Math. J. Okayama Univ. **53** (2011), 75–82

TORSION OF ELLIPTIC CURVES OVER QUADRATIC CYCLOTOMIC FIELDS

Filip Najman

Abstract. In this paper we study the possible torsions of elliptic curves over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

1. Introduction

For an elliptic curve E over a number field K, it is well known, by the Mordell-Weil theorem, that the set $E(K)$ of K-rational points on E is a finitely generated abelian group. The group $E(K)$ is isomorphic to $T \oplus \mathbb{Z}^r$, where r is a non-negative integer and T is the torsion subgroup. When $K = \mathbb{Q}$, by Mazur's Theorem, the torsion subgroup is either cyclic of order m, where $1 \leq m \leq 10$ or $m = 12$, or of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$, where $1 \leq m \leq 4$. If K is a quadratic field, then the following theorem classifies the possible torsions.

Theorem(Kamienny, [5]*, Kenku and Momose,* [6]*).* Let K be a quadratic field and E an elliptic curve over K. Then the torsion subgroup $E(K)_{tors}$ of $E(K)$ is isomorphic to one of the following 26 groups:

$$\mathbb{Z}_m, \text{ for } 1 \leq m \leq 18, \ m \neq 17,$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}, \text{ for } 1 \leq m \leq 6,$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_{3m}, \text{ for } m = 1, 2$$
$$\mathbb{Z}_4 \oplus \mathbb{Z}_4.$$

Moreover, the only quadratic field over which torsion $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ appears is $\mathbb{Q}(i)$ and the only quadratic field over which torsions $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ appear is $\mathbb{Q}(\sqrt{-3})$.

In [4], Theorem 3.5, it is proved that if we let the quadratic fields vary, then all of the 26 torsion subgroups appear infinitely often.

In this paper we will take a different approach. We will fix the quadratic field and then study the possible torsions. The fields that we are going to study, $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, are somewhat special, as they are the only fields containing roots of unity apart from 1 and -1, i.e. they are the only cyclotomic quadratic fields. Also, over each of these fields, torsion subgroups appear that appear over no other fields. Note that the rings of integers of both these fields are unique factorization domains.

Mathematics Subject Classification. Primary 11G05; Secondary 14G05.

The results obtained for elliptic curves over $\mathbb{Q}(i)$ are presented in the following theorem.

Theorem 1. (i) Let E be an elliptic curve with rational coefficients. Then $E(\mathbb{Q}(i))_{tors}$ is either one of the groups from Mazur's Theorem or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.
(ii) Let E be an elliptic curve defined over $\mathbb{Q}(i)$. Then $E(\mathbb{Q}(i))_{tors}$ is either one of the groups from Mazur's Theorem, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_{13}$.

The first part of this theorem is the best possible, while for the second part we believe that $\mathbb{Z}_{13}$ does not appear as a torsion subgroup, but we were unable to prove this.

Note that the torsion subgroup $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ appears infinitely often. Elliptic curves with this torsion can be written in the form

$$y^2 = x(x + m^2)(x + n^2),\ m, n \in \mathbb{Z}[i],$$

where $m^2 - n^2$ is a square in $\mathbb{Z}[i]$. This is an easy corollary of the 2-descent proposition (see [7], Theorem 4.2, p. 85).
The results obtained for elliptic curves over $\mathbb{Q}(\sqrt{-3})$ are presented in the following theorem.

Theorem 2. (i) Let E be an elliptic curve with rational coefficients. Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is either one of the groups from Mazur's Theorem, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.
(ii) Let E be an elliptic curve defined over $\mathbb{Q}(\sqrt{-3})$.
Then $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ is either one of the groups from Mazur's Theorem, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_6$, $\mathbb{Z}_{13}$ or $\mathbb{Z}_{18}$.

Again, the first part of this theorem is the best possible($\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ appear infinitely often), while for the second part we believe that $\mathbb{Z}_{13}$ and $\mathbb{Z}_{18}$ do not appear as torsion subgroups, but we were unable to prove this.

2. Torsion over $\mathbb{Q}(i)$

Throughout this chapter, the following extension of the Lutz-Nagell Theorem is used to compute torsion groups of elliptic curves.

Theorem (Extended Lutz-Nagell Theorem). Let $E : y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}[i]$. If a point $(x, y) \in E(\mathbb{Q}(i))$ has finite order, then

(1) $x, y \in \mathbb{Z}[i]$.
(2) Either $y = 0$ or $y^2 | 4A^3 + 27B^2$.

The proof of the Lutz-Nagell Theorem can easily be extended to elliptic curves over $\mathbb{Q}(i)$. Details of the proof can be found in [12], Chapter 3. An implementation in Maple can be found in [12], Appendix A.
Next, we give a result that applies to elliptic curves over all quadratic fields and that is an immediate corollary of the main result of [8] (see also [2]).

Lemma 3. Let E be an elliptic curve with rational coefficients and d a square-free integer. Then $E(\mathbb{Q}(\sqrt{d}))_{tors}$ cannot be $\mathbb{Z}_{11}, \mathbb{Z}_{13}$ or $\mathbb{Z}_{14}$.

Next we give a series of lemmas that will prove Theorem 1.

Lemma 4. $E(\mathbb{Q}(i))_{tors}$ cannot be $\mathbb{Z}_{11}, \mathbb{Z}_{18}$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$.

Proof: It is proved in [6], Example 3.2 that the torsion of an elliptic curve over $\mathbb{Q}(i)$ cannot be $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$. It is proved in [10], Theorem 2 that the torsion cannot be $\mathbb{Z}_{11}$. Since the rational prime 3 remains prime in $\mathbb{Z}[i]$, condition i) of Proposition 2.4 from [6] is satisfied and hence, the torsion cannot be $\mathbb{Z}_{18}$. □

Lemma 5. $E(\mathbb{Q}(i))_{tors}$ cannot be $\mathbb{Z}_{16}$.

Proof: By [9], case 2.5.5., page 37, we see that elliptic curves with torsion $\mathbb{Z}_{16}$ over $\mathbb{Q}(i)$ are induced by the solutions of the equation

$$s^2 = t(t^2+1)(t^2+2t-1),\ s,t \in \mathbb{Q}(i), \tag{1}$$

where t satisfies

$$t(t^4-1)(t^2+2t-1)(t^2-2t-1) \neq 0. \tag{2}$$

It follows that it is enough to prove that this equation has no solutions. Let

$$t = \alpha\square, \tag{3}$$

$$t^2+1 = \beta\square \tag{4}$$

and

$$t^2+2t-1 = \gamma\square, \tag{5}$$

where α, β and γ are square-free, nonzero Gaussian integers. Also, let $t = \frac{u}{v}$, where u and v are coprime, nonzero Gaussian integers. First, we prove that α is relatively prime to β and γ. Suppose a Gaussian prime π divides both α and β. From (3) it follows that π divides either u or v an odd number of times. From (4), it follows that π divides u^2+v^2, and since it divides exactly one of u, v, this is impossible. Suppose a Gaussian prime π divides both α and γ. Again, π divides exactly one of u, v. From (5), it follows that π divides $u^2+2uv-v^2$, which is again impossible. Since -1 is a square in $\mathbb{Z}[i]$, we conclude that $\alpha \in \{1, i\}$.

Next, we prove that $\gcd(\beta, \gamma) = 1$ or $1 + i$. Let π be a Gaussian prime dividing both β and γ. By subtracting (4) from (5), we conclude that π divides $2uv - 2v^2 = 2v(u - v)$. As it was already proved, since π divides β, π cannot divide u, implying $\pi|2(u - v)$. Suppose $\pi|(u - v)$, i.e. $u \equiv v \pmod{\pi}$. Now, (4) implies $2u^2 \equiv 0 \pmod{\pi}$, again implying $\pi|2$. Since $2 = -i(1 + i)^2$, we conclude that the only possibilities for β and γ are $\beta, \gamma \in \{1, i, 1 + i, i(1 + i)\}$.

We assert that none of these are possible. Suppose $\beta = 1$. Since $\alpha = 1$ or i, we can write $t = \frac{x^2}{y^2}$ or $t = \frac{ix^2}{y^2}$, i.e. $t^2 = \pm\frac{x^4}{y^4}$. Multiplying (4) by y^4 we get $x^4 \pm y^4 = \pm z^2$. It was proved by Hilbert(see [3]) that this equation has only trivial solutions in Gaussian integers, implying $t = 0$.

Suppose $\beta = i$. Multiplying (3) and (4) we obtain $iy^2 = t^3 + t$ or $-y^2 = t^3+t$, leading to elliptic curves in Weierstrass form $y^2 = x^3-x$ and $y^2 = x^3+x$ respectively. Using the program [11], written in PARI, we compute that the rank of this curve is 0. It is easy to compute, using the Extended Lutz-Nagell Theorem that the torsion subgroup of both these curves over $\mathbb{Q}(i)$ is $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. All the torsion points of these curves satisfy $t(t^4 - 1) = 0$.

Suppose $\beta = 1 + i$ or $i(1 + i)$. Multiplying (3) and (4) we obtain one of the following three elliptic curves $(1 + i)y^2 = t^3 + t$, $i(1 + i)y^2 = t^3 + t$ and $-(1 + i)y^2 = t^3 + t$. These curves induce the curves $y^2 = x^3 + 2ix$ and $y^2 = x^3 - 2ix$ in Weierstrass form, both of them having rank 0 (again, this is computed using [11]) and torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. All of the torsion points induce t satisfying $t(t^4 - 1) = 0$. Hence, the starting equation has no solutions. □

Lemma 6. $E(\mathbb{Q}(i))_{tors}$ cannot be $\mathbb{Z}_{15}$.

Proof: By [9], case 2.5.4, pages 34 and 35, elliptic curves with torsion subgroups isomorphic to $\mathbb{Z}_{15}$ are induced by the solutions over $\mathbb{Q}(i)$ of

$$s^2 + st + s = t^3 + t^2 \tag{6}$$

satisfying

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

Using [11], we compute that the rank of (6) over $\mathbb{Q}(i)$ is 0 and the torsion points give $t = 0$ or -1, implying that the equation has no solutions. □

Lemma 7. $E(\mathbb{Q}(i))_{tors}$ cannot be $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$.

Proof: By [9], case 2.5.8, pages 42–44, elliptic curves with torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$ are induced by the solutions over $\mathbb{Q}(i)$ of the equation

$$s^2 = (2t^2 - 2t + 1)(6t^2 - 6t + 1) \tag{7}$$

satisfying

$$t(t-1)(2t-1)(2t^2-2t+1)(3t^2-3t-1)(6t^2-6t+1)\neq 0. \tag{8}$$

The elliptic curve (7) has the Weirstrass form

$$y^2=x^3-x^2+x.$$

This curve has rank 0 and 8 torsion points. They are $\{O,(0,0),(1,\pm 1),(\pm i,\pm 1)\}$ in Weierstrass form, inducing $t=0,1,\frac{1}{2}$ or $\frac{1\pm i}{2}$, none of them satisfying (8). □

Lemma 8. $E(\mathbb{Q}(i))_{tors}$ cannot be $\mathbb{Z}_{14}$.

Proof: By [9], case 2.5.3, page 31, elliptic curves with torsion $\mathbb{Z}_{14}$ are induced by the solutions over $\mathbb{Q}(i)$ of the equation

$$s^2+st+s=t^3-t$$

satisfying

$$t(t^2-1)(t^3-9t^2-t+1)(t^3-2t^2-t+1)\neq 0.$$

The given curve has rank 0 and 6 torsion points over $\mathbb{Q}(i)$, all of them satisfying $t=0$ or ± 1. □

Lemmas 4, 5, 6, 7 and 8 prove Theorem 1, (ii). Combining this with Lemma 3, we get Theorem 1, (i).

3. Torsion over $\mathbb{Q}(\sqrt{-3})$

As some of the proofs in this section are similar to the ones in the previous section, some technical details will be omitted. Let $\omega=\frac{1-\sqrt{-3}}{2}$. It is easy to see that ω is a primitive sixth root of unity and $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}(\sqrt{-3})$.

Lemma 9. $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ cannot be $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$, or $\mathbb{Z}_2\oplus\mathbb{Z}_{12}$.

Proof: It is proved in [6] that the torsion subgroup cannot be $\mathbb{Z}_{14}$(Example 2.5) or $\mathbb{Z}_2\oplus\mathbb{Z}_{12}$(Example 3.2). The proof that the torsion cannot be $\mathbb{Z}_{15}$ is completely analogous to the proof of Lemma 7. □

Lemma 10. $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ cannot be $\mathbb{Z}_{11}$.

Proof: As can be seen in [9], case 2.5.1, page 25, the solutions $s,t\in\mathbb{Q}(\sqrt{-3})$ of the equation

$$s^2-s=t^3-t^2$$

satisfying

$$t(t-1)(t^5-18t^4+35t^3-16t^2-2t+1)\neq 0$$

induce elliptic curves with torsion $\mathbb{Z}_{11}$ over $\mathbb{Q}(\sqrt{-3})$. The rank of this curve is 0 and there are 5 torsion points, all of them satisfying $t = 0$ or 1 (see [9], Lemma 2.1). □

Lemma 11. $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ cannot be $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$.

Proof: As can be seen in [9], case 2.5.7, pages 39–40, the solutions $s, t \in \mathbb{Q}(\sqrt{-3})$ of the equation

$$s^2 = t^3 + t^2 - t$$

satisfying

$$t(t^2 - 1)(t^2 - 4t - 1)(t^2 + t - 1) \neq 0$$

induce elliptic curves with torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$ over $\mathbb{Q}(\sqrt{-3})$. The rank of this curve is 0 and there are 6 torsion points, all of them satisfying $t = 0, -1$ or 1 (see [9], Lemma 2.4). □

As in the proof of Theorem 1, the hardest part of the proof of Theorem 2 is eliminating the possibility of the torsion being $\mathbb{Z}_{16}$.

Lemma 12. $E(\mathbb{Q}(\sqrt{-3}))_{tors}$ cannot be $\mathbb{Z}_{16}$.

Proof: Again, we have to prove that the equation (1) has no solutions satisfying (2). We follow the same strategy of the proof of Lemma 6, and define α, β and γ in the same way. It can be proved in the same way as in Lemma 6 that α is a unit and that each of β and γ is either a unit or twice a unit. As every unit is a square or ω times a square, and as $\gamma = \alpha\beta \pmod{(\mathbb{Q}(\sqrt{-3})^*)^2}$, we see that we have 8 possibilities for the triples (α, β, γ). If t is a solution of (1), then t has to be the first coordinate of a point on both curves

$$E_1 : \alpha\beta y^2 = t^3 + t$$

and

$$E_2 : \alpha\gamma y^2 = t^3 + 2t^2 - t.$$

In the following table we give the ranks of these curves depending on α and β.

α	β	γ	$\operatorname{rank}(E_1(\mathbb{Q}(\sqrt{-3}))$	$\operatorname{rank}(E_2(\mathbb{Q}(\sqrt{-3}))$
1	1	1	1	0
1	ω	ω	1	0
1	2	2	0	2
1	2ω	2ω	0	0
ω	1	ω	1	0
ω	ω	1	1	0
ω	2ω	2	0	0
ω	2	2ω	0	2

As it can be seen, for each case there either E_1 or E_2 has rank 0, and thus only the torsion points are possible solutions. It remains to check the torsion points of the following four curves:

$$y^2 = x^3 + 2x^2 - x, \tag{9}$$

$$y^2 = x^3 + 2\omega x^2 - \omega^2 x, \tag{10}$$

$$y^2 = x^3 + 4x, \tag{11}$$

$$y^2 = x^3 + 4\omega^2 x. \tag{12}$$

The torsion groups were now computed in APECS([1]). The torsion of the curves (11) and (12) is $\mathbb{Z}_4$, corresponding to $t = 0, \pm 1$ on the curve E_1. The torsion of the curves (9) and (10) is $\mathbb{Z}_2$, corresponing to $t = 0$ on the curve E_2. We obtain that none of the t induced by the torsion points satisfies (2). We conclude that the torsion $\mathbb{Z}_{16}$ is impossible. □

Lemmas 9, 10, 11 and 12 combined with Lemma 3 prove Theorem 2.

Remark. In order to prove that there are no elliptic curves with torsion $\mathbb{Z}_{13}$ over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, one would have to prove that there are no solutions in the respective quadratic field of the equation

$$s^2 = t^6 - 2t^5 + t^4 - 2t^3 + 6t^2 - 4t + 1 \tag{13}$$

satisfying

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

Similarly, to prove that there are no elliptic curves with torsion $\mathbb{Z}_{18}$ over $\mathbb{Q}(\sqrt{-3})$ one would have to prove that there do not exist $s, t \in \mathbb{Q}(\sqrt{-3})$ satisfying

$$s^2 = t^6 + 2t^5 + 5t^4 + 10t^3 + 10t^2 + 4t + 1 \tag{14}$$

and

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

Note that (13) and (14) are both hyperelliptic curves of genus 2.

Acknowledgements

The author would like to thank Andrej Dujella for motivating and helpful discussions. Also, the author is grateful to Mirela Jukić-Bokun and the referee for pointing out some mistakes in earlier versions of this manuscript.

References

[1] I. Connell, *APECS*, ftp://ftp.math.mcgill.ca/pub/apecs/.
[2] Y. Fujita, *Torsion subgroups of elliptic curves in elementary abelian* 2*-extensions of* $\mathbb{Q}$, J. Number Theory **114** (2005), 124–134.
[3] D. Hilbert, *Jahresbericht d. Deutschen Math.-Vereinigung*, 4, 1894/1895, 517–525.
[4] D. Jeon, C. H. Kim and E. Park, *On the torsion of elliptic curves over quartic number fields*, J. London Math. Soc. (2) **74** (2006), 1–12.
[5] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 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] A. Knapp, *Elliptic curves*, Princeton Univ. Press, 1992.
[8] 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.
[9] F. P. Rabarison, *Torsion et rang des courbes elliptiques definies sur les corps de nombres algebriques*, Doctorat de Universite de Caen, 2008.
[10] M. A. Reichert, *Explicit Determination of Nontrivial Torsion Structures of Elliptic Curves Over Quadratic Number Fields*, Math. Comp. **174** (1986), 637–658.
[11] D. Simon, *Le fichier gp*, http://www.math.unicaen.fr/∼simon/ell.gp.
[12] T. Thongjunthug, *Elliptic curves over* $\mathbb{Q}(i)$, Honours thesis (2006).

Department of Mathematics
University of Zagreb
Bijenička cesta 30, 10000 Zagreb
Croatia
e-mail address: fnajman@math.hr

(*Received June 5, 2009*)
(*Revised August 2, 2009*)