1. *High rank elliptic curves with torsion group* $\mathbb{Z}/\mathbf{16}\mathbb{Z}$. In [12, p. 38], Rabarison listed a single $\mathbb{Z}/16\mathbb{Z}$ curve of rank 1 over $\mathbb{Q}(\sqrt{10})$, and in [1], an example of a curve of rank 2 over $\mathbb{Q}(\sqrt{1\,785})$ is provided. In [10], Najman used the 2-isogeny method to construct a $\mathbb{Z}/16\mathbb{Z}$ curve over $\mathbb{Q}(\sqrt{34\,720\,105})$ of proven rank 3 and conditional rank 4, starting from a rank-3 curve with the torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. The three curves mentioned above can be reproduced by using formula (6.3) for $m = 3$, $m = 4$, and $m = 12/17$, respectively.

As [3] lists only the smallest, by magnitude, d-values for quadratic fields $\mathbb{Q}(\sqrt{d})$, the third author has shown that a $\mathbb{Z}/16\mathbb{Z}$ curve of conditional rank 4 can be built over $\mathbb{Q}(\sqrt{17\,381\,446})$ by using $m = 29/65$ in formula (6.3). This is a current record for $\mathbb{Z}/16\mathbb{Z}$ curves of conditional rank 4.

By implementing the 2-isogeny method [10], we have found new $\mathbb{Z}/16\mathbb{Z}$ curves of rank 3 for $m = 5/8$, $m = 3/13$, and $m = 13/3$ over $\mathbb{Q}(\sqrt{413\,049})$, $\mathbb{Q}(\sqrt{105\,910})$, and $\mathbb{Q}(\sqrt{36\,490})$, respectively. For $m = 3/13$, it required a point search performed by `MAGMA` up to height 10^{16} on the 8-coverings of the quadratic twist by $d = 105\,910$.

By using $m = -9$ in formula (6.3), we found a new $\mathbb{Z}/16\mathbb{Z}$ curve over $\mathbb{Q}(\sqrt{205})$ isomorphic to

$$y^2 = x^3 + 10226878\,x^2 + 43046721\,x,$$

that ties a current record for $\mathbb{Z}/16\mathbb{Z}$ curves of rank 3, with the three generators

$$P_1 = (4961, -1108800\,\sqrt{205}),$$

$$P_2 = (67081/81, -1935672760/729),$$

$$P_3 = (279524961, -332320219200\,\sqrt{205}).$$

Uncovering generators on the d-twists to prove rank 4 unconditionally for $\mathbb{Z}/16\mathbb{Z}$ curves over $\mathbb{Q}(\sqrt{d})$ remains a challenge. The only `MAGMA` calculation that has not resulted in a crash corresponds to the curve with $m = 12/17$. After successfully performing both 8-descent and 3-descent in 68 hours, no generator was found on the quadratic twist.

Acknowledgements.

We would like to thank Andrej Dujella for many fruitful hints. We appreciate Zev Klagsbrun's expertise that resolved isogeneity challenges for $\mathbb{Z}/14\mathbb{Z}$ curves, and his efforts to uncover the last generator in the mentioned $\mathbb{Z}/10\mathbb{Z}$ case. We commend Yusuf AttarBashi for sieving promising candidates in $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/12\mathbb{Z}$ torsion groups, and discovering many high-rank exemplars in the process. We also thank the referee for the careful reading and the corrections.

References

[1] J. Aguirre, A. Dujella, M. Jukić Bokun, and J. C. Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields*, Period. Math. Hungar. **68(2)** (2014), 222–230.

[2] A. Dujella, *High rank elliptic curves with prescribed torsion*, https://web.math.pmf.unizg.hr/∼duje/tors/tors.html. Accessed: 2022-05-18.

[3] A. Dujella, *High rank elliptic curves with prescribed torsion over quadratic fields*, https://web.math.pmf.unizg.hr/∼duje/tors/torsquad.html. Accessed: 2022-05-18.

[4] A. Dujella, Number Theory, Manualia Universitatis Studiorum Zagrabiensis, Zagreb, 2021.

[5] L. Halbeisen and N. Hungerbühler, *Constructing cubic curves with involutions*, Beitr. Algebra Geom. (to appear)
open access: https://link.springer.com/article/10.1007/s13366-021-00593-0

[6] D. S. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. Lond. Math. Soc. (3) **33(2)** (1976), 193–237.

[7] L. Kulesz, *Courbes elliptiques de rang élevé, possédant un sous-groupe de torsion non trivial sur* $\mathbb{Q}$, (article provided by Andrej Dujella).

[8] L. Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over* $\mathbb{Q}$, Acta Arith. **108(4)** (2003), 339–356.

[9] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48(177)** (1987), 243–264.

[10] F. Najman, *Some rank records for elliptic curves with prescribed torsion over quadratic fields*, An. Ştiinţ. "Ovidius" Constanţa. Ser. Mat. **22** (2014), 215–219.
[11] F. P. Rabarison, *Construction of elliptic curves with high rank and large torsion group*, (article provided by Andrej Dujella).
[12] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144(1)** (2010), 17–52.
[13] H. Schroeter, Die Theorie der ebenen Curven dritter Ordnung, B. G. Teubner, Leipzig, 1888.
[14] L. C. Washington, Elliptic Curves: Number Theory and Cryptography, CRC Press, Taylor & Francis Group, Boca Raton, 2nd edition, 2008.

Geometrijski pristup eliptičkim krivuljama s torzijskim grupama $\mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ i $\mathbb{Z}/16\mathbb{Z}$

Lorenz Halbeisen, Norbert Hungerbühler, Arman Shamsi Zargar, Maksym Voznyy

Sažetak. Dajemo nove parametrizacije eliptičkih krivulja u Weierstrassovom normalnom obliku $y^2 = x^3 + ax^2 + bx$ s torzijskim grupama $\mathbb{Z}/10\mathbb{Z}$ i $\mathbb{Z}/12\mathbb{Z}$ nad $\mathbb{Q}$, te sa $\mathbb{Z}/14\mathbb{Z}$ i $\mathbb{Z}/16\mathbb{Z}$ nad kvadratnim poljima. Iako su parametrizacije ekvivalentne onima koje su dali Kubert i Rabarison, s novim parametrizacijama pronašli smo tri familije eliptičkih krivulja s torzijskom grupom $\mathbb{Z}/12\mathbb{Z}$ i pozitivnim rangom. Osim toga, pronašli smo eliptičke krivulje s torzijskom grupom $\mathbb{Z}/14\mathbb{Z}$ i rangom 3 – što je novi rekord za takve krivulje – kao i neke nove eliptičke krivulje s torzijskom grupom $\mathbb{Z}/16\mathbb{Z}$ i rangom 3.

Lorenz Halbeisen
Department of Mathematics
ETH Zentrum Rämistrasse 101
8092 Zürich, Switzerland
E-mail: lorenz.halbeisen@math.ethz.ch

Norbert Hungerbühler
Department of Mathematics
ETH Zentrum Rämistrasse 101
8092 Zürich, Switzerland
E-mail: norbert.hungerbuehler@math.ethz.ch

Arman Shamsi Zargar
Department of Mathematics and Applications
University of Mohaghegh Ardabili
Ardabil, Iran
E-mail: zargar@uma.ac.ir

Maksym Voznyy
Department of Technology
Stephen Leacock CI
Toronto District School Board
Toronto, Canada
E-mail: maksym.voznyy@tdsb.on.ca