High-rank elliptic curves induced by Diophantine triples

Andrej Dujella

Department of Mathematics
University of Zagreb, Croatia
E-mail: duje@math.hr
URL: http://web.math.pmf.unizg.hr/~duje/

Joint work with Juan Carlos Peral
Torsion and rank of elliptic curves over $\mathbb{Q}$

Let $E$ be an elliptic curve over $\mathbb{Q}$.

By the Mordell-Weil theorem, the group $E(\mathbb{Q})$ of rationals points on $E$ is a finitely generated abelian group. Hence, it is the product of the torsion group and $r \geq 0$ copies of the infinite cyclic group:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r.$$
By Mazur’s theorem, we know that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups:

- $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$,
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$.

On the other hand, it is not known which values of rank $r$ are possible for elliptic curves over $\mathbb{Q}$. The “folklore” conjecture is that a rank can be arbitrary large, but it seems to be very hard to find examples with large rank. The current record is an example of elliptic curve over $\mathbb{Q}$ with rank $\geq 28$, found by Elkies in May 2006.
There is even a stronger conjecture that for any of 15 possible torsion groups $T$ we have $B(T) = \infty$, where

$$B(T) = \sup\{\text{rank } (E(\mathbb{Q})) : \text{torsion group of } E \text{ over } \mathbb{Q} \text{ is } T\}.$$ 

Montgomery (1987): Proposed the use of elliptic curves with large torsion group and positive rank in factorization.

It follows from results of Montgomery, Suyama, Atkin & Morain (Finding suitable curves for the elliptic curve method of factorization, 1993), that $B(T) \geq 1$ for all torsion groups $T$.

Womack (2000): $B(T) \geq 2$ for all $T$

D. (2003): $B(T) \geq 3$ for all $T$
\[ B(T) = \sup \{ \text{rank} (E(\mathbb{Q})) : E(\mathbb{Q})_{\text{tors}} \cong T \} \]

<table>
<thead>
<tr>
<th>( T )</th>
<th>( B(T) \geq )</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>28</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} )</td>
<td>19</td>
<td>Elkies (2009)</td>
</tr>
<tr>
<td>( \mathbb{Z}/3\mathbb{Z} )</td>
<td>13</td>
<td>Eroshkin (2007, 2008, 2009)</td>
</tr>
<tr>
<td>( \mathbb{Z}/4\mathbb{Z} )</td>
<td>12</td>
<td>Elkies (2006), D. &amp; Peral (2014)</td>
</tr>
<tr>
<td>( \mathbb{Z}/5\mathbb{Z} )</td>
<td>8</td>
<td>D. &amp; Lecacheux (2009), Eroshkin (2009)</td>
</tr>
<tr>
<td>( \mathbb{Z}/8\mathbb{Z} )</td>
<td>6</td>
<td>Elkies (2006), D., MacLeod &amp; Peral (2013)</td>
</tr>
<tr>
<td>( \mathbb{Z}/9\mathbb{Z} )</td>
<td>4</td>
<td>Fisher (2009), van Beek (2015)</td>
</tr>
<tr>
<td>( \mathbb{Z}/12\mathbb{Z} )</td>
<td>4</td>
<td>Fisher (2008)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} )</td>
<td>15</td>
<td>Elkies (2009)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} )</td>
<td>9</td>
<td>D. &amp; Peral (2012)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} )</td>
<td>6</td>
<td>Elkies (2006), D., Peral &amp; Tadić (2015)</td>
</tr>
</tbody>
</table>
Construction of high-rank curves

1. Find a parametric family of elliptic curves over $\mathbb{Q}$ that contains curves with relatively high rank (i.e. an elliptic curve over $\mathbb{Q}(t)$ with large generic rank); e.g. by Mestre’s polynomial method or by using elliptic curves induced by Diophantine triples.

2. Choose in given family best candidates for higher rank.

General idea: a curve is more likely to have large rank if $|E(\mathbb{F}_p)|$ is relatively large for many primes $p$.

Precise statement: Birch and Swinnerton-Dyer conjecture.
More suitable for computation: Mestre’s conditional upper bound (assuming BSD and GRH), Mestre-Nagao sums, e.g. the sum:

\[ s(N) = \sum_{p \leq N, \ p \ \text{prime}} \frac{|E(\mathbb{F}_p)| + 1 - p}{|E(\mathbb{F}_p)|} \log(p) \]

3. Try to compute the rank (Cremona’s program \texttt{mwrank} - very good for curves with rational points of order 2), or at least good lower and upper bounds for the rank.
\[ G(T) = \sup \{ \text{rank } E(\mathbb{Q}(t)) : E(\mathbb{Q}(t))_{\text{tors}} \cong T \}. \]

<table>
<thead>
<tr>
<th>( T )</th>
<th>( G(T) \geq )</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>18</td>
<td>Elkies (2006)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} )</td>
<td>11</td>
<td>Elkies (2009)</td>
</tr>
<tr>
<td>( \mathbb{Z}/3\mathbb{Z} )</td>
<td>7</td>
<td>Elkies (2007)</td>
</tr>
<tr>
<td>( \mathbb{Z}/4\mathbb{Z} )</td>
<td>5</td>
<td>Kihara (2004), Elkies (2007), D., Peral &amp; Tadić (2014)</td>
</tr>
<tr>
<td>( \mathbb{Z}/5\mathbb{Z} )</td>
<td>3</td>
<td>Lecacheux (2001), Eroshkin (2009), MacLeod (2014)</td>
</tr>
<tr>
<td>( \mathbb{Z}/7\mathbb{Z} )</td>
<td>1</td>
<td>Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009), MacLeod (2014)</td>
</tr>
<tr>
<td>( \mathbb{Z}/8\mathbb{Z} )</td>
<td>2</td>
<td>D. &amp; Peral (2012), MacLeod (2013)</td>
</tr>
<tr>
<td>( \mathbb{Z}/9\mathbb{Z} )</td>
<td>0</td>
<td>Kubert (1976)</td>
</tr>
<tr>
<td>( \mathbb{Z}/10\mathbb{Z} )</td>
<td>0</td>
<td>Kubert (1976)</td>
</tr>
<tr>
<td>( \mathbb{Z}/12\mathbb{Z} )</td>
<td>0</td>
<td>Kubert (1976)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} )</td>
<td>7</td>
<td>Elkies (2007)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} )</td>
<td>4</td>
<td>D. &amp; Peral (2012)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} )</td>
<td>2</td>
<td>D. &amp; Peral (2012), MacLeod (2013)</td>
</tr>
<tr>
<td>( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} )</td>
<td>0</td>
<td>Kubert (1976)</td>
</tr>
</tbody>
</table>
Diophantine $m$-tuples

Diophantus: Find four numbers such that the product of any two of them, increased by 1, is a perfect square:

\[
\left\{ \frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16} \right\}
\]

Fermat: \{1, 3, 8, 120\}

\[
\begin{align*}
1 \cdot 3 + 1 &= 2^2, \\
1 \cdot 8 + 1 &= 3^2, \\
1 \cdot 120 + 1 &= 11^2,
\end{align*}
\begin{align*}
3 \cdot 8 + 1 &= 5^2, \\
3 \cdot 120 + 1 &= 19^2, \\
8 \cdot 120 + 1 &= 31^2.
\end{align*}
\]
**Definition:** A set \( \{a_1, a_2, \ldots, a_m\} \) of \( m \) non-zero integers (rational numbers) is called a (rational) Diophantine \( m \)-tuple if \( a_i \cdot a_j + 1 \) is a perfect square for all \( 1 \leq i < j \leq n \).

**Conjecture:** There does not exist a Diophantine quintuple.

Baker & Davenport (1969):
\( \{1, 3, 8, d\} \Rightarrow d = 120 \)

D. & Pethő (1998): \( \{1, 3\} \) cannot be extended to a Diophantine quintuple

D. (2004): There does not exist a Diophantine sextuple. There are only finitely many Diophantine quintuples.
There is no known upper bound for the size of rational Diophantine tuples.

**Euler:** \(\{1, 3, 8, 120, \frac{777480}{8288641}\}\)

**Gibbs (1999):** \(\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\}\)

**D. (2009):** \(\{\frac{27}{35}, -\frac{35}{36}, -\frac{352}{315}, \frac{1007}{1260}, -\frac{5600}{4489}, \frac{72765}{106276}\}\)

**D., Kazalicki, Mikić, Szikszai (2015):** There are infinitely many rational Diophantine sextuples.
Let \( \{a, b, c\} \) be a (rational) Diophantine triple. Define nonnegative rational numbers \( r, s, t \) by

\[
ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2.
\]

In order to extend this triple to a quadruple, we have to solve the system

\[
ax + 1 = \Box, \quad bx + 1 = \Box, \quad cx + 1 = \Box. \quad (\ast)
\]

It is natural idea to assign to this system the elliptic curve

\[
E : \quad y^2 = (ax + 1)(bx + 1)(cx + 1),
\]

and we will say that elliptic curve \( E \) is \textit{induced by the Diophantine triple} \( \{a, b, c\} \).
Three rational points on $E$ of order 2:

$$T_1 = [-1/a, 0], \quad T_2 = [-1/b, 0], \quad T_3 = [-1/c, 0],$$

and also other obvious rational points

$$P = [0, 1], \quad S = [1/abc, 1/rst],$$

$$Q = [(rs + rt + st + 1)/abc, (r + s)(r + t)(s + t)/abc].$$

Note that $S = 2Q$.

By Mazur’s theorem: $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $m = 1, 2, 3, 4$.

D. & Mikić (2014): If $a, b, c$ are positive integers, then the cases $m = 2$ and $m = 4$ are not possible.
D. (2007), Aguirre & D. & Peral (2012): For each $1 \leq r \leq 11$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the rank equal to $r$.

D. (2007), D. & Peral (2014): For each $0 \leq r \leq 9$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and the rank equal to $r$.

D. (2007): For each $1 \leq r \leq 4$, there exists a Diophantine triple $\{a, b, c\}$ such that the elliptic curve $y^2 = (ax + 1)(bx + 1)(cx + 1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and the rank equal to $r$. 
D. (2007): For each $0 \leq r \leq 3$, there exists a Diophantine triple \{a, b, c\} such that the elliptic curve $y^2 = (ax+1)(bx+1)(cx+1)$ has the torsion group isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ and the rank equal to $r$.

Every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by a Diophantine triple (D., Campbell & Goins).
D. & Peral (2014):
Elliptic curves with the torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

Such curves have an equation of the form

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

The point $[x_1x_2, x_1x_2(x_1 + x_2)]$ is a rational point on the curve of order 4.

The coordinate transformation $x \mapsto \frac{x}{abc}, \ y \mapsto \frac{y}{abc}$ applied to the curve $E$ leads to $y^2 = (x + ab)(x + ac)(x + bc)$, and by translation we obtain the equation

$$y^2 = x(x + ac - ab)(x + bc - ab).$$
If we can find a Diophantine triple $a, b, c$ such that $ac - ab$ and $bc - ab$ are perfect squares, then the elliptic curve induced by $\{a, b, c\}$ will have the torsion subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We may expect that this curve will have positive rank, since it also contains the point $[ab, abc]$.

A convenient way to fulfill these conditions is to choose $a$ and $b$ such that $ab = -1$. Then $ac - ab = ac + 1 = s^2$ and $bc - ab = bc + 1 = t^2$. It remains to find $a$ and $c$ such that $\{a, -1/a, c\}$ is a Diophantine triple. A parametric solution is

$$a = \frac{\alpha \tau + 1}{\tau - \alpha}, \quad c = \frac{4\alpha \tau}{(\alpha \tau + 1)(\tau - \alpha)}.$$
After some simplifications, we get the elliptic curve
\[ y^2 = x^3 + 2(\alpha^2 + \tau^2 + 4\alpha^2\tau^2 + \alpha^4\tau^2 + \alpha^2\tau^4)x^2 
+ (\tau + \alpha)^2(\alpha\tau - 1)^2(\tau - \alpha)^2(\alpha\tau + 1)^2x \].

To increase the rank, we now force the points with \(x\)-coordinates
\[(\tau + \alpha)^2(\alpha\tau - 1)(\alpha\tau + 1) \quad \text{and} \quad (\tau + \alpha)(\alpha\tau - 1)^2(\tau - \alpha)\]
to lie on the elliptic curve. We get the conditions
\[\tau^2 + \alpha^2 + 2 = \Box \quad \text{and} \quad \alpha^2\tau^2 + 2\alpha^2 + 1 = \Box,\]
with a parametric solution
\[\tau = \frac{(3t^2 + 6t + 1)(5t^2 + 2t - 1)}{4t(t - 1)(3t + 1)(t + 1)},\]
\[\alpha = -\frac{(t + 1)(7t^2 + 2t + 1)}{t(t^2 + 6t + 3)}\].
We get the elliptic curve

\[ y^2 = x^3 + A(t)x^2 + B(t)x, \]

where

\[
A(t) = 2(87671889t^{24} + 854321688t^{23} + 3766024692t^{22} + 9923033928t^{21} \\
+ 17428851514t^{20} + 21621621928t^{19} + 19950275060t^{18} \\
+ 15200715960t^{17} + 11789354375t^{16} + 10470452464t^{15} + 8925222696t^{14} \\
+ 5984900048t^{13} + 2829340620t^{12} + 820299856t^{11} + 59930952t^{10} \\
- 66320528t^9 - 35768977t^8 - 9381000t^7 - 1017244t^6 + 262760t^5 \\
+ 159130t^4 + 41096t^3 + 6468t^2 + 600t + 25),
\]

\[
B(t) = (t^2 - 2t - 1)^2(69t^4 + 148t^3 + 78t^2 + 4t + 1)^2(13t^2 - 2t - 1)^2 \\
\times (9t^4 + 28t^3 + 18t^2 + 4t + 1)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2 \\
\times (9t^2 + 14t + 7)^2(31t^4 + 52t^3 + 22t^2 - 4t - 1)^2(3t^2 + 2t + 1)^2,
\]

with rank \( \geq 4 \) over \( \mathbb{Q}(t) \). Indeed, it contains the points whose \( x \)-coordinates are
\[
X_1 = (9t^4 + 28t^3 + 18t^2 + 4t + 1)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2 \\
   \times (69t^4 + 148t^3 + 78t^2 + 4t + 1)^2,
\]
\[
X_2 = (3t^2 + 2t + 1)(9t^2 + 14t + 7)^2(13t^2 - 2t - 1) \\
   \times (9t^4 + 28t^3 + 18t^2 + 4t + 1)(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2 \\
   \times (31t^4 + 52t^3 + 22t^2 - 4t - 1),
\]
\[
X_3 = (3t^2 + 2t + 1)(9t^2 + 14t + 7)^2(13t^2 - 2t - 1) \\
   \times (9t^4 + 28t^3 + 18t^2 + 4t + 1)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1) \\
   \times (69t^4 + 148t^3 + 78t^2 + 4t + 1),
\]
\[
X_4 = -(3t^2 + 2t + 1)^2(9t^2 + 14t + 7)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2 \\
   \times (31t^4 + 52t^3 + 22t^2 - 4t - 1)^2.
\]

and a specialization, e.g. \( t = 2 \), shows that the four points \( P_1, P_2, P_3, P_4 \), having these \( x \)-coordinates, are independent points of infinite order.

Moreover, since our curve has full 2-torsion, by applying the recent algorithm by Gusić & Tadić (2012, 2015) we can show that \( \text{rank}(E(\mathbb{Q}(t))) = 4 \) and that the four points \( P_1, P_2, P_3, P_4 \) are free generators of \( E(\mathbb{Q}(t)) \).
In the search for particular elliptic curves over \( \mathbb{Q} \) with torsion group \( \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \) and high rank, we considered solutions of

\[
\tau^2 + \alpha^2 + 2 = \square
\]

given by

\[
\tau = \frac{r^2 - s^2 - 2t^2 + 2v^2}{2(rt + sv)}, \quad \alpha = \frac{rs - 2tv}{rt + sv}.
\]

We covered the range \( |r| + |s| + |t| + |v| \leq 420 \).

We use sieving methods, which include computing Mestre-Nagao sum, Selmer rank and Mestre’s conditional upper bound, to locate good candidates for high rank, and then we compute the rank with \texttt{mwrank}.
In that way, we found five curves with rank 8 and one curve with rank equal to 9. The rank 9 curve corresponds to the parameters \((r, s, t, v) = (155, 54, 96, 106)\). The curve is induced by the Diophantine triple
\[
\left\{ \frac{301273}{556614}, -\frac{556614}{301273}, -\frac{535707232}{290125899} \right\}.
\]
The minimal Weierstrass form of the curve is
\[
y^2 = x^3 + x^2 - 6141005737705911671519806644217969840x + 5857433177348803158586285785929631477808095171159063188.
\]