# HIGH-RANK ELLIPTIC CURVES WITH GIVEN TORSION GROUP AND SOME APPLICATIONS

ANDREJ DUJELLA

Abstract. In this survey paper, we describe several methods for constructing elliptic curves with a given torsion group and high rank over the rationals and quadratic fields. We also discuss potential applications of such curves in the elliptic curve factorization method and their role in the construction of rational Diophantine sextuples.

## 1. Introduction

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 $\mathrm{char}(\mathbb{K}) \neq 2, 3$, 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 non-zero. 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 with the law of addition defined by the secant and tangent method.

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:

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

The subgroup $E(\mathbb{Q})_{\mathrm{tors}}$ of $E(\mathbb{Q})$, which consists of all points of finite order, is called the *torsion group* of $E$, and the non-negative integer $r$ is called the *rank* of $E$, and it is denoted by $\mathrm{rank}(E)$ (or, more precisely, by $\mathrm{rank}(E(\mathbb{Q}))$). Natural questions arise: which are possible values of $E(\mathbb{Q})_{\mathrm{tors}}$ and $\mathrm{rank}(E)$, and, more ambitiously, which combinations of $E(\mathbb{Q})_{\mathrm{tors}}$ and $\mathrm{rank}(E)$ are possible.

In 1978, Mazur [44] proved that there are precisely 15 possible torsion groups for elliptic curves over $\mathbb{Q}$:

$$\begin{aligned} \mathbb{Z}/k\mathbb{Z}, &\qquad \text{for } k = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/k\mathbb{Z}, &\qquad \text{for } k = 2, 4, 6, 8. \end{aligned}$$

2020 *Mathematics Subject Classification.* Primary 11G05; Secondary 11Y05.
*Key words and phrases.* Torsion group, rank, elliptic curves, factorization.

On the other hand, 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, 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 than 21 (see [53]). The current record is an example of an elliptic curve over $\mathbb{Q}$ with rank $\geq 28$, found by Elkies in 2006 ([31]).

Finding elliptic curves with positive rank and large torsion 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 [48] and Atkin and Morain [4]. Also, examining elliptic curves with large torsion over number fields of small degrees has some additional benefits (see [7, 8, 25, 49]).

In this paper, we will describe several methods for constructing elliptic curves with a given torsion group and high rank over $\mathbb{Q}(t)$ and $\mathbb{Q}$. After describing general ideas in Section 4, in Sections 5 and 6, we will describe some connections between elliptic curves and rational Diophantine $m$-tuples, i.e. sets of $m$ non-zero rational such that the product of any two of them is one less than a perfect square. In Section 7, we will see how elliptic curves induced by rational Diophantine triples can be used to construct curves with record ranks for certain torsion groups. We will also, in Section 2, give some information on torsion groups and ranks for elliptic curves over quadratic fields. In Section 3, we will discuss the potential advantages of using curves with large torsion in the elliptic curve factorization method.

## 2. Elliptic curves over quadratic fields

Let $E$ be an elliptic curve over a quadratic field $E(\mathbb{K})$. Kenku and Momose [42] and Kamienny [40] proved that the torsion group of $E(\mathbb{K})$ is isomorphic to one of the following 26 groups:

$$\begin{aligned} \mathbb{Z}/k\mathbb{Z}, &\quad 1 \leq k \leq 18,\ k \neq 17, \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2k\mathbb{Z}, &\quad 1 \leq k \leq 6, \\ \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3k\mathbb{Z}, &\quad k = 1, 2, (\text{only if } \mathbb{K} = \mathbb{Q}(\sqrt{-3})), \\ \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, &\quad (\text{only if } \mathbb{K} = \mathbb{Q}(i)). \end{aligned}$$

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

In 2014, Bosman, Bruin, Dujella and Najman [7] proved several results concerning torsion groups and ranks of elliptic curves over number fields with small degrees. In particular, they proved that there exist elliptic curves over quadratic fields with positive rank and torsion $\mathbb{Z}/15\mathbb{Z}$ (rank $\geq 1$ over $\mathbb{Q}(\sqrt{345})$, $\mathbb{Z}/18\mathbb{Z}$ (rank $\geq 2$ over $\mathbb{Q}(\sqrt{26521})$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ (rank $\geq 4$ over $\mathbb{Q}(\sqrt{55325286553})$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ (rank $\geq 4$ over $\mathbb{Q}(\sqrt{2947271015})$).

Together with previous results of Rabarison [54], this implies that there exist curves with positive rank for all 26 possible torsion groups over quadratic fields. After the results of Aguirre, Dujella, Jukić Bokun and Peral [1], Najman [51] and Voznyy [59] (see also [37]), we know that for each of 26 possible torsion groups, there exists an elliptic curve over some quadratic field with this torsion group and with rank $\geq 2$.

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. In order to determine their rank over a quadratic field $\mathbb{Q}(\sqrt{d})$ we can use the formula

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

where $E^{(d)}$ denotes the $d$-quadratic twist of $E$ (the $d$-quadratic twist of $y^2 = x^3 + ax + b$ is $y^2 = x^3 + d^2ax + d^3b$). Thus, in these cases, we may apply methods for finding high-rank curves over $\mathbb{Q}$, which will be described in Section 4.

## 3. Applications of elliptic curves in factorization

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's theorem we have

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

In 1974, Pollard proposed the so-called *Pollard's $p-1$ factorization method*. Let $n$ be a composite integer with an 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 $m = \operatorname{lcm}(1, 2, ..., B)$ for a suitable number $B$.

In 1985, Lenstra [43] 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 the chosen elliptic curve will have smooth order over a prime field.

It is now a classical method to use for that purpose elliptic curve $E$ with large torsion group over $\mathbb{Q}$ (and fixed point of infinite order), as the torsion group injects 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) by using elliptic curves over number fields of small degrees have been provided by Brier and Clavier [8]. They used elliptic curves over cyclotomic fields with torsion groups $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. E.g. they found a factor

$$5546025484206613872527377154544456740766039233$$

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

$$158121477354328935576369480818420506251681 7$$

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 curve $E$ such that the order $E(\mathbb{F}_p)$ is smooth. Standard heuristics say that larger torsion group of $E(\mathbb{Q})$ implies a greater probability that $|E(\mathbb{F}_p)|$ is smooth.

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

**Example 3.1.** (Bosman, Bruin, Dujella and Najman [7])
Using the construction by Jeon, Kim and Lee [39], we take a rational curve with torsion $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ 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 $E_2$. To explain this, let us 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 $E_1(\mathbb{Q}(\sqrt{-3}))_{\text{tors}} \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $E_1(\mathbb{Q}(\sqrt{217}))_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. 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 $E_2$.

## 4. Construction of high-rank elliptic curves

The general method for finding a curve with large rank consists of the following three phases:

- *Construction of a family:* We generate 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). According to Silverman's specialization theorem [55, Chapter 3.11], for all except finitely many rational numbers $t_0$, the rank over $\mathbb{Q}$ of the curve, which is obtained by specializing $t = t_0$, will be greater than or equal to the generic rank. Let us mention that for

curves with at least one point of order 2 over $\mathbb{Q}(t)$, the algorithm by Gusić and Tadić [35, 36] enables finding corresponding injective specializations $t = t_0$ and calculating the generic rank. Methods used for construction of such families of curves include *Mestre's polynomial method* [47] (based on "square rooting with a remainder", i.e. writting a monic polynomial $p(x)$ of even degree in the form $q^2(x) - r(x)$, where the degree of $r$ is the smallest possible), *Elkies' method* [30] which uses tools from arithmetic geometry (we will apply it in Section 7.4) and *elliptic curves induced by Diophantine triples* [2, 13, 16, 24, 26, 27, 28] (we will provide more details on this method and its background in next sections).

- *Sieve:* We want to choose the best candidates for higher rank in the considered family of curves. For that purpose, for curves in the family (with not too huge coefficients), we calculate some data which gives us certain information about the rank (perhaps under the assumption that certain widely accepted conjectures hold, like Birch and Swinnerton-Dyer conjecture). Here, it is important that those imprecise information about the rank can be calculated much faster than the rank itself. Thus, instead of using the Birch and Swinnerton-Dyer conjecture directly, we use certain related quantities which are more suitable for computation, like *Mestre's conditional upper bound* [46] (which assumes BSD and GRH) and the so-called *Mestre-Nagao sums* [45, 50], e.g. the sum

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

  (see [32] for some optimizations and [41] for using deep convolutional neural networks in this context and comparison of several similar sums). Based on this information, we choose ("sieve") a small subset of the best candidates for the large rank in the considered family.
- *Calculating the rank:* For all curves from the (small) set of the best candidates, we try to calculate the rank exactly or at least to find a good lower bound for the rank to confirm that the curve indeed has large rank. For that purpose, we can use Cremona's program `mwrank` [10] (very good for curves with rational points of order 2), `MordellWeilShaInformation` in `Magma` [6] or `ellrank` in `PARI/GP` [52].

## 5. Diophantine $m$-tuples

As we mentioned in the previous section, Diophantine $m$-tuples, and in particular Diophantine triples, can be used in the construction of elliptic curves with high rank. Therefore, we will give a brief overview of the main definitions, problems and results about them. More information on this subject can be found e.g. in [17] and [18, Sections 14.6 and 16.7].

The Greek mathematician Diophantus of Alexandria first studied the problem of finding four numbers such that the product of any two of them, increased by 1, is a perfect square. He found a set of four positive rationals with this property:

$$\left\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\right\}.$$

The first set of four positive integers with the same property, $\{1, 3, 8, 120\}$, was found by Fermat.

The above examples motivate the following definition.

**Definition 5.1.** 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 $1 \leq i < j \leq m$.

It is natural to ask how large these sets, i.e. integer or rational Diophantine tuples, can be. This question was recently completely solved in the integer case. Euler proved that there exist infinitely many integer Diophantine quadruples. E.g. $\{k-1, k+1, 4k, 16k^3 - 4k\}$ is a Diophantine quadruple for $k \geq 2$. More generally, if $a$, $b$ and $r$ are positive integers such that $ab+1 = r^2$, then $\{a, b, a+b+2r, 4r(a+r)(b+r)\}$ is a Diophantine quadruple. The first important result concerning the problem of (non)existence of Diophantine quintuples was proved in 1969 by Baker and Davenport. Using Baker's theory on linear forms in logarithms of algebraic numbers and a reduction method based on continued fractions, they proved that if $d$ is a positive integer such that $\{1, 3, 8, d\}$ forms a Diophantine quadruple, then $d$ has to be 120 (this problem was raised by Denton [11], Gardner [33] and van Lint [58]). Their result implies that Fermat's set $\{1, 3, 8, 120\}$ cannot be extended to a Diophantine quintuple. In 2004, Dujella [15] proved that a Diophantine sextuple does not exist and that there are only finitely many Diophantine quintuples. Finally, in 2019, He, Togbé and Ziegler [38] proved that there does not exist a Diophantine quintuple.

5.1. **Rational Diophantine $m$-tuples.** Unlike the integer case, there is no known upper bound for the size of rational Diophantine tuples. Here Euler also made important contribution by proving that there are infinitely many rational Diophantine quintuples. More precisely, he proved that any pair $\{a, b\}$ such that $ab+1 = r^2$ can be extended to a quintuple. E.g. Fermat's quadruple can be extended to a rational Diophantine quintuple $\{1, 3, 8, 120, \frac{777480}{8288641}\}$. Much later, in 2019, Stoll [56] proved that this extension is unique.

In 1979, Arkin, Hoggatt and Strauss [3] generalized Euler's result by showing that any rational Diophantine triple $\{a, b, c\}$ can be extended to a quintuple, while in 1997, Dujella [12] proved that 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 Arkin-Hoggatt-Strauss constructions), in which case one of the extensions is the trivial extension by 0). Let us mention that if $abcd = 1$, then $ab$, $ac$, $ad$, $bc$, $bd$, $cd$ are all perfect squares (see [22]), and $\{a, b, c, d\}$ can be extended to a rational Diophantine quintuple by $e = \frac{(a+b-c-d)^2 - 4(ab+1)(cd+1)}{4d(ab+1)(ac+1)(bc+1)}$.

We may ask if $\{a, b, c, d, e\}$ and $\{a, b, c, d, f\}$ are two extensions from [12] and $ef \neq 0$, is it possible that $ef + 1$ is a perfect square? If the answer to this question is affirmative, it will provide examples of rational Diophantine sextuples. The rationals $e$ and $f$ are given by the following expressions:

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

where

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

By following this idea, in 1999, Gibbs [34] found the first rational Diophantine sextuple

$$\left\{\frac{5}{36}, \frac{5}{4}, \frac{32}{9}, \frac{189}{4}, \frac{665}{1521}, \frac{3213}{676}\right\},$$

while in 2016, Dujella, Kazalicki, Mikić and Szikszai [20] proved that there exist infinitely many rational Diophantine sextuples. Moreover, they proved that there are infinitely many rational Diophantine sextuples with positive elements, and also with any combination of signs.

## 6. 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 that $\mathcal{E}$ is induced by the triple $\{a, b, c\}$.

There are three rational points on $\mathcal{E}$ of order 2, namely

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

and also two 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. Now the above-mentioned result from [12] can be reformulated in this form: $x(T)x(T \pm S) + 1$ is always a perfect square ([14]). With $x(T) = d$, the numbers $x(T \pm S)$ are exactly $e$ and $f$ given above.

To describe the construction of infinite families of rational Diophantine sextuples from [20], we need the following generalization of this result.

**Proposition 6.1.** *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 (a curve of the degree 2) which contains three collinear points $Q$, $T$, $-(Q + T)$, so it has to be a union of two rational lines, i.e. 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 6.1 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 common 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 6.1 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 $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

By direct computation, we can write this condition explicitly, as in the following lemma.

**Lemma 6.2.** *For the point $S' = [1, rst]$ on $E'$ it holds $[3]S' = \mathcal{O}$ if and only if*

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

By writing (5) in terms of elementary symmetric polynomials, we find the following family of rational Diophantine triples satisfying the condition of Lemma 6.2:

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

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

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

## 7. 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, we know that $E(\mathbb{Q})_{\rm tors}=\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2m\mathbb{Z}$ with $m=1,2,3,4$. It is known (see [23]) that if $a,b,c$ are positive integers, then the cases $m=2$ and $m=4$ are not possible. On the other hand, if we allow $a,b,c$ to be rationals, then all possibilities $m=1,2,3,4$ can occur.

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 $\geq 5$ (torsion group is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$).

This result was improved in 2020 by Dujella and Peral [28], and 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 $\mathbb{Q}$ induced by rational Diophantine triples were constructed.

7.1. **Torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$.** 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 of 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, e.g. the curve induced by the rational Diophantine triple

$$\left\{\frac{7567037280}{7833785281}, \frac{4161669360289}{569762123040}, \frac{1359453258559}{948852707040}\right\},$$

which both tie the current records of ranks for curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ (see [27]).

7.2. **Torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$.** Elliptic curves with the torsion subgroup $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ 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 be 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 has 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 appear if

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

are perfect squares. In this way, Dujella and Peral [26, 27] obtained curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and rank 4 over $\mathbb{Q}(t)$ (the 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).

7.3. **Torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$.** An interesting fact is that any elliptic curve over $\mathbb{Q}$ with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ can be induced by a rational Diophantine triple (see [9, 16]). Thus, all results on the rank of elliptic curves with the torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ can be interpreted in terms of rational Diophantine triples. In 2007, Dujella [16] proved that for each $0\le r\le 3$, 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 $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ and the rank equal to $r$. In particular, the rational Diophantine triple

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

induces the curve with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/8\mathbb{Z}$ and rank 3, what is the current record for this torsion group.

7.4. **Torsion group $\mathbb{Z}/4\mathbb{Z}$.** We will sketch the recent construction, due to Dujella and Peral, of an elliptic curve over $\mathbb{Q}(t)$ with torsion $\mathbb{Z}/4\mathbb{Z}$ and rank 6 (see [29] for details). Previously only rank 5 examples for such curves were known.

The starting point is the construction of Elkies [30], who notices that this torsion group and rank 4 can be obtained for some elliptic $K3$ surfaces. The maximal 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 rank 4 can be obtained for the following values of $a$ and $b$:

$$\begin{aligned} a&=(8t-1)(32t+7)\\ b&=8(t+1)(15t-8)(31t-7). \end{aligned}$$

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

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

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 gives the condition $-(-4+7t)(4+17t)=\square$, which can be satisfied with

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

The resulting curve has rank 5 over $\mathbb{Q}(u)$.

On the other hand, imposing

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

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

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

The corresponding curve also has rank 5 over $\mathbb{Q}(u)$.

But now we observe that both conditions

$$\begin{aligned} -(-4+7t)(4+17t)&=\square\\ (-4+7t)(-1324+5551t)&=\square, \end{aligned}$$

can be satisfied simultaneously since the factor $(-4+7t)$ appear in both of them. We satisfy both conditions with

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

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 the Gusić-Tadić algorithm [35, 36]).

## 8. Tables with current records

Let $T$ be an admissible torsion group for an elliptic curve over the rationals. Define

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

It follows from the results of Montgomery [48], Suyama [57] and Atkin and Morain [4], motivated by finding suitable curves for the elliptic curve method of factorization, that $B(T) \geq 1$ for all 15 possible torsion groups $T$. This result was improved to $B(T) \geq 2$ by Womack in 2000 and to $B(T) \geq 3$ by Dujella in 2003, and this is still the best general result valid for all torsion groups $T$. However, there are better results for all torsion groups except for $T = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. The current records for all torsion groups are given in the following table (the details on the record curves can be found at [19]). The records which correspond to elliptic curves induced by rational Diophantine triples are indicated in bold.

| $T$ | $B(T) \geq$ | 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) |

As we mentioned above, the first step in finding elliptic curves with large rank is the construction of a parametric family of elliptic curves with the considered property (e.g. with a given torsion group). Thus, it is of interest to study the following quantity:

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

The current records for $G(T)$ for all possible torsion groups are given in the following table. Again, the records which correspond to elliptic curves induced by rational Diophantine triples are indicated in bold.

| $T$ | $G(T) \geq$ | 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) |
| $\mathbb{Z}/5\mathbb{Z}$ | 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) |

We may note that for certain (large) torsion groups, we know just a seemingly trivial bound $G(T) \geq 0$. The bound is not completely trivial since it implicitly includes the result that there are infinitely many elliptic curves with that torsion group. However, for the applications in factorization, we need curves with large torsion and positive rank. Therefore, it makes sense to consider not just infinite families parametrized by rational functions but also infinite families parametrized by rational points of some elliptic curves with positive rank. Let us define

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

The current records for $C(T)$ for all possible torsion groups are given in the following table. If the current record for $C(T)$ is strictly greater than the current record for $G(T)$, it means that the current record for $C(T)$ comes from a parametrization by rational points of some elliptic curves with positive rank.

| $T$ | $C(T) \geq$ | 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) |

We indicated in bold the four cases where the known lower bound for $C(T)$ coincide with the heuristic upper bound due to Park, Poonen, Voight and Wood [53]. These heuristic upper bounds are given in the column denoted by PPVW. If the heuristic is correct, then these four results are the best possible. However, in the recent paper by Dujella, Kazalicki and Peral [21], the families with (record) rank 3 for torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ were examined. The experiments suggest that in these families root numbers 1 and $-1$ (which conjecturally means even and odd ranks) are equidistributed, which would imply that there are infinitely many curves with rank $\geq 4$ for these torsion groups. This might indicate that the heuristic in [53] needs some adjustments, at least in the case of curves with torsion groups $\mathbb{Z}/8\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$.

**Acknowledgments.** The author acknowledges support from the QuantiXLie Center of Excellence, a project co-financed by the Croatian Government and European Union through the European Regional Development Fund - the Competitiveness and Cohesion Operational Programme (Grant KK.01.1.1.01.0004).

## References

[1] J. Aguirre, A. Dujella, M. Jukić Bokun and J. C. Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields*, Period. Math. Hungar. 68 (2014), 222–230.

[2] J. Aguirre, A. Dujella and J. C. Peral, *On the rank of elliptic curves coming from rational Diophantine triples*, Rocky Mountain J. Math. 42 (2012), 1759–1776.

[3] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. 17 (1979), 333–339.

[4] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. 60 (1993), 399–405.
[5] A. Baker and H. Davenport, *The equations* $3x^2 - 2 = y^2$ *and* $8x^2 - 7 = z^2$, Quart. J. Math. Oxford Ser. (2) 20 (1969), 129–137.
[6] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. 24 (1997), 235–265.
[7] J. Bosman, P. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN 2014 (2014), no. 11, 2885–2923.
[8] E. Brier and C. Clavier, *New families of ECM curves for Cunningham Numbers*, in: Proceedings of ANTS IX, Lecture Notes in Comput. Sci. 6197, Springer, Heidelberg, 2010, pp. 96–109.
[9] G. Campbell and E. H. Goins, *Heron triangles, Diophantine problems and elliptic curves*, preprint, 2007.
[10] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press, Cambridge, 1997.
[11] A. D. Denton, *A holiday brain teaser*, The Sunday Times, 4th August 1957, 18th August 1957.
[12] A. Dujella, *On Diophantine quintuples*, Acta Arith. 81 (1997), 69–79.
[13] A. Dujella, *Diophantine triples and construction of high-rank elliptic curves over* $\mathbb{Q}$ *with three non-trivial* 2*-torsion points*, Rocky Mountain J. Math. 30 (2000), 157–164.
[14] A. Dujella, *Diophantine* $m$*-tuples and elliptic curves*, J. Théor. Nombres Bordeaux 13 (2001), 111–124.
[15] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. 566 (2004), 183–214.
[16] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser. III 42 (2007), 3–18.
[17] A. Dujella, *What is ... a Diophantine* $m$*-tuple?*, Notices Amer. Math. Soc. 63 (2016), 772–774.
[18] A. Dujella, *Number Theory*, Školska knjiga, Zagreb, 2021.
[19] A. Dujella, *High rank elliptic curves with prescribed torsion*, `https://web.math.pmf.unizg.hr/~duje/tors/tors.html`
[20] A. Dujella, M. Kazalicki, M. Mikić and M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN 2017 (2017), no. 2, 490–508.
[21] A. Dujella, M. Kazalicki and J. C. Peral, *Elliptic curves with torsion groups* $\mathbb{Z}/8\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM 115 (2021), Article 169.
[22] A. Dujella, M. Kazalicki and V. Petričević, $D(n)$*-quintuples with square elements*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM 115 (2021), Article 172.
[23] A. Dujella and M. Mikić, *On the torsion group of elliptic curves induced by* $D(4)$*-triples*, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. 22 (2014), 79–90.
[24] A. Dujella and M. Mikić, *Rank zero elliptic curves induced by rational Diophantine triples*, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. 24 (2020), 29–37.
[25] A. Dujella and F. Najman, *Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization*, Period. Math. Hungar. 65 (2012), 193–203.
[26] A. Dujella and J. C. Peral, *High rank elliptic curves with torsion* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ *induced by Diophantine triples*, LMS J. Comput. Math. 17 (2014), 282–288.
[27] A. Dujella and J. C. Peral, *Elliptic curves induced by Diophantine triples*, Rev. R. Acad. Cienc. Exactas Fis. Nat. Ser. A Math. RACSAM 113 (2019), 791–806.
[28] A. Dujella and J. C. Peral, *High rank elliptic curves induced by rational Diophantine triples*, Glas. Mat. Ser. III 55 (2020), 237–252.
[29] A. Dujella and J. C. Peral, *An elliptic curve over* $\mathbb{Q}(u)$ *with torsion* $\mathbb{Z}/4\mathbb{Z}$ *and rank* 6, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. 28 (2024), to appear.
[30] N. D. Elkies, *Three lectures on elliptic surfaces and curves of high rank*, lecture notes, Oberwolfach, 2007, arXiv:0709.2908.
[31] N. D. Elkies, $\mathbb{Z}^{28}$ *in* $E(\mathbb{Q})$*, etc.*, Number Theory Listserver, May 2006.
[32] N. D. Elkies and Z. Klagsbrun, *New rank records for elliptic curves having rational torsion*, in: Proceedings of the Fourteenth Algorithmic Number Theory Symposium, Mathematical Sciences Publishers, Berkeley, 2020, pp. 233-250.

[33] M. Gardner, *Mathematical games*, Scientific American 216 (1967), March 1967, p. 124; April 1967, p.119.
[34] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III 41 (2006), 195–203.
[35] I. Gusić and P. Tadić, *A remark on the injectivity of the specialization homomorphism*, Glas. Mat. Ser. III 47 (2012), 265–275.
[36] I. Gusić and P. Tadić, *Injectivity of the specialization homomorphism of elliptic curves*, J. Number Theory 148 (2015), 137–152.
[37] L. Halbeisen, N. Hungerbühler, A. Shamsi Zargar and M. Voznyy, *A geometric approach to elliptic curves with torsion groups* $\mathbb{Z}/10\mathbb{Z}$*,* $\mathbb{Z}/12\mathbb{Z}$*,* $\mathbb{Z}/14\mathbb{Z}$*, and* $\mathbb{Z}/16\mathbb{Z}$, Rad Hrvat. Akad. Znan. Umjet. Mat. Znan. 27 (2023), 87–109.
[38] B. He, A. Togbé and V. Ziegler, *There is no Diophantine quintuple*, Trans. Amer. Math. Soc. 371 (2019), 6665–6709.
[39] D. Jeon, C. H. Kim, Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. 80 (2011), 2395–2410.
[40] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. 109 (1992), 221–229.
[41] M. Kazalicki and D. Vlah, *Ranks of elliptic curves and deep neural networks*, Res. Number Theory 9 (2023), Article 53.
[42] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. 109 (1988), 125–149.
[43] H. W. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. of Math. 126 (1987) 649–673.
[44] B. Mazur, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.
[45] J.-F. Mestre, *Construction d'une courbe elliptique de rang* $\geq 12$, C. R. Acad. Sci. Paris Ser I Math. 295 (1982), 643–644.
[46] J.-F. Mestre, *Formules explicites et minorations de conducteurs de variétés algébriques*, Compositio Math. 58 (1986), 209–232.
[47] J.-F. Mestre, *Courbes elliptiques de rang* $\geq 11$ *sur* $\mathbb{Q}(t)$, C. R. Acad. Sci. Paris Ser. I 313 (1991), 139–142.
[48] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. 48 (1987), 243–264.
[49] F. Morain, *Modular curves over number fields and ECM*, Res. Number Theory 8 (2022), no. 4, Paper No. 97, 17 pp.
[50] K. Nagao, *An example of elliptic curve over Q with rank* $\geq 20$, Proc. Japan Acad. Ser. A Math. Sci. 69 (1993), 291–293.
[51] F. Najman, *Some rank records for elliptic curves with prescribed torsion over quadratic fields*, An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. 22 (2014), 215–220.
[52] PARI Group, PARI/GP version 2.15.2, Bordeaux, 2022, http://pari.math.u-bordeaux.fr/
[53] J. Park, B. Poonen, J. Voight and M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, J. Eur. Math. Soc. (JEMS) 21 (2019), 2859–2903.
[54] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. 144 (2010), 17–52.
[55] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.
[56] M. Stoll, *Diagonal genus* 5 *curves, elliptic curves over* $\mathbb{Q}(t)$*, and rational diophantine quintuples*, Acta Arith. 190 (2019), 239–261.
[57] H. Suyama, *Informal preliminary report (8)*, October 1985.
[58] J. H. van Lint, *On a set of diophantine equations*, T. H.-Report 68 - WSK-03, Department of Mathematics, Technological University Eindhoven, Eindhoven, 1968.
[59] M. Voznyy, Personal communication, 2022.

Department of Mathematics, Faculty of Science, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia
*Email address*: duje@math.hr