High-rank elliptic curves with given torsion group and some applications

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

Number-Theoretic Methods in Cryptology, Poznań, 2022

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

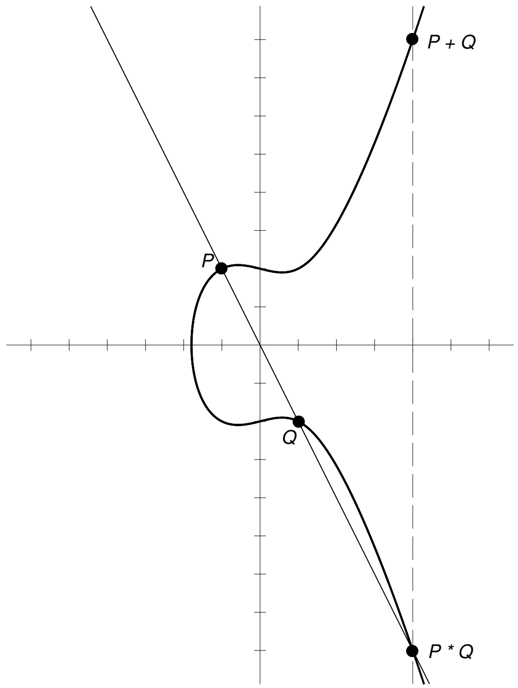
$$y^2 = x^3 + ax + b, \tag{2}$$

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.

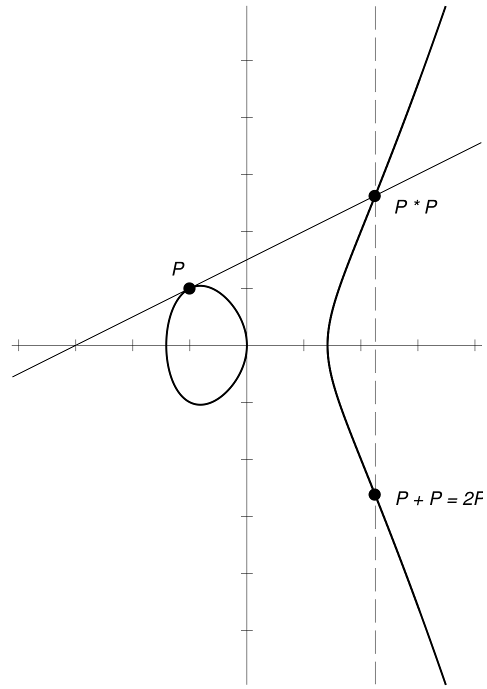
One of the most important facts about elliptic curves is that the set $E(\mathbb{K})$ of $\mathbb{K}$-rational points on an elliptic curve over $\mathbb{K}$ (affine points (x, y) satisfying (1) along with the point at infinity) forms an abelian group in a natural way.

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:

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{\mathrm{tors}} \times \mathbb{Z}^r.$$

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.

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

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

Elliptic curves over quadratic fields

Kenku & Momose (1988), Kamienny (1992):
Let E be an elliptic curve over a quadratic field $E(\mathbb{K})$. The torsion group of $E(\mathbb{K})$ is isomorphic to one of the following groups:
$\mathbb{Z}/n\mathbb{Z}$, where $n = 1, 2, 3, \ldots 16$ or 18;
$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$, where $n = 1, 2, 3, 4, 5, 6$;
$\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3n\mathbb{Z}$, where $n = 1$ or 2 (only if $\mathbb{K} = \mathbb{Q}(\sqrt{-3})$);
$\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ (only if $\mathbb{K} = \mathbb{Q}(i)$).

Note that if torsion group over a number field $\mathbb{K}$ contains $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$, then the m-th roots of unity lie in $\mathbb{K}$.

Bosman, Bruin, D., Najman (2014):
There exist elliptic curves over quadratic fields with positive rank and torsion $\mathbb{Z}/15\mathbb{Z}$ (rank ≥ 1 over $\mathbb{Q}(\sqrt{345})$, $\mathbb{Z}/18\mathbb{Z}$ (rank ≥ 2 over $\mathbb{Q}(\sqrt{26521})$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ (rank ≥ 4 over $\mathbb{Q}(\sqrt{55325286553})$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ (rank ≥ 4 over $\mathbb{Q}(\sqrt{2947271015})$).

Together with Rabarison (2010), this implies that there exist curves with positive rank for all 26 possible torsion groups over quadratic fields.

All elliptic curves over quadratic fields with torsions $\mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ have even rank (*false complex multiplication*).

Similar results for cubic and quartic fields.

Aguirre, D., Jukić Bokun, Peral (2014), Najman (2014), Voznyy (2022):
For each of 26 possible torsion groups there exist an elliptic curve over some quadratic field with this torsion group and with rank ≥ 2.

In the case of the 15 possible torsion groups of elliptic curves over $\mathbb{Q}$ (and other torsion groups which admit a model with rational coefficients), we consider curves with rational coefficients, and in order to determine their rank over a quadratic field $\mathbb{Q}(\sqrt{d})$ we use the formula

$$\text{rank}(E(\mathbb{Q}(\sqrt{d})) = \text{rank}(E(\mathbb{Q})) + \text{rank}(E^{(d)}(\mathbb{Q})), \quad (3)$$

where $E^{(d)}$ denotes the d-quadratic twist of E.

Applications of elliptic curves in factorization

Finding elliptic curves with positive rank and large torsion over number fields is not just a curiosity. Elliptic curves with large torsion and positive rank over the rationals have long been used for factorization, starting with Montgomery, Atkin and Morain.

Also examining the torsion of an elliptic curve over number fields of small degree has some additional benefits (Brier & Clavier (2010), D. & Najman (2012), Bosman, Bruin, D. & Najman (2014), Morain (2022, ANTS)).

It is well-known that elliptic curves have applications in public-key cryptography and also in factorization of large integers and primality proving.

The main idea is to replace the group $\mathbb{F}_p^*$ with (fixed) order $p-1$, by a group $E(\mathbb{F}_p)$ with more flexible order. Namely, by Hasse theorem we have

$$p+1-2\sqrt{p} < |E(\mathbb{F}_p)| < p+1+2\sqrt{p}.$$

Pollard's $p-1$ factorization method (1974):

Let n be a composite integer with unknown prime factor p. For any multiple m of $p-1$ we have $a^m \equiv 1 \pmod{p}$, and thus $p \mid \gcd(a^m-1, n)$. If $p-1$ is smooth (divisible only by small primes), then we can guess a multiple of $p-1$ by taking $m = \mathrm{lcm}(1, 2, ..., B)$ for a suitable number B.

Lenstra's Elliptic curve factorization method (1985):

In 1985, Lestra proposed the Elliptic curve factorization method (ECM), in which the group $\mathbb{F}_p^*$ is replaced by a group $E(\mathbb{F}_p)$, for a suitable chosen elliptic curve E. In ECM, one hopes that the chosen elliptic curve will have smooth order over a prime field.

It is now a classical method to use for that purpose elliptic curves E with large rational torsion over $\mathbb{Q}$ (and known point of infinite order), as the torsion will inject into $E(\mathbb{F}_p)$ for all primes p of good reduction. This in turn makes the order of $E(\mathbb{F}_p)$ more likely to be smooth.

Nice explicit examples of factorization of large numbers (Cunningham numbers in this case) by using elliptic curves over number fields of small degree have been provided by Brier and Clavier (2010). They used elliptic curves over cyclotomic fields with torsion groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. E.g. they found a factor

5546025484206613872527377154544456740766039233

of $2^{1048} + 1$ and a factor

1581214773543289355763694808184205062516817

of $2^{972} + 1$.

We say that an integer m is n-*smooth*, for some fixed value n if all the prime divisors of m are $\leq n$. For the elliptic curve factoring method, one wants to choose elliptic curves E such that the order $E(\mathbb{F}_p)$ is smooth. Standard heuristics say that larger torsion of $E(\mathbb{Q})$ implies a greater probability that $|E(\mathbb{F}_p)|$ is smooth. This is because the torsion of $E(\mathbb{Q})$ will inject into $E(\mathbb{F}_p)$ for all primes p of good reduction, making $|E(\mathbb{F}_p)|$ divisible by the order of the torsion of $E(\mathbb{Q})$.

But this is not necessary so straightforward, as a curve with smaller $E(\mathbb{Q})_{\text{tors}}$ can have much larger torsion over fields of small degree, giving all together a greater probability of $|E(\mathbb{F}_p)|$ to be smooth. We give an example of this phenomenon.

Example 1. (Bosman, Bruin, D. & Najman (2014))
Using the construction from Jeon, Kim and Lee (2011), let us take a rational curve with torsion $\mathbb{Z}/6\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ over the field $\mathbb{K} = \mathbb{Q}(\sqrt{-3}, \sqrt{217})$ and torsion $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}$. The curve is:

$$E_1 : y^2 = x^3 - 17811145/19683x - 81827811574/14348907.$$

Now take

$$E_2 : y^2 = x^3 - 25081083x + 44503996374.$$

The torsion of $E_2(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$, implying that by standard heuristics (examining only the rational torsion), $|E_2(\mathbb{F}_p)|$ should be more often smooth than $|E_1(\mathbb{F}_p)|$. Note that both curves have rank 1 over $\mathbb{Q}$, so the rank should not play a role.

We examine how often $|E_i(\mathbb{F}_p)|$, $i = 1, 2$, are 100-smooth and 200-smooth, where p_n, the n-th prime number, runs through the first 10000 and 100000 primes, excluding the first ten primes (to get rid of the primes of bad reduction). For comparison, we also take the elliptic curve

$$E_3 : y^2 = x^3 + 3,$$

with a trivial torsion group and rank 1.

	$10 < n < 10010$	$10 < n < 100010$
#100-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	4843	22872
#100-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	4302	20379
#100-sm. $\lvert E_3(\mathbb{F}_{p_n})\rvert$	2851	12344
#200-sm. $\lvert E_1(\mathbb{F}_{p_n})\rvert$	6216	35036
#200-sm. $\lvert E_2(\mathbb{F}_{p_n})\rvert$	5690	32000
#200-sm. $\lvert E_3(\mathbb{F}_{p_n})\rvert$	4134	21221

We see that, contrary to what one would expect if examining only the rational torsion, E_1 is consistently more likely to be smooth than E_2. Why does this happen? Examine the behavior of the torsion of $E_1(\mathbb{K})$ and $E_2(\mathbb{K})$ as $\mathbb{K}$ varies through all quadratic fields. The torsion of $E_2(\mathbb{K})$ will always be $\mathbb{Z}/7\mathbb{Z}$, while $E_1(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and $E_1(\mathbb{Q}(\sqrt{217}))_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. One fourth of the primes will split in $\mathbb{Q}(\sqrt{-3})$ and not in $\mathbb{Q}(\sqrt{217})$, one fourth vice versa, one fourth will split in neither field and one fourth will split in both fields (and thus splitting completely in $\mathbb{Q}(\sqrt{-3}, \sqrt{217})$). This implies that we know that $|E_1(\mathbb{F}_p)|$ is divisible by 6, 12, 18 and 36, each for one fourth of the primes, while all we can say for $|E_2(\mathbb{F}_p)|$ is that it is divisible by 7. We also see that $|E_3(\mathbb{F}_p)|$ is much less likely to be smooth than both E_1 and E_2.

Construction of high-rank elliptic 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 ("square rooting with a remainder" $p(x) = q^2(x) - r(x)$), by Elkies' method which use tools from arithmetic geometry 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:

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

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.

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 $1 \leq i < j \leq m$.

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 $k \geq 2$.

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.

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.

Induced elliptic curves

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

$$ax + 1 = \square, \qquad bx + 1 = \square, \qquad cx + 1 = \square. \tag{4}$$

It is natural to assign the elliptic curve

$$\mathcal{E}: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1) \tag{5}$$

to the system (4). 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 (4) 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 (4), 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. $[3]S' = \mathcal{O}$. In that case, curve $\mathcal{E}$ would have torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

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

$$3 + 4(ab+ac+bc) + 6abc(a+b+c) + 12(abc)^2 \\ - (abc)^2(a^2+b^2+c^2-2ab-2ac-2bc) = 0 \quad (6)$$

By writing (6) 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

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

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 (6), 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): $\boxed{r = 3}$

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

Torsion group $\mathbb{Z}/4\mathbb{Z}$

We will sketch the construction of an elliptic curve over $\mathbb{Q}(t)$ with torsion $\mathbb{Z}/4\mathbb{Z}$ and rank 6 (D. & Peral (2022)). Previously only rank 5 examples for such curves were known.

Our starting point is the construction of Elkies (2007) who notices that this torsion and rank 4 can be obtained for some elliptic $K3$ surfaces. In this case the maximum rank is obtained with the following type of reducible fibers for such a surface: four of type I_4, two of type I_2 and four of type I_1, so giving a contribution to the Néron-Severi group of $4(4-1)+2(2-1)) = 14$, hence the rank over this surface is at most $20-2-14 = 4$, so in this sense the Elkies example is optimal.

The general curve with torsion $\mathbb{Z}/4\mathbb{Z}$ is given by

$$Y^2 + aXY + abY = X^3 + bX^2,$$

where $ab(a^2 - 16b) \neq 0$. A torsion point of order 4 in this model is $(0,0)$. With a simple change of variables the surface can be written as

$$Y^2 = X^3 + (a^2 - 8b)X^2 + 16b^2X.$$

Elkies has shown that the discriminant -163 surface does have an elliptic model that attains rank 4 with torsion group $\mathbb{Z}/4\mathbb{Z}$, for the following values

$$a = (8t-1)(32t+7)$$
$$b = 8(t+1)(15t-8)(31t-7).$$

Inserting the values of a and b, we get the following $K3$ elliptic surface E:

$$\begin{aligned} E:\ Y^2 = X^3 &+ (65536t^4 - 17472t^3 - 10176t^2 + 18672t - 3535)X^2 \\ &+ 1024(t+1)^2(15t-8)^2(31t-7)^2 X \end{aligned}$$

It has torsion group $\mathbb{Z}/4\mathbb{Z}$ and rank 4. A torsion point of order 4 in this model is

$$(32(t+1)(15t-8)(31t-7), 2^5(1+t)(-1+8t)(-8+15t)(-7+31t)(7+32t))$$

and the X-coordinates of four independent points of infinite order are:

$$\begin{aligned} X_1 &= -361(t+1)(31t-7), \\ X_2 &= -4(t+1)(15t-8)(16t-7)^2, \\ X_3 &= -16(t+1)(8t+7)^2(15t-8), \\ X_4 &= 4(15t-8)(16t+1)^2(31t-7). \end{aligned}$$

To increase the rank, we impose

$$\frac{-64(1+t)^2(-4+7t)(4+17t)}{(1+4t)^2}$$

as the X-coordinate of a new point on E. This given the condition $-(-4+7t)(4+17t) = \Box$, which can be solved with

$$t \mapsto \frac{4(-1+u^2)}{(17+7u^2)}.$$

The resulting curve has rank 5.

On the other hand, imposing

$$\frac{576(-4+7t)(-8+15t)^2(-1324+5551t)}{49(-39+28t)^2}$$

as a the X-coordinate of a new point on E leads to the condition $(-4+7t)(-1324+5551t) = \square$, which can be solved with

$$t \mapsto \frac{4(-331+u^2)}{7(-793+u^2)}.$$

The corresponding curve also has rank 5.

But now we observe that both conditions

$$-(-4+7t)(4+17t) = \square$$
$$(-4+7t)(-1324+5551t) = \square,$$

can be solved simultaneously since when we apply the solution of the first condition to the second we have to solve $-(-1863+539u^2) = \square$. This can be done with

$$u \mapsto \frac{-7007-28r+13r^2}{7(539+r^2)}.$$

So we solve both conditions with

$$t \mapsto \frac{4\left(3r^2-14r-5390\right)\left(10r^2-14r-1617\right)}{7\left(72r^4-182r^3-13279r^2+98098r+20917512\right)}.$$

By inserting this into E, we get the curve over $\mathbb{Q}(r)$ with rank 6 (that rank is exactly 6 can be shown by Gusić-Tadić algorithm).

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

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), Flores, Jones, Rollick & Weigandt (2007), Fisher (2009), AttarBashi, Rathbun & Voznyy (2022)

induced by Diophantine triples

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

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)
$\mathbb{Z}/4\mathbb{Z}$	6	Dujella & Peral (2022)
$\mathbb{Z}/5\mathbb{Z}$	3	Lecacheux (2001), Eroshkin (2009), MacLeod (2014)
$\mathbb{Z}/6\mathbb{Z}$	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)
$\mathbb{Z}/3\mathbb{Z}$	7	9	Elkies (2007)
$\mathbb{Z}/4\mathbb{Z}$	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)
$\mathbb{Z}/8\mathbb{Z}$	**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)

Thank you very much
for your attention!