GLASNIK MATEMATIČKI
Vol. 47(67)(2012), 277 – 284

ELLIPTIC CURVES OVER QUADRATIC FIELDS WITH FIXED TORSION SUBGROUP AND POSITIVE RANK

Mirela Jukić Bokun
University of Osijek, Croatia

Abstract. For each of the torsion groups $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$ we find the quadratic field with the smallest absolute value of its discriminant such that there exists an elliptic curve with that torsion and positive rank. For the torsion groups $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ we solve the analogous problem after assuming the Parity conjecture.

1. Introduction

According to the Mordell-Weil theorem, the group of K-rational points $E(K)$ of an elliptic curve E over a number field K is a finitely generated abelian group. Therefore, the group $E(K)$ is isomorphic to $E(K)_{\text{tors}} \oplus \mathbb{Z}^r$, where $E(K)_{\text{tors}}$ is the torsion subgroup and the non-negative integer r is the rank. When $K = \mathbb{Q}$, by Mazur's theorem ([11]) the torsion group is one of the following 15 groups: $\mathbb{Z}/n\mathbb{Z}$ with $1 \leq n \leq 10$ or $n = 12$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2m\mathbb{Z}$ with $1 \leq m \leq 4$. If K is a quadratic field, the following theorem of Kenku and Momose ([9]) and Kamienny ([7]) describes the possible torsions.

Theorem 1.1. *Let K be a quadratic field and E an elliptic curve over K. Then the torsion subgroup $E(K)_{\text{tors}}$ of $E(K)$ is isomorphic to one of the following* 26 *groups:*

- $\mathbb{Z}/n\mathbb{Z}$, *for* $1 \leq n \leq 16$, $n = 18$,
- $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2n\mathbb{Z}$, *for* $1 \leq n \leq 6$,
- $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3n\mathbb{Z}$, *for* $n = 1, 2$, $K = \mathbb{Q}(\sqrt{-3})$,
- $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ *for* $K = \mathbb{Q}(i)$.

2010 *Mathematics Subject Classification.* 11G05, 14H52, 11R11.
Key words and phrases. Elliptic curve, torsion group, rank, quadratic field.

Kamienny and Najman ([8]) described methods that can be used to find all possible torsions over a given quadratic field. For each possible torsion group G, they found the exact quadratic field K with the smallest absolute value of the discriminant Δ such that there exists an elliptic curve over K with torsion group G. Curves with positive ranks over quadratic fields can be found in [2, 5, 6, 12]. In [2], the authors give examples of elliptic curves with positive ranks and given torsion over fields of degree 2, 3 and 4.

In this article we use techniques from [8] in order to establish, for each of the torsion groups $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}$, the quadratic field with the smallest absolute value of its discriminant such that there exists an elliptic curve with that torsion and positive rank (the problem is in [8] solved without the request on the positivity of the rank). In the case of the torsion subgroups $\mathbb{Z}/11\mathbb{Z}$, $\mathbb{Z}/14\mathbb{Z}$ the problem is solved conditionally - we conclude that, if the Parity conjecture holds (i.e., the algebraic rank of the elliptic curve E over a number field K has the same parity as the analytic rank which is given by the root number (see, for example, [4])), then the elliptic curves that we find have positive rank.

Torsion groups that we deal with are parameterized by modular curves of genus 1. Each of the torsion groups $\mathbb{Z}/4\mathbb{Z}\oplus\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z}$ appears over only one quadratic field (see Theorem 1.1) and elliptic curves with some of these torsion groups and positive rank over quadratic field can be found in [5,6,12]. Other torsion groups which appear over quadratic fields and do not appear over the rationals ($\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$, $\mathbb{Z}/18\mathbb{Z}$) are parametrized by modular curves of genus 2. We were unable to find any elliptic curve with these torsion groups and positive rank over quadratic fields which are determined in [8].

For elliptic curves rank computation we use Cremona's MWRANK ([3]) (for elliptic curve with rational coefficients) and an implementation of 2-descent over number fields of Simon ([13]) in PARI/GP. We also use MAGMA ([1]) for computing 2-Selmer ranks and root numbers.

2. Elliptic curves with given torsions and positive ranks over smallest fields

2.1. *Torsion group* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$. First we will derive an equation for elliptic curve with torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$.

According to [10], the elliptic curve with equation

$$\mathcal{E}^{(10)}: \quad y^2 + \frac{2t^3+2t^2+2t+1}{(t+1)^2}xy + \frac{t^2(2t+1)}{(t+1)^2}y = x^3 + \frac{t^2(2t+1)}{(t+1)^2}x^2$$

has a $\mathbb{Q}(t)$-rational torsion point

$$Q = \left(-\frac{t^2(2t+1)}{(t+1)^3}, -\frac{t^3(2t+1)^2}{(t+1)^5}\right)$$

of order 10. It can be shown that the curve $\mathcal{E}^{(10)}$ is birationally equivalent to the elliptic curve

$$\begin{aligned} \mathcal{E}'^{(10)}: \quad y^2 = {} & x^3 - 2(1+2t-5t^2-5t^4-2t^5+t^6)x^2 \\ & + (-1+t^2)^5(-1-4t+t^2)x. \end{aligned} \tag{2.1}$$

The right hand side of the equation (2.1) has a linear and a quadratic factor. The curve will have more points of order 2 over the field K if the discriminant of the quadratic factor is a full square in K. This leads to the condition that if the parameter t is the x-coordinate of the point on the curve $X_1(2,10)(K)$, where

$$X_1(2,10): \quad s^2 = t^3 + t^2 - t,$$

then the curve $\mathcal{E}'^{(10)}(K)$ has torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ generated by the points

$$\begin{aligned} T_2 &= \left(1+2t-5t^2-5t^4-2t^5+t^6-8t^2s, 0\right), \\ T_{10} &= \left((1+t)^3(1+3t-5t^2+t^3), -4t(1+t)^3(1+3t-5t^2+t^3)\right). \end{aligned}$$

Theorem 2.1. *The quadratic field K with smallest $|\Delta|$ over which there appears an elliptic curve with a torsion group $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ and positive rank is $K = \mathbb{Q}(\sqrt{-2})$.*

Proof. Note that, according to [8, Theorem 8], the minimal quadratic field K such that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-2})$. The elliptic curve $X_1(2,10)$ over the field $\mathbb{Q}(\sqrt{-2})$ has rank equal to 1 with the generator $P = (-2, -\sqrt{-2})$. The elliptic curve generated from (2.1) by the point $2P$, i.e., by the parameters

$$(t,s) = \left(-\frac{25}{8}, \frac{95}{32}\sqrt{-2}\right),$$

is

$$E^{(2,10)}: \quad y^2 = x^3 - \frac{261214369}{131072}x^2 + \frac{75626226572068161}{68719476736}x.$$

This elliptic curve has rational coefficients and we can use MWRANK to show that it has rank equal to 1 over $\mathbb{Q}$. The rank of this curve over $\mathbb{Q}(\sqrt{-2})$ is then at least 1 and that proves the theorem. ∎

Remark 2.2. It can be shown that the elliptic curve from the last proof has rank equal to 3 over the field $K = \mathbb{Q}(\sqrt{-2})$ (using the fact that if E is an elliptic curve over $\mathbb{Q}$, then the rank of E over $\mathbb{Q}(\sqrt{-2})$ is given by $\operatorname{rank}(E(\mathbb{Q}(\sqrt{-2}))) = \operatorname{rank}(E(\mathbb{Q})) + \operatorname{rank}(E_{-2}(\mathbb{Q}))$, where E_{-2} is the (-2)-twist of E over $\mathbb{Q}$).

2.2. *Torsion group* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$. According to [10], the point

$$Q = \left(-\frac{1}{8}(t+1)(t^2-2t+5), -\frac{1}{32}(t+1)(t^2-1)(t^2-2t+5)\right)$$

is a torsion point of the order 12 on the elliptic curve

$$\mathcal{E}^{(12)}: \quad y^2 - \frac{(t^4-6t^2+24t-3)}{4(t-1)^2}xy - \frac{(t+1)^2(t^2-2t+5)}{4(t-1)^2}y = x^3.$$

It can be shown that this curve is birationally equivalent to the curve

$$\begin{aligned} \mathcal{E}^{(2,12)}: \ y^2 \ &= \ x^3 + 256(1-4t+4t^2+20t^3-26t^4+20t^5+4t^6-4t^7+t^8) \\ &\quad \times(1+4t+4t^3+t^4-4z-2t^2(1+2z))x^2 \\ &\quad +1048576(t-1)^6(t+1)^2(t-z)^6(-1+t-t^2+z)^2x. \end{aligned} \tag{2.2}$$

Similarly to the previous case, this curve has more points of order 2 over the field K if $(t,z) \in X_1(2,12)(K)$, where

$$X_1(2,12): \quad z^2 = t^3 - t^2 + t.$$

In that case, the points

$$\begin{aligned} T_2 &= (-4096t^3(t^2-t+1)(1+4t+4t^3+t^4-4z-2t^2(1+2z)), 0), \\ T_{12} &= \big(-1024(t-1)^5(t+1)(-2t-2t^3+z+t^2(2+z)), \\ &\quad -16384(t-1)^5(1+t+t^2+t^3)(-6t^7-z+t^6(-2+z)-5t^2(2+z) \\ &\quad +6t^5(1+2z)+t(2+4z)+2t^3(7+8z)-t^4(20+11z))\big). \end{aligned}$$

generate a torsion subgroup $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ on $\mathcal{E}^{(2,12)}(K)$.

THEOREM 2.3. *The quadratic field K with smallest $|\Delta|$ over which there appears an elliptic curve with a torsion group $\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/12\mathbb{Z}$ and positive rank is $K = \mathbb{Q}(\sqrt{13})$.*

PROOF. According to [8, Theorem 9], the minimal quadratic field K such that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{13})$. The elliptic curve $X_1(2,12)$ over the field $\mathbb{Q}(\sqrt{13})$ has rank equal to 1 with the generator $P = (-2, -\sqrt{-2})$. The elliptic curve generated from (2.2) by the point P is

$$\begin{aligned} E^{(2,12)}: \quad y^2 = x^3 &+ \frac{1}{65536}(-4289032\sqrt{13}+15673889)x^2 \\ &+ \frac{1}{4194304}(-32028469200\sqrt{13}+115490749725)x, \end{aligned}$$

and has rank equal to 1. A point of infinite order is

$$Q = \left(-\frac{153}{256}\sqrt{13}+\frac{4473}{2048}, -\frac{9046125}{131072}\sqrt{13}+\frac{130609215}{524288}\right).$$

∎

2.3. *Torsion group* $\mathbb{Z}/15\mathbb{Z}$. According to [12], the general equation of the elliptic curve with points of order 15 is

$$\begin{aligned} \mathcal{E}^{(15)}: \quad & y^2+axy+by=x^3+bx^2, \\ a &= \frac{(t^2-t)s+(t^5+5t^4+9t^3+7t^2+4t+1)}{(t+1)^3(t^2+t+1)}, \\ b &= \frac{t(t^4-2t^2-t-1)s+t^3(t+1)(t^3+3t^2+t+1)}{(t+1)^6(t^2+t+1)}, \end{aligned} \tag{2.3}$$

with $(t,s)\in X_1(15)$, where

$$X_1(15): \quad s^2+st+s=t^3+t^2,$$

and

$$t(t+1)(t^2+t+1)(t^4+3t^3+4t^2+2t+1)(t^4-7t^3-6t^2+2t+1)\neq 0.$$

THEOREM 2.4. *The quadratic field K with smallest $|\Delta|$ over which there appears an elliptic curve with a torsion group $\mathbb{Z}/15\mathbb{Z}$ and positive rank is $K=\mathbb{Q}(\sqrt{-7})$.*

PROOF. According to [8, Theorem 5], the minimal quadratic field K such that $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion group over K is $K=\mathbb{Q}(\sqrt{5})$. The elliptic curve $X_1(15)$ over the field $\mathbb{Q}(\sqrt{5})$ has rank equal to 0 and torsion group $\mathbb{Z}/8\mathbb{Z}$. It is easy to see that only 4 torsion points generate elliptic curve from (2.3), i.e., they are not the cusps, and that all of them generate mutually isomorphic elliptic curves with ranks equal to 0.

Next we look at elliptic curves over the field $\mathbb{Q}(\sqrt{-7})$. We find that $X_1(15)$ over this field has rank equal to 1 with the point

$$P=\left(\frac{1}{8}(-\sqrt{-7}-5),\frac{1}{16}(\sqrt{-7}+5)\right)$$

of infinite order. The elliptic curve generated from (2.3) by the point $-P$ i.e., the point with parameters

$$(t,s)=-P=\left(\frac{1}{8}(-\sqrt{-7}-5),\frac{1}{16}(\sqrt{-7}-11)\right)\in X_1(15)(\mathbb{Q}(\sqrt{-7})),$$

is

$$E^{(15)}: \quad y^2+(-2\sqrt{-7}+15)xy+(26\sqrt{-7}-14)y=x^3+(26\sqrt{-7}-14)x^2.$$

The 2-descent procedure implemented in `ell.gp` shows that this curve has rank ≤ 1 over $\mathbb{Q}(\sqrt{-7})$. The root number calculated by MAGMA and the Parity conjecture suggest that this curve, conditionally, has rank 1. Finally, in the set

$$\left\{a+b\sqrt{-7}:|a|,|b|\leq 100\right\}$$

we successfully find x-coordinate of the non-torsion point

$$Q=(6\sqrt{-7}-98,136\sqrt{-7}+1064)$$

on the curve $E^{(15)}(\mathbb{Q}(\sqrt{-7}))$ and this completes the proof. ∎

2.4. *Torsion group* $\mathbb{Z}/11\mathbb{Z}$. According to [12], the general equation of the elliptic curve with points of order 11 is

$$\mathcal{E}^{(11)}: \quad y^2+(st+t-s^2)xy+s(s-1)(s-t)t^2y = x^3+s(s-1)(s-t)tx^2, \tag{2.4}$$

with $P=(t,s)\in X_1(11)$, where

$$X_1(11): \quad s^2-s=t^3-t^2$$

and

$$\Delta_{\mathcal{E}^{(11)}} = t(t-1)(t^5-18t^4+35t^3-16t^2-2t+1)\neq 0.$$

THEOREM 2.5. *Assume the Parity conjecture. The quadratic field K with smallest $|\Delta|$ over which there appears an elliptic curve with a torsion group $\mathbb{Z}/11\mathbb{Z}$ and positive rank is $K=\mathbb{Q}(\sqrt{-7})$.*

PROOF. According to [8, Theorem 2], the minimal quadratic field K such that $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion group over K is $K=\mathbb{Q}(\sqrt{-7})$. The elliptic curve $X_1(11)$ over the field $\mathbb{Q}(\sqrt{-7})$ has rank equal to 1. The point of infinite order is

$$P=\left(-\frac{4}{7},\frac{1}{98}(49+19\sqrt{-7})\right),$$

and generates, from (2.4), the elliptic curve

$$\begin{aligned}E^{(11)}: \quad & y^2+(-209\sqrt{-7}-579)xy-(10486784\sqrt{-7}+57953280)y\\ &= x^3+(26752\sqrt{-7}+147840)x^2,\end{aligned}$$

with the torsion group $\mathbb{Z}/11\mathbb{Z}$. The root number of this elliptic curve over the field $\mathbb{Q}(\sqrt{-7})$ is -1 so, according to the Parity conjecture, we can conclude that this is elliptic curve has conditionally positive rank. Unfortunately, we were unable to determine any point of infinite order on this curve. ∎

2.5. *Torsion group* $\mathbb{Z}/14\mathbb{Z}$. The general equation of the elliptic curve with points of order 14, according to [12], is

$$\begin{aligned}&\mathcal{E}^{(14)}: \quad y^2+axy+by=x^3+bx^2,\\ &a=\frac{t^4-st^3+(2s-4)t^2-st+1}{(t+1)(t^3-2t^2-t+1)},\\ &b=\frac{-t^7+2t^6+(2s-1)t^5+(-2s-1)t^4+(-2s+2)t^3+(3s-1)t^2-st}{(t+1)^2(t^3-2t^2-t+1)^2},\end{aligned} \tag{2.5}$$

where $P=(t,s)\in X_1(14)$ and

$$\begin{aligned}&X_1(14): \quad s^2+st+s=t^3-t,\\ &\Delta_{\mathcal{E}^{(14)}} = t(t-1)(t+1)(t^3-9t^2-t+1)(t^3-2t^2-t+1)\neq 0.\end{aligned}$$

THEOREM 2.6. *Assume the Parity conjecture. The quadratic field K with smallest $|\Delta|$ over which there appears an elliptic curve with a torsion group $\mathbb{Z}/14\mathbb{Z}$ and positive rank is $K = \mathbb{Q}(\sqrt{-11})$.*

PROOF. According to [8, Theorem 4], the minimal quadratic field K such that $\mathbb{Z}/14\mathbb{Z}$ appears as a torsion group over K is $K = \mathbb{Q}(\sqrt{-7})$. The elliptic curve $X_1(14)$ over the field $\mathbb{Q}(\sqrt{-7})$ has rank equal to 0. It can be shown that the torsion points of this curve which are not the cusps generate two non-isomorphic elliptic curves with ranks equal to 0. Over the fields $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{2})$, the elliptic curve $X_1(14)$ has rank equal to 0 and torsion $\mathbb{Z}/6\mathbb{Z}$. All the torsion points are cusps so we conclude that an elliptic curve with the torsion group $\mathbb{Z}/14\mathbb{Z}$ over these two fields does not exist.

Over the field $\mathbb{Q}(\sqrt{-11})$ the curve $X_1(14)$ has rank equal to 1, with the generator

$$P = \left(-\frac{5}{4}, -\frac{1}{4}\sqrt{-11} + \frac{1}{8}\right).$$

The linear combination $-2P + T$, where $T = (1, -2)$ is a torsion point on $X_1(14)(\mathbb{Q}(\sqrt{-11}))$, generates the elliptic curve

$$\begin{aligned} E^{(14)} : \quad & y^2 + (-2601888534886283704\sqrt{-11} + 1542527334075125818577)xy \\ & -(43286504429925775681153399339981518914403432663035092419000\sqrt{-11} \\ & -239448337641930912934754848966237361950084593095601008052000)y \\ & = x^3 + (-313766195076761969526071169866614175160\sqrt{-11} \\ & +1735663223649526033628839600302712469280)x^2 \end{aligned}$$

with the torsion group $\mathbb{Z}/11\mathbb{Z}$. The root number of this elliptic curve over the field $\mathbb{Q}(\sqrt{-11})$ is -1 so, if we assume that the Parity conjecture holds, we can conclude that this is an elliptic curve with a conditionally positive rank. $\square$

ACKNOWLEDGEMENTS.

The author would like to thank the referees for the careful reading of the paper and for the helpful suggestions. The author was supported by the Ministry of Science, Education and Sports, Republic of Croatia, grant 235-2352818-1042.

REFERENCES

[1] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.

[2] J. Bosman, P. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, preprint.

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

[4] T. Dokchitser, *Notes on the Parity Conjecture*, to appear in a CRM Advanced Courses volume, Birkhauser.

[5] A. Dujella and 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.
[6] 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.
[7] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.
[8] S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta. Arith. **152** (2012), 291–305.
[9] M. A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.
[10] L. Kulesz, *Families of elliptic curves of high rank with nontrivial torsion group over* $\mathbb{Q}$, Acta Arith. **108** (2003), 339–356.
[11] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
[12] F. P. Rabarison, *Structure de torsion des courbes elliptiques sur les corps quadratiques*, Acta Arith. **144** (2010), 17–52.
[13] D. Simon, *Le fichier gp*, http://www.math.unicaen.fr/~simon/ell.gp.

M. Jukić Bokun
Department of Mathematics
University of Osijek
Trg Ljudevita Gaja 6, 31 000 Osijek
Croatia
E-mail: mirela@mathos.hr

Received: 6.12.2011.
Revised: 11.1.2012.