On the torsion group of elliptic curves induced by Diophantine triples over quadratic fields

Andrej Dujella, Mirela Jukić Bokun and Ivan Soldo

Abstract

The possible torsion groups of elliptic curves induced by Diophantine triples over quadratic fields, which do not appear over $\mathbb{Q}$, are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. In this paper, we show that all these torsion groups indeed appear over some quadratic field. Moreover, we prove that there are infinitely many Diophantine triples over quadratic fields which induce elliptic curves with these torsion groups.

Keywords: Elliptic curve, quadratic field, torsion group, Diophantine triple
Mathematics Subject Classification (2010): 11G05, 11R11, 14H52

1 Introduction

A set $\{a_1, a_2, \ldots, a_m\}$ of m distinct nonzero rationals is called *a rational Diophantine m-tuple* if $a_i a_j + 1$ is a perfect square for all $1 \leq i < j \leq m$. The Greek mathematician Diophantus of Alexandria was the first who studied the existence of Diophantine quadruples in rationals. He discovered a rational Diophantine quadruple $\{\frac{1}{16}, \frac{33}{16}, \frac{17}{4}, \frac{105}{16}\}$. The first example of a Diophantine quadruple in integers, the set $\{1, 3, 8, 120\}$, was found by Fermat. In 1969, Baker and Davenport [3] proved that Fermat's set cannot be extended to a Diophantine quintuple in integers. It was proved in [11] that there does not exist a Diophantine sextuple of integers and there are only finitely many such quintuples. Euler extended the Fermat set to a rational quintuple $\{1, 3, 8, 120, \frac{777480}{8288641}\}$, and found infinitely many rational Diophantine quintuples (see [20]). The first example of rational Diophantine sextuple was given by Gibbs in [18]. It was the set $\{\frac{11}{192}, \frac{35}{192}, \frac{155}{27}, \frac{512}{27}, \frac{1235}{48}, \frac{180873}{16}\}$.

Authors were supported by the Croatian Science Foundation under the project no. 6422. A.D. acknowledges support from the QuantiXLie Center of Excellence.

Recently, in [15], it was proved that there are infinitely many rational Diophantine sextuples.

The problem of extendibility and existence of Diophantine m-tuples is closely connected with the properties of elliptic curves associated with them. Let $\{a, b, c\}$ be a rational Diophantine triple. This means that there exist nonnegative rationals r, s, t such that

$$ab + 1 = r^2, \quad ac + 1 = s^2, \quad bc + 1 = t^2. \tag{1}$$

If we want to extend Diophantine triple $\{a, b, c\}$ to a quadruple, we have to solve the system

$$ax + 1 = \square, \quad bx + 1 = \square, \quad cx + 1 = \square. \tag{2}$$

The elliptic curve assigned to the system (2) is

$$E: \qquad y^2 = (ax + 1)(bx + 1)(cx + 1). \tag{3}$$

We say that the elliptic curve E is induced by Diophantine triple $\{a, b, c\}$.

By Mazur's theorem [26], there are at most four possibilities for the torsion group over $\mathbb{Q}$ for such curves: $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$. In [12], it was shown that all these torsion groups actually appears. Moreover, it was shown that every elliptic curve with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}$ is induced by Diophantine triple (see also [7]). Questions about the ranks of elliptic curves induced by Diophantine triples was studied in several articles ([1, 10, 12, 16]). In particular, such curves were used for finding elliptic curves with the largest known rank with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ([16]).

In this paper, we study possible torsion groups of elliptic curves induced by Diophantine triples over quadratic fields, i.e., we will suppose that a, b, c are elements of some quadratic field and $ab + 1$, $ac + 1$ and $bc + 1$ are squares in the field. According to [23, 24], possible torsion groups for such curves which do not appear over $\mathbb{Q}$ are $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The last one can only appear over quadratic field $\mathbb{Q}(i)$. We show that all these torsion groups indeed appear over some quadratic field and that there are infinitely many Diophantine triples over quadratic fields which induce elliptic curves with these torsion groups. In Section 3, for each of three considered torsion groups, we present particular examples of elliptic curves over quadratic fields with reasonably large rank.

2 Torsion groups

The coordinate transform $x \mapsto \frac{x}{abc}, y \mapsto \frac{y}{abc}$ applied on the curve E leads to the elliptic curve

$$\begin{aligned} E': \qquad y^2 &= (x+ab)(x+bc)(x+ac) \\ &= x^3 + (ab+bc+ac)x^2 + (a^2bc + ab^2c + abc^2)x + a^2b^2c^2 \end{aligned} \tag{4}$$

in the Weierstrass form. There are three rational points on E' of order 2:

$$T_1 = [-ab, 0], \quad T_2 = [-bc, 0], \quad T_3 = [-ac, 0],$$

and other two obvious rational points

$$P = [0, abc], \quad Q = [1, rst].$$

2.1 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

A method for construction of Diophantine triples was known already to Euler, and in details is described in [9]. From that method and (1) we have

$$b = \frac{r^2-1}{a}, \quad c = a + b + 2r, \qquad r \notin \{-1, 1, 1-a, -1-a\}. \tag{5}$$

Our intention is to construct an elliptic curve E' on which the point $P = [0, abc]$ will be of order 5, i.e., $5P = \mathcal{O}$.

Lemma 1 *For the point $P = [0, abc]$ on E' satisfying condition (5) it holds $5P = \mathcal{O}$ if and only if*

$$\begin{aligned} &(-4r^2 + 4r^4)a^4 + (4r - 20r^3 + 16r^5)a^3 + (-1 + 16r^2 - 40r^4 + 24r^6)a^2 \\ &+(-4r + 24r^3 - 36r^5 + 16r^7)a - 4r^2 + 12r^4 - 12r^6 + 4r^8 = 0. \end{aligned}$$

Proof: The statement of Lemma 1 follows directly from the condition $\psi_5(P) = 0$, where

$$mP = \left(\frac{\phi_m(P)}{\psi_m(P)^2}, \frac{\omega_m(m)}{\psi_m(P)^3} \right),$$

and ϕ_m, ψ_m, ω_m are multiplication polynomials [29, Section 1.3]. □

Theorem 1 *There exist infinitely many quadratic fields $\mathbb{K}$ such that for each of them there exist infinitely many Diophantine triples which induce elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ over $\mathbb{K}$.*

Proof: If r^2-1 is a perfect square, then the polynomial from Lemma 1 factorizes as the product of two quadratic factors in a. This condition is satisfied for $r=\dfrac{t^2+1}{2t}$, $t\in\mathbb{Q}\setminus\{0\}$, which gives

$$\begin{aligned}&((4t^6-4t^2)a^2+(4t^7+4t^5+4t^3-4t)a+t^8-2t^6+2t^2-1)\\ &\times((4t^6-4t^2)a^2+(4t^7-4t^5-4t^3-4t)a+t^8-2t^6+2t^2-1).\end{aligned}$$

The roots of the factors are elements of quadratic fields $\mathbb{Q}(\sqrt{t^4+t^2-1})$, respectively $\mathbb{Q}(\sqrt{-t^4+t^2+1})$. Note that t^4+t^2-1 and $-t^4+t^2+1$ are not rational squares, since both conditions $t^4+t^2-1=\tilde{y}^2$ and $-t^4+t^2+1=\tilde{y}^2$ are birationally equivalent to the elliptic curve

$$E_1: \qquad y^2=x^3+x^2+4x+4,$$

with the torsion group $\mathbb{Z}/6\mathbb{Z}$ and the rank equal to 0 over $\mathbb{Q}$ (and torsion points correspond to $t=\pm1$ for the first curve and $t=0,\pm1$ for the second curve, which are excluded values since $t=\pm1$ gives $r=\pm1$).

In what follows, let $u\in\mathbb{Q}\setminus\{-1,0,1\}$. The elliptic curve E_1 over the quadratic field $\mathbb{Q}(v)$, $v=\sqrt{(2u^2+2u+1)(1-u^2)}$, contains the point

$$P_1=\left[\frac{-6u-4}{u-1},\frac{10v}{u-1}\right].$$

We will show that for all but finitely many rational numbers u the point P_1 is a point of infinite order on the curve E_1 over $\mathbb{Q}(v)$. Let us consider under which conditions the point P_1 will be a torsion point on the elliptic curve E_1 over $\mathbb{Q}(v)$. To check that, we try to find quadratic fields $\mathbb{K}$ for which $E_1(\mathbb{K})_{\text{tors}}$ is strictly larger than $E_1(\mathbb{Q})_{\text{tors}}$.

According to [19], for an elliptic curve with the torsion group $\mathbb{Z}/6\mathbb{Z}$ over $\mathbb{Q}$, its torsion group over a quadratic field can be extended to $\mathbb{Z}/12\mathbb{Z}$, over at most two quadratic fields, and to $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ over at most one quadratic field, each.

- We can use [19, Proposition 12] (see also [21]) to check if torsion group $\mathbb{Z}/6\mathbb{Z}$ extends to torsion group $\mathbb{Z}/12\mathbb{Z}$ over some quadratic field. Transformation $x\mapsto x+4$, $y\mapsto y$, transform the elliptic curve E_1 to

  $$E_1': \qquad y^2=x^3+13x^2+60x+100,$$

  where the point $[0,10]$ is point of order 6. From the mentioned proposition we conclude that there does not exist a quadratic field over which E_1 has torsion $\mathbb{Z}/12\mathbb{Z}$.

- According to [24], the torsion $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ can appear only over $\mathbb{Q}(\sqrt{-3})$. It is easy to show that over $\mathbb{Q}(\sqrt{-3})$ elliptic curve E_1 has torsion $\mathbb{Z}/6\mathbb{Z}$ and rank 0.

- Over $\mathbb{Q}(i)$, the curve E_1 has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and rank 0. The point P_1 is a torsion point over $\mathbb{Q}(i)$ for

$$u \in \left\{ -\frac{2}{3}, -1-i, -1+i, -\frac{1}{2}(1-i), -\frac{1}{2}(1+i) \right\},$$

  and in all other cases P_1 is a point of infinite order over $\mathbb{Q}(i)$.

We conclude that for every rational parameter $u \notin \{-1, -\frac{2}{3}, 0, 1\}$ the point P_1 is a point of infinite order on the curve E_1 over $\mathbb{Q}(v)$. Every multiple mP_1 of P_1 generates a Diophantine triple such that the induced elliptic curve E over $\mathbb{Q}(v)$ has torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$. Therefore, there exist infinitely many Diophantine triples which induce elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$, over $\mathbb{Q}(v)$.

To show that there are infinitely many different quadratic fields obtained with this construction, note that, according to Siegel's theorem [30, Chapter IX.3], there are only finitely many integer points on the curve

$$dy^2 = (2u^2 + 2u + 1)(1 - u^2),$$

for fixed square-free integer d.

□

2.2 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

We prove the following theorem:

Theorem 2 *There exist infinitely many quadratic fields $\mathbb{K}$ such that for each of them there exist infinitely many Diophantine triples which induce elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ over $\mathbb{K}$.*

Proof: By the results presented in [15], Diophantine triples $\{a, b, c\}$, where

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

induce elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/6\mathbb{Z}$ and positive rank (the point of infinite order is $P=[0,abc]$), for rationals $t\neq -1,0,1$. In order to obtain a point of the order 12 on that curve, we consider the point of the order 6 which has x-coordinate

$$x(P_6)=\frac{2t^4+3t^3-14t^2+3t+2}{3t(t^2-6t+1)}. \tag{7}$$

According to 2-descent proposition [25, Proposition 4.2.], we obtain conditions

$$\begin{aligned}(t^2-6t+1)(t^2+18t+1) &= u^2, &(8)\\ 6t(t^2+1) &= v^2. &(9)\end{aligned}$$

The condition (8) leads to the elliptic curve

$$y^2=x^3-x^2-225x-1215, \tag{10}$$

which has torsion group $\mathbb{Z}/2\mathbb{Z}$ and rank equal to 1 over $\mathbb{Q}$. The point of infinite order is $P_\infty=[27,-108]$.

For every parameter t which is generated by multiples mP_∞ ($m\geq 2$) of the point P_∞, from (9) we get the elliptic curve over the quadratic field $\mathbb{Q}(\sqrt{6t(1+t^2)})$. Therefore, over this quadratic field the Diophantine triple (6) induces the elliptic curve with torsion $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/12\mathbb{Z}$.

We conclude that there are infinitely many such quadratic fields, since, according to Falting's theorem [17], for fixed square-free integer d there are only finitely many rational points on the curve

$$dy^2=6t(t^2+1)(t^2-6t+1)(t^2+18t+1),$$

of genus 3.

This completes the proof of the Theorem 2. □

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

We show that there are infinitely many Diophantine triples which induce elliptic curves with torsion $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and we give their parameterization.

Theorem 3 *There exist infinitely many Diophantine triples which induce elliptic curves with torsion $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(i)$. Moreover, there exists a Diophantine triple which induces an elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/4\mathbb{Z}$ and positive rank over $\mathbb{Q}(i)(t)$.*

Proof: Diophantine triples $\{a, b, c\}$, where

$$\begin{aligned} a &= \frac{tu+1}{t-u}, \\ b &= -\frac{1}{a}, \\ c &= \frac{4tu}{(tu+1)(t-u)}, \end{aligned} \tag{11}$$

induce elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, over $\mathbb{Q}$, for admissible rational t, u (see [12]). As in proof of the Theorem 2, we apply 2-descent proposition to get torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. We obtain conditions

$$-(tu-1)^2 = m^2, \tag{12}$$

$$(t^3+t)u^3 + (t^3+t)u = n^2. \tag{13}$$

The condition (12) is always satisfied over $\mathbb{Q}(i)$. From (13), by using substitutions $U = (t^3+t)u, N = (t^3+t)n$, we get the elliptic curve

$$U^3 + (t^3+t)^2 U = N^2,$$

with the point $P_t = [t^2+1, (t^2+1)^2]$. It is easy to check that the point P_t does not generate an appropriate Diophantine triple, but its multiples $mP_t, m > 1$, do. For $m = 2$, we obtain

$$u = \frac{(t^2-1)^2}{4t(t^2+1)}. \tag{14}$$

Inserting (14) into (11), we obtain a parametric family of Diophantine triples $\{a, b, c\}$ where

$$\begin{aligned} a &= \frac{t(t^4+2t^2+5)}{3t^4+6t^2-1}, \\ b &= \frac{-3t^4-6t^2+1}{t^5+2t^3+5t}, \\ c &= \frac{16t(t^4-1)(t^2-1)}{(t^4+2t^2+5)(3t^4+6t^2-1)}, \end{aligned}$$

which induces an elliptic curve with torsion $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$, over $\mathbb{Q}(i)(t)$. By applying Silverman's specialization theorem [31, Theorem 11.4] (using, for example, the specialization $t = 2$) it can be shown that the point $P = [0, abc]$ is point of infinite order. □

3 Ranks

By the results of Kenku and Momose [24] and Kamienny [23], there are exactly 26 possibilities for the torsion group of elliptic curves defined over quadratic fields. Several authors constructed elliptic curves with reasonably large rank and given torsion group over quadratic fields (see [2, 6, 14, 22, 27, 28]). The current records can be found on the web page [13]. Here we show that in the cases of three torsion groups considered in the previous section, curves with positive rank can be induced by Diophantine triples over certain quadratic fields. In computations of the ranks, we will use `mwrank` [8] and `Magma` [5]. Since our curve will have rational coefficients, and in order to determine their rank over a quadratic field $\mathbb{Q}(\sqrt{d})$ we will use the formula (see [4])

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

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

3.1 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$

By taking $u = 3$, i.e. $v = -\frac{25}{8}$, in construction from Section 2.1, we get the curve with rank 3 and torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z}$ over $\mathbb{Q}(\sqrt{-2})$. In this case, $P_1 = [-11, 25\sqrt{-2}]$, $t = \frac{2}{5}\sqrt{-2}$ and $a = \frac{475}{561} + \frac{12737}{22440}\sqrt{-2}$. Hence, the curve is induced by the Diophantine triple

$$\left\{\frac{475}{561} + \frac{12737}{22440}\sqrt{-2}, -\frac{475}{561} + \frac{12737}{22440}\sqrt{-2}, \frac{160}{561}\sqrt{-2}\right\}.$$

The Weierstrass equation of the curve is

$$y^2 = x^3 + x^2 - 61404142096090881x - 20861928799251086002759425.$$

Three independent points of infinite order are:

$$[865303425, 23956226997120],$$
$$\left[\frac{48954515537984337}{16008001}, \frac{10791931818384647817975000}{64048012001}\right],$$
$$\left[\frac{86963667871383}{299209}, \frac{435438077091034960800}{163667323}\sqrt{-2}\right].$$

Let us mention that the current record for the rank for arbitrary elliptic curves over quadratic fields with torsion group $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/10\mathbb{Z}$ is 4 (see [6, 2]).

3.2 Torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$

By taking multiples $2P_\infty$ and $3P_\infty$ from Section 2.2, we get $t = 6/35$ and $t = 41615/426$, and in both cases we obtain curves with rank between 1 and 3. For larger multiples, the coefficients of the curves are too large and we are not able to compute reasonable bounds for the rank. For $t = 41615/426$, we can conclude that the rank of the corresponding curve over $\mathbb{Q}(\sqrt{5117449349905165})$ is equal to 3 assuming the Parity conjecture.

We can use other parametric families of rational Diophantine triples which satisfy the condition of [15, Lemma 1], and hence induce elliptic curves over $\mathbb{Q}$ with torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, as the starting point for our construction, e.g.,

$$a = \frac{u^3 - 9u}{6(u^2-1)}, b = -\frac{9(u^2-1)}{2(u^3-9u)}, c = -\frac{16u(u^2-3)}{3(u^4-10u^2+9)}.$$

Now the condition for the torsion $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ becomes $3(u-1)(u+1)(u^2+15) = v^2$. Thus, we may take here $u = -7$, and we get the curve induced by the Diophantine triple

$$\left\{-\frac{35}{36}, \frac{27}{35}, \frac{161}{180}\right\},$$

which has torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ and rank (unconditionally) equal to 2 over $\mathbb{Q}(\sqrt{-155})$. The Weierstrass equation of the curve is

$$y^2 + xy + y = x^3 - 49428958x + 130902669056,$$

and two independent points of infinite order are:

$$[-2510, -487783], \left[-\frac{95078581}{245}, \frac{166483532709}{8575}\sqrt{-155}\right].$$

The current record for the rank for arbitrary elliptic curves over quadratic fields with torsion group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$ is 4 (see [6]).

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

Inserting $t = 4/3$ in the family of Diophantine triples from Section 2.3, we obtain the curve with rank 6 and torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ over $\mathbb{Q}(i)$. The curve is induced by the Diophantine triple

$$\left\{\frac{3796}{4653}, -\frac{4653}{3796}, \frac{78400}{490633}\right\}.$$

The Weierstrass equation of the curve is

$$y^2 = x^3+x^2-158862757398228713194320 0x-5071615458843295013016280004920406 52.$$

Six independent points of infinite order are:

$$\begin{gathered}
[-890497354044, 448726623142928130], \\
[-899563900533, 440419889828558640], \\
\left[\frac{2502824381840097811}{632025}, \frac{37365382686655876101118750 16}{502459875}\right], \\
[-1089076885194, 262231774368503940\,i], \\
[-1926913622169, 2144909371334503410\,i], \\
\left[-\frac{10573435624608518034}{6175225}, \frac{25709440364558354804130497052}{15345434125}\,i\right].
\end{gathered}$$

The current record for the rank over $\mathbb{Q}(i)$ for arbitrary elliptic curves with torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ is 7 (see [14]).

References

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

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

[3] A. Baker, 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.

[4] B. J. Birch, *Elliptic curves and modular functions*, in: Symposia Mathematica, Vol. IV, Academic Press, London, 1970, pp. 27–32.

[5] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), 235–265.

[6] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN **2014 (11)** (2014), 2885–2923.

[7] G. Campbell, E. H. Goins, *Heron triangles, Diophantine problems and elliptic curves*, preprint, `http://www.swarthmore.edu/NatSci/gcampbe1/papers/heron-Campbell-Goins.pdf`

[8] J. Cremona, Algorithms for Modular Elliptic Curves, Cambridge University Press, Cambridge, 1997.

[9] A. Dujella, *Some polynomial formulas for Diophantine quadruples*, Grazer Math. Ber. **328** (1996), 25–30.

[10] 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.

[11] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183–214.

[12] A. Dujella, *On Mordell-Weil groups of elliptic curves induced by Diophantine triples*, Glas. Mat. Ser III **42** (2007), 3–18.

[13] A. Dujella, *High rank elliptic curves with prescribed torsion over quadratic fields*, `http://web.math.pmf.unizg.hr/~duje/tors/torsquad.html`

[14] A. Dujella, M. Jukić Bokun, *On the rank of elliptic curves over $\mathbb{Q}(i)$ with torsion group $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$*, Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), 93–96.

[15] A. Dujella, M. Kazalicki, M. Mikić, M. Szikszai, *There are infinitely many rational Diophantine sextuples*, Int. Math. Res. Not. IMRN, to appear.

[16] A. Dujella, 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.

[17] G. Faltings, *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern*, Invent. Math. **73** (1983), 349–366.

[18] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195–203.

[19] E. González Jiménez, J. M. Tornero, *Torsion of rational elliptic curves over quadratic fields II*, Rev. R. Acad. Cienc. Exactas Fís. Nat. Ser. A Math. RACSAM **108** (2014), 923–934.

[20] T. L. Heath, Diophantus of Alexandria. A Study in the History of Greek Algebra. Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003.

[21] D. Jeon, C. H. Kim, Y. Lee, *Infinite families of elliptic curves over dihedral quartic number fields*, J. Number Theory **133** (2013), 115–122.

[22] M. Jukić Bokun, *On the rank of elliptic curves over* $\mathbb{Q}(\sqrt{-3})$ *with torsion groups* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *and* $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, Proc. Japan Acad. Ser. A Math. Sci. **87** (2011), 61–64.

[23] S. Kamienny, *Torsion points on elliptic curves and q-coeficients of modular forms*, Invent. Math. **109** (1992), 221–229.

[24] M. A. Kenku, F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[25] A. Knapp, Elliptic Curves, Princeton Univ. Press, New Jersey, 1992.

[26] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

[27] 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.

[28] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144** (2010), 17–52.

[29] S. Schmitt, H. G. Zimmer, Elliptic Curves: A Computational Approach, Walter de Gruyter, Berlin-New York, 2003.

[30] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer, New York, 1986.

[31] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer, New York, 1994.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30

10000 Zagreb, Croatia
e-mail: duje@math.hr

Mirela Jukić Bokun
Department of Mathematics
University of Osijek
Trg Ljudevita Gaja 6
31000 Osijek, Croatia
e-mail: mirela@mathos.hr

Ivan Soldo
Department of Mathematics
University of Osijek
Trg Ljudevita Gaja 6
31000 Osijek, Croatia
e-mail: isoldo@mathos.hr