High rank elliptic curves and related Diophantine problems

Andrej Dujella

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

Elliptic curves

Let $\mathbb{K}$ be a field. An *elliptic curve* over $\mathbb{K}$ is a nonsingular projective cubic curve over $\mathbb{K}$ with at least one $\mathbb{K}$-rational point. Each such curve can be transformed by birational transformations to the equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad (1)$$

which is called the *Weierstrass form*.

If char($\mathbb{K}$) $\neq 2, 3$, then the equation (1) can be transformed to the form

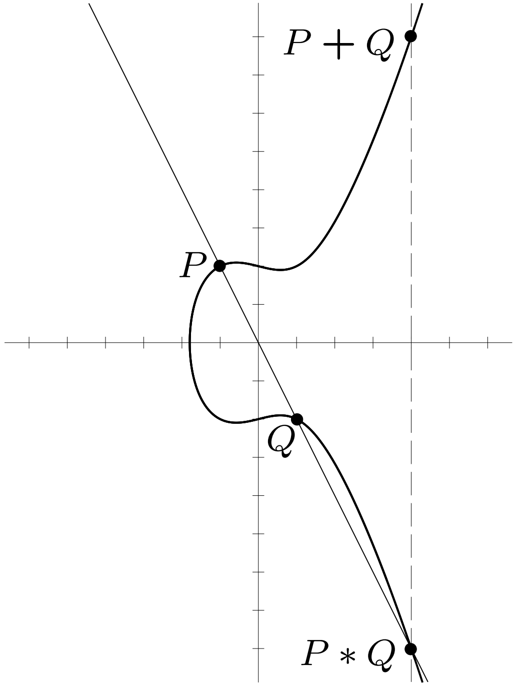
$$y^2 = x^3 + ax + b, \tag{2}$$

which is called the *short Weierstrass form*. Now the nonsingularity means that the cubic polynomial $f(x) = x^3+ax+b$ has no multiple roots (in algebraic closure $\overline{\mathbb{K}}$), or equivalently that the *discriminant* $\Delta = -4a^3 - 27b^2$ is nonzero.

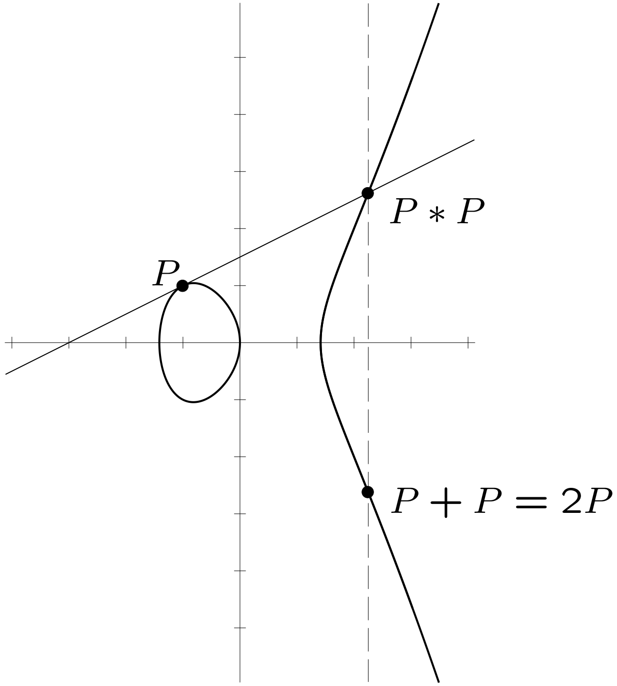
One of the most important facts about elliptic curves is that the set $E(\mathbb{K})$ of $\mathbb{K}$-rational points on an elliptic curve over $\mathbb{K}$ (affine points (x, y) satisfying (1) along with the point at infinity) forms an abelian group in a natural way.

In order to visualize the group operation, assume for the moment that $\mathbb{K} = \mathbb{R}$ and consider the set $E(\mathbb{R})$. Then we have an ordinary curve in the plane. It has one or two components, depending on the number of real roots of the cubic polynomial $f(x) = x^3 + ax + b$.

Let E be an elliptic curve over $\mathbb{R}$, and let P and Q be two points on E. We define $-P$ as the point with the same x-coordinate but negative y-coordinate of P. If P and Q have different x-coordinates, then the straight line though P and Q intersects the curve in exactly one more point, denoted by $P * Q$. We define $P + Q$ as $-(P * Q)$. If $P = Q$, then we replace the secant line by the tangent line at the point P. We also define $P + \mathcal{O} = \mathcal{O} + P = P$ for all $P \in E(\mathbb{R})$, where $\mathcal{O}$ is the point in infinity.



secant line



tangent line

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

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 ≥ 28, found by Elkies in May 2006.

History of elliptic curves rank records:

rank $\geq$	year	Author(s)
3	1938	Billing
4	1945	Wiman
6	1974	Penney & Pomerance
7	1975	Penney & Pomerance
8	1977	Grunewald & Zimmert
9	1977	Brumer - Kramer
12	1982	Mestre
14	1986	Mestre
15	1992	Mestre
17	1992	Nagao
19	1992	Fermigier
20	1993	Nagao
21	1994	Nagao & Kouya
22	1997	Fermigier
23	1998	Martin & McMillen
24	2000	Martin & McMillen
28	2006	Elkies

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

Dujella (2003): $B(T) \geq 3$ for all T

$$B(T) = \sup\{\mathrm{rank}\,(E(\mathbb{Q})) \,:\, E(\mathbb{Q})_{\mathrm{tors}} \cong T\}$$

T	$B(T) \geq$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	19	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	13	Eroshkin (2007,2008,2009)
$\mathbb{Z}/4\mathbb{Z}$	12	Elkies (2006)
$\mathbb{Z}/5\mathbb{Z}$	8	Dujella & Lecacheux (2009), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	8	Eroshkin (2008), Dujella & Eroshkin (2008), Elkies (2008), Dujella (2008), Dujella & Peral (2012)
$\mathbb{Z}/7\mathbb{Z}$	5	Dujella & Kulesz (2001), Elkies (2006), Eroshkin (2009), Dujella & Lecacheux (2009), Dujella & Eroshkin (2009)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006), Dujella, MacLeod & Peral (2013)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006)
$\mathbb{Z}/12\mathbb{Z}$	4	Fisher (2008)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	15	Elkies (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	9	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	6	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	3	Connell (2000), Dujella (2000,2001,2006,2008), Campbell & Goins (2003), Rathbun (2003,2006,2013), Flores, Jones, Rollick & Weigandt (2007), Fisher (2009)

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 `mwrank` - very good for curves with rational points of order 2), or at least good lower and upper bounds for the rank.

$$G(T) = \sup\{\operatorname{rank} E(\mathbb{Q}(t)) \,:\, E(\mathbb{Q}(t))_{\text{tors}} \cong T\}.$$

T	$G(T) \geq$	Author(s)
0	18	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	Elkies (2009)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/4\mathbb{Z}$	5	Kihara (2004), Elkies (2007)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008), Dujella & Peral (2012), MacLeod (2014)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella & Peral (2012), MacLeod (2013)
$\mathbb{Z}/9\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/10\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/12\mathbb{Z}$	0	Kubert (1976)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	7	Elkies (2007)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	4	Dujella & Peral (2012)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	2	Dujella & Peral (2012), MacLeod (2013)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

High-rank elliptic curves with some other additional properties:

- Mordell curves ($j = 0$): $y^2 = x^3 + k$,
  $r = 15$, Elkies (2009)

- congruent numbers: $y^2 = x^3 - n^2 x$,
  $r = 7$, Rogers (2004), Watkins et al. (2011–2014)

- taxicab problem (Ramanujan numbers): $x^3 + y^3 = m$,
  $r = 11$, Elkies & Rogers (2004)

- Diophantine triples:
  $y^2 = (ax + 1)(bx + 1)(cx + 1)$
  $r = 11$, Aguirre, Dujella & Peral (2012)

- $E(\mathbb{Q}(i))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$
  $r = 7$, Dujella & Jukić Bokun (2010)

- $E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$
  $r = 7$, resp. $r = 6$, Jukić Bokun (2011)

Diophantine m-tuples

A set $\{a_1, a_2, \ldots, a_m\}$ of m non-zero integers (rationals) is called *a (rational) Diophantine m-tuple* if $a_i \cdot a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$.

Diophantus of Alexandria: $\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}$

Fermat: $\{1, 3, 8, 120\}$ (Euler: $777480/2879^2$)

Baker & Davenport (1969): Fermat's set cannot be extended to a Diophantine quintuple.

Dujella (2004): There does not exist a Diophantine sextuple and there are only finitely many Diophantine quintuples.

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

$$ax + 1 = \square, \quad bx + 1 = \square, \quad cx + 1 = \square. \qquad (*)$$

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 *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

$$P = [0, 1], \quad Q = [1/abc, 1/rst],$$
$$R = [(rs + rt + st + 1)/abc, (r + s)(r + t)(s + t)/abc].$$

Note that $Q = 2R$, so $Q \in 2E(\mathbb{Q})$.

The x-coordinate of the point $T \in E(\mathbb{Q})$ satisfies system (*) if and only if $T - P \in 2E(\mathbb{Q})$.

D. (1997,2001): If x-coordinate of the point $T \in E(\mathbb{Q})$ satisfies system (*), then for the points $T \pm Q = (u, v)$ it holds that $xu + 1$ is a square, i.e. the sets

$$\{a, b, c, x(T), x(T \pm Q)\}$$

are rational Diophantine quintuples (if elements are nonzero).

D. (2000):

Let $x(P+Q)=d$, $x(P-Q)=e$. Assume that $de \neq 0$ and $de+1=\square$. Note: this is not possible if $\{a,b,c\}$ are integers, but there are (parametric families) solutions in rationals. Consider the elliptic curve

$$y^2 = (ax+1)(dx+1)(ex+1).$$

It has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and (in general) rank at least 4, with points of infinite order with coordinates

$$0,\ 1/ade,\ b,\ c.$$

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 $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}}$ and the rank equal to r.

D. (2007), D. & Peral (2012): 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 $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$ 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 $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$ 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 $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}}$ 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).

Connell, D. (2000): $\boxed{r = 3}$

$$\left\{\frac{408}{145}, -\frac{145}{408}, -\frac{145439}{59160}\right\}.$$

D. (2007): $\boxed{r = 3}$ (4-descent, MAGMA)

$$\left\{\frac{451352}{974415}, -\frac{974415}{451352}, -\frac{745765964321}{439804159080}\right\}.$$

D. & Peral (2012):

Elliptic curves with the torsion subgroup $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}}$

Such curves have an equation of the form

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

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

$$y^2 = x^3 + 2(\alpha^2 + \tau^2 + 4\alpha^2\tau^2 + \alpha^4\tau^2 + \alpha^2\tau^4)x^2 \\ + (\tau+\alpha)^2(\alpha\tau-1)^2(\tau-\alpha)^2(\alpha\tau+1)^2 x.$$

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

$$\tau^2 + \alpha^2 + 2 = \square \quad \text{and} \quad \alpha^2\tau^2 + 2\alpha^2 + 1 = \square,$$

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

$$\begin{aligned} A(t) = {} & 2(87671889t^{24} + 854321688t^{23} + 3766024692t^{22} + 9923033928t^{21} \\ & + 17428851514t^{20} + 21621621928t^{19} + 19950275060t^{18} \\ & + 15200715960t^{17} + 11789354375t^{16} + 10470452464t^{15} + 8925222696t^{14} \\ & + 5984900048t^{13} + 2829340620t^{12} + 820299856t^{11} + 59930952t^{10} \\ & - 66320528t^9 - 35768977t^8 - 9381000t^7 - 1017244t^6 + 262760t^5 \\ & + 159130t^4 + 41096t^3 + 6468t^2 + 600t + 25), \\ B(t) = {} & (t^2 - 2t - 1)^2(69t^4 + 148t^3 + 78t^2 + 4t + 1)^2(13t^2 - 2t - 1)^2 \\ & \times (9t^4 + 28t^3 + 18t^2 + 4t + 1)^2(11t^4 + 12t^3 + 2t^2 - 4t - 1)^2 \\ & \times (9t^2 + 14t + 7)^2(31t^4 + 52t^3 + 22t^2 - 4t - 1)^2(3t^2 + 2t + 1)^2, \end{aligned}$$

with rank ≥ 4 over $\mathbb{Q}(t)$. Indeed, it contains the points whose x-coordinates are

$$
\begin{aligned}
X_1 &= (9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad \times (69t^4+148t^3+78t^2+4t+1)^2, \\
X_2 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1) \\
&\quad \times (9t^4+28t^3+18t^2+4t+1)(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad \times (31t^4+52t^3+22t^2-4t-1), \\
X_3 &= (3t^2+2t+1)(9t^2+14t+7)^2(13t^2-2t-1) \\
&\quad \times (9t^4+28t^3+18t^2+4t+1)^2(11t^4+12t^3+2t^2-4t-1) \\
&\quad \times (69t^4+148t^3+78t^2+4t+1), \\
X_4 &= -(3t^2+2t+1)^2(9t^2+14t+7)^2(11t^4+12t^3+2t^2-4t-1)^2 \\
&\quad \times (31t^4+52t^3+22t^2-4t-1)^2.
\end{aligned}
$$

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) we can show that 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 `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

$$y^2 = x^3 + x^2 - 6141005737705911671519806644217969840x$$
$$+ 5857433177348803158586285785929631477808095171159063188.$$

Independent points of infinite order are:

$$
\begin{gathered}
[-612695149795875652, 30643098243490773810273083358], \\
[-431590874944672564, 29030057680838731041588594 30], \\
[187501554154394546, 21708470738974153948323510 00], \\
[-138350070896717 3302, 34213149431638337745679174 08], \\
[142851904723904 9546, 45515491200217791375480 00], \\
[143024871383773 1282, 81822600086915483159364 0], \\
[142930579293119 4266, 29012125229927554835577 60], \\
[103900694057898826, 22848413651245620790872062 40], \\
[142985429110233 1316, 17269365047672031757199 10].
\end{gathered}
$$

Arithmetic progressions on Pellian equations

Let us consider arithmetic progressions consisting of integers which are y-components of solutions of a Pellian equation of the form

$$x^2 - dy^2 = m.$$

Pethő & Ziegler (2008):

- for the four-term arithmetic progression $1, 3, 5, 7$ there exists Pellian equation $x^2 - dy^2 = m$, where d is not a square, such that $1, 3, 5, 7$ are y-components of the solutions of this equation.

- for the arithmetic progressions $0, 1, 2, 3$ such an equation does not exist.

- for a five-terms arithmetic progression $y_1 < y_2 < y_3 < y_4 < y_5$ (such that $|y_i| \neq |y_j|$ for any $i \neq j$) there are at most finitely many $d, m \in \mathbb{Z}$ such that d is not a square, $m \neq 0$ and $\gcd(d, m)$ is square-free such that y_1, y_2, y_3, y_4, y_5 are the y-components of solutions to $x^2 - dy^2 = m$.

D. & Pethő & Tadić (2008):

- apart from $0, 1, 2, 3$ and $-3, -2, -1, 0$, for all four-term arithmetic progression consisting of integers there exist infinitely many equations of the form $x^2 - dy^2 = m$, where d is not a square (if d is a square and $m = 0$, the problem is trivial) and $\gcd(d, m)$ is square-free (so that the equations are essentially distinct) for which the elements of the given progression form y-components of solutions.

- there exist arithmetic progressions with five, six and seven elements which are y-components of solutions of a Pellian equation.

The system

$$\begin{aligned} X_1^2 - da^2 &= m, \\ X_2^2 - d(a+k)^2 &= m, \\ X_3^2 - d(a+2k)^2 &= m, \\ X_4^2 - d(a+3k)^2 &= m \end{aligned}$$

of Diophantine equations defines the curve of genus 1.

It can be transformed ($T = a/k$) to the elliptic curve $\mathcal{E}$:

$$\begin{aligned} y^2 &= x^3 + (176T^2 + 672T + 628)x^2 + (9216T^4 + 72192T^3 + 209664T^2 \\ &+ 267648T + 126720)x + 147456T^6 + 1769472T^5 + 8773632T^4 \\ &+ 23003136T^3 + 33629184T^2 + 25989120T + 8294400. \end{aligned}$$

Shioda's formula $\Rightarrow$ $\text{rang}_{\mathbb{Q}(T)}\mathcal{E} = 1$.
generator:

$P := [-64T^2 - 256T - 240, 128T^3 + 640T^2 + 992T + 480]$

e.g. rang $= 7$ for $T = 619/6089$

For $(a,k) = (-461, 166)$ we obtain the elliptic curve

$$y^2 = x^3 + 3283392x^2 + 1816362270720x + 233361525187805184$$

of rank 2, with generators

$$P_1 = [2025472, 5068743680],\ P_2 = [-183168, 68382720].$$

The point P_2 gives the equation

$$x^2 + 1245y^2 = 375701326$$

with the property that the seven numbers $a, a+k, a+2k, a+3k, a+4k, a+5k, a+6k$, i.e.

$$y = -461, -295, -129, 37, 203, 369, 535$$

are solutions of this equation.

Aguirre & D. & Peral (2013):

- there are infinitely many pairs d, m (parametrized by points of an elliptic curve of positive rank) for which the corresponding Pellian equations have solutions whose y-components form a six-term arithmetic progression.

- new seven-term examples:

e.g. the equation

$$x^2 - 37569y^2 = 27833977600$$

has the property that the seven numbers
$a, a+k, a+2k, a+3k, a+4k, a+5k, a+6k$, i.e.

$$y = -5956, -4167, -2378, -589, 1200, 2989, 4778$$

are solutions of this equation.

Congruent and θ-congruent number curves

A positive square-free integer n is called a congruent number if it is the area of a right triangle with rational sides; n if congruent if and only if the congruent number elliptic curve $y^2 = x^3 - n^2 x$ has positive rank.

Rogers (2004): An example of rank 7 congruent number curve, and several examples with rank 6.
(hash table of curves with many points of small height).

D. & Janfada & Salami (2009): New examples of rank 6 congruent number curves
(Monsky's formula for computing 2-Selmer rank (an upper bound for the rank; the same parity as the rank) and Mestre-Nagao's sum).

Watkins, Donnelly, Elkies, Fisher, Granville, Rogers (2011–2014):

New examples of rank 7 congruent number curves (16 rank 7 curves are known).

(a variant of Monsky's formula, due to Rogers, applicable to isogenous curves for computing 2-Selmer rank; Mestre-Nagao's sum; 4-Selmer rank via the Cassels-Tate pairing as implemented in `Magma` by Donnelly; 8-Selmer rank via higher descent pairings due to Fisher).

No example with rank 8 is known.

Granville's heuristic might lead one to suspect that rank 7 is the maximal rank in this family.

Koblitz (1993), Fujiwara (1997): θ-congruent number curve:

$$y^2 = x^3 + 2snx - (r^2 - s^2)n^2x,$$

where $0 < \theta < \pi$, $\cos(\theta) = s/r$ with $0 \leq |s| < r$ and $\gcd(r, s) = 1$. A positive integer n is called a θ-congruent number if there is a triangle with rational sides, with one angle θ and the area equal to $n\sqrt{r^2 - s^2}$.

$\theta = \pi/2$ ($r = 1$, $s = 0$) - ordinary congruent number curve
$\theta = \pi/3$ and $2\pi/3$ ($r = 2$, $s = \pm1$) - also studied by several authors

Kan (2000): If n is the square-free part of $pq(p+q)(2rq+p(r-s))$, for some positive integers p, q with $\gcd(p,q)=1$, then n is a θ-congruent number (i.e. corresponding elliptic curve has positive rank).

Janfada & Salami & D. & Peral (2014):
$\pi/3$-congruent number curve of rank 7;
$2\pi/3$-congruent number curve of rank 7 (current records)
(we found families with rank 3 and 4, but a family with rank 2 was more suitable for searching for curves with high rank; 2-Selmer rank; Mestre-Nagao's sum; Mestre's conditional upper bound for rank (assuming the Birch and Swinnerton-Dyer conjecture and GRH); `mwrank` on the original and also on 2-isogenous curves).