An example of elliptic curve over $\mathbb{Q}$ with rank equal to 15

Andrej Dujella

Abstract

We construct an elliptic curve over $\mathbb{Q}$ with non-trivial 2-torsion point and rank exactly equal to 15.

1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$. By Mordell's theorem, $E(\mathbb{Q})$ is a finitely generated abelian group. This means that $E(\mathbb{Q}) \simeq E(\mathbb{Q})_{\text{tors}} \times \mathbb{Z}^r$. By Mazur's theorem, we know that $E(\mathbb{Q})_{\text{tors}}$ is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$.

On the other hand, we do not know what values of rank r are possible for elliptic curves over $\mathbb{Q}$. The "folklore" conjecture is that a rank can be arbitrary large, but at present only an example of elliptic curve with rank ≥ 24 is known [10]. There is even a stronger conjecture that, for any of 15 possible torsion groups T, we have $B(T) = \infty$, where

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

It follows from results of Montgomery [13] and Atkin-Morain [1] that $B(T) \geq 1$ for all torsion groups T. Womack [16] proved that $B(T) \geq 2$ for all T, while Dujella [5] proved that $B(T) \geq 3$ for all T. The best known lower bounds for $B(T)$ can be found at [5].

In the present paper, we describe the construction of an elliptic curve over $\mathbb{Q}$ with a nontrivial 2-torsion point whose rank is exactly equal to 15. This gives the current record for the rank of curves with nontrivial torsion, and also the highest example of the rank of an elliptic curve which is known exactly (not only a lower bound for rank). It improves previous records due

[0]2000 Mathematics Subject Classification: 11G05.
Key words: Elliptic curve; rank.

to Kretschmer [8] (rank = 10), Schneiders & Zimmer [15] (rank = 11) and Fermigier [6] (rank = 14).

In the above notation, we have

Theorem 1 $B(\mathbb{Z}/2\mathbb{Z}) \geq 15$.

2 Fermigier's construction

In [6], Fermigier constructed an elliptic curve over $\mathbb{Q}(t)$, of rank at least 8, with a point of order 2. By specialization, he obtained an elliptic curve over $\mathbb{Q}$ whose rank is equal to 14. In [9], Kulesz and Stahlke obtained the same results by another construction. Both constructions are variants of the construction of Mestre [12]. In [7], Kihara improved Fermigier's result by constructing an elliptic curve over $\mathbb{Q}(t)$ with a non-trivial 2-torsion point and rank ≥ 9.

Our construction of the curve with rank = 15 will start with Fermigier's family of curves with rank ≥ 8. Thus, let us describe Fermigier's construction.

Let $x_1, x_2, \ldots, x_8$ be rational numbers such that

$$x_1^2 + x_2^2 = x_3^2 + x_4^2 = x_5^2 + x_6^2 = x_7^2 + x_8^2 = s. \tag{1}$$

Define the polynomial

$$p(x) = (x - x_1)(x - x_2) \cdots (x - x_8).$$

We can write the polynomial $q(x) = p(x)p(-x)$ as $q(x) = g^2(x) - r(x)$, where g is a polynomial of degree 8 and r is an even polynomial of degree at most 4.

Let us consider the curve

$$C: \quad y^2 = r(x) = r_4x^4 + r_2x^2 + r_0.$$

It has at least 32 rational points, namely $(\pm x_i, \pm g(x_i))$ for $i = 1, \ldots, 8$. If we choose $(x_1, g(x_1))$ as the origin, then we find that the curve C is birationally equivalent to the elliptic curve E given by

$$E: y^2 = x^3 + Ax^2 + Bx,$$

where $A = -r_2/2$ and $B = (a^2 - r_0r_4)/4$. The point $(0, 0)$ is 2-torsion point on E, while the images of the points $(-x_1, g(x_1))$, $(x_i, g(x_i)$, $i = 2, \ldots, 8$ are 8 independent points of infinite order on E.

We can also express A and B in terms of $x_1, \ldots, x_8$:

$$A = \frac{-s}{16} \prod_{\varepsilon} \Big(x_1^2 x_2^2 + \varepsilon_1 x_3^2 x_4^2 + \varepsilon_2 x_5^2 x_6^2 + \varepsilon_3 x_7^2 x_8^2 \Big),$$

where ε runs over all triples $(\varepsilon_1, \varepsilon_2, \varepsilon_3)$ such that $\varepsilon_i \in \{1, -1\}$ and $\varepsilon_1 + \varepsilon_2 + \varepsilon_3 = -1$, and

$$B = \frac{A}{128s} \prod_{\delta} \Big(x_1^2 + \delta_1 x_3^2 + \delta_2 x_5^2 + \delta_3 x_7^2 + S(\delta) \Big),$$

where δ runs over all triples $(\delta_1, \delta_2, \delta_3)$ such that $\delta_i \in \{1, -1\}$ and where $S(\delta) = -s(1 + \delta_1 + \delta_2 + \delta_3)/2$.

3 A curve with rank = 15

In order to satisfy the relation (1), we will assume that s is a positive integer of the form $s = p_1 p_2 p_3$, where p_1, p_2, p_3 are primes which are $\equiv 1 \pmod 4$ (the similar idea was used in [9]). Then there exist positive integers $a, b, \ldots, f$, such that $p_1 = a^2 + b^2$, $p_2 = c^2 + d^2$, $p_3 = e^2 + f^2$, and we may take

$$\begin{aligned}
x_1 &= e(ac + bd) + f(ad - bc), \quad & x_2 &= f(ac + bd) - e(ad - bc), \\
x_3 &= e(ac + bd) - f(ad - bc), \quad & x_4 &= f(ac + bd) + e(ad - bc), \\
x_5 &= e(ac - bd) + f(ad + bc), \quad & x_6 &= f(ac - bd) - e(ad + bc), \\
x_7 &= e(ac - bd) - f(ad + bc), \quad & x_8 &= f(ac - bd) + e(ad + bc).
\end{aligned}$$

Let us denote the elliptic curve obtained by this construction by E_{p_1,p_2,p_3}.

For an elliptic curve E over $\mathbb{Q}$, and a prime number p, we put $a_p = a_p(E) = p + 1 - |E(\mathbb{F}_p)|$. For a fixed integer N, we define

$$S(N, E) = \sum_{p \le N,\ p \text{ prime}} \Big(1 - \frac{p-1}{|E(\mathbb{F}_p)|} \Big) \log(p) = \sum_{p \le N,\ p \text{ prime}} \frac{-a_p + 2}{p + 1 - a_p} \log(p).$$

It is experimentally known (see [11], [14]) that we may expect that high rank curves have large $S(N, E)$. In [2], some arguments were given which show that the Birch and Swinnerton-Dyer conjecture gives support to this idea.

We apply the above idea to the family of elliptic curves

$$\{E_{p_1,p_2,p_3} \,:\, 5 \le p_1 < p_2 < p_3 < 2000\}.$$

We search for curves $E = E_{p_1,p_2,p_3}$ in this family satisfying $S(523, E) > 30$, $S(1979, E) > 40$, $S(3559, E) > 50$ and $S(7907, E) > 69$.

We found 120 curves satisfying these conditions, and we computed the rank (or at least an upper bound for the rank) for all of them. In that way, we found 5 curves with rank equal to 14 and one curve with rank equal to 15.

rank	$s = p_1p_2p_3$
15	$1134231997 = 829 \cdot 881 \cdot 1553$
14	$16657049 = 29 \cdot 613 \cdot 937$
14	$23246533 = 89 \cdot 149 \cdot 1753$
14	$71531609 = 53 \cdot 1109 \cdot 1217$
14	$128675609 = 193 \cdot 653 \cdot 1021$
14	$642455533 = 293 \cdot 1373 \cdot 1597$

Perhaps it is interesting to mention that the curve which corresponds to $s = 134930249 = 113 \cdot 1069 \cdot 1117$ has 2-Selmer rank 16, but its rank is only 12.

In the computation of the ranks, we used Cremona's programs MWRANK [4]. This program uses 2-descent (via 2-isogeny if possible) to determine the rank of an elliptic curve E over $\mathbb{Q}$. Originally, we computed the rank of the curve with rank = 15 "by hand", using Connell's package APECS [3] and Stoll's program RATPOINTS. The author is grateful to Professor John Cremona for the information that the version of MWRANK which uses multiprecision real arithmetic is capable to compute the rank of this curve.

Let us give few more details about the record curve with rank = 15. The corresponding x_i's from Fermigier's construction:

$$x_1 = 30906, \quad x_2 = 13381, \quad x_3 = 22534, \quad x_4 = 25029,$$

$$x_5 = 32166, \quad x_6 = -9979, \quad x_7 = 794, \quad x_8 = 33669.$$

The equation in minimal Weierstrass form:

$$y^2 + xy + y = x^3 + 343182146424416463624356325625799087 47x + 3184376895814127197244886284686214848599453811643486936756$$

Torsion points:

$$\mathcal{O},\ [-55741267008740887705/4, 55741267008740887701/8]$$

Independent points of infinite order:

$$\begin{aligned}
P_1 &= [-5955399047526089895, -526191924860735567896798519 28],\\
P_2 &= [4996845231479851005, 5899680706891155858093203 2822],\\
P_3 &= [-13155206566829859045, -213607291702321571271986 38028],\\
P_4 &= [5982316535030750730, 600314511510893531151736949 47],\\
P_5 &= [3520990345094746477605, 208928587539794577855401843236822],\\
P_6 &= [-149780582516304339030/289,\\
&\quad -27646056139485808550006630111601 4/4913],\\
P_7 &= [5537764707520796477505/256,\\
&\quad 485495189997228202630782626087287/4096],\\
P_8 &= [10379720384859947873670/529,\\
&\quad 1299762167535132813050160826170149/12167],\\
P_9 &= [3607902715536254330407755/36481,\\
&\quad 68762868744139351690191647917980287 12/6967871],\\
P_{10} &= [575451914344737045120/18769,\\
&\quad 14512614987370823294128193393531 8916/2571353],\\
P_{11} &= [-635343181823720560310/81,\\
&\quad -35955391603910411255538526302302/729],\\
P_{12} &= [385275433846822770303250/9,\\
&\quad 23914261908419657063984735109733 6094/27],\\
P_{13} &= [11630065797764473356485380/349281,\\
&\quad 41921913401808378926412528792277717237/206425071],\\
P_{14} &= [21308620872052945650115 55/206116,\\
&\quad 63770176603198110103715767985205574 33/93576664],\\
P_{15} &= [36188621806079319636815219 2851/82159049956,\\
&\quad 13773978125070149790227487991947013955706396 71/23549577125088104]
\end{aligned}$$

References

[1] A. O. L. Atkin and F. Morain, Finding suitable curves for the elliptic curve method of factorization, Math. Comp. **60**, 399–405 (1993).

[2] G. Campbell, Finding Elliptic Curves and Families of Elliptic Curves over $\mathbb{Q}$ of Large Rank, Dissertation, Rutgers, 1999.

[3] I. Connell, APECS, `ftp://ftp.math.mcgill.ca/pub/apecs/`

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

[5] A. Dujella, High rank elliptic curves with prescribed torsion, `http://www.math.hr/ duje/tors/tors.html`

[6] S. Fermigier, Exemples de courbes elliptiques de grand rang sur $\mathbb{Q}(t)$ et sur $\mathbb{Q}$ possedant des points d'ordre 2, C. R. Acad. Sci. Paris Ser. I **322**, 949–952 (1996).

[7] S. Kihara, On an elliptic curve over $\mathbb{Q}(t)$ of rank ≥ 9 with a non-trivial 2-torsion point, Proc. Japan Acad. Ser. A Math. Sci. **77**, 11–12 (2001).

[8] T. J. Kretschmer, Construction of elliptic curves with large rank, Math. Comp. **46**, 627–635 (1986)

[9] L. Kulesz and C. Stahlke, Elliptic curves of high rank with a non-trivial torsion group over $\mathbb{Q}$, preprint.

[10] R. Martin and W. McMillen, An elliptic curve over $\mathbb{Q}$ with rank at least 24, Number Theory Listserver, May 2000.

[11] J.-F. Mestre, Construction de courbes elliptiques sur $\mathbb{Q}$ de rang ≥ 12, C. R. Acad. Sci. Paris Ser. I **295**, 643–644 (1982).

[12] J.-F. Mestre, Courbes elliptiques de rang ≥ 11 sur $\mathbb{Q}(T)$, C. R. Acad. Sci. Paris Ser. I **313**, 139–142 (1991).

[13] P. L. Montgomery, Speeding the Pollard and elliptic curve methods of factorization, Math. Comp. **48**, 243–264 (1987).

[14] K. Nagao, An example of elliptic curve over $\mathbb{Q}$ with rank ≥ 20, Proc. Japan Acad. Ser. A Math. Sci. **69**, 291–293 (1993).

[15] U. Schneiders and H. G. Zimmer, The rank of elliptic curves upon quadratic extension, in: Computational Number Theory (A. Pethő, H. C. Williams, H. G. Zimmer, eds.), de Gruyter, Berlin, 1991, pp. 239–260.

[16] T. Womack, Curves with moderate rank and interesting torsion group, `http://www.maths.nott.ac.uk/personal/pmxtow/torsion.htm`

Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia

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