Journal of Number Theory 130 (2010) 1964–1968

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Complete classification of torsion of elliptic curves over quadratic cyclotomic fields

Filip Najman

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

ARTICLE INFO

Article history:
Received 10 October 2009
Available online 1 April 2010
Communicated by David Goss

MSC:
11G05
11G30
14H40

Keywords:
Elliptic curves
Quadratic fields
Hyperelliptic curves

ABSTRACT

Text. In a previous paper Najman (in press) [9], the author examined the possible torsions of an elliptic curve over the quadratic fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. Although all the possible torsions were found if the elliptic curve has rational coefficients, we were unable to eliminate some possibilities for the torsion if the elliptic curve has coefficients that are not rational. In this note, by finding all the points of two hyperelliptic curves over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, we solve this problem completely and thus obtain a classification of all possible torsions of elliptic curves over $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$.

Video. For a video summary of this paper, please click here or visit http://www.youtube.com/watch?v=VPhCkJTGB_o.

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 $1 \leqslant m \leqslant 10$ or $m = 12$, or of the form $\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}$, where $1 \leqslant m \leqslant 4$.

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:*

$$\mathbb{Z}_m, \quad \textit{for } 1 \leqslant m \leqslant 18,\ m \neq 17,$$

E-mail address: fnajman@math.hr.

0022-314X/$ – see front matter © 2010 Elsevier Inc. All rights reserved.
doi:10.1016/j.jnt.2009.12.008

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{2m}, \quad \textit{for } 1 \leqslant m \leqslant 6,$$

$$\mathbb{Z}_3 \oplus \mathbb{Z}_{3m}, \quad \textit{for } m = 1, 2,$$

$$\mathbb{Z}_4 \oplus \mathbb{Z}_4.$$

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.

Unfortunately, if we fix a quadratic field, this theorem does not tell us which of the 26 listed groups actually appear as torsion subgroups. In [9], we took this approach, fixing the fields $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$. These fields are somewhat special among quadratic fields, as they are the only cyclotomic quadratic fields ($\mathbb{Q}(i) = \mathbb{Q}(\zeta_4)$ and $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_6)$, where ζ_n is a primitive n-th root of unity). Also, as already mentioned, 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.

The main results of [9] are given 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 $\mathbb{Z}_{13}$.*
(iii) *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 $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.*
(iv) *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 $\mathbb{Z}_{18}$.*

While it is not hard to show that (i) and (iii) are best possible, we conjectured that the possible torsion $\mathbb{Z}_{13}$ could be removed from (ii) and the possible torsions $\mathbb{Z}_{13}$ and $\mathbb{Z}_{18}$ could be removed from (iv). In this note we prove this conjecture, thus proving the following theorem.

Theorem 2.

(i) *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 or $\mathbb{Z}_4 \oplus \mathbb{Z}_4$.*
(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, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ or $\mathbb{Z}_3 \oplus \mathbb{Z}_6$.*

2. Torsion over $\mathbb{Q}(i)$ cannot be $\mathbb{Z}_{13}$

As seen from [12], case 2.5.2, page 30, elliptic curves with torsion $\mathbb{Z}_{13}$ over $\mathbb{Q}(i)$ exist if and only if the curve C_1 defined by

$$C_1\colon \quad y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1 \tag{1}$$

has points over $\mathbb{Q}(i)$ satisfying

$$x(x-1)\bigl(x^3 - 4x^2 + x + 1\bigr) \neq 0. \tag{2}$$

As the points of a hyperelliptic curve have no structure, it is useful to examine the Jacobian variety of a curve (see [3]). Let J_1 be the Jacobian of C_1, $C_1^{(d)}$ the quadratic twist of C_1 by d and $J_1^{(d)}$ the Jacobian of $C_1^{(d)}$.

Lemma 3. $J_1(\mathbb{Q}(i)) \simeq \mathbb{Z}_{19}$.

Proof. In MAGMA [2] there exists a implementation of 2-descent on Jacobians (the RankBounds function, see [13] for the algorithm), but unfortunately only over $\mathbb{Q}$. However, we can compute $rank(J_1(\mathbb{Q})) = 0$ and $rank(J_1^{(-1)}(\mathbb{Q})) = 0$, and thus

$$rank\big(J_1\big(\mathbb{Q}(i)\big)\big) = rank\big(J_1(\mathbb{Q})\big) + rank\big(J_1^{(-1)}(\mathbb{Q})\big) = 0.$$

Again for the torsion of the Jacobian, MAGMA has implemented functions only over the rationals. For an algorithm for computing the torsion, see [11]. The discriminant of the C_1 is $2^{20} \cdot 13^2$, so 2 and 13 are the only rational primes with bad reduction.

We compute $J_1(\mathbb{Q})_{tors} \simeq \mathbb{Z}_{19}$. If p is a Gaussian prime of good reduction, then the prime-to-p part of $J_1(Q(i))_{tors}$ injects to $J_1(F_p(i))$. As $p \equiv 3 \pmod 4$ remains prime in $\mathbb{Z}[i]$ and $F_p(i) \simeq F_{p^2}$, by computing

$$\big|J_1(F_{121})\big| = \big|J_1\big(F_{11}(i)\big)\big| = 7^2 \cdot 19^2,$$
$$\big|J_1(F_{529})\big| = \big|J_1\big(F_{23}(i)\big)\big| = 3 \cdot 7 \cdot 19 \cdot 229,$$
$$\big|J_1(F_{961})\big| = \big|J_1\big(F_{31}(i)\big)\big| = 2^8 \cdot 3^2 \cdot 19^2,$$

we conclude that $|J_1(Q(i))_{tors}| = 19$ and thus $J_1(\mathbb{Q}(i)) \simeq \mathbb{Z}_{19}$. □

Lemma 4. $C_1(\mathbb{Q}(i)) = \{\infty_+, \infty_-, (1, \pm 1), (0, \pm 1)\}$.

Proof. The 18 non-zero elements of $J_1(\mathbb{Q}) = J_1(\mathbb{Q}(i))$, in the Mumford representation that MAGMA uses (see [8] for details, and [1] for the particular implementation in MAGMA) are

$$\big(x^2, -2x+1, 2\big), \quad \big(x-1, -x^3, 2\big), \quad \big(x, x^3-1, 2\big), \quad \big(x, x^3+1, 2\big), \quad \big(x^2-x, -1, 2\big),$$
$$\big(x^2-x, -2x+1, 2\big), \quad \big(1, x^3-x^2, 2\big), \quad \big(x^2-2x+1, x, 2\big), \quad \big(x-1, x^3-2, 2\big),$$
$$\big(x-1, -x^3+2, 2\big), \quad \big(x^2-2x+1, -x, 2\big), \quad \big(1, -x^3+x^2, 2\big), \quad \big(x^2-x, 2x-1, 2\big),$$
$$\big(x^2-x, 1, 2\big), \quad \big(x, -x^3-1, 2\big), \quad \big(x, -x^3+1, 2\big), \quad \big(x-1, x^3, 2\big), \quad \big(x^2, 2x-1, 2\big),$$

and we easily see that the points mentioned are the only ones on this curve. □

By proving Lemma 4, we have actually proven Theorem 2(i).

3. Torsion over $\mathbb{Q}(\sqrt{-3})$ cannot be $\mathbb{Z}_{13}$ or $\mathbb{Z}_{18}$

To prove that the torsion cannot be $\mathbb{Z}_{13}$, we again have to prove that there are no points on C_1 over $\mathbb{Q}(\sqrt{-3})$ satisfying (2).

Lemma 5. $J_1(\mathbb{Q}(\sqrt{-3})) \simeq \mathbb{Z}_{19}$.

Proof. We compute $rank(J_1^{(-3)}(\mathbb{Q})) = 0$, and thus

$$rank\big(J_1\big(\mathbb{Q}(\sqrt{-3})\big)\big) = rank\big(J_1(\mathbb{Q})\big) + rank\big(J_1^{(-3)}(\mathbb{Q})\big) = 0.$$

As 5 and 17 are rational primes of good reduction that remain prime in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, and

$$\left|J_1(F_{25})\right| = \left|J_1\big(F_5(\sqrt{-3}\,)\big)\right| = 19^2,$$
$$\left|J_1(F_{289})\right| = \left|J_1\big(F_{17}(\sqrt{-3}\,)\big)\right| = 2^6 \cdot 3^2 \cdot 7 \cdot 19,$$

we conclude that $J_1(\mathbb{Q}(\sqrt{-3}\,)) \simeq \mathbb{Z}_{19}$. □

Lemma 6. $C_1(\mathbb{Q}(\sqrt{-3})) = \{\infty_+, \infty_-, (1, \pm 1), (0, \pm 1)\}$.

Proof. The proof is the same as the proof of Lemma 4. □

As seen from [12], case 2.5.6, pages 38–39, elliptic curves with torsion $\mathbb{Z}_{18}$ over $\mathbb{Q}(\sqrt{-3}\,)$ exist if and only if the curve C_2 defined by

$$y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1 \tag{3}$$

has points over $\mathbb{Q}(\sqrt{-3}\,)$ satisfying

$$x(x+1)\big(x^2+x+1\big)\big(x^3-3x-1\big) \neq 0. \tag{4}$$

Let J_2 be the Jacobian of C_2, $C_2^{(d)}$ the quadratic twist of C_2 by d and $J_2^{(d)}$ the Jacobian of $C_2^{(d)}$.

Lemma 7. $J_2(\mathbb{Q}(\sqrt{-3}\,)) \simeq \mathbb{Z}_3 \oplus Z_{21}$.

Proof. In MAGMA [2] we compute $rank(J_2(\mathbb{Q})) = 0$ and $rank(J_2^{(-3)}(\mathbb{Q})) = 0$, and thus

$$rank\big(J_2\big(\mathbb{Q}(\sqrt{-3}\,)\big)\big) = rank\big(J_2(\mathbb{Q})\big) + rank\big(J_2^{(-3)}(\mathbb{Q})\big) = 0.$$

The discriminant of C_2 is $2^{23} \cdot 3^4$, so 2 and 3 are the only rational primes with bad reduction. We find the divisors in Mumford representation $(x^2+x+1, -\sqrt{-3}x - \sqrt{-3}, 2)$ and $(1, -x^3 - x^2, 2)$ that generate a group isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_{21}$. As the rational primes 5 and 11 remain prime in $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, we have

$$\left|J_2(F_{25})\right| = \left|J_2\big(F_5(\sqrt{-3}\,)\big)\right| = 3^2 \cdot 7^2,$$
$$\left|J_2(F_{121})\right| = \left|J_2\big(F_{11}(\sqrt{-3}\,)\big)\right| = 2^4 \cdot 3^2 \cdot 7 \cdot 13.$$

We conclude that $J_2(\mathbb{Q}(\sqrt{-3}\,))_{tors} \simeq \mathbb{Z}_3 \oplus \mathbb{Z}_{21}$. □

Lemma 8. $C_2(\mathbb{Q}(\sqrt{-3})) = \{\infty_+, \infty_-, (-1, \pm 1), (0, \pm 1), (\frac{-1-\sqrt{-3}}{2}, \pm\frac{-3-\sqrt{-3}}{2}), (\frac{-1+\sqrt{-3}}{2}, \pm\frac{-3+\sqrt{-3}}{2})\}$.

Proof. Searching throught the 62 non-zero elements of $J_2(\mathbb{Q}(\sqrt{-3}))$, we see that all the points, besides the obvious rational ones, satisfy $x^2+x+1 = 0 = y - x + 1$, and hence we obtain our result. □

By Lemma 6 the torsion of an elliptic curve over $\mathbb{Q}(\sqrt{-3}\,)$ cannot be $\mathbb{Z}_{13}$ and by Lemma 8, the torsion cannot be $\mathbb{Z}_{18}$. Thus we have proved Theorem 2.

Remark. The fact that $J_1(\mathbb{Q})_{tors} \simeq \mathbb{Z}_{19}$ and $J_2(\mathbb{Q})_{tors} \simeq \mathbb{Z}_{21}$ was proven already 35 years ago by Ogg in [10], and the existence of rational 19-torsion points on $J_1(\mathbb{Q})$ was used by Mazur and Tate [7] to prove the non-existence of rational points on elliptic curves of order 13 over $\mathbb{Q}$.

Supplementary material

The online version of this article contains additional supplementary material. Please visit doi:10.1016/j.jnt.2009.12.008.

References

[1] W. Bosma, J. Cannon, Handbook of Magma Functions, http://www.msri.org/about/computing/docs/magma/Handbook.pdf.

[2] The MAGMA computer algebra system is described in W. Bosma, J. Cannon, Catherine Playoust, The Magma algebra system. I. The user language, J. Symbolic Comput. 24 (1997) 235–265.

[3] H. Cohen, G. Frey, Handbook of Elliptic and Hyperelliptic Curve Cryptography, Discrete Math. Appl., Chapman & Hall/CRC, 2006.

[4] D. Jeon, C.H. Kim, 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, F. Momose, Torsion points on elliptic curves defined over quadratic fields, Nagoya Math. J. 109 (1988) 125–149.

[7] B. Mazur, J. Tate, Points of order 13 on elliptic curves, Invent. Math. 22 (1973/1974) 41–49.

[8] D. Mumford, Tata lectures on theta II, Progr. Math., vol. 43, Birkhauser, Boston, MA, 1984.

[9] F. Najman, Torsion of elliptic curves over quadratic cyclotomic fields, Math. J. Okayama U., in press.

[10] A. Ogg, Rational points on certain elliptic modular curves, Analytic number theory, in: Proc. Sympos. Pure Math., vol. XXIV, St. Louis Univ., St. Louis, MO, 1972, Amer. Math. Soc., Providence, RI, 1973, pp. 221–231.

[11] B. Poonen, Computing torsion points on curves, Experiment. Math. 10 (2001) 449–466.

[12] F.P. Rabarison, Torsion et rang des courbes elliptiques definies sur les corps de nombres algebriques, Doctorat de Universite de Caen, 2008.

[13] M. Stoll, Implementing 2-descent on Jacobians of hyperelliptic curves of genus two, II, Acta Arith. 98 (2001) 245–277.