Elliptic curves and Diophantine m-tuples

Andrej Dujella

Department of Mathematics
Faculty of Science
University of Zagreb, Croatia
e-mail: `duje@math.hr`
URL: `https://web.math.pmf.unizg.hr/~duje/`

Supported by the QuantiXLie Center of Excellence.

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

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{1}$$

which is called the *Weierstrass form*.

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

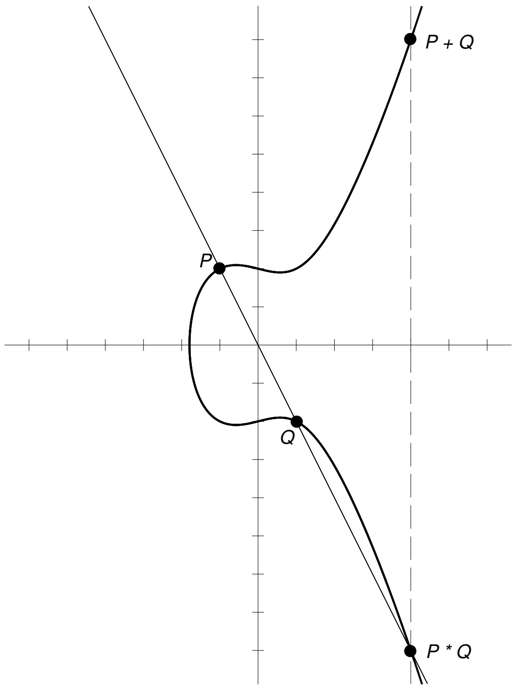
$$y^2 = x^3 + ax + b, \tag{2}$$

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.

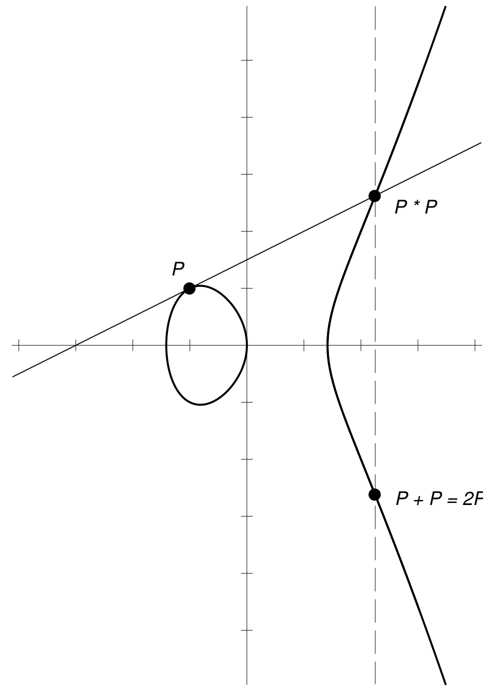
One of the most important facts about elliptic curves is that the set $E(\mathbb{K})$ of $\mathbb{K}$-rational points on an elliptic curve over $\mathbb{K}$ (affine points (x, y) satisfying (1) along with the point at infinity) forms an abelian group in a natural way.

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

It is not known which values of rank r are possible for elliptic curves over $\mathbb{Q}$. It has been conjectured that there exist elliptic curves of arbitrarily high rank, and even for each of the torsion groups in Mazur's theorem.

However there are also recent heuristic arguments that suggest the boundedness of the rank of elliptic curves. According to this heuristic, only a finite number of curves would have rank higher that 21.

The current record is an example of elliptic curve over $\mathbb{Q}$ with rank ≥ 28, found by Elkies in 2006.

Diophantine m-tuples

Diophantus: Find four (positive rational) 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: $\{1, 3, 8, 120\}$

$$\begin{aligned} 1\cdot 3+1 &= 2^2, & 3\cdot 8+1 &= 5^2, \\ 1\cdot 8+1 &= 3^2, & 3\cdot 120+1 &= 19^2, \\ 1\cdot 120+1 &= 11^2, & 8\cdot 120+1 &= 31^2. \end{aligned}$$

Definition: 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 $1 \le i < j \le m$.

Question: How large such sets can be?

Euler: There are infinitely many Diophantine quadruples. E.g. $\{k-1, k+1, 4k, 16k^3 - 4k\}$ for $k \ge 2$.

Baker & Davenport (1969): $\{1, 3, 8, d\} \Rightarrow d = 120$ (problem raised by Denton (1957), Gardner (1967), van Lint (1968))

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

He, Togbé & Ziegler (2019): There does not exist a Diophantine quintuple.

Arkin, Hoggatt & Strauss (1978): Let

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2$$

and define

$$d_{+,-} = a + b + c + 2abc \pm 2rst.$$

Then $\{a, b, c, d_{+,-}\}$ is a Diophantine quadruple (if $d_- \neq 0$).

Conjecture: If $\{a, b, c, d\}$ is a Diophantine quadruple, then $d = d_+$ or $d = d_-$, i.e. all Diophantine quadruples satisfy

$$(a - b - c + d)^2 = 4(ad + 1)(bc + 1).$$

Such quadruples are called *regular*.

D. & Pethő (1998): All quadruples containing $\{1, 3\}$ are regular.

Fujita (2008), Bugeaud, D. & Mignotte (2007): All quadruples containing $\{k-1, k+1\}$ are regular.

Cipu, Fujita & Miyazaki (2018): Any fixed Diophantine triple can be extended to a Diophantine quadruple in at most 8 ways by joining a fourth element exceeding the maximal element in the triple (and in at most 2 ways by joining a fourth element which is smaller than the minimal element in the triple – Cipu, D. & Fujita (2022)).

Rational Diophantine m-tuples

There is no known upper bound for the size of rational Diophantine tuples.

Euler: There are infinitely many rational Diophantine quintuples. Any pair $\{a,b\}$ such that $ab+1=r^2$ can be extended to a quintuple. E.g. $\{1,3,8,120,\frac{777480}{8288641}\}$.

Arkin, Hoggatt & Strauss (1979): Any rational Diophantine triple $\{a,b,c\}$ can be extended to a quintuple.

D. (1997): Any rational Diophantine quadruple $\{a,b,c,d\}$, such that $abcd \neq 1$, can be extended to a quintuple (in two different ways, unless the quadruple is "regular" (such as in the Euler and AHS construction), in which case one of the extensions is trivial extension by 0).

Question: If $\{a, b, c, d, e\}$ and $\{a, b, c, d, f\}$ are two extensions from D. (1997) and $ef \neq 0$, is it possible that $ef + 1$ is a perfect square?

$$e, f = \frac{(a+b+c+d)(abcd+1) + 2abc + 2abd + 2acd + 2bcd \pm 2\sqrt{D}}{(abcd-1)^2},$$

where

$$D = (ab+1)(ac+1)(ad+1)(bc+1)(bd+1)(cd+1).$$

Gibbs (1999): $\left\{\frac{5}{36}, \frac{5}{4}, \frac{32}{9}, \frac{189}{4}, \frac{665}{1521}, \frac{3213}{676}\right\}$

D., Kazalicki, Mikić & Szikszai (2017): There are infinitely many rational Diophantine sextuples.

Moreover, there are infinitely many rational Diophantine sextuples with positive elements, and also with any combination of signs.

Open question: Is there any rational Diophantine septuple?

Herrmann, Pethő & Zimmer (1999): A rational Diophantine quadruple has only finitely many extensions to a rational Diophantine quintuple. They showed that the conditions on the fifth element of the quintuple lead to a curve of genus 4, and then they applied Faltings' theorem.

Lang's conjecture on varieties of general type implies that there is no rational Diophantine m-tuple if m is large enough.

Stoll (2019): If $\{1, 3, 8, 120, e\}$ is a rational Diophantine quintuple, then $e = \frac{777480}{8288641}$. Fermat's set cannot be extended to a rational Diophantine sextuple.

By DKMS (2017), there exist infinitely many triples, each of which can be extended to sextuples in infinitely many ways.

D., Kazalicki & Petričević (2019): Infinitely many rational Diophantine sextuples such that denominators of all the elements are perfect squares. E.g. $\{75/8^2, -3325/64^2, -12288/125^2, 123/10^2, 3498523/2260^2, 698523/2260^2\}$.

Gibbs (2016), D., Kazalicki & Petričević (2018): Examples of "almost" septuples – rational Diophantine quintuples which can be extended to rational Diophantine sextuples in two different ways, so that only one condition is missing for these seven numbers to form a rational Diophantine septuple, e.g.

$\{243/560, 1147/5040, 1100/63, 7820/567, 95/112\}$
can be extended with $38269/6480$ or $196/45$.

Gibbs (2016): Rational Diophantine quadruples which can be extended to quintuples in six different ways, e.g.

$$\{81/1400, 5696/4725, 2875/168, 4928/3\}$$

can be extended to a quintuple using any one of these: 98/27, 104/525, 96849/350, 1549429/1376646, 3714303488/6103383075, 7694337252154322/1857424629984075.

D., Kazalicki & Petričević (2018): Rational Diophantine quadruple which can be extended to rational Diophantine sextuples in three different ways:

$$\{11825/2016, 51200/693, 9163/92160, 497/990\}$$

can be extended with $\{10989/280, 551/3080\}$, $\{10989/280, 19035/9856\}$ or $\{551/3080, 17577/1760\}$.

Elliptic curves induced by Diophantine triples

Let $\{a, b, c\}$ be a rational Diophantine triple. To extend this triple to a quadruple, we consider the system

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{3}$$

It is natural to assign the elliptic curve

$$\mathcal{E}: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1) \tag{4}$$

to the system (3). We say $\mathcal{E}$ is induced by the triple $\{a, b, c\}$.

Three rational points on the $\mathcal{E}$ of order 2:

$$A = [-1/a, 0], \quad B = [-1/b, 0], \quad C = [-1/c, 0]$$

and also other obvious rational points

$$P = [0, 1], \quad S = [1/abc, \sqrt{(ab + 1)(ac + 1)(bc + 1)}/abc].$$

The x-coordinate of a point $T \in \mathcal{E}(\mathbb{Q})$ satisfies (3) if and only if $T - P \in 2\mathcal{E}(\mathbb{Q})$.

It holds that $S \in 2\mathcal{E}(\mathbb{Q})$. Indeed, if $ab+1 = r^2$, $ac+1 = s^2$, $bc+1 = t^2$, then $S = [2]V$, where

$$V = \left[\frac{rs+rt+st+1}{abc}, \frac{(r+s)(r+t)(s+t)}{abc}\right].$$

This implies that if $x(T)$ satisfies system (3), then also the numbers $x(T \pm S)$ satisfy the system.

D. (1997,2001): $x(T)x(T \pm S) + 1$ is always a perfect square. With $x(T) = d$, the numbers $x(T \pm S)$ are exactly e and f.

Proposition 1: Let Q, T and $[0, \alpha]$ be three rational points on an elliptic curve $\mathcal{E}$ over $\mathbb{Q}$ given by the equation $y^2 = f(x)$, where f is a monic polynomial of degree 3. Assume that $\mathcal{O} \notin \{Q, T, Q + T\}$. Then

$$x(Q)x(T)x(Q+T) + \alpha^2$$

is a perfect square.

Proof: Consider the curve

$$y^2 = f(x) - (x - x(Q))(x - x(T))(x - x(Q+T)).$$

It is a conic which contains three collinear points: Q, T, $-(Q+T)$. Thus, it is the union of two rational lines, e.g. we have

$$y^2 = (\beta x + \gamma)^2.$$

Inserting here $x = 0$, we get

$$x(Q)x(T)x(Q+T) + \alpha^2 = \gamma^2.$$

The transformation $x \mapsto x/abc$, $y \mapsto y/abc$, applied to $\mathcal{E}$ leads to

$$E' : \qquad y^2 = (x+ab)(x+ac)(x+bc)$$

The points P and S become $P' = [0, abc]$ and $S' = [1, rst]$, respectively.

If we apply Proposition 1 with $Q = \pm S'$, since $x(S') = 1$, we get a simple proof of the fact that $x(T)x(T \pm S) + 1$ is a perfect square (after dividing $x(T')x(T' \pm S') + a^2b^2c^2 = \square$ by $a^2b^2c^2$).

Now we have a general construction which produces two rational Diophantine quintuples with four joint elements. So, the union of these two quintuples,

$$\{a, b, c, x(T-S), x(T), x(T+S)\},$$

is "almost" a rational Diophantine sextuple.

Assuming that $T, T \pm S \notin \{\mathcal{O}, \pm P\}$, the only missing condition is

$$x(T-S) \cdot x(T+S) + 1 = \square.$$

To construct examples satisfying this last condition, we will use Proposition 1 with $Q = [2]S'$. To get the desired conclusion, we need the condition $x([2]S') = 1$ to be satisfied. This leads to $[2]S' = -S'$, i.e. $[3]S' = \mathcal{O}$.

Lemma 1: For the point $S' = [1, rst]$ on E' it holds $[3]S' = \mathcal{O}$ if and only if

$$\begin{aligned} &3 + 4(ab + ac + bc) + 6abc(a + b + c) + 12(abc)^2 \\ &\quad - (abc)^2(a^2 + b^2 + c^2 - 2ab - 2ac - 2bc) = 0 \qquad (5) \end{aligned}$$

By writing (5) in terms of elementary symmetric polynomials, we find the following family of rational Diophantine triples satisfying the condition of Lemma 1:

$$a = \frac{18t(t-1)(t+1)}{(t^2-6t+1)(t^2+6t+1)},$$
$$b = \frac{(t-1)(t^2+6t+1)^2}{6t(t+1)(t^2-6t+1)},$$
$$c = \frac{(t+1)(t^2-6t+1)^2}{6t(t-1)(t^2+6t+1)}.$$

Consider now the elliptic curve over $\mathbb{Q}(t)$ induced by the triple $\{a, b, c\}$. It has positive rank since the point $P = [0, 1]$ is of infinite order. Thus, the above described construction produces infinitely many rational Diophantine sextuples containing the triple $\{a, b, c\}$. One such sextuple $\{a, b, c, d, e, f\}$ is obtained by taking x-coordinates of points $[3]P$, $[3]P + S$, $[3]P - S$.

We get $d = d_1/d_2$, $e = e_1/e_2$, $f = f_1/f_2$, where

$$\begin{aligned}
d_1 &= 6(t+1)(t-1)(t^2+6t+1)(t^2-6t+1) \\
&\quad \times (8t^6+27t^5+24t^4-54t^3+24t^2+27t+8) \\
&\quad \times (8t^6-27t^5+24t^4+54t^3+24t^2-27t+8) \\
&\quad \times (t^8+22t^6-174t^4+22t^2+1), \\
d_2 &= t(37t^{12}-885t^{10}+9735t^8-13678t^6+9735t^4-885t^2+37)^2, \\
e_1 &= -2t(4t^6-111t^4+18t^2+25) \\
&\quad \times (3t^7+14t^6-42t^5+30t^4+51t^3+18t^2-12t+2) \\
&\quad \times (3t^7-14t^6-42t^5-30t^4+51t^3-18t^2-12t-2) \\
&\quad \times (t^2+3t-2)(t^2-3t-2)(2t^2+3t-1) \\
&\quad \times (2t^2-3t-1)(t^2+7)(7t^2+1), \\
e_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1) \\
&\quad \times (16t^{14}+141t^{12}-1500t^{10}+7586t^8-2724t^6+165t^4+424t^2-12)^2, \\
f_1 &= 2t(25t^6+18t^4-111t^2+4) \\
&\quad \times (2t^7-12t^6+18t^5+51t^4+30t^3-42t^2+14t+3) \\
&\quad \times (2t^7+12t^6+18t^5-51t^4+30t^3+42t^2+14t-3) \\
&\quad \times (2t^2+3t-1)(2t^2-3t-1)(t^2-3t-2) \\
&\quad \times (t^2+3t-2)(t^2+7)(7t^2+1), \\
f_2 &= 3(t+1)(t^2-6t+1)(t-1)(t^2+6t+1) \\
&\quad \times (12t^{14}-424t^{12}-165t^{10}+2724t^8-7586t^6+1500t^4-141t^2-16)^2.
\end{aligned}$$

These formulas produce infinitely many rational Diophantine sextuples. Moreover, by choosing the rational parameter t from the appropriate interval, we get infinitely many sextuples for each combination of signs. E.g., for $5.83 < t < 6.86$ all elements are positive. As a specific example, let us take $t = 6$, for which we get a sextuple with all positive elements:

$$\Big\{\frac{3780}{73}, \frac{26645}{252}, \frac{7}{13140}, \frac{791361752602550684660}{1827893092234556692801},$$

$$\frac{95104852709815809228981184}{35104191165465133563326955},$$

$$\frac{3210891270762333567521084544}{2171271922392358100535}\Big\}.$$

Alternative construction

Piezas (2016), D. & Kazalicki (2017), D., Kazalicki, Petričević (2019)

If $\{a, b, c, d\}$ is a rational Diophantine quadruple such that

$$(abcd - 3)^2 = 4(ab + cd + 3),$$

and e and f are extensions from D. (1997), then

$$ef + 1 = \left(\frac{a + b - c - d}{abcd - 1}\right)^2,$$

so (assuming that $ef \neq 0$) $\{a, b, c, d, e, f\}$ is a rational Diophantine sextuple.

Edwards curve:

$(x^2-1)(y^2-1)=m$, where $m = abcd = \frac{2t^2+t-1}{t-1}$.

Birationally equivalent to the elliptic curve

$$S^2 = T^3 - 2\cdot\frac{2t^2-t+1}{t-1}T^2 + \frac{(2t-1)^2(t+1)^2}{(t-1)^2}T.$$

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

is a point of infinite order,

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

is a point of order 4.

Additional point if $t-1$ is a square.

"Simplest" known family of rational Diophantine sextuples:

$$a = \frac{(t^2-2t-1)\cdot(t^2+2t+3)\cdot(3t^2-2t+1)}{4t\cdot(t^2-1)\cdot(t^2+2t-1)},$$

$$b = \frac{4t\cdot(t^2-1)\cdot(t^2-2t-1)}{(t^2+2t-1)^3},$$

$$c = \frac{4t\cdot(t^2-1)\cdot(t^2+2t-1)}{(t^2-2t-1)^3},$$

$$d = \frac{(t^2+2t-1)\cdot(t^2-2t+3)\cdot(3t^2+2t+1)}{4t\cdot(t^2-1)\cdot(t^2-2t-1)},$$

$$e = \frac{-t\cdot(t^2+4t+1)\cdot(t^2-4t+1)}{(t-1)\cdot(t+1)\cdot(t^2+2t-1)\cdot(t^2-2t-1)},$$

$$f = \frac{(t-1)\cdot(t+1)\cdot(3t^2-1)\cdot(t^2-3)}{4t\cdot(t^2+2t-1)\cdot(t^2-2t-1)}.$$

High rank curves with given torsion group

Let $\{a, b, c\}$ be a (rational) Diophantine triple and E the elliptic curve

$$y^2 = (ax + 1)(bx + 1)(cx + 1)$$

induced by this triple.

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.

Parametric formulas for the rational Diophantine sextuples $\{a,b,c,d,e,f\}$ can be used to obtain an elliptic curve over $\mathbb{Q}(t)$ with reasonably high rank. Consider the curve

$$E: \quad y^2 = (dx+1)(ex+1)(fx+1).$$

It has three obvious points of order two, but also points with x-coordinates

$$0,\ \frac{1}{def},\ a,\ b,\ c.$$

It can be checked (by suitable specialization) that these five points are independent points of infinite order on the curve E over $\mathbb{Q}(t)$. Therefore, we get that the rank of E over $\mathbb{Q}(t)$ is ≥ 5 (torsion group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$).

Aguirre, D. & Peral (2012), D. & Peral (2020): Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and rank 6 over $\mathbb{Q}(t)$ and rank 12 over $\mathbb{Q}$.

For rational Diophantine triples $\{a, b, c\}$ satisfying condition (5), the induced elliptic curve has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, since it contains the point S of order 3. Our parametric family for triples $\{a, b, c\}$ gives a curve over $\mathbb{Q}(t)$ with generic rank 1.

Within this family of curves, it is possible to find subfamilies of generic rank 2 and particular examples with rank 6, which both tie the current records of ranks of curve with torsion $\boxed{\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}}$ (**D. & Peral (2019)**).

$$\left\{\frac{7567037280}{7833785281}, \frac{41616693602 89}{569762123040}, \frac{1359453258559}{948852707040}\right\}$$

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

An elliptic curve induced by triple $\{a, b, c\}$ can we written in the form

$$y^2 = x(x + ac - ab)(x + bc - ab).$$

By comparing these two equations, we get conditions that $ac - ab$ and $bc - ab$ are perfect squares. We may expect that this curve will have positive rank, since it also contains the point $[ab, abc]$.

A convenient way to fulfill these two 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

$$a = \frac{\alpha\tau + 1}{\tau - \alpha}, \quad c = \frac{4\alpha\tau}{(\alpha\tau + 1)(\tau - \alpha)}.$$

Additional points of infinite order if

$$\tau^2 + \alpha^2 + 2 \quad \text{or} \quad \alpha^2\tau^2 + 2\alpha^2 + 1$$

are perfect squares.

D. & Peral (2014, 2019): Curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ and rank 4 over $\mathbb{Q}(t)$ (Gusić & Tadić algorithm shows that rank is exactly 4) and rank 9 over $\mathbb{Q}$ (both results are current records for ranks with this torsion).

Every elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by a rational Diophantine triple (**D. (2007), Campbell & Goins (2007)**).

D. (2007): For each $0 \leq r \leq 3$, there exists a rational 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.

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

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

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

T	$B(T) \geq$	Author(s)
0	28	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	20	Elkies & Klagsbrun (2020)
$\mathbb{Z}/3\mathbb{Z}$	15	Elkies & Klagsbrun (2020)
$\mathbb{Z}/4\mathbb{Z}$	13	Elkies & Klagsbrun (2020)
$\mathbb{Z}/5\mathbb{Z}$	9	Klagsbrun (2020)
$\mathbb{Z}/6\mathbb{Z}$	9	Klagsbrun (2020), Voznyy (2020)
$\mathbb{Z}/7\mathbb{Z}$	6	Klagsbrun (2020)
$\mathbb{Z}/8\mathbb{Z}$	6	Elkies (2006), Dujella, MacLeod & Peral (2013), Voznyy (2021)
$\mathbb{Z}/9\mathbb{Z}$	4	Fisher (2009), van Beek (2015), Dujella & Petričević (2021), Dujella, Petričević & Rathbun (2022)
$\mathbb{Z}/10\mathbb{Z}$	4	Dujella (2005,2008), Elkies (2006), Fisher (2016)
$\mathbb{Z}/12\mathbb{Z}$	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 (2012,2019), Klagsbrun (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	**6**	Elkies (2006), Dujella, Peral & Tadić (2015), Dujella & Peral (2020)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	**3**	Connell (2000), Dujella (2000,2001,2006,2008), Campbell & Goins (2003), Rathbun (2003,2006,2013,2022), Flores, Jones, Rollick & Weigandt (2007), Fisher (2009), AttarBashi, Rathbun & Voznyy (2022), AttarBashi, Fisher, Rathbun & Voznyy (2022), AttarBashi, Fisher & Voznyy (2022)

induced by Diophantine triples

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; `Magma`; `ellrank` in `PARI/GP`), 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), Dujella & Peral (2023)
$\mathbb{Z}/3\mathbb{Z}$	7	Elkies (2007), Eroshkin (2023)
$\mathbb{Z}/4\mathbb{Z}$	6	Dujella & Peral (2022)
$\mathbb{Z}/5\mathbb{Z}$	4	Eroshkin (2020)
$\mathbb{Z}/6\mathbb{Z}$	3	Lecacheux (2001), Kihara (2006), Eroshkin (2008), Woo (2008), Dujella & Peral (2012,2020), MacLeod (2014,2015), Voznyy (2021)
$\mathbb{Z}/7\mathbb{Z}$	1	Kulesz (1998), Lecacheux (2003), Rabarison (2008), Harrache (2009), MacLeod (2014)
$\mathbb{Z}/8\mathbb{Z}$	2	Dujella & Peral (2012), MacLeod (2013), Dujella, Kazalicki & Peral (2021)
$\mathbb{Z}/9\mathbb{Z}$	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 (2012,2015,2017), MacLeod (2013), Dujella, Kazalicki & Peral (2021)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	0	Kubert (1976)

induced by Diophantine triples

$$C(T) = \limsup\{\text{rank}\, E(\mathbb{Q}) \,:\, E(\mathbb{Q})_{\text{tors}} \cong T\}$$

T	$C(T) \geq$	PPVW	Author(s)
0	19	21	Elkies (2006)
$\mathbb{Z}/2\mathbb{Z}$	11	13	Elkies (2007,2009) Dujella & Peral (2023)
$\mathbb{Z}/3\mathbb{Z}$	8	9	Eroshkin (2023)
$\mathbb{Z}/4\mathbb{Z}$	6	7	Elkies (2007), Dujella & Peral (2021,2022)
$\mathbb{Z}/5\mathbb{Z}$	4	5	Eroshkin (2009)
$\mathbb{Z}/6\mathbb{Z}$	**5**	5	Eroshkin (2009)
$\mathbb{Z}/7\mathbb{Z}$	2	3	Lecacheux (2003), Elkies (2006), Rabarison (2008), Harrache (2009), Voznyy (2022)
$\mathbb{Z}/8\mathbb{Z}$	**3**	3	Dujella & Peral (2012), Dujella, Kazalicki & Peral (2021)
$\mathbb{Z}/9\mathbb{Z}$	1	2	Atkin & Morain (1993), Kulesz (1998), Rabarison (2008), Gasull, Manosa & Xarles (2010)
$\mathbb{Z}/10\mathbb{Z}$	1	2	Atkin & Morain (1993), Kulesz (1998), Rabarison (2008)
$\mathbb{Z}/12\mathbb{Z}$	1	2	Suyama (1985), Kulesz (1998), Rabarison (2008), Halbeisen, Hungerbühler, Voznyy & Zargar (2021)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$	8	9	Elkies (2007)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$	**5**	5	Eroshkin (2009)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$	**3**	3	Dujella & Peral (2013), Dujella, Kazalicki & Peral (2021)
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$	1	2	Atkin & Morain (1993), Kulesz (1998), Lecacheux (2002), Campbell & Goins (2003), Rabarison (2008)

known lower bound coincide with heuristic upper bound due to
Park, Poonen, Voight and Wood (2019)

Rank 3 family with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$

D., Kazalicki & Peral (2021):
We start with the curve $Y^2 = X^3 + AX^2 + BX$ of rank 2 over $\mathbb{Q}(u)$ obtained by using Diophantine triples (D. & Peral (2015)):

$$\begin{aligned} A = {} & u^{16} - 60u^{15} + 1634u^{14} - 27768u^{13} + 334132u^{12} - 3017412u^{11} \\ & + 20987282u^{10} - 113627424u^9 + 480725533u^8 - 1590783936u^7 \\ & + 4113507272u^6 - 8279778528u^5 + 12836014912u^4 - 14934296832u^3 \\ & + 12303261824u^2 - 6324810240u + 1475789056, \\ B = {} & -27u^3(u-4)^3(2u-7)^3(u^4 - 24u^3 + 152u^2 - 336u + 196) \\ & \times (u^4 - 12u^3 + 62u^2 - 168u + 196)^3(2u^4 - 30u^3 + 169u^2 - 420u + 392). \end{aligned}$$

The X-coordinates of two independent points of infinite order are

$$\begin{aligned} & -27u^2(u-4)^2(2u-7)^2(u^2 - 8u + 14)^2(u^4 - 24u^3 + 152u^2 - 336u + 196), \\ & -\frac{27}{4}u^2(u-4)^2(2u-7)^2(u^2 - 7u + 14)^2(u^4 - 24u^3 + 152u^2 - 336u + 196). \end{aligned}$$

Imposing

$$\frac{27}{4}u(u-4)(2u-7)(u^2-7u+14)^2(u^4-12u^3+62u^2-168u+196)^2$$

as the X-coordinate of a new point, leads to the condition

$$4u^4-66u^3+383u^2-924u+784=t^2,$$

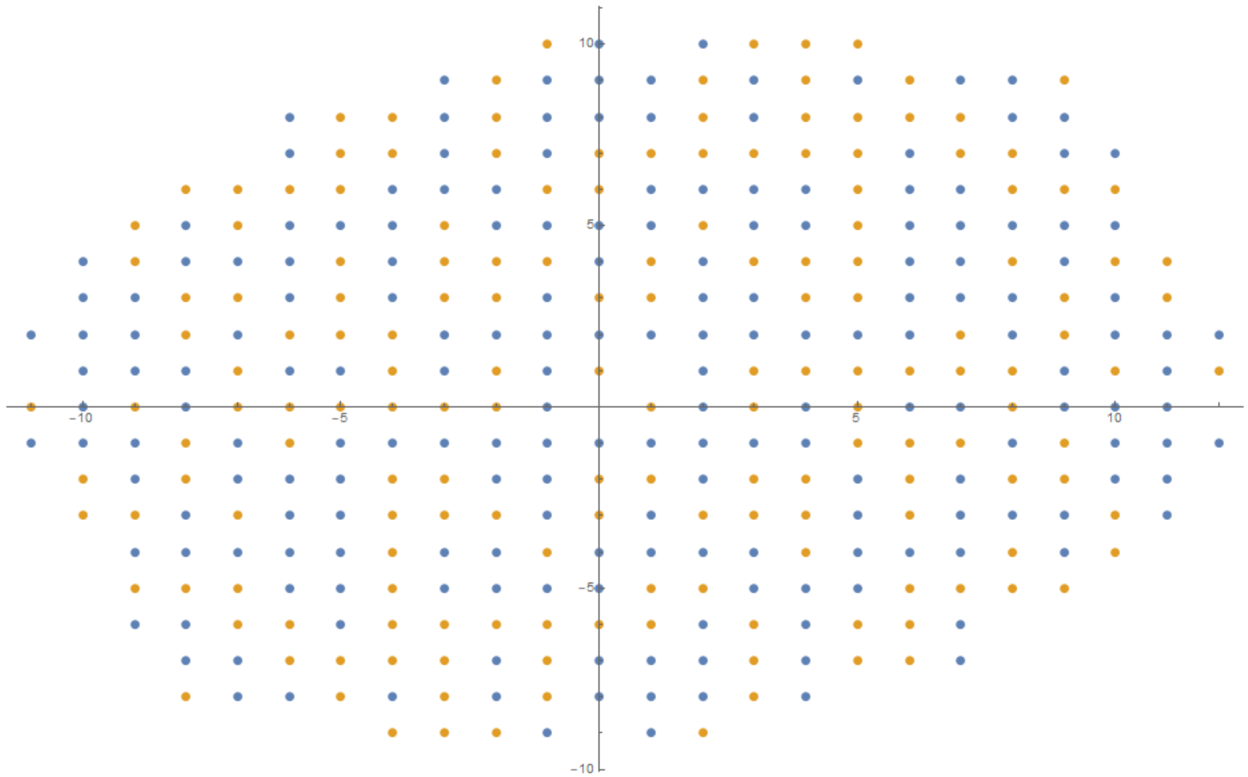
which has a rational solution $(u,t)=(0,28)$, and thus can be transformed into elliptic curve

$$y^2=x^3-x^2-456x+3456$$

of rank 2 (with generators $R_1=(20,-44)$ and $R_2=(4/9,-1540/27)$) and torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$.

The root numbers of elliptic curves corresponding to the points nR_1+mR_2 for small $n,m \in \mathbb{Z}$ are presented in next figure (the points which differ by the point of order two correspond to the isomorphic elliptic curves, so they are not included in the figure). There are 194 curves with the root number 1 (conjecturally rank is even), and 168 curves with the root number -1 (conjecturally rank is odd), which suggests that the root numbers are evenly distributed in this family.

That would imply that there are infinitely many elliptic curves with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank ≥ 4, which indicates that the heuristic in [PPVW] needs some adjustments, at least in the case of curves with torsion groups $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ (similar result were obtained for torsion group $\mathbb{Z}/8\mathbb{Z}$ and are expected for $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$).



The blue (orange) point with coordinates (n, m) represents the elliptic curve with root number one (minus one) that corresponds to the point $nR_1 + mR_2$.

Thank you very much
for your attention!