An Elementary Approach to
Elliptic Curves with Torsion Group
\( \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \) or \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \)

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

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

key-words: Elliptic curve, prescribed torsion group

2010 Mathematics Subject Classification: 11G05 11D09

Abstract

Let \( \text{Tor}_{10}, \text{Tor}_{12}, \text{Tor}_{2 \times 6}, \) and \( \text{Tor}_{2 \times 8} \) be the set of all regular, rational elliptic curves with torsion group \( \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}, \) and \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}, \) respectively. We provide simple maps which assign to each positive rational number \( \frac{p}{q} \neq 1 \) a curve in \( \text{Tor}_{10}, \) a curve in \( \text{Tor}_{12}, \) a curve in \( \text{Tor}_{2 \times 6} \) (except for \( \frac{p}{q} = \frac{1}{2} \)), and a curve in \( \text{Tor}_{2 \times 8}, \) respectively. The maps are such that each curve in \( \text{Tor}_{10}, \text{Tor}_{12}, \text{Tor}_{2 \times 6}, \) or \( \text{Tor}_{2 \times 8} \) is isomorphic to the image of some positive rational number. For example, the so far only elliptic curve in \( \text{Tor}_{12} \) with rank 4 is isomorphic to the curve which corresponds to the rational 726/133. Even though the maps we provide are equivalent to the parametrisations discovered by Kubert [11], our approach is elementary and does not use any tools from algebraic geometry.

1 Basic Results

It is well-known that every rational cubic curve with a rational point can be transformed into Weierstrass Normal Form

\[
y^2 = x^3 + ax^2 + bx + c
\]

with \( a, b, c \in \mathbb{Q} \) (see Silverman and Tate [13, Sec. 1.3]). Moreover, if the cubic has a rational point of order 2, then we can assume that \( c = 0 \) (see Silverman and Tate [13, Sec. 2.1]).

Let now

\[
\Gamma_{a,b} : y^2 = x^3 + ax^2 + bx
\]
with \( a, b \in \mathbb{Q} \) be a cubic and let \( T := (0, 0) \). Then \( T \) belongs to \( \Gamma_{a,b} \) and \( T + T = \mathcal{O} \), where \( \mathcal{O} \) denotes the neutral element of the Mordell–Weil group of \( \Gamma_{a,b} \). If \( A \) is a point on \( \Gamma_{a,b} \), then we call the point \( \tilde{A} := T + A \) the **conjugate of** \( A \). Since \( T + T = \mathcal{O} \), we have

\[
\tilde{A} = T + A = T + T + A = \mathcal{O} + A = A.
\]

Furthermore, for points \( A, B \) on an elliptic curve \( \Gamma \), 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 result gives a connection between conjugate points and tangents (see Figure 1).

**Fact 1.** If \( A, \tilde{A}, B \) are three points on \( \Gamma_{a,b} \) which lie on a straight line, then \( A \# A = \tilde{B} \).

**Proof.** If \( A, \tilde{A}, B \) are three points on \( \Gamma_{a,b} \) on a straight line, then \( A + \tilde{A} = -B \). Thus, \( A + T + A = T + A + A = -B \), which implies

\[
A + A = T + (T + A + A) = T + (-B) = (-T) + (-B) = -(T + B) = -\tilde{B},
\]

and therefore, the line \( AB \) is tangent to \( \Gamma_{a,b} \) with contact point \( A \), i.e., \( A \# A = \tilde{B} \).

\( q.e.d. \)

![Figure 1: Conjugate points and tangents.](image-url)
In homogeneous coordinates, the curve \( y^2 = x^3 + ax^2 + bx \) becomes

\[
\Gamma : Y^2Z = X^3 + aX^2Z + bXZ^2.
\]

Assume now that \( \tilde{A} = (\frac{n_0}{m_0}, \frac{n_1}{m_1}, 1) \) is a rational point on the cubic \( \Gamma \), where \( n_0, m_0, n_1, m_1 \) are integers and \( n_0 \neq 0 \neq n_1 \). Then the point \( (1, 1, 1) \) is on the curve

\[
\frac{n_1^2}{m_1^2} Y^2 Z = \frac{n_0^3}{m_0^3} X^3 + a \frac{n_0^2}{m_0^2} X^2 Z + b \frac{n_0}{m_0} X Z^2.
\]

Now, by exchanging \( X \) and \( Z \) (i.e., \( (X, Y, Z) \mapsto (Z, Y, X) \)), dehomogenising with respect to the third coordinate (i.e., \( (Y, X, Z) \mapsto (\frac{Y}{Z}, \frac{X}{Z}, 1) \)), and multiplying with \( m_1^2/n_1^2 \), 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

\[
\alpha = \frac{n_0^3 \cdot m_1^2}{m_0^3 \cdot n_1^2}, \quad \beta = \frac{n_0^2 \cdot m_1^2}{m_0^2 \cdot n_1^2}, \quad \gamma = b \cdot \frac{n_0 \cdot m_1^2}{m_0 \cdot n_1^2}.
\]

Notice that since \( A = (1, 1) \) is on \( \Gamma_{\alpha, \beta, \gamma} \), we have \( \alpha + \beta + \gamma = 1 \).

A generalisation of this observation is given by the following

**Lemma 2.** Let \( \tilde{A}_0 = (\frac{n_0}{m_0}, \frac{n_1}{m_1}) \) be a rational point on the cubic \( \Gamma_{a, b} : y^2 = x^3 + ax^2 + bx \), where \( a, b \in \mathbb{Q}, n_0, m_0, n_1, m_1 \in \mathbb{Z} \), and \( n_0 \neq 0 \neq n_1 \).

(a) Then there exists a rational projective transformation \( \Phi \) which maps the curve \( \Gamma_{a, b} \) to \( \Gamma_{\alpha, \beta, \gamma} : y^2 x = \alpha + \beta x + \gamma x^2 \) and \( \tilde{A}_0 \) to \( A_0 = (1, 1) \), where \( \alpha + \beta + \gamma = 1 \).

(b) If \( \tilde{A}_0 = \tilde{P} + \tilde{P} \) for some rational point \( \tilde{P} \) on \( \Gamma_{a, b} \), then \( \alpha \) is a square, i.e., \( \sqrt{\alpha} \in \mathbb{Q} \).

(c) If \( \tilde{A}_0 \) and \( \alpha \) are as in (b) and if \( B = (x_2, y_2) \) is a rational point on \( \Gamma_{\alpha, \beta, \gamma} \) with \( y_2 \neq 0 \) and \( B = Q + Q \) for some rational point \( Q \), then the \( x \)-coordinate of \( B \) is a square.

**Proof.** (a) follows directly from the observation above.

(b) If \( \tilde{A}_0 = (\tilde{x}_0, \tilde{y}_0) \) is a rational point on \( \Gamma_{a, b} \) with \( \tilde{y}_0 \neq 0 \) and \( \tilde{A}_0 = \tilde{P} + \tilde{P} \) for some \( \tilde{P} = (\tilde{x}_1, \tilde{y}_1) \), then, by Silverman and Tate [13, Sec. 1.4],

\[
\tilde{x}_0 = \left( \frac{\tilde{x}_1^2 - b}{2\tilde{y}_1} \right)^2.
\]

Hence, if \( \tilde{A}_0 = (\frac{n_0}{m_0}, \frac{n_1}{m_1}) \), then \( \frac{n_0}{m_0} \) is a square, i.e., there are \( \nu, \mu \in \mathbb{Z} \) such that \( n_0 = \nu^2 \) and \( m_0 = \mu^2 \), and therefore we have

\[
\alpha = \frac{n_0^3 \cdot m_1^2}{m_0^3 \cdot n_1^2} = \left( \frac{\nu^3 \cdot m_1}{\mu^3 \cdot n_1} \right)^2.
\]
(c) Let \( \tilde{B} := \Phi^{-1}(B) \) and let \( \tilde{Q} := \Phi^{-1}(Q) \). Then \( \tilde{B} = \tilde{Q} + \tilde{Q} \), and similar as above we have that for \( \tilde{B} = (\tilde{x}_2, \tilde{y}_2) \), \( \tilde{x}_2 \) is a square, say \( \tilde{x}_2 = \frac{r^2}{\gamma^2} \). Now, for \( \tilde{A}_0 = (\frac{\nu^2}{\mu}, \frac{m_1}{m_1}) \) we obtain

\[
B = \left( \frac{\nu^2 \cdot s^2}{\mu^2 \cdot r^2}, \frac{m_1 \cdot \nu^2 \cdot s^2}{n_1 \cdot \mu^2 \cdot r^2} \cdot \tilde{y}_2 \right),
\]

which shows that the \( x \)-coordinate of \( B \) is a square. \( \Box \)

In homogeneous coordinates, the neutral element of \( \Gamma_{\alpha,\beta,\gamma} \) is \( \Theta = (0, 1, 0) \) and the image under \( \Phi \) 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 can compute the conjugate of a point by the following

**Fact 3.** Let \( P = (x_1, y_1) \) be a point on \( \Gamma_{\alpha,\beta,\gamma} \). Then

\[
\tilde{P} = \left( \frac{\alpha}{\gamma x_1}, -y_1 \right).
\]

**Proof.** Let \( P = (x_1, y_1) \) be a point on \( \Gamma_{\alpha,\beta,\gamma} \). Then

\[
y_1^2 = \frac{\alpha}{x_1} + \beta + \gamma x_1,
\]

which implies that \( x_1 \) is a root of

\[
x^2 \gamma + x(\beta - y_1^2) + \alpha = \frac{(x - x_1)(x \cdot \gamma x_1 - \alpha)}{x_1}.
\]

The other root is \( \frac{\alpha}{\gamma x_1} \) and we obtain \( \tilde{P} = \left( \frac{\alpha}{\gamma x_1}, -y_1 \right) \). \( \Box \)

The next result can be found in Schroeter \[12\], but without proof (see Figure 2).

**Proposition 4.** Let \( A = (x_0, y_0) \) be an arbitrary but fixed point on \( \Gamma_{\alpha,\beta,\gamma} \). For every point \( P \) on \( \Gamma_{\alpha,\beta,\gamma} \) which is different from \( A \) and \( A \), let \( g := AP \) and \( \bar{g} := A\bar{P} \). Then the mapping \( I_A : g \mapsto \bar{g} \) is a line involution.

**Proof.** It is enough to show that there exists a point \( \zeta_0 \) (called the centre of the involution) on the line \( h : x = 0 \), such that the product of the distances between \( \zeta_0 \) and the intersections of \( g \) and \( \bar{g} \) with \( h \) is constant.

Since \( \tilde{T} = T + T = \Theta \), with respect to \( T \) we have \( g : y = y_0 \) and \( \bar{g} : x = x_0 \), which implies that \( \zeta_0 = (0, y_0) \). Now, let \( P = (x_1, y_1) \) be a point on \( \Gamma_{\alpha,\beta,\gamma} \) which is different from \( A, \bar{A}, T, \Theta \), and let \( g := AP \) and \( \bar{g} := A\bar{P} \). Since \( \tilde{P} = \left( \frac{\alpha}{\gamma x_1}, -y_1 \right) \), the slopes \( \lambda_P \) and \( \lambda_{\tilde{P}} \) of \( g \) and \( \bar{g} \), respectively, are

\[
\lambda_P = \frac{y_1 - y_0}{x_1 - x_0} \quad \text{and} \quad \lambda_{\tilde{P}} = \frac{-y_1 - y_0}{\alpha \gamma x_1 - x_0}.
\]

Thus, the distances \( s_P \) and \( s_{\tilde{P}} \) between \( \zeta_0 \) and the intersections of \( g \) and \( \bar{g} \) with \( h \), respectively, are

\[
s_P = -\frac{x_0(y_1 - y_0)}{x_1 - x_0} \quad \text{and} \quad s_{\tilde{P}} = \frac{x_0(y_1 + y_0) \cdot \gamma x_1}{\alpha - \gamma x_1 x_0}.
\]
Now,
\[ s_P \cdot s_P = -\frac{x_0^2(y_1 - y_0)(y_1 + y_0)\gamma x_1}{\gamma x_1} = -\frac{x_0^2(y_1^2 - y_0^2)\gamma x_1}{(x_1 - x_0)(\alpha - \gamma x_0x_1)}, \]
and using the fact that for \( i \in \{0, 1\}, \ y_i^2 = \frac{2i}{\alpha_i} + \beta + \gamma x_i, \) we obtain
\[ s_P \cdot s_P = \gamma \cdot x_0, \]
which is independent of the particular point \( P = (x_1, y_1). \)

q.e.d.

Notice that, since involutions are projectively invariant, Proposition 4 holds for all elliptic curves.

The parametrisation of elliptic curves with prescribed torsion group, and in particular the search for such curves of high rank, has a long tradition. We refer in this regard to the extensive literature on this subject: [1–11].
2 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 $\mathbb{Z}/10\mathbb{Z}$. Each element of the group $\mathbb{Z}/10\mathbb{Z} = \{0, 1, \ldots, 9\}$ corresponds to a rational point on $\Gamma_{a,b}$. Let $T$ be the unique point of order 2. Then $T$ correspond to 5. Furthermore, let $\bar{A}$ be the rational point on $\Gamma_{a,b}$ which corresponds to 2. Then $\bar{A}$ is of order 5. Finally, let $\bar{B}$ be the rational point on $\Gamma_{a,b}$ which corresponds to 6. Then $\bar{B} + \bar{B} = \bar{A}$. Now, by Lemma 2.(a), there is a projective transformation $\Phi$ which maps the curve $\Gamma_{a,b}$ to the curve $\Gamma_{\alpha,\beta,\gamma}$ and the point $\bar{A}$ to the point $A = (1, 1)$. Moreover, since $\bar{B} + \bar{B} = \bar{A}$, by Lemma 2.(b) we obtain that $\alpha$ is a square, say 

$$\alpha = u^2 \quad \text{for some } u \in \mathbb{Q}.$$ 

Let $B := \Phi(\bar{B})$ and $T := \Phi(T)$. Then for $A, -A, \bar{A}, \ldots$ we obtain the following correspondence between these points on $\Gamma_{\alpha,\beta,\gamma}$ and the elements of the group $\mathbb{Z}/10\mathbb{Z}$:

<table>
<thead>
<tr>
<th>elements of $\mathbb{Z}/10\mathbb{Z}$</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
</tr>
</thead>
<tbody>
<tr>
<td>points on $\Gamma_{\alpha,\beta,\gamma}$</td>
<td>$\emptyset$</td>
<td>$\bar{B}$</td>
<td>$A$</td>
<td>$-A$</td>
<td>$-B$</td>
<td>$T$</td>
<td>$B$</td>
<td>$\bar{A}$</td>
<td>$-A$</td>
<td>$-\bar{B}$</td>
</tr>
</tbody>
</table>

By definition, we have (see Figure 3):

(i) $A \# A = B$

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

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

Lemma 5. If $B = (x_2, y_2)$, then 

$$x_2 = \frac{4\alpha}{(\alpha - \gamma)^2}.$$

Proof. Let $g := AB$ and $\bar{g} := A\bar{B}$. Then, by Proposition 4, $I_A : g \mapsto \bar{g}$ is a line involution. Let $s_B$ and $s_{\bar{B}}$ be as in the proof of Proposition 4. Then, since $A = (1, 1)$, $s_B \cdot s_{\bar{B}} = \gamma$.

We first compute $s_{\bar{B}}$. Notice that by (ii), $\bar{g} = A\bar{A}$. Let $\tilde{g} : y = \tilde{\lambda}x + d$. Then, since $\tilde{A} = (\frac{\alpha}{\gamma}, -1)$, we have 

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

and therefore 

$$s_{\bar{B}} = \frac{2\gamma}{\alpha - \gamma}.$$ 

Now, since $s_B \cdot s_{\bar{B}} = \gamma$, it follows that 

$$s_B = \frac{\alpha - \gamma}{2}.$$
Figure 3: A curve $\Gamma_{\alpha,\beta,\gamma}$ with torsion group $\mathbb{Z}/10\mathbb{Z}$.

Notice that $g : y = -\frac{\alpha-\gamma}{2}x + d'$.

In the next step we use (i) which states that the line $AB$ is tangent to $\Gamma_{\alpha,\beta,\gamma}$ with contact point $A$: The line $AB$ is of the form

$$y = -\frac{\alpha - \gamma}{2}x + \frac{\alpha - \gamma + 2}{2}.$$

Thus,

$$y^2x = \left(\frac{\alpha - \gamma}{2}\right)^2 x^3 - \frac{(\alpha - \gamma)(\alpha - \gamma + 2)}{2} x^2 + \left(\frac{\alpha - \gamma + 2}{2}\right)^2 x,$$

where

$$\frac{(\alpha - \gamma)(\alpha - \gamma + 2)}{2} = \frac{(\alpha - \gamma)^2}{2} + \alpha - \gamma.$$

Since

$$\alpha + \beta x + \gamma x^2 - y^2 x = -\left(\frac{\alpha - \gamma}{2}\right)^2 x^3 + \left(\frac{(\alpha - \gamma)^2}{2} + \alpha\right) x^2 + \left(\beta - \left(\frac{\alpha - \gamma + 2}{2}\right)^2\right) x + \alpha$$

has a double zero at $x = 1$ and a third zero at $x = x_2$, we obtain by Vieta’s Theorem

$$x_2 = \frac{4\alpha}{(\alpha - \gamma)^2}.$$

q.e.d.

Since $\alpha = u^2$ for $u \in \mathbb{Q}$, we obtain as an immediate consequence of Lemma 5

**Corollary 6.** If $B = (x_2, y_2)$, then $x_2 = v^2$ for some $v \in \mathbb{Q}$, i.e., $x_2 = \frac{p^2}{q^2}$ for some $p, q \in \mathbb{Z}$, $q \neq 0$.  

7
The following result gives a relation between \( u, v, \) and \( \gamma \).

**Lemma 7.** If \( \alpha = u^2 \) and \( x_2 = v^2 \), then

\[
\gamma = u^2 - \frac{2u}{v}.
\]

**Proof.** By Lemma 5 we have \( x_2 = \frac{4\alpha}{(\alpha - \gamma)^2} \). So, since \( \alpha = u^2 \) and \( x_2 = v^2 \), we have

\[
x_2 = \frac{4u^2}{(u^2 - \gamma)^2} = \left(\frac{2u}{u^2 - \gamma}\right)^2 = v^2,
\]

which implies \( v = \frac{2u}{u^2 - \gamma} \), and hence, \( \gamma = u^2 - \frac{2u}{v} \).

\( q.e.d. \)

The next result connects \( u \) and \( v \).

**Proposition 8.** If \( \alpha = u^2, x_2 = v^2 \), and the curve \( \Gamma_{\alpha,\beta,\gamma} \) is regular, then we have

\[
u = \frac{2v^2}{(v - 1)(v + 1)^2} \quad \text{or} \quad u = \frac{2v^2}{(v - 1)^2(v + 1)}.
\]

**Proof.** If \( B = (x_2, y_2) \), then \( -B = (x_2, -y_2) \). Now, since by (iii), the points \( -B, -\bar{B}, \bar{A} \) are collinear and \( x_2 = \frac{4\alpha}{(\alpha - \gamma)^2} \), we have

\[
y_2 = \frac{\alpha - \gamma}{2}x_2 - \frac{\alpha - \gamma}{2} - 1.
\]

Let \( g : y = \lambda x + d \) be the equation of the line through the points \( -B, -\bar{B}, \bar{A} \). Then, with respect to the points \( -B \) and \( \bar{A} \), where \( \bar{A} = \left(\frac{\alpha}{\gamma}, -1\right) \), we have

\[
\lambda = \frac{-y_2 + 1}{x_2 - \frac{\alpha}{\gamma}}.
\]

On the other hand, with respect to the points \( -B \) and \( -\bar{B} \), where \( -\bar{B} = \left(\frac{\alpha}{\gamma x_2}, y_2\right) \), we have

\[
\lambda = \frac{-2y_2}{x_2 - \frac{\alpha}{\gamma x_2}}.
\]

Thus, for \( \alpha = u^2 \) and \( \gamma = u^2 - \frac{2u}{v} \), we obtain

\[
u = \frac{2v^2}{(v - 1)(v + 1)^2}, \quad u = \frac{2v^2}{(v - 1)^2(v + 1)}, \quad u = \frac{2}{v},
\]

where the solution \( u = \frac{2}{v} \) leads to \( \gamma = 0 \), which corresponds to a singular curve \( \Gamma_{\alpha,\beta,\gamma} \).

\( q.e.d. \)

We are now ready to prove the main result of this section.
Theorem 9. Let \( \frac{p}{q} \neq 1 \) be a positive rational in lowest terms and let
\[
a_1 = (p^2 + q^2)(p^4 - 2p^3q - 6p^2q^2 + 2pq^3 + q^4), \quad b_1 = 16p^5q^5(p^2 + pq - q^2).
\]

Then, the curve
\[
\Gamma_{a_1,b_1} : y^2 = x^3 + a_1x^2 + b_1x
\]
is an elliptic curve with torsion group \( \mathbb{Z}/10\mathbb{Z} \). Conversely, if \( \Gamma_{a,b} \) is a regular elliptic curve with torsion group \( \mathbb{Z}/10\mathbb{Z} \), then there exists a positive rational \( \frac{p}{q} \) such that \( \Gamma_{a,b} \) is isomorphic to \( \Gamma_{a_1,b_1} \).

Proof. Let \( v = \frac{p}{q} \) be a positive rational and let
\[
u_1 = \frac{2v^2}{(v-1)(v+1)^2} \quad \text{and} \quad \nu_2 = \frac{2v^2}{(v-1)(v+1)}.
\]
Furthermore, let \( \alpha_1 = u_1^2, \alpha_2 = u_2^2 \), and for \( i \in \{1,2\} \), let \( \gamma_i = u_i^2 - \frac{2u_i}{v} \) and \( \beta_i = 1 - (\alpha_i + \gamma_i) \).
Then, by our construction above and by Proposition 8, for \( i \in \{1,2\} \),
\[
\Gamma_\alpha_{i,\beta_i,\gamma_i} : Y^2X = \alpha Z^3 + \beta XZ^2 + \gamma X^2Z
\]
are elliptic curves with torsion group \( \mathbb{Z}/10\mathbb{Z} \). Now, by exchanging \( X \) and \( Z \) and dehomogenising with respect to \( Z \), we obtain the curves
\[
\tilde{\Gamma}_\alpha_{\tilde{\alpha}_i,\tilde{\beta}_i,\tilde{\gamma}_i} : \tilde{y}^2 = \alpha \tilde{x}^3 + \beta \tilde{x}^2 + \gamma \tilde{x},
\]
and after multiplying with \( \alpha_i^2 \) we get
\[
(\alpha_i \tilde{y})^2 = (\alpha_i \tilde{x})^3 + \beta_i (\alpha_i \tilde{x})^2 + \alpha_i \gamma_i (\alpha_i \tilde{x}).
\]
Thus, for \( \tilde{x} := \alpha_i \tilde{x}, \tilde{y} := \alpha_i \tilde{y}, \tilde{\alpha}_i := \beta_i, \) and \( \tilde{\beta}_i := \alpha_i \gamma_i, \) we finally obtain the curves
\[
\Gamma_{\tilde{\alpha}_i,\tilde{\beta}_i} : \tilde{y}^2 = \tilde{x}^3 + \tilde{\alpha}_i \tilde{x}^2 + \tilde{\beta}_i \tilde{x}.
\]
By definition, we have
\[
\tilde{a}_1 = \frac{(p^2 + q^2)(p^4 - 2p^3q - 6p^2q^2 + 2pq^3 + q^4)}{(p-q)^2(p+q)^4}, \quad \tilde{b}_1 = \frac{16p^5q^5(p^2 + pq - q^2)}{(p-q)^4(p+q)^8},
\]
\[
\tilde{a}_2 = \frac{(p^2 + q^2)(p^4 + 2p^3q - 6p^2q^2 - 2pq^3 + q^4)}{(p-q)^4(p+q)^2}, \quad \tilde{b}_2 = \frac{16p^5q^5(-p^2 + pq + q^2)}{(p-q)^6(p+q)^4}.
\]
Thus, by setting
\[
x := \frac{\tilde{x}}{(p-q)^2(p+q)^4} \quad \text{and} \quad y := \frac{\tilde{y}}{(p-q)^3(p+q)^6} \quad \text{for} \ i = 1,
\]
and
\[
x := \frac{\tilde{x}}{(p-q)^4(p+q)^2} \quad \text{and} \quad y := \frac{\tilde{y}}{(p-q)^6(p+q)^3} \quad \text{for} \ i = 2,
\]
we finally obtain the curves $\Gamma_{a_i,b_i}$, where
\[
  a_2 = (p^2 + q^2)(p^4 + 2p^3q - 6p^2q^2 - 2pq^3 + q^4), \quad b_2 = 16p^5q^5(-p^2 + pq + q^2).
\]

In order to emphasise that $a_i$ and $b_i$ depend on the fraction $\frac{p}{q}$, we write $a_i(\frac{p}{q})$ and $b_i(\frac{p}{q})$, respectively. First notice that for $i \in \{1, 2\}$, $a_i(\frac{p}{q}) = a_i(\frac{-q}{p})$ and $b_i(\frac{p}{q}) = b_i(\frac{-q}{p})$, and that for $\{i, j\} = \{1, 2\}$, $a_i(\frac{p}{q}) = a_j(\frac{q}{p})$ and $b_i(\frac{p}{q}) = b_j(\frac{q}{p})$.

Assume now that $\Gamma_{a,b}$ is an elliptic curve with torsion group $\mathbb{Z}/10\mathbb{Z}$. Then we find a non-zero rational $\frac{p}{q}$ such that $\Gamma_{a,b}$ is isomorphic to either $\Gamma_{a_1,b_1}$ or $\Gamma_{a_2,b_2}$. If $\frac{p}{q} > 0$ and $\Gamma_{a,b} \cong \Gamma_{a_1,b_1}$, then we are done. If $\frac{p}{q} < 0$ and $\Gamma_{a,b} \cong \Gamma_{a_1,b_1}$, consider $\frac{q}{p}$, if $\frac{p}{q} > 0$ and $\Gamma_{a,b} \cong \Gamma_{a_2,b_2}$, consider $\frac{q}{p}$, and if $\frac{p}{q} < 0$ and $\Gamma_{a,b} \cong \Gamma_{a_2,b_2}$, consider $-\frac{p}{q}$.

As a consequence of Theorem 9 we get that in order to investigate elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$, it is enough to consider curves $\Gamma_{a_1,b_1}$ for positive rational numbers $\frac{p}{q}$.

Kubert's Parametrisation of Curves with Torsion Group $\mathbb{Z}/10\mathbb{Z}$

In [11, 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 $\mathbb{Z}/10\mathbb{Z}$:
\[
  \tau = \frac{p}{q}, \quad d = \frac{\tau^2}{\tau - (\tau - 1)^2}, \quad c = \tau(d - 1), \quad b = cd.
\]

After transforming Kubert's curve into the form
\[
y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x
\]
we find
\[
  \tilde{a} = -(2p^2 - 2pq + q^2)(4p^4 - 12p^3q + 6p^2q^2 + 2pq^3 - q^4), \quad \tilde{b} = 16p^5(p - q)^5(p^2 - 3pq + q^2),
\]
and since $\tilde{a}(\frac{p}{q+p}) = a_1(\frac{p}{q})$ and $\tilde{b}(\frac{p}{q+p}) = b_1(\frac{p}{q})$, the two parametrisations are equivalent.

Curves of Rank at Least 3

Recall that the Calkin-Wilf sequence
\[
s_0 = 1, \quad s_{n+1} = \frac{1}{2\lfloor s_n \rfloor - s_n + 1}
\]
lists every positive rational number exactly once. By checking the first 22'000 fractions in this sequence we found with the help of magma that the following fractions lead to elliptic curves with torsion group $\mathbb{Z}/10\mathbb{Z}$ and rank 3:
The fractions highlighted in boldface correspond to new curves which are nor yet listed in [2] (status on June 11, 2020). For 463/335, neither magma nor sage could compute the rank of the corresponding elliptic curve.

As a matter of fact, we would like to mention that the fraction 280/1131 leads to the curve
\[ y^2 = x^3 + 2445233546783622841 x^2 - 45052118849993255238591966412800000 x \]
which is a curve of rank 4. This curve is isomorphic to the curve
\[ y^2 + xy = x^3 - 127381738643041574974581021420318985 x + 1749559404661203976686496413577998621608407092547225 \]
discovered by Dujella in 2005 (see [2]).

3 Elliptic Curves with Torsion Group \( \mathbb{Z}/12\mathbb{Z} \)

Let \( \Gamma_{a,b} : y^2 = x^3 + ax^2 + bx \) be a regular curve with torsion group \( \mathbb{Z}/12\mathbb{Z} \), let \( \tilde{A} \) be a point on \( \Gamma_{a,b} \) of order 6, and let \( \tilde{B} \) be such that \( \tilde{B} + \tilde{B} = \tilde{A} \). Furthermore, let \( \tilde{T} \) be the point of order 2 and let \( \tilde{C} = \tilde{A} \# \tilde{B} \). As in the previous section, there is a projective transformation \( \Phi \) which maps the curve \( \Gamma_{a,b} \) to the curve \( \Gamma_{\alpha,\beta,\gamma} \) and the point \( \tilde{A} \) to the point \( A = (1,1) \). Notice that since \( \tilde{B} + \tilde{B} = \tilde{A} \), by Lemma 2.(b) we obtain again that \( \alpha \) is a square, say
\[ \alpha = u^2 \quad \text{for some } u \in \mathbb{Q}. \]

Let \( B := \Phi(\tilde{B}), T := \Phi(\tilde{T}), \) and \( C := \Phi(\tilde{C}) \). Then, as above, for \( A, -A, \tilde{A}, \ldots \) we obtain the following correspondence between these points on \( \Gamma_{\alpha,\beta,\gamma} \) and the elements of the group \( \mathbb{Z}/12\mathbb{Z} \):

<table>
<thead>
<tr>
<th>( \mathbb{Z}/12\mathbb{Z} )</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Gamma_{\alpha,\beta,\gamma} )</td>
<td>( \emptyset )</td>
<td>( B )</td>
<td>( A )</td>
<td>( -C )</td>
<td>( -A )</td>
<td>( -B )</td>
<td>( T )</td>
<td>( \tilde{B} )</td>
<td>( \tilde{A} )</td>
<td>( C )</td>
<td>( -A )</td>
<td>( -B )</td>
</tr>
</tbody>
</table>

Figure 4 shows a curve \( \Gamma_{\alpha,\beta,\gamma} \) with the points in the table and some of the relevant geometric relations: For example, \( A \# A = \tilde{A} \) corresponds to the tangent in \( A \) passing through \( \tilde{A} \), and \( A \# B = C \) means that \( A, B, C \) are collinear.

We start by showing that \( \gamma \) is a square.
Lemma 10. $\gamma = w^2$ for some $w \in \mathbb{Q}$ and $x_3 = \frac{u}{w}$.

Proof. First notice that $\bar{C} = T + C = -C$. So, if $C = (x_3, y_3)$, then $\bar{C} = (x_3, -y_3)$. On the other hand, by Fact 3 we obtain $\bar{C} = (\frac{\alpha}{\gamma x_3}, -y_3)$. Thus, $x_3 = \frac{\alpha}{\gamma x_3}$, which implies

$$x_3 = \pm \sqrt{\frac{\alpha}{\gamma}} = \pm \sqrt{\frac{u}{\pm \sqrt{\gamma}}}.$$ 

Hence, $\gamma$ is a square, i.e., $\gamma = w^2$ for some $w \in \mathbb{Q}$, and $x_3 = \frac{u}{w}$. q.e.d.

The next result connects $u$ and $w$.

Lemma 11. If $u = \frac{p}{q}$, then $p^2 + q^2 = c^2$ for some $c \in \mathbb{Z}$ and

$$w = \pm 1 + \frac{c}{q}.$$ 

Proof. Let $A \# A = (x_2, y_2)$. Then, by Lemma 5, $x_2 = \frac{4\alpha}{(\alpha - \gamma)^2}$. On the other hand, since $A \# A = \bar{A}$, by Fact 3 we obtain $x_2 = \frac{\alpha}{\gamma}$. Thus, $\alpha = \frac{4\alpha}{(\alpha - \gamma)^2}$, i.e., $(\alpha - \gamma)^2 = 4\gamma$, and since $\alpha = u^2$ and $\gamma = w^2$, we obtain

$$(u^2 - w^2)^2 = 4w^2,$$

which implies that

$$w = \pm 1 \pm \sqrt{u^2 + 1}.$$
Now, for \( u = \frac{p}{q} \), we have
\[
 w = \pm 1 \pm \frac{\sqrt{p^2 + q^2}}{q},
\]
and since \( w \in \mathbb{Q} \), the integer \( p^2 + q^2 \) is a square, say \( p^2 + q^2 = c^2 \) for some \( c \in \mathbb{Z} \). Hence, we have \( w = \pm 1 + \frac{c}{q} \).

The equality \( p^2 + q^2 = c^2 \) leads to a kind of normal form for \( u \).

**Lemma 12.** There are \( m, n \in \mathbb{N} \) such that
\[
 u = \frac{m^2 - n^2}{2mn}.
\]

**Proof.** Assume that \( u = \frac{p}{q} \) with \( p \neq 0 \) and \( q > 0 \). Since by Lemma 11, \( p^2 + q^2 = c^2 \) for some \( c \in \mathbb{Z} \), there are \( m, n \in \mathbb{N} \) such that \( (m, n) = 1 \), either \( m \) or \( n \) is even, and either \( p = m^2 - n^2 \) and \( q = 2mn \), or \( p = 2mn \) and \( q = m^2 - n^2 \). In the former case, we are done. In the latter case, let \( \tilde{m} = m + n \) and \( \tilde{n} = m - n \). Then \( \tilde{m} \) and \( \tilde{n} \) are both odd, and since just one of \( m \) and \( n \) is even and \( (m, n) = 1 \), we have \( (\tilde{m}, \tilde{n}) = 1 \). Let \( \tilde{p} = m^2 - \tilde{n}^2 \) and \( \tilde{q} = 2\tilde{m}\tilde{n} \). Then \( \tilde{p} = 4mn = 2p \) and \( \tilde{q} = 2(m^2 - n^2) = 2q \). Hence,
\[
 u = \frac{p}{q} = \frac{2p}{2q} = \frac{\tilde{p}}{\tilde{q}} = \frac{\tilde{m}^2 - \tilde{n}^2}{2\tilde{m}\tilde{n}},
\]
where \( (\tilde{m}, \tilde{n}) = 1 \), which completes the proof. \( q.e.d. \)

Let us now turn back to \( x_3 = \frac{u}{w} \), where by Lemma 10, \( x_3 \) is the \( x \)-coordinate of the point \( C \).

**Lemma 13.** Let \( u = \frac{m^2 - n^2}{2mn} \) where \( m, n \in \mathbb{N} \) and \( (m, n) = 1 \). Then there are \( r, s \in \mathbb{N} \) with \( (r, s) = 1 \), such that either
\[
 n = r^2 + s^2 \quad \text{and either} \quad m = (r \pm s)^2 \quad \text{or} \quad m = 2r^2,
\]
or
\[
 m = r^2 + s^2 \quad \text{and either} \quad n = (r \pm s)^2 \quad \text{or} \quad n = 2r^2.
\]

**Proof.** Assume that \( u = \frac{p}{q} \) with \( p \neq 0 \) and \( q > 0 \). Then, by Lemma 13, \( p = m^2 - n^2 \) and \( q = 2mn \) for some \( m, n \in \mathbb{N} \) with \( (m, n) = 1 \). Hence, since by Lemma 11, \( c^2 = p^2 + q^2 \), we obtain \( c = \pm(m^2 + n^2) \). Furthermore, we have
\[
 \alpha = u^2 = \frac{p^2}{q^2} = \frac{m^4 - 2m^2n^2 + n^4}{4m^2n^2}, \quad w = \pm 1 + \frac{c}{q} = \pm 1 \pm \frac{m^2 + n^2}{2mn}, \quad \gamma = w^2,
\]
and \( \beta = 1 - (\alpha + \gamma) \). Now, consider the point \( C = (x_3, y_3) \) where \( x_3 = \frac{u}{w} \). Then for \( y_3 \) we have
\[
 y_3 = \frac{\alpha}{x_3} + \beta + \gamma x_3,
\]

13
which implies that
\[ y_3 = \sqrt{\pm m(2n+m)} \quad \text{or} \quad y_3 = \sqrt{\pm n(2m+n)} . \]

Since \( y_3 \in \mathbb{Q} \) and since \( m, n \in \mathbb{N} \), we have that
\[ m(2n-m) = \square \quad \text{or} \quad n(2m-n) = \square . \]

By symmetry it is enough to consider the case when \( m(2n-m) = \xi^2 \) for some \( \xi \in \mathbb{Z} \). Let \( m = \mu + \nu \) and \( n = \mu \). Then
\[ m(2n-m) = (\mu + \nu)(2\mu - \mu - \nu) = \mu^2 - \nu^2 = \xi^2 . \]

Hence, we have \( \mu^2 = \xi^2 + \nu^2 \), which implies that there are \( r, s \in \mathbb{N} \) with \( (r, s) = 1 \), such that \( \mu = \pm(r^2 + s^2) \), and therefore, since \( n > 0 \), we have \( n = r^2 + s^2 \). Furthermore, we have either \( \nu = \pm 2rs \) or \( \nu = r^2 - s^2 \). In the former case we obtain \( m = (r \pm s)^2 \), and in the latter case we obtain \( m = 2r^2 \).

q.e.d.

We are now ready to prove the main result of this section.

**Theorem 14.** Let \( \frac{r}{s} \neq 1 \) be a positive rational in lowest term and let
\[ a_1 = 6r^8 + 48r^6s^2 + 12r^4s^4 - 2s^8, \quad b_1 = (r^2 - s^2)^6 (3r^2 + s^2)^2 . \]

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 \( \frac{r}{s} \) such that \( \Gamma_{a,b} \) is isomorphic to \( \Gamma_{a_1,b_1} \).

**Proof.** Similar as in the proof of Theorem 9, starting with \( r, s \in \mathbb{N} \) we can compute in different ways first \( m \) and \( n \), then \( p \) and \( q \), then \( u \) and \( w \), then \( \alpha, \beta, \gamma \), and finally we obtain the integers \( a_1 \) and \( b_1 \). As a matter of fact we would like to mention that because we can exchange \( m \) and \( n \), the 6 possibilities to compute \( m \) and \( n \) we have in Lemma 13 lead only to the following 3 possible pairs of values:
\[ a_1 = 6r^8 + 48r^6s^2 + 12r^4s^4 - 2s^8, \quad b_1 = (r^2 - s^2)^6 (3r^2 + s^2)^2 . \]

Notice that \( \tilde{a}_2(\frac{r}{s}) = \tilde{a}_3(-\frac{r}{s}) = \tilde{a}_3(-\frac{r}{s}) \) and \( \tilde{b}_2(\frac{r}{s}) = \tilde{b}_3(-\frac{r}{s}) = \tilde{b}_3(-\frac{r}{s}) \). Furthermore, we have
\[ \tilde{a}_2\left(\frac{r-s}{r+s}\right) = 2^2 \cdot a_1(\frac{r}{s}) \quad \text{and} \quad \tilde{b}_2\left(\frac{r-s}{r+s}\right) = 2^4 \cdot b_1(\frac{r}{s}) . \]

Now, since \( (x, y) \in \Gamma_{a_1,b_1} \) if and only if \( (2^2 \cdot x, 2^4 \cdot y) \in \Gamma_{2^2a_1,2^4b_1} \), we obtain that the curves \( \Gamma_{a_1(\frac{r}{s}),b_1(\frac{r}{s})} \) and \( \tilde{a}_2(\frac{r-s}{r+s}),\tilde{b}_2(\frac{r-s}{r+s}) \) are equivalent.

Finally, notice that \( a_1(\frac{r}{s}) = a_1(\frac{-r}{s}) \) and \( b_1(\frac{r}{s}) = b_1(\frac{-r}{s}) \), and therefore, by our construction we get that for every elliptic curve \( \Gamma_{a,b} \) with torsion group \( \mathbb{Z}/12\mathbb{Z} \) we find \( r, s \in \mathbb{N} \) with \( (r, s) = 1 \) such that \( \Gamma_{a,b} \) is isomorphic to \( \Gamma_{a_1,b_1} \).

q.e.d.
Kubert’s Parametrisation of Curves with Torsion Group $\mathbb{Z}/12\mathbb{Z}$

In [11, 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 $\mathbb{Z}/12\mathbb{Z}$:

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

After transforming Kubert’s curve into the form

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

we find

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

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

Now, since $\tilde{a}(\frac{s}{s-r}) = \tilde{a}_2(\frac{r}{s})$ and $\tilde{b}(\frac{s}{s-r}) = \tilde{b}_2(\frac{r}{s})$, these parametrisations are equivalent, and consequently, also the curves $\Gamma_{\tilde{a}, \tilde{b}}$ and $\Gamma_{a_1, b_1}$ are equivalent.

Curves of Rank at Least 2

By checking the first $3'441$ fractions $\frac{r}{s}$ of the Calkin-Wilf sequence we found with the help of magma 125 fractions which lead to elliptic curves of type $\Gamma_{\tilde{a}_2, \tilde{b}_2}$ with torsion group $\mathbb{Z}/12\mathbb{Z}$ and rank 2, and among these $3'441$ fractions, we even found some which lead to curves of type $\Gamma_{\tilde{a}_2, \tilde{b}_2}$ and rank 3, namely $88/65, 125/27, 86/13, 87/40, 13/86$. For some of the fractions, neither magma nor sage could compute the rank of the corresponding elliptic curve.

As a matter of fact, we would like to mention that until today (June 2020), up to isomorphisms only one curve of rank 4 is known, namely

$$y^2 + xy = x^3 - 4422329901784763147754792226039053294186858800x + 98943710602886706347390586357680210847183561679806360624530387016000$$

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

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

which is a curve of type $\Gamma_{a_1, b_1}$ and corresponds to the fraction $726/133$. 

15
4 Elliptic Curves with Torsion Group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

Let $\Gamma_{a,b} : y^2 = x^3 + ax^2 + bx$ be a regular curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, and let $\bar{A}$ be a point on $\Gamma_{a,b}$ of order 3. Furthermore, let $\bar{T} = (0,0)$, and let $\bar{S}$ be another point of order 2. Finally, for a point $\bar{P}$ on $\Gamma_{a,b}$, define $\bar{P}_1 := \bar{S} + \bar{P}$. As in the previous sections, there is a projective transformation $\Phi$ which maps the point $\bar{A}$ to the point $A = (1,1)$ and the curve $\Gamma_{a,b}$ to the curve $\Gamma_{\alpha,\beta,\gamma}$. Notice that since $\bar{A} \neq \bar{A} = \bar{A}$, $\alpha$ is a square, say $\alpha = \left(\frac{p}{q}\right)^2$ for some $\frac{p}{q} \in \mathbb{Q}$.

Let $T := \Phi(\bar{T})$ and $S := \Phi(\bar{S})$. Then, as above, for $A, -A, \bar{A}, \ldots$ we obtain the following correspondence between these points on $\Gamma_{\alpha,\beta,\gamma}$ and the elements of the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$:

<table>
<thead>
<tr>
<th>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$</th>
<th>$(0,0)$</th>
<th>$(0,1)$</th>
<th>$(0,2)$</th>
<th>$(0,3)$</th>
<th>$(0,4)$</th>
<th>$(0,5)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma_{\alpha,\beta,\gamma}$</td>
<td>$\mathcal{O}$</td>
<td>$\bar{A}$</td>
<td>$A$</td>
<td>$T$</td>
<td>$-A$</td>
<td>$\bar{A}$</td>
</tr>
<tr>
<td>$\Gamma_{\alpha,\beta,\gamma}$</td>
<td>$S$</td>
<td>$\bar{A}_1$</td>
<td>$A_1$</td>
<td>$\bar{S}$</td>
<td>$-A_1$</td>
<td>$\bar{A}_1$</td>
</tr>
<tr>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$</td>
<td>$(1,0)$</td>
<td>$(1,1)$</td>
<td>$(1,2)$</td>
<td>$(1,3)$</td>
<td>$(1,4)$</td>
<td>$(1,5)$</td>
</tr>
</tbody>
</table>

First, we compute $\gamma$ is terms of $p$ and $q$.

**Lemma 15.** If $\alpha = \left(\frac{p}{q}\right)^2$ for $\frac{p}{q} \in \mathbb{Q}$, then

$$\gamma = \frac{p(p \pm 2q)}{q^2}.$$  

**Proof.** First notice that $\bar{A} \neq \bar{A} = A$ and recall that $\bar{A} = (\frac{a}{\gamma},-1)$. Now, consider the line $g = A\bar{A}$. We have $g : \lambda x + d$, where

$$\lambda = \frac{1 + \frac{1}{\gamma} - \frac{\alpha}{\gamma}}{1 - \frac{\alpha}{\gamma}} = \frac{2\gamma}{\gamma - \alpha} = \frac{2q^2\gamma}{q^2\gamma - p^2}.$$  

On the other hand, we can compute $\lambda$ by the gradient of $\Gamma_{\alpha,\beta,\gamma}$ at the point $\bar{A}$, which gives us

$$\lambda = \frac{q^2\gamma^2 - p^2\gamma}{2p^2}.$$  

Hence, we have

$$\gamma(p^4 - 4p^2q^2 - 2p^2q^2\gamma + q^4\gamma^2) = 0,$$

which implies $\gamma = 0$ or $\gamma = \frac{p(p \pm 2q)}{q^4}$, where $\gamma = 0$ leads to a singular curve.  

**q.e.d.**

By considering the points $S$ and $\bar{S}$, we obtain the following

**Lemma 16.** If $\alpha = \left(\frac{p}{q}\right)^2$ for $\frac{p}{q} \in \mathbb{Q}$, then there are $k, l \in \mathbb{N}$ such that

$$p = l(k \pm l) \quad \text{and} \quad q = k^2.$$  

16
Proof. By Lemma 15 we have $\gamma = \frac{p(p+2q)}{q^2}$. Since the $y$-coordinate of the points $S$ and $\bar{S}$ equals 0, for $S = (x, 0)$ we have $\alpha + \beta x + \gamma x^2 = 0$, which leads to
\[p^2 - (2p^2 \pm 2pq + q^2)x + p(p \pm 2q)x^2 = 0.\]
Hence,
\[x = \frac{2p^2 \pm 2pq - q^2 + q\sqrt{q^2 \mp 4pq}}{2p(p \pm 2q)} \quad \text{or} \quad \frac{2p^2 \pm 2pq - q^2 - q\sqrt{q^2 \mp 4pq}}{2p(p \pm 2q)},\]
and since $x \in \mathbb{Q}$, we have $q^2 \mp 4pq = \Box$.

We first show that $q = (2l + 1)^2$ for some $l \in \mathbb{N}$: Let $t$ be a prime and assume that $t^{2j+1} \mid q$ and $t^{2j+2} \not\mid q$. Since $(p, q) = 1$ and $q^2 \mp 4pq = \Box$, we obtain $t \mid 4$, and hence, $t = 2$. Therefore, $q = 2 \cdot 2^j w$, for some odd $w$, where all odd primes which divide $w$ appear with an even power, i.e., $w$ is a square, say $w = v^2$ for some odd $v \in \mathbb{N}$. Thus,
\[q(q \mp 4p) = 2^{2j+1} v^2 (2^{2j+1} v^2 \mp 4p) = 2 \cdot 2^{2j} v^2 (2 \cdot 2^{2j+1} v^2 \mp 2 \cdot 2p).\]
Hence,
\[v^2 (2^{2j} v^2 \mp 2p) = \Box.\]
Since $(q, p) = 1$ and $2 \mid q, p$ is odd. So, we have $v^2 \equiv 1 \mod 8$, $2^{2j} v^2 \equiv 0, 1, 4 \mod 8$, and $2p \equiv 2, 6 \mod 8$, which shows that the equation $q^2 \mp 4pq = \Box$ does not have a solution in integers.

So, there is no prime $t$ such that $t^{2j+1} \mid q$ and $t^{2j+2} \not\mid q$, which implies that $q$ is a square, say $q = k^2$ for some $k \in \mathbb{N}$. Thus, we have $k^2 \mp 4p = \Box$, where $\Box = \frac{k^2}{4^j}$. In particular, $q$ has the same parity as $\Box$, and therefore, $\Box = (k \pm 2l)^2$ for some $l \in \mathbb{N}$, which implies that $p = l(k-l)$ in the case when $k^2 > \Box$, and $p = l(k+l)$ otherwise.

q.e.d.

Now, we are ready to prove the following

**Theorem 17.** Let $\frac{k}{l} \notin \{\frac{1}{2}, 1\}$ be a positive rational in lowest terms and let
\[a_1 = k^4 - 2k^3l + 4kl^3 - 2l^4, \quad b_1 = l^3(k-l)^3(2k-l)(k+l).\]
Then the curve
\[\Gamma_{a_1,b_1} : y^2 = x^3 + a_1x^2 + b_1x\]
is an elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Conversely, if $\Gamma_{a,b}$ is a regular elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, then there exists a positive rational $\frac{k}{l}$ such that $\Gamma_{a,b}$ is isomorphic to $\Gamma_{a_1,b_1}$.

**Proof.** The proof is analogous to the proof of Theorem 9: Similarly as in the that proof, we also obtain the values
\[a_2 = k^4 + 2k^3l - 4kl^3 - 2l^4, \quad b_2 = l^3(k+l)^3(l^2 + kl - 2k^2),\]
but one can show that $a_2(\frac{k}{l}) = a_1(\frac{k}{l^4})$ and that $b_2(\frac{k}{l}) = b_1(\frac{k}{l^4})$, thus, all values of $(a_2, b_2)$ appear also as values of $(a_1, b_1)$, and it is enough to consider the curves $\Gamma_{a_1,b_1}$. q.e.d.
Kubert’s Parametrisation of Curves with Torsion Group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

In [11, 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$:

$$\tau = \frac{k}{l}, \quad c = \frac{10 - 2\tau}{\tau^2 - 9}, \quad b = c + c^2.$$ 

After transforming Kubert’s curve into the form

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

we find

$$\tilde{a} = k^4 - 12k^3l + 30k^2l^2 + 228kl^3 - 759l^4$$

and

$$\tilde{b} = 128l^3(k - 5l)^3(k^2 - 9l^2).$$

Now, $\tilde{a}(\frac{l - 5k}{l - k}) = a_1(\frac{k}{l})$ and $\tilde{b}(\frac{l - 5k}{l - k}) = b_1(\frac{k}{l})$, which shows that these parametrisations are equivalent.

5 Elliptic Curves with Torsion Group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$

Let $\Gamma_{a,b} : y^2 = x^3 + ax^2 + bx$ be a regular curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$, let $\tilde{A}$ be a point on $\Gamma_{a,b}$ of order 4, and let $\tilde{B}$ be such that $\tilde{B} + \tilde{B} = \tilde{A}$. Furthermore, let $\tilde{C} = \tilde{A} + \tilde{B}$, let $\tilde{T} = (0,0)$, and let $\tilde{S}$ be another point of order 2. Finally, for a point $\tilde{P}$ on $\Gamma_{a,b}$, define $\tilde{P}_1 := \tilde{S} + \tilde{P}$. As in the previous sections, there is a projective transformation $\Phi$ which maps the point $\tilde{A}$ to the point $A = (1,1)$ and the curve $\Gamma_{a,b}$ to the curve $\Gamma_{a,b,\gamma}$. Notice that since $\tilde{B} + \tilde{B} = \tilde{A}$, $a$ is a square, say $a = (\frac{p}{q})^2$ for some $\frac{p}{q} \in \mathbb{Q}$.

Let $T := \Phi(\tilde{T})$, $B := \Phi(\tilde{B})$, $C := \Phi(\tilde{C})$, and $S := \Phi(\tilde{S})$. Then, as above, for $A, -A, \tilde{A}, \ldots$ we obtain the following correspondence between these points on $\Gamma_{a,b,\gamma}$ and the elements of the group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$:

<table>
<thead>
<tr>
<th>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$</th>
<th>(0, 0)</th>
<th>(0, 1)</th>
<th>(0, 2)</th>
<th>(0, 3)</th>
<th>(0, 4)</th>
<th>(0, 5)</th>
<th>(0, 6)</th>
<th>(0, 7)</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma_{a,b,\gamma}$</td>
<td>$\emptyset$</td>
<td>$B$</td>
<td>$A$</td>
<td>$C$</td>
<td>$T$</td>
<td>$B$</td>
<td>$A$</td>
<td>$C$</td>
</tr>
<tr>
<td>$\Gamma_{a,b,\gamma}$</td>
<td>$S$</td>
<td>$B_1$</td>
<td>$A_1$</td>
<td>$C_1$</td>
<td>$S_1$</td>
<td>$B_1$</td>
<td>$A_1$</td>
<td>$C_1$</td>
</tr>
<tr>
<td>$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$</td>
<td>(1, 0)</td>
<td>(1, 1)</td>
<td>(1, 2)</td>
<td>(1, 3)</td>
<td>(1, 4)</td>
<td>(1, 5)</td>
<td>(1, 6)</td>
<td>(1, 7)</td>
</tr>
</tbody>
</table>

First, we compute $\gamma$. 18
Lemma 18. $\gamma = \alpha$.

Proof. First notice that $\bar{A} = -A$ and recall that $\bar{A} = (\frac{\alpha}{\gamma}, -1)$ and $A = (1, -1)$. Thus, $\frac{\alpha}{\gamma} = 1$ which implies $\alpha = \gamma$. \hspace{1cm} q.e.d.

By considering the points $S$ and $\bar{S}$, we obtain the following

Lemma 19. If $\alpha = (\frac{p}{q})^2$ for $\frac{p}{q} \in \mathbb{Q}$, then there are $r, s \in \mathbb{N}$ with $(r, s) = 1$ such that $p = \pm rs$ and $q = \pm (r^2 + s^2)$.

Proof. Let $\alpha = \gamma = u^2$ and $u = \frac{p}{q}$. Since the $y$-coordinate of the points $S$ and $\bar{S}$ equals 0, for $S = (x, 0)$ we have $u^2 + (1 - 2u^2)x + u^2x^2 = 0$. Hence,

$$x = \frac{2u^2 - 1 \pm \sqrt{1 - 4u^2}}{2u^2},$$

and since $x \in \mathbb{Q}$, we have $1 - 4u^2 = \square$. Thus,

$$1 - \frac{4p^2}{q^2} = \frac{q^2 - 4p^2}{q^2} = \square,$$

which implies $q^2 - 4p^2 = q^2 - (2p)^2 = \square$. Since $(p, q) = 1$, there are some $r, s \in \mathbb{N}$ with $(r, s) = 1$ such that $p = \pm rs$ and $q = \pm (r^2 + s^2)$. \hspace{1cm} q.e.d.

Using the fact that $B \# B = -A$, we can show the following

Lemma 20. For $p = \pm rs$ and $q = \pm (r^2 + s^2)$ we find $m, n \in \mathbb{N}$ such that $r = 2mn$ and $s = m^2 - n^2$.

Proof. First notice that $B \# B = -A$ and recall that $-A = (1, -1)$. Let $B = (x_2, y_2)$ and consider the line $g : \lambda x + d$ through $B$ and $-A$. We can compute $\lambda$ and $d$ by the gradient of $\Gamma_{\alpha, \beta, \gamma}$ at the point $B$. In particular, we get

$$\lambda = \frac{r^4 + s^4 + 2r^2s^2x_2 - r^4y_2^2 - 2r^2s^2y_2^2 - s^4y_2^2}{2(r^2 + s^2)^2x_2y_2},$$

$$d = \frac{3r^2s^2 + 2r^4x_2 + 2s^4x_2 + r^2s^2x_2^2}{2(r^2 + s^2)^2x_2y_2},$$

and since $y_2 = \lambda x_2 + d$, we obtain

$$y_2^2 = \frac{(s^2 + r^2x_2)(r^2 + s^2x_2)}{(r^2 + s^2)^2x_2}.$$

On the other hand, we also have

$$\lambda = \frac{-1 - y_2}{1 - x_2},$$

19
which gives us
\[ x_2 = \pm r^2 + rs \pm s^2 \pm (r - s)\sqrt{r^2 + s^2}. \]
Since \( x_2 \in \mathbb{Q} \), we have \( r^2 + s^2 = \Box \), which implies that there are \( m, n \in \mathbb{N} \) with \( (m, n) = 1 \) such that \( r = 2mn \) and \( s = m^2 - n^2 \).

Now, we are ready to prove the following

**Theorem 21.** Let \( \frac{m}{n} \neq 1 \) be a positive rational in lowest terms and let
\[ a_1 = 16m^4n^4 + (m^2 - n^2)^4, \quad b_1 = 16m^4n^4(m^2 - n^2)^4. \]

Then the curve
\[ \Gamma_{a_1, b_1} : y^2 = x^3 + a_1x^2 + b_1x \]
is an elliptic curve with torsion group \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \). Conversely, if \( \Gamma_{a, b} \) is a regular elliptic curve with torsion group \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \), then there exists a positive rational \( \frac{m}{n} \) such that \( \Gamma_{a, b} \) is isomorphic to \( \Gamma_{a_1, b_1} \).

**Proof.** The proof is analogous to the proof of Theorem 9. q.e.d.

Notice that the coefficients \( a_1, b_1 \) in Theorem 21 are symmetric in \( m \) and \( n \). This means that it is enough to consider either the fractions \( \frac{m}{n} > 1 \) or the positive fractions \( \frac{m}{n} < 1 \), i.e., only every second element in the Calkin-Wilf sequence. Furthermore, we have
\[ a_1\left(\frac{m+n}{m-n}\right) = 16 \cdot a_1\left(\frac{m}{n}\right) \quad \text{and} \quad b_1\left(\frac{m+n}{m-n}\right) = 16^2 \cdot b_1\left(\frac{m}{n}\right), \]
which implies that the curves \( \Gamma_{a_1\left(\frac{m}{n}\right), b_1\left(\frac{m}{n}\right)} \) and \( \Gamma_{a_1\left(\frac{m+n}{m-n}\right), b_1\left(\frac{m+n}{m-n}\right)} \) are equivalent.

**Kubert’s Parametrisation of Curves with Torsion Group** \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \)

In [11, 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 \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \):
\[ \tau = \frac{m}{n}, \quad d = \frac{\tau(8\tau + 2)}{(8\tau^2 - 1)}, \quad c = \frac{(2d - 1)(d - 1)}{d}, \quad b = (2d - 1)(d - 1). \]

After transforming Kubert’s curve into the form
\[ y^2 = x^3 + \tilde{a}x^2 + \tilde{b}x, \]
we find
\[ \tilde{a} = 256m^4(2m + n)^4 + (4m^2 - (2m + n)^2)^4 \quad \text{and} \quad \tilde{b} = 256m^4n^4(2m + n)^4(4m + n)^4. \]

Now, \( \tilde{a}(\frac{m}{2(m-n)}) = a_1\left(\frac{m}{n}\right) \) and \( \tilde{b}(\frac{m}{2(m-n)}) = b_1\left(\frac{m}{n}\right) \), which shows that these parametrisations are equivalent.
References


