On the rank of elliptic curves over $\mathbf{Q}(\sqrt{-3})$ with torsion groups $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ and $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$

By Mirela Jukić Bokun

Department of Mathematics, University of Osijek, Trg Ljudevita Gaja 6, 31000 Osijek, Croatia

(Communicated by Shigefumi Mori, M.J.A., April 12, 2011)

Abstract: We construct elliptic curves over the field $\mathbf{Q}(\sqrt{-3})$ with torsion group $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ and ranks equal to 7 and an elliptic curve over the same field with torsion group $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ and rank equal to 6.

Key words: Elliptic curve; torsion group; rank.

1. Introduction. Let as suppose that E is an elliptic curve defined over a number field K. According to the Mordell-Weil theorem, the group of K-rational points $E(K)$ of E is a finitely generated abelian group. Therefore,

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

where $E(K)_{\rm tors}$ is the torsion group and integer $r\geq 0$ is the rank of E. By Mazur's theorem [8], when $K=\mathbf{Q}$, the torsion group is one of the following 15 groups: $\mathbf{Z}/n\mathbf{Z}$ with $1\leq n\leq 10$ or $n=12$, $\mathbf{Z}/2\mathbf{Z}\times\mathbf{Z}/2m\mathbf{Z}$ with $1\leq m\leq 4$. If $K=\mathbf{Q}(\sqrt{-3})$, Najman [10,11] recently showed that possible torsion group is either one of the groups from Mazur's theorem, or $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ or $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ (the last two groups are possible only over this quadratic field [5,6]). It is not known which values of rank are possible. In the case of field $K=\mathbf{Q}$, elliptic curves of rank greater from 28 haven't yet been found (current records of ranks for each of 15 possible torsion groups can be found at `http://web.math.hr/~duje/tors/tors.html`) but the conjecture that there is no upper bound for the rank of elliptic curve is widely accepted.

In this paper we focused on elliptic curves over the field $\mathbf{Q}(\sqrt{-3})$ with torsion groups $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$. Rabarison [13] constructed elliptic curves with these torsion groups and ranks ≥ 2, ≥ 3, respectively. We have improved these results and described how we find elliptic curves over the field $\mathbf{Q}(\sqrt{-3})$ with ranks equal to 7 for torsion group $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/3\mathbf{Z}$ and an elliptic curve with rank equal to 6 for torsion group $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$. It is interesting to mention that curves with torsion group $\mathbf{Z}/3\mathbf{Z}\times\mathbf{Z}/6\mathbf{Z}$ and positive rank are used for factoring numbers of the form $a^{3n}\pm b^{3n}$ (see [2]).

Our main tool for calculating the rank over $\mathbf{Q}(\sqrt{-3})$ is the fact (see, for example, [14]) that if E is an elliptic curve over $\mathbf{Q}$, then the rank of E over $\mathbf{Q}(\sqrt{-3})$ is given by

$$\text{(1)}\quad \mathrm{rank}(E(\mathbf{Q}(\sqrt{-3})))=\mathrm{rank}(E(\mathbf{Q}))+\mathrm{rank}(E_{-3}(\mathbf{Q})),$$

where E_{-3} is the (-3)-twist of E over $\mathbf{Q}$. Searching methods that we used are similar as methods used in [4] (we have implemented them in `PARI/GP` [12]).

We started with a family of elliptic curves $E(t)$ and for curves $E\in E(t)$ with property $t=t_1/t_2$, $|t_1|\leq 100$, $t_2\leq 500$, we maximize the sum $S(N,E)+S(N,E_{-3})$ (it is experimentally known that sum $S(N,E)$ is relatively large for curve E with large rank, see [9]), where

$$S(N,E)=\sum_{p\leq N,p\,\mathrm{prime}}\frac{2-a_p}{p+1-a_p},$$
$$a_p=a_p(E)=p+1-\#E(\mathbf{F}_p),$$

and we used $N=1999$.

In the next step we used Mestre's conditional upper bound [7] for the rank: if

$$G_\lambda(E)=\frac{\pi^2}{8\lambda}\left(\log N-2\sum_{p^m\leq e^\lambda}b(p^m)F_\lambda(m\log p)\frac{\log p}{p^m}-M_\lambda\right),$$

where N is the conductor, $b(p^m)=a_p^m$ if $p\mid N$ and $b(p^m)=\alpha_p^m+\alpha_p'^m$ if $p\nmid N$ where α_p, α_p' are the roots of x^2-a_px+p,

$$M_\lambda=2\left(\log 2\pi+\int_0^{+\infty}(F_\lambda(x)/(e^x-1)-e^{-x}/x)dx\right),$$

2000 Mathematics Subject Classification. Primary 11G05, 14H52, 11R11.

doi: 10.3792/pjaa.87.61

$F_\lambda(x) = F(x/\lambda)$ and

$$F(x) = \begin{cases} (1-x)\cos(\pi x) + \sin(\pi x)/\pi, & x \in [-1,1] \\ 0, & \text{elsewhere} \end{cases},$$

then the rank of elliptic curve E over $\mathbf{Q}$ is $\leq G_\lambda(E)$ (assuming the Birch and Swinnerton-Dyer conjecture and GRH). For curves with large value of $S(N,E) + S(N,E_{-3})$ we used Mestre's upper bound with parameter $\lambda = 12$ to select elliptic curve E which has potentially large rank over $\mathbf{Q}$. To find independent points of infinite order on elliptic curves E and E_{-3} over $\mathbf{Q}$ we used Cremona's program `MWRANK` [3] for curves which have rational 2-torsion points. For other elliptic curves we used Connell's `APECS` [1] or Stoll's `RATPOINTS` [15].

2. Elliptic curves over $\mathbf{Q}(\sqrt{-3})$ with torsion subgroup $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$. According to Rabarison's article [13], a general form of elliptic curves over $\mathbf{Q}(\sqrt{-3})$ with torsion group $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ is

$$\begin{aligned} &y^2 + s(ts^2 - 12)xy + 4t(144s^2 - 24ts^4 + 432ts \\ &\quad + 432t^2 + t^2s^6 - 36t^2s^3)y = x^3. \end{aligned} \tag{2}$$

The torsion group is generated by the points $T_1 = [0,0]$ and (with corrections of misprints in Rabarison's article)

$$\begin{aligned} T_2 = \Bigg[&12t^2s^3 - 144t^2 + 8ts^4 - 144ts - 48s^2 - \frac{t^2s^6}{3}, \\ &\frac{(3+\sqrt{-3})(ts^3 + (6\sqrt{-3} - 18)t - 12s)}{18} \\ &\times (ts^3 - (6\sqrt{-3} + 18)t - 12s)^2 \Bigg]. \end{aligned}$$

For fixed small s'es we used searching methods that we described earlier, with the following alternation: after calculating Mestre's upper bound for rank, for selected curves we calculated analytic rank by `MAGMA`. For example, for $s = 1$ we get five elliptic curves with the ranks equal to 6 ($t = -51/20, -97/425, -95/389, -74/297, 69/262$), and for $s = 2$ we get two elliptic curves with ranks equal to 6 ($t = -53/247$, $33/313$) and two elliptic curves with ranks equal to 7 ($t = 43/171, 97/133$). We will now proceed with giving details only for the last two curves.

When we put $s = 2$ in equation (2) we get the following family of elliptic curves

$$y^2 + (8t - 24)xy + 64t(13t^2 + 30t + 36)y = x^3$$

and family of (-3)-twists

$$\begin{aligned} &y^2 + (8t - 24)xy + 64t(13t^2 + 30t + 36)y = x^3 \\ &\quad - 64(t-3)^2x^2 + 2048t(13t^3 - 9t^2 - 54t - 108)x \\ &\quad - 28672t^2(13t^2 + 30t + 36)^2. \end{aligned}$$

For $t = 43/171$ we have the elliptic curve with minimal Weierstrass equation

$$\begin{aligned} E: \quad &y^2 + y = x^3 + x^2 - 42484096963x \\ &+ 3506965787198963, \end{aligned}$$

and independent points of infinite order

$$\begin{aligned} &[-114191, 82881102], [-71449, 78598173], \\ &[127323, 12721285], [277613, 114491289], \\ &\left[-\frac{742000}{3}, -\frac{1}{2} - \frac{347102063}{18}\sqrt{-3}\right], \\ &\left[-\frac{14508298}{3}, -\frac{1}{2} - \frac{110421361925}{18}\sqrt{-3}\right], \\ &\Bigg[-\frac{522977855649598}{2051310603}, \\ &\quad -\frac{1}{2} - \frac{878052700102249164615}{321838325747082}\sqrt{-3}\Bigg]. \end{aligned}$$

For $t = 97/133$ we have the elliptic curve with minimal Weierstrass equation

$$\begin{aligned} E': \quad &y^2 + y = x^3 + x^2 - 36348070599x \\ &+ 4166981243028849. \end{aligned}$$

Independent points of infinite order are

$$\begin{aligned} &[-138469, 80901936], [2068591, 2963211943], \\ &\left[\frac{17313869}{4}, \frac{71974844343}{8}\right], \\ &\left[\frac{15483229569}{64}, \frac{1926602838263967}{512}\right], \\ &\left[-\frac{81123124}{27}, -\frac{1}{2} - \frac{1458267957839}{486}\sqrt{-3}\right], \\ &\left[-\frac{706816}{3}, -\frac{1}{2} - \frac{193750613}{18}\sqrt{-3}\right], \\ &\left[-\frac{147741896293}{164268}, -\frac{1}{2} - \frac{55330636651296391}{115316136}\sqrt{-3}\right]. \end{aligned}$$

The curves E and E' have ranks equal to 4 over $\mathbf{Q}$ and twisted curves have ranks equal to 3 (we searched for the points on these or isogenous curves by `RATPOINTS` and the numbers of found independent points on all of these curves coincide with their 2-Selmer ranks calculated by `MAGMA`).

3. Elliptic curves over $\mathbf{Q}(\sqrt{-3})$ with torsion subgroup $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$. A general form of an elliptic curve over $\mathbf{Q}(\sqrt{-3})$ with torsion group $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/6\mathbf{Z}$ is (see [13])

$$\begin{aligned} &y^2 + 2(9t^3 - 30t^2 + 60t - 40)xy \\ &- 144(3t-2)(3t^2+4)(3t^2-6t+4)(t-2)^3 y = x^3 \\ &- 16(3t-2)(3t^2+4)(3t^2-6t+4)x^2. \end{aligned}$$

The torsion group is generated by the points $T_1 = [0, 0]$ and

$$\begin{aligned} T_2 = \Big[&-12(t-2)^2(3t^2-6t+4)(3t^2+4), \\ &324(3+\sqrt{-3})(t-2)^2\left(t-\frac{2}{3}\sqrt{-3}\right)^2\left(t-1-\frac{1}{3}\sqrt{-3}\right) \\ &\times\left(t-1+\frac{1}{3}\sqrt{-3}\right)^2\left(t+\frac{2}{3}\sqrt{-3}\right)^2\Big]. \end{aligned}$$

The (-3)-twist of this elliptic curve is given with

$$\begin{aligned} &y^2 + 2(9t^3 - 30t^2 + 60t - 40)xy - 144(t-2)^3 \\ &\quad\times (27t^5 - 72t^4 + 108t^3 - 120t^2 + 96t - 32)y \\ &= x^3 - 4(81t^6 - 864t^5 + 2844t^4 - 5616t^3 + 7440t^2 \\ &\quad - 5952t + 1984)x^2 - 1152(t-2)^3 \\ &\quad\times (243t^8 - 1458t^7 + 4752t^6 - 9720t^5 + 13824t^4 \\ &\quad - 14688t^3 + 11520t^2 - 5760t + 1280)x - 145152 \\ &\quad\times (t-2)^6(-27t^5 + 72t^4 - 108t^3 + 120t^2 - 96t + 32)^2. \end{aligned}$$

We noticed that parameters t and $4/(3t)$ give isomorphic elliptic curves over $\mathbf{Q}(\sqrt{-3})$. For parameter $t = -74/469$ we have an elliptic curve with rank equal to 6 $(r(E(\mathbf{Q})) = r(E_{-3}(\mathbf{Q})) = 3)$. The minimal Weierstrass equations is

$$\begin{aligned} E: \quad &y^2 + xy + y = x^3 - x^2 \\ &- 187646882683490022342866999027x \\ &- 432857468986549830576994867433761557017770349. \end{aligned}$$

Independent points of infinite order are

$$\begin{aligned} &[707406059162101, 13340697112791107526174], \\ &\left[\frac{770832044105421579309 79}{9162729}, \frac{213721052822394312029045911698065 42}{27735580683}\right], \\ &\left[\frac{1901766270755934739691839}{63632529}, \frac{2622344436598590959558761413133872862}{507596683833}\right], \\ &\Big[-216659438724672, \frac{216659438724671}{2} - \frac{41312721225800672633337}{2}\sqrt{-3}\Big], \\ &\left[\frac{-4488915509374394670}{3481}, \frac{4488915509374391189}{6962} - \frac{1046086431060231938666332 8165}{410758}\sqrt{-3}\right], \\ &\Big[-\frac{9770285635149371157870573}{37725681361}, \frac{4885142817574666716094606}{37725681361} - \frac{2220522030861081094274292}{7327496816428391} \\ &\quad\times 6615985671527\sqrt{-3}\Big], \end{aligned}$$

Furthemore, for parameters $t = 22/89$, $35/43$, $30/149$, $56/117$, $104/201$, $138/89, -20/59, -38/153$ we have elliptic curves with ranks equal to 5 over $\mathbf{Q}(\sqrt{-3})$ (curve with parameter $22/89$ and (-3)-twist of the curve with parameter $56/117$ are isogenous elliptic curves and same happens with the pairs $30/149$, $104/201$ and $35/43$, $-38/153$).

Acknowledgements. The author would like to thank Prof. Andrej Dujella, Prof. Filip Najman and referee for helpful suggestions. Also, the author is grateful to Prof. Juan Carlos Peral for information about recent investigations on related topics. The author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 235-2352818-1042.

References

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

[2] E. Brier and C. Clavier, New Families of ECM Curves for Cunningham Numbers. In Proceedings of ANTS. 2010, 96–109.

[3] J. E. Cremona, *Algorithms for modular elliptic curves*, second edition, Cambridge Univ. Press, Cambridge, 1997.

[4] A. Dujella and M. Jukić Bokun, On the rank of elliptic curves over $\mathbf{Q}(i)$ with torsion group $\mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$, Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), no. 6, 93–96.

[5] S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, Invent. Math. **109** (1992), no. 2, 221–229.

[6] M. A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. **109** (1988), 125–149.
[7] J.-F. Mestre, Formules explicites et minorations de conducteurs de variétés algébriques, Compositio Math. **58** (1986), no. 2, 209–232.
[8] B. Mazur, Rational isogenies of prime degree (with an appendix by D. Goldfeld), Invent. Math. **44** (1978), no. 2, 129–162.
[9] K. Nagao, Construction of high-rank elliptic curves with a nontrivial torsion point, Math. Comp. **66** (1997), no. 217, 411–415.
[10] F. Najman, Torsion of elliptic curves over quadratic cyclotomic fields, Math J. Okayama Univ. **53** (2011), 75–82.
[11] F. Najman, Complete classification of torsion of elliptic curves over quadratic cyclotomic fields, J. Number Theory **130** (2010), no. 9, 1964–1968.
[12] PARI/GP, version 2.3.3, Bordeaux, 2008. `http://pari.math.u-bordeaux.fr/`.
[13] F. P. Rabarison, Structure de torsion des courbes elliptiques sur les corps quadratiques, Acta Arith. **144** (2010), no. 1, 17–52.
[14] U. Schneiders and H. G. Zimmer, The rank of elliptic curves upon quadratic extension, in *Computational number theory* (*Debrecen,* 1989), 239–260, de Gruyter, Berlin.
[15] M. Stoll, RATPOINTS. `http://www.mathe2.uni-bayreuth.de/stoll/programs/`.