SOME RANK RECORDS FOR ELLIPTIC CURVES WITH PRESCRIBED TORSION OVER QUADRATIC FIELDS

FILIP NAJMAN

Abstract. In this paper we construct elliptic curves over quadratic fields with prescribed torsion group and record rank. We do this using theoretical arguments and keeping lengthy computations to a minimum.

1. Introduction

One of the most important open questions in the theory of elliptic curves is whether the rank of an elliptic curve over a fixed number field can be arbitrarily large. The answer is not known even over the rational numbers. In the absence of theoretical results, there has been great interest in computing explicit examples of elliptic curves with high rank. The elliptic curve with the largest known rank over the rational number was found by Elkies in 2006 and has rank 28.

Apart from simply finding high rank elliptic curves, it is of interest to find high rank elliptic curves with a prescribed torsion group and rank as large as possible. For the current rank records of elliptic curves over $\mathbb{Q}$ with prescribed torsion, their history and relevant references (60 at the moment of writing) see Andrej Dujella's webpage [4].

While historically most of the attention has been given to elliptic curves over $\mathbb{Q}$, in recent years many authors have started looking at high rank elliptic curves over number fields. One of the reasons is because this has become possible because of recent advances in algorithms and computational power. But another (theoretical) reason is that over number fields the torsion groups can constrain the rank; for example elliptic curves over quadratic fields with torsion groups $\mathbb{Z}/13\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$ necessarily have even rank [3]. Most of the work has been done over quadratic fields [2, 5, 9, 11], although in [3] results for cubic and quartic fields are also given.

Note that elliptic curves with large torsion and positive rank can also be interesting from a computational perspective, especially for factorization [6].

In this paper we obtain several rank records for elliptic curves with prescribed torsion over quadratic fields. We do not do long computations that search for elliptic curves with large rank, but instead obtain our results by applying theoretical results.

2. The 2-isogeny method

Let $E/\mathbb{Q}$ be an elliptic curve such that $E(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$ for $n = 1, 2, 3, 4$. Let $P \in E(\mathbb{Q})[2]$ be a point that is not divisible by 2. Now define $\phi : E \to E'$ to be the 2-isogeny for E to $E' = E/\langle P \rangle$, and let $\hat{\phi}$ be the dual isogeny

2010 *Mathematics Subject Classification.* 11G05, 11R11.
Key words and phrases. elliptic curves, rank records, quadratic fields.

of ϕ. It follows that $E'(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2n\mathbb{Z}$ and that

$$U := (\hat{\phi})^{-1}(E(\mathbb{Q})_{tors}/\langle P\rangle)$$

is a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant subgroup of order $4n$ containing $E'(\mathbb{Q})_{tors}$. It is now easy to work out that all the points in U will be defined over some quadratic field K (see [10, Remarks 2.6. (d)] for details); hence $E'(K) \simeq \mathbb{Z}/4n\mathbb{Z}$. We call this construction the 2-*isogeny method*.

We now apply the 2-isogeny method. We start with the curve

$$E : y^2 + xy = x^3 - 1574593253082908988 0x + 2402821995709596942633927840 0,$$

which has $E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}^3$; see [4]. We compute the 2-isogenous curve

$$E' : y^2 + xy = x^3 - 748692454000090200x + 559647059958559043288903232$$

and the field $K = \mathbb{Q}(\sqrt{34720105})$ such that $E'(K)_{tors} \simeq \mathbb{Z}/16\mathbb{Z}$. Recall that

$$\mathrm{rk}(E(\mathbb{Q}(\sqrt{d})) = \mathrm{rk}(E(\mathbb{Q})) + \mathrm{rk}(E^{(d)}(\mathbb{Q})). \tag{1}$$

is true for any elliptic curve $E/\mathbb{Q}$. Let $d = 34720105$. As K-isogenous curves have the same rank over K, it follows that

$$\mathrm{rk}(E'(K)) = \mathrm{rk}(E(K)) = \mathrm{rk}(E(\mathbb{Q})) + \mathrm{rk}(E^{(d)}(\mathbb{Q})).$$

We compute in Magma [1] that the 2-Selmer of $E^{(d)}(\mathbb{Q})$ group has rank 5 and that $(\mathbb{Z}/2\mathbb{Z})^2 \subset Ш(E^{(d)}(\mathbb{Q}))[4] \subset (\mathbb{Z}/2\mathbb{Z})^2 \oplus \mathbb{Z}/4\mathbb{Z}$. Note that the Tate-Shafarevich conjecture states that $Ш(E^{(d)}(\mathbb{Q}))$ should be finite and hence, by the Cassels-Tate pairing, a square. Since two copies of $\mathbb{Z}/2\mathbb{Z}$ in the 2-Selmer group come from the torsion, if one assumes that the Tate-Shafevich group is finite, it follows $Ш(E^{(d)}(\mathbb{Q}))[4] \simeq (\mathbb{Z}/2\mathbb{Z})^2$, and hence $\mathrm{rk}(E^{(d)}(\mathbb{Q})) = 1$.

Hence we have obtained an elliptic curve E' over a quadratic field K such that $E'(K)_{tors} \simeq \mathbb{Z}/16\mathbb{Z}$ and $\mathrm{rk}(E'(K)) \geq 3$ unconditionally and $\mathrm{rk}(E'(K)) \geq 4$ assuming the Tate-Shafarevich conjecture. Note that even the unconditional result breaks the current rank record for an elliptic curve over a quadratic field with torsion $\mathbb{Z}/16\mathbb{Z}$ [2].

Using a similar construction we start with the elliptic curve E with rank 15 from [4], and construct an isogenous elliptic curve E' and a quadratic field $\mathbb{Q}(\sqrt{d})$ such that $E'(\mathbb{Q}(\sqrt{d}))$ has torsion $\mathbb{Z}/4\mathbb{Z}$. We find that the twist $E^{(d)}(\mathbb{Q})$ has 2-Selmer rank equal to 7, and hence we conclude that, assuming the Tate-Shafarevich conjecture,it should hold that $\mathrm{rk}\, E'(\mathbb{Q}(\sqrt{d})) \geq 16$, which would break the record form [2].

3. Complex multiplication

In [8], the authors find the elliptic curve

$$E : x^3 + y^3 = 1329399805658495217415723 5$$

with rank ≥ 11 over $\mathbb{Q}$. This curve has complex multiplication by the ring of integers of $\mathbb{Q}(\sqrt{-3})$, is 3-isogenous to $E^{(-3)}$, the twistof E by -3. Note that $E^{(-3)}(\mathbb{Q})_{tors} \simeq \mathbb{Z}/3\mathbb{Z}$. Hence

$$\mathrm{rk}(E(\mathbb{Q}(\sqrt{-3})) = \mathrm{rk}(E(\mathbb{Q})) + \mathrm{rk}(E^{(-3)}(\mathbb{Q})) = 2\,\mathrm{rk}(E(\mathbb{Q})) \geq 22,$$

since the isogenous curves E and $E^{(-3)}$ have the same rank over $\mathbb{Q}$. Hence we have constructed an elliptic curve over $\mathbb{Q}(\sqrt{-3})$ with torsion $\mathbb{Z}/3\mathbb{Z}$ and rank ≥ 22. The previous rank record for an elliptic curve over a quadratic field with this torsion was 15 [2], so our example brakes it by a margin of 7.

Similarly, the elliptic curve

$$E : y^2 = x^3 + 469745529818636761156474 17,$$

taken form [7], has rank 15 over $\mathbb{Q}$ and is isogenous to its -3-twist. Thus, by the same argument as above, this curve has rank at least 30 over $\mathbb{Q}(\sqrt{-3})$ (and trivial torsion). This equals the current rank record over quadratic fields (for any torsion group), but has the advantage that the field over which the curve has rank 30 and the points generating a subgroup of rank 30 are explicitly known (these are the 15 points from [7] together with their images under the 3-isogeny to $E^{(-3)}$) and are relatively small in size.

References

[1] W. Bosma, J. J. Cannon, C. Fieker, A. Steel (eds.), Handbook of Magma functions, Edition 2.18 (2012),

[2] J. Aguirre, A. Dujella, M. Jukic Bokun, J. C. Peral, *High rank elliptic curves with prescribed torsion group over quadratic fields,* Period. Math. Hungar., to appear.

[3] J. Bosman, P. Bruin, A. Dujella, F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, Int. Math. Res. Not. IMRN, to appear.

[4] A. Dujella, *High rank elliptic curves with prescribed torsion,* `http://web.math.hr/~duje/tors/tors.html`

[5] A. Dujella, M. Jukić Bokun, *On the rank of elliptic curves over $\mathbb{Q}(i)$ with torsion group $\mathbb{Z}_4 \oplus \mathbb{Z}_4$,* Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), 93–96.

[6] A. Dujella, F. Najman, *Elliptic curves with large torsion and positive rank over number fields of small degree and ECM factorization,* Period. Math. Hungar., to appear.

[7] N. Elkies, *$j = 0$, rank 15; also 3-rank 6 and 7 in real and imaginary quadratic fields,* Number Theory Listserv posting, December 30, 2009, `http://listserv.nodak.edu/cgi-bin/wa.exe?A2=ind0912&L=NMBRTHRY&F=&S=&P=14012`

[8] N. D. Elkies, N. F. Rogers, *Elliptic curves $x^3 + y^3 = k$ of high rank,* in Algorithmic number theory (ANTS-VI), ed. D. Buell, Lecture Notes in Comput. Sci. **3076**, Springer, Berlin, 2004, 184–193.

[9] M. Jukić Bokun, *On the rank of elliptic curves over $\mathbb{Q}(\sqrt{-3})$ with torsion group $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$,* Proc. Japan Acad. Ser. A Math. Sci. **87** (2011), 61–64.

[10] M. Laska and M. Lorenz, *Rational points on elliptic curves over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$*, J. Reine Angew. Math. **355** (1985), 163–172.

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

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

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