

**DIOPHANTINE TRIPLES AND CONSTRUCTION OF  
HIGH-RANK ELLIPTIC CURVES OVER  $\mathbf{Q}$  WITH  
THREE NON-TRIVIAL 2-TORSION POINTS**

ANDREJ DUJELLA

## 1 Introduction

Let  $E$  be an elliptic curve over  $\mathbf{Q}$ . The famous theorem of Mordell-Weil states that

$$E(\mathbf{Q}) \simeq E(\mathbf{Q})_{\text{tors}} \times \mathbf{Z}^r,$$

and by a theorem of Mazur [15] we know that only possible torsion groups over  $\mathbf{Q}$  are

$$E(\mathbf{Q})_{\text{tors}} = \begin{cases} \mathbf{Z}/m\mathbf{Z}; & m = 1, 2, \dots, 10 \text{ or } 12, \\ \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2m\mathbf{Z}; & m = 1, 2, 3, 4. \end{cases}$$

Let

$$B(F) = \sup\{\text{rank}(E) : E \text{ curve over } \mathbf{Q} \text{ with } E(\mathbf{Q})_{\text{tors}} \simeq F\},$$

$$B_r(F) = \limsup\{\text{rank}(E) : E \text{ curve over } \mathbf{Q} \text{ with } E(\mathbf{Q})_{\text{tors}} \simeq F\}.$$

An open question is whether  $B(F) < \infty$ .

The examples of Martin-McMillen and Fermigier [8] show that  $B(0) \geq 23$  and  $B(\mathbf{Z}/2\mathbf{Z}) \geq 14$ . It follows from results of Montgomery [18] and Atkin-Morain [1] that  $B_r(F) \geq 1$  for all torsion groups  $F$ . Kihara [11] proved that  $B_r(0) \geq 14$  and Fermigier [8] that  $B_r(\mathbf{Z}/2\mathbf{Z}) \geq 8$ . Recently, Kihara [12] and Kulesz [14] proved using parametrization by  $\mathbf{Q}(t)$  and  $\mathbf{Q}(t_1, t_2, t_3, t_4)$  that  $B_r(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \geq 4$ , and Kihara [13] proved using parametrization by rational points of an elliptic curve that  $B_r(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \geq 5$ . Kulesz also proved that  $B_r(\mathbf{Z}/3\mathbf{Z}) \geq 6$ ,  $B_r(\mathbf{Z}/4\mathbf{Z}) \geq 3$ ,  $B_r(\mathbf{Z}/5\mathbf{Z}) \geq 2$ ,  $B_r(\mathbf{Z}/6\mathbf{Z}) \geq 2$  and  $B_r(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}) \geq 2$ . The methods used in [12] and [14] are similar to the method of Mestre [16, 17].

In the present paper we prove that  $B_r(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \geq 4$  by different method. Namely, we use the theory of, so called, Diophantine  $m$ -tuples. By specialization, we obtain an example of elliptic curve over  $\mathbf{Q}$  with torsion group  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  whose rank is equal 7, which shows that  $B(\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}) \geq 7$ .

## 2 Construction

A set of  $m$  non-zero rationals  $\{a_1, a_2, \dots, a_m\}$  is called a (*rational*) *Diophantine  $m$ -tuple* if  $a_i a_j + 1$  is a perfect square for all  $1 \leq i < j \leq m$  (see [4]).

Let  $\{a, b, c\}$  be a Diophantine triple, i.e.

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

Define

$$d = a + b + c + 2abc + 2qrs, \quad e = a + b + c + 2abc - 2qrs.$$

Then it can be easily checked that  $ad + 1$ ,  $bd + 1$ ,  $cd + 1$ ,  $ae + 1$ ,  $be + 1$  and  $ce + 1$  are perfect squares. For example,  $ad + 1 = (as + qr)^2$ .

Let us mention that for  $a, b, c$  positive integers there is a conjecture that if  $x$  is a positive integer such that  $\{a, b, c, x\}$  is a Diophantine quadruple, then  $x$  has to be equal to  $d$  or  $e$ . This conjecture was verified for some special Diophantine triples (see [2, 5, 6, 7, 10]).

Furthermore, assume that  $de + 1$  is also a perfect square. Note that this is impossible if  $a, b, c$  are positive integers and  $de \neq 0$ , but it is possible for rationals  $a, b, c$ .

Consider now the elliptic curve

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

One may expect that  $E$  has at least four independent points of infinite order, namely, points with  $x$ -coordinates

$$0, \quad a, \quad c, \quad \frac{1}{bde}.$$

The main problem is to satisfy condition  $de + 1 = w^2$ . It can be done, for example, in the following way. Let  $a$  be fixed. Put  $b = ak^2 + 2k$ . Then  $q = ak + 1$ , and put  $c = 4q(q - a)(b - q)$ . It is easy to check that now  $\{a, b, c\}$

is a Diophantine triple. Namely,  $r = q^2 + ab - 2aq$  and  $s = q^2 + ab - 2bq$ . Furthermore, let  $ak = t$ . Now the condition  $de + 1 = w^2$  becomes

$$[k^2(t+2)(2t+1)(2t+3) - 4k(t+1)(2t^2+4t+1) + t(2t+1)(2t+3)]^2 - k^2(4t^2 + 8t + 3) = w^2. \quad (1)$$

There are two obvious solutions of (1), namely,  $(k_0, w_0) = (0, t(2t+1)(2t+3))$  and  $(k_1, w_1) = (1, 1)$ , but in both cases we have  $bcd = 0$ , and therefore they do not lead to a usable formula. However, using the solution  $(k_0, w_0)$  we may construct a non-trivial and usable solution of (1). Denote the polynomial on the left side of (1) by  $F(k, t)$ . Choose the polynomial  $f(k, t) = \alpha(t)k^2 + \beta(t)k + \gamma(t)$  such that

$$F(k, t) - [f(k, t)]^2 = k^3 \cdot G(k, t).$$

Then from the condition  $G(k, t) = 0$  we obtain a non-trivial solution of (1):

$$k_2 = \frac{16t(t+1)(2t^2+4t+1)}{16t^4+64t^3+76t^2+24t-1}. \quad (2)$$

Using (2) we obtain the following expressions for  $b$ ,  $d$  and  $e$ :

$$b(t) = \frac{16t(t+1)(t+2)(2t^2+4t+1)}{16t^4+64t^3+76t^2+24t-1}, \quad (3)$$

$$d(t) = \frac{256t^8 + 2048t^7 + 6272t^6 + 8960t^5 + 5424t^4 + 192t^3 - 888t^2 - 112t + 33}{16(16t^4 + 64t^3 + 76t^2 + 24t - 1)(2t^2 + 4t + 1)(t + 1)}, \quad (4)$$

$$e(t) = \frac{(4096t^{12} + 49152t^{11} + 262144t^{10} + 819200t^9 + 1665024t^8 + 2310144t^7 + 2233728t^6 + 1507584t^5 + 697856t^4 + 211968t^3 + 38624t^2 + 3520t + 105)}{[16(16t^4 + 64t^3 + 76t^2 + 24t - 1)(2t^2 + 4t + 1)(t + 1)]}. \quad (5)$$

**Theorem 1** *Let  $b(t)$ ,  $d(t)$  and  $e(t)$  be defined by (3), (4) and (5). Then the elliptic curve*

$$E : y^2 = (b(t)x + 1)(d(t)x + 1)(e(t)x + 1) \quad (6)$$

*over  $\mathbf{Q}(t)$  has the torsion group isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  and the rank greater or equal 4.*

*Proof.* The points  $\mathcal{O}$ ,  $A = (-\frac{1}{b(t)}, 0)$ ,  $B = (-\frac{1}{d(t)}, 0)$ ,  $C = (-\frac{1}{e(t)}, 0)$  form a subgroup of the torsion group  $E_{\text{tors}}(\mathbf{Q}(t))$  which is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . By Mazur's theorem and a theorem of Silverman ([19, Theorem 11.4, p.271]), it suffices to check that there is no point on  $E(\mathbf{Q}(t))$  of order four or six.

If there is a point  $D$  on  $E(\mathbf{Q}(t))$  such that  $2D \in \{A, B, C\}$ , then 2-descent Proposition (see [9, 4.1, p.37]) implies that at least one of the expressions  $\pm b(t)[e(t) - d(t)]$ ,  $\pm d(t)[e(t) - b(t)]$ ,  $\pm e(t)[d(t) - b(t)]$  is a perfect square. However, by specialization  $t = 1$  we see that this is not the case.

If there is a point  $F = (x, y)$  on  $E(\mathbf{Q}(t))$  such that  $3F = A$ ,  $F \neq A$ , then from  $2F = -F + A$  we obtain the equation

$$x^4 - 6g(t)x^2 - 4g(t)h(t)x - 3h(t)^2 = 0, \quad (7)$$

where  $g(t) = b(t)e(t) + d(t)e(t) - 2b(t)d(t)$ ,  $h(t) = b(t)d(t)[e(t) - d(t)][e(t) - b(t)]$ . One can easily check that e.g. for  $t = 1$  the equation (7) has no rational solution. Similarly we can prove that there is no point  $F$  on  $E(\mathbf{Q}(t))$  such that  $3F = B$ ,  $F \neq B$  or  $3F = C$ ,  $F \neq C$ . Therefore, we conclude that  $E_{\text{tors}}(\mathbf{Q}(t))$  is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ .

Now, we will prove that four points with  $x$ -coordinates 0,

$$a(t) = \frac{16t^4 + 64t^3 + 76t^2 + 24t - 1}{16(2t^2 + 4t + 1)(t + 1)},$$

$$c(t) = \frac{(t + 1)(16t^4 + 64t^3 + 68t^2 + 8t + 1)(16t^4 + 64t^3 + 100t^2 + 72t + 17)}{4(16t^4 + 64t^3 + 76t^2 + 24t - 1)(2t^2 + 8t + 1)}$$

and

$$\frac{1}{b(t)d(t)e(t)}$$

are independent  $\mathbf{Q}(t)$ -rational points. Since the specification map is always a homomorphism, we only have to show that there is a rational number  $t$  for which above four points are specialized to four independent  $\mathbf{Q}$ -rational points. We claim that this is the case for  $t = 1$ .

We obtain the elliptic curve

$$\begin{aligned} E^* : \quad y^2 = x^3 &+ 6039621860663185x^2 \\ &+ 4139229575576935297875399628800x \\ &+ 48358738060886226093564403421659325399040000 \end{aligned}$$

and the points

$$P = (0, 6954044726695840435200),$$

$$\begin{aligned} Q &= (2322788497348275, 234053443113019268212650), \\ R &= (48986399479921200, 11499867835919119918338000), \\ S &= (51511970169856/9, 229496624258539337814016/27). \end{aligned}$$

Then  $S = 2S_1$ ,  $P - Q = 2Q_1$ ,  $P - R = 2R_1$ , where

$$\begin{aligned} Q_1 &= (265264199014080, -39874704566573066299200), \\ R_1 &= (3714953903426304, 387359212888080790925568), \\ S_1 &= (2452641432447360, 247558457515476853468800). \end{aligned}$$

It is sufficient to prove that the points  $P, Q_1, R_1, S_1$  are independent. The curve  $E^*$  has three 2-torsion points:

$$\begin{aligned} A^* &= (-11888861752320, 0), \\ B^* &= (-5253470166461440, 0), \\ C^* &= (-774262832449425, 0). \end{aligned}$$

Consider all points of the form

$$X = \varepsilon_1 P + \varepsilon_2 Q_1 + \varepsilon_3 R_1 + \varepsilon_4 S_1 + T,$$

where  $\varepsilon_i \in \{0, 1\}$  for  $i = 1, 2, 3, 4$ ,  $T \in \{\mathcal{O}, A^*, B^*, C^*\}$  and  $X = (x, y) \neq \mathcal{O}$ . For all of these 63 points at least one of the numbers  $x + 11888861752320$  and  $x + 5253470166461440$  is not a perfect square. Hence, from 2-descent Proposition ([9, 4.1, p.37]) it follows that  $X \notin 2E(\mathbf{Q})$ .

Assume now that  $P, Q_1, R_1, S_1$  are dependent modulo torsion, i.e. that there exist integers  $i, j, m, n$  such that  $|i| + |j| + |m| + |n| \neq 0$  and

$$iP + jQ_1 + mR_1 + nS_1 = T,$$

where  $T \in \{\mathcal{O}, A^*, B^*, C^*\}$ . Then the result which we just proved shows that  $i, j, m, n$  are even, say  $i = 2i_1$ ,  $j = 2j_1$ ,  $m = 2m_1$ ,  $n = 2n_1$ , and  $T = \mathcal{O}$ . Thus we obtain

$$i_1 P + j_1 Q_1 + m_1 R_1 + n_1 S_1 \in \{\mathcal{O}, A^*, B^*, C^*\}.$$

Arguing as above, we conclude that  $i_1, j_1, m_1, n_1$  are even, and continuing this process we finally obtain that  $i = j = m = n = 0$ , a contradiction. ■

By a theorem of Silverman ([19, Theorem 11.4, p. 271]), the specialization map is an injective homomorphism for all but finitely many points  $t \in \mathbf{Q}$ . This fact implies that by specialization of the parameter  $t$  to a rational number one gets in all but finitely many cases elliptic curves over  $\mathbf{Q}$  of rank at least four, and with subgroup of the torsion group which is isomorphic to  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$ . Hence, we have

**Corollary 1** *There is an infinite number of elliptic curves over  $\mathbf{Q}$  with three non-trivial 2-torsion points whose rank is greater or equal 4.*

### 3 An example of high-rank curve

We used the program *mwrank* (see [3]) for computing the rank of elliptic curves obtained from (6) by specialization of parameter  $t$ . However, since the coefficients in the corresponding Weierstraß form are usually very large, we were able to determine the rank unconditionally only for a few values of  $t$ . The following table shows the values of  $t$  for which we were able to compute the rank.

$t$	$\frac{1}{4}$	$\frac{1}{2}$	1	$\frac{3}{2}$	2
Selmer rank	8	4	5	8	9
rank	4	4	5	6	7

Hence, we obtain

**Theorem 2** *There is an elliptic curve over  $\mathbf{Q}$  with the torsion group  $\mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$  whose rank is equal 7.*

Let us write this example of the curve with rank equal 7 explicitly:

$$y^2 = \left(\frac{2176}{373}x + 1\right)\left(\frac{192386145}{101456}x + 1\right)\left(\frac{122265}{101456}x + 1\right)$$

or in Weierstraß form:

$$\begin{aligned}
 y^2 = & x^3 + 19125010376436745905x^2 \\
 & + 52038165131253677052054066913723699200x \\
 & + 521987941186440643611574160434960523120404754595840000.
 \end{aligned} \tag{8}$$

Seven independent points on (8) are

$$\begin{aligned}
 P_1 &= (727040606274688800, 6989234854370183719797420000), \\
 P_2 &= \left( \frac{106210585076366036700000}{12769}, \frac{69679298576214445317616490513378400}{1442897} \right), \\
 P_3 &= \left( \frac{335675366319765814629760}{71289}, \frac{529539341511970538352844395949129600}{19034163} \right), \\
 P_4 &= \left( \frac{8891873190221412964144}{81}, \frac{910251624041798036784012061900208}{729} \right), \\
 P_5 &= \left( \frac{101700294221755145291440}{841}, \frac{34956857441184030025736520646806800}{24389} \right), \\
 P_6 &= \left( \frac{73133606420424854742955}{114921}, \frac{251397104609526457099162042379450150}{38958219} \right), \\
 P_7 &= (-11146430015095060400, 20291973801839968429609236400).
 \end{aligned}$$

**Acknowledgements.** The author would like to thank J.E. Cremona and the referee for helpful suggestions and L. Kulesz for kindly providing his recent preprint.

## References

- [1] A. O. L. Atkin and F. Morain, *Finding suitable curves for the elliptic curve method of factorization*, Math. Comp. **60** (1993), 399–405.
- [2] 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.
- [3] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, 1997.
- [4] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69–79.
- [5] A. Dujella, *The problem of the extension of a parametric family of Diophantine triples*, Publ. Math. Debrecen **51** (1997), 311–322.

- [6] A. Dujella, *A proof of the Hoggatt-Bergum conjecture*, Proc. Amer. Math. Soc., to appear.
- [7] A. Dujella and A. Pethő, *Generalization of a theorem of Baker and Davenport*, Quart. J. Math. Oxford Ser. (2), **49** (1998), 291–306.
- [8] S. Fermigier, *Exemples de courbes elliptiques de grand rang sur  $\mathbf{Q}(t)$  et sur  $\mathbf{Q}$  possédant des points d'ordre 2*, C. R. Acad. Sci. Paris Sér. I Math. **332** (1996), 949–952.
- [9] D. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.
- [10] K. S. Kedlaya, *Solving constrained Pell equations*, Math. Comp. **67** (1998), 833–842.
- [11] S. Kihara, *On an infinite family of elliptic curves with rank  $\geq 14$  over  $\mathbf{Q}$* , Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), 32.
- [12] S. Kihara, *On the rank of elliptic curves with three rational points of order 2*, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), 77–78.
- [13] S. Kihara, *On the rank of elliptic curves with three rational points of order 2. II*, Proc. Japan Acad. Ser. A Math. Sci. **73** (1997), 151.
- [14] L. Kulesz, *Courbes elliptiques de rang élevé, possédant un sous-groupe de torsion non trivial sur  $\mathbf{Q}$* , preprint.
- [15] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
- [16] J.-F. Mestre, *Courbes elliptiques de rang  $\geq 11$  sur  $\mathbf{Q}(t)$* , C. R. Acad. Sci. Paris Sér I Math. **313** (1991), 139–142.
- [17] J.-F. Mestre, *Courbes elliptiques de rang  $\geq 12$  sur  $\mathbf{Q}(t)$* , C. R. Acad. Sci. Paris Sér I Math. **313** (1991), 171–174.
- [18] P. L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*, Math. Comp. **48** (1987), 243–264.
- [19] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ZAGREB, BIJENIČKA CESTA 30,  
10000 ZAGREB, CROATIA

*E-mail address:* duje@math.hr