Indian J. Pure Appl. Math., **50**(1): 161-169, March 2019
 DOI: 10.1007/s13226-019-0314-y

TORSION OF ELLIPTIC CURVES OVER REAL QUADRATIC FIELDS OF SMALLEST DISCRIMINANT

Naba Kanta Sarma

Department of Mathematics, Assam University, Silchar, Cachar 788 011, *Assam, India*
e-mail: naba.sarma@iitg.ernet.in

(*Received* 30 *September* 2016; *after final revision* 19 *March* 2018;
accepted 22 *March* 2018)

In [9] and [10], Filip Najman examined the torsion of elliptic curves over the number fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$. In this paper, we study the torsion structures of elliptic curves over the real quadratic number fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$, which have the smallest discriminants among all real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \bmod 4$ and $d \equiv 1 \bmod 4$ respectively.

Key words : Elliptic curve; Torsion subgroup; cusp; discriminant.

1. INTRODUCTION

An elliptic curve (see [6]) over a field K is a smooth projective variety of genus 1 with a specified K-rational base point O. If the characteristic of K is not equal to 2 or 3, an elliptic curve can be represented by a Weierstrass equation of the form

$$y^2 = x^3 + Ax + B, \qquad A, B \in K.$$

Over a field of characteristic 2 and 3, one needs to work with a more general equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K.$$

Around 1900, Poincaré showed that the set

$$E(K) = \{(x, y) \in K : y^2 = x^3 + Ax + B, A, B \in K\} \cup \{O\}$$

of all K-rational points on E, together with the base point O, is an abelian group. He also conjectured that this group is finitely generated when K is the field $\mathbb{Q}$ of rational numbers. In 1922, Mordell proved this conjecture and in 1928, André Weil generalized this result not only for elliptic curves over algebraic number fields but also for abelian varieties.

In this paper, we are mainly interested in the torsion part of the group $E(K)$, which we denote by $E(K)_{\text{tors}}$. The most significant result regarding the torsion part of $E(\mathbb{Q})$ is the following theorem due to Mazur.

***Theorem* 1.1** — *(Mazur [7]). Let E be any elliptic curve over $\mathbb{Q}$. Then $E(\mathbb{Q})_{\text{tors}}$ must be one of the following 15 groups:*

$$\begin{aligned} &\mathbb{Z}_n && 1 \leq n \leq 12, \quad n \neq 11 \\ &\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} && 1 \leq n \leq 4 \end{aligned}$$

where $\mathbb{Z}_n$ denote the finite cyclic group of order n.

Several mathematicians worked on the possibilities for the torsion structure that can appear over quadratic extensions of $\mathbb{Q}$, culminating in the following theorem.

***Theorem* 1.2** — *(Kenku-Momose [8] and Kamienny [4]). Let E be an elliptic curve over a quadratic extension K of $\mathbb{Q}$. Then as K varies, $E(K)_{\text{tors}}$ is isomorphic to one of the following 26 groups:*

$$\begin{aligned} &\mathbb{Z}_n && 1 \leq n \leq 18, \quad n \neq 17 \\ &\mathbb{Z}_2 \oplus \mathbb{Z}_{2n} && 1 \leq n \leq 6 \\ &\mathbb{Z}_3 \oplus \mathbb{Z}_{3n} && 1 \leq n \leq 2 \\ &\mathbb{Z}_4 \oplus \mathbb{Z}_4 \end{aligned}$$

It was also shown that the groups $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ occur over the quadratic field $\mathbb{Q}(\sqrt{-3})$ only, while the group $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ occurs over the quadratic field $\mathbb{Q}(\sqrt{-1})$ only. In 2010, Najman [9, 10] took a different approach by fixing a quadratic extension K of $\mathbb{Q}$ and then looking for possible torsion structure over K. A precise list of torsion subgroups for the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ was obtained.

Given a number field K, $E(K)_{\text{tors}}$ is always of the form $\mathbb{Z}_m \oplus \mathbb{Z}_n$ for some $m, n \geq 1$ as it is a subgroup of $E(\mathbb{C})_{\text{tors}}$. Further, it is well-known that the isomorphism classes of elliptic curves with $\mathbb{Z}_m \oplus \mathbb{Z}_n$ as torsion are parametrized by the points on the modular curve $Y_1(m, n)$ (see [14] for details). In 2012, Kamienny and Najman [5] outlined an approach that can be used to find all possible torsion structures over a given quadratic field K. In order to find whether there exists an elliptic curve with torsion $\mathbb{Z}_m \oplus \mathbb{Z}_n$ over a quadratic field K, one needs to determine whether the modular curve

$X_1(m,n)$, which is the compactification of $Y_1(m,n)$ by adjoining cusps, has a K-rational point that is not a cusp. We use this approach to determine exactly the torsion structures over the real quadratic fields $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$. We recall that the discriminant of a quadratic field $\mathbb{Q}(\sqrt{d})$ is given by

$$\text{Disc}(\mathbb{Q}(\sqrt{d})) = \begin{cases} d & \text{if } d \equiv 1 \bmod 4 \\ 4d & \text{if } d \not\equiv 1 \bmod 4. \end{cases}$$

So the above two fields have the smallest discriminants among all real quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1 \bmod 4$ and $d \equiv 1 \bmod 4$ respectively.

2. Main Results

The main results of this paper is the following:

- The possibilities for the torsion part of an elliptic curve over the real quadratic field $\mathbb{Q}(\sqrt{2})$ are the torsion groups appearing in Mazur's theorem together with $\mathbb{Z}_{11}$.
- The possibilities for the torsion part of an elliptic curve over the real quadratic field $\mathbb{Q}(\sqrt{5})$ are the torsion groups appearing in Mazur's theorem together with $\mathbb{Z}_{15}$.

3. Key Steps

We have nice models for the curve $X_1(n)$ in [1, 12] while the curves $X_1(2,n)$ that we need can be found in [12]. It turns out that the defining equations for $X_1(13), X_1(16)$ and $X_1(18)$ are hyperelliptic curves, while the defining equations of $X_1(m,n)$ for the values of m,n that we need, are elliptic curves. We adopt the following steps in determining the torsion subgroup (see [5]).

- If $X_1(m,n)$ is an elliptic curve, then the usual method of computing the rank is to perform 2-descent. In MAGMA, we can compute the rank of any elliptic curve over $\mathbb{Q}$ only. However, the rank of the elliptic curve E over the quadratic field $\mathbb{Q}(\sqrt{d})$ can be computed from the relation:

  $$\text{rank } (E(\mathbb{Q}(\sqrt{d}))) = \text{ rank}(E(\mathbb{Q})) + \text{ rank } (E^d(\mathbb{Q}))$$

  where E^d denote the quadratic twist of E (see Ex 10.16, [6]). On the other hand, having computed the torsion subgroups of the elliptic curves E and E^d over the rationals, the torsion subgroup of E over $K = \mathbb{Q}(\sqrt{d})$ can be computed by the relation,

  $$E(K)[n] = E(\mathbb{Q})[n] \oplus E^d(\mathbb{Q})[n]$$

  when n is odd. (See [15]).

- If the rank over the relevant field K is positive, then there will be infinitely many elliptic curves with torsion $\mathbb{Z}_m \oplus \mathbb{Z}_n$ over K.
- If the rank is zero, then one has to check whether all the torsion points are cusps. If not, then there will be finitely many, explicitly computable, elliptic curves with the given torsion subgroup.
- If $X_1(m,n)$ is hyperelliptic curve, namely $X_1(13)$, $X_1(16)$, or $X_1(18)$, then by a celebrated theorem of Faltings, there are only finitely many K-rational points, implying that there are finitely many elliptic curves, up to isomorphism, with torsion $\mathbb{Z}_m \oplus \mathbb{Z}_n$ over K. In order to find all these points, one can sometimes proceed to compute the rank of the Jacobian using 2-descent on Jacobians. This can be done in MAGMA. However, 2-descent is not an algorithm, so there is no guarantee of obtaining the rank using it. It guarantees only an upper bound for the rank. Subsequently, they gave an alternative approach using the method of Mazur that gives a criterion when the Jacobian of $X_1(13)$ and $X_1(18)$ has rank 0.
- If the rank of the Jacobian is zero, one has to find the torsion of the Jacobian and check whether any of the torsion points arise from a K-rational point that is not a cusp.
- If the rank is positive, the problem becomes complicated and one can try to apply the Chabauty method (if the rank is one) or other similar methods.
- The only other hyperelliptic curve, $X_1(16)$, is usually easier to deal with, since $f(x)$, where $y^2 = f(x)$ is a model of $X_1(16)$, is not irreducible. This allows one to find all the points with more elementary methods, like covering the hyperelliptic curve with 2 elliptic curves.
- Having found a K-rational point on $Y_1(m,n)$, one can construct (Rabarison [12]) an elliptic curve with torsion $\mathbb{Z}_m \oplus \mathbb{Z}_n$ over K.

Note that the torsion groups appearing in Mazur's theorem will appear over any number field. So we are left to examine the additional 11 torsion structures in the theorem 1.2, namely $\mathbb{Z}_{11}$, $\mathbb{Z}_{13}$, $\mathbb{Z}_{14}$, $\mathbb{Z}_{15}$, $\mathbb{Z}_{16}$, $\mathbb{Z}_{18}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$, $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$. Since $\mathbb{Z}_3 \oplus \mathbb{Z}_3$ and $\mathbb{Z}_3 \oplus \mathbb{Z}_6$ occur only over $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ occurs only over $\mathbb{Q}(\sqrt{-1})$, our study can exclude these as well. We use MAGMA for our computations (see [2, 3 and 13]).

4. The Torsion $\mathbb{Z}_{11}$

From now on, we denote the elliptic curve over K defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in K$$

by $[a_1, a_2, a_3, a_4, a_6]$.

By [12], elliptic curves with torsion $\mathbb{Z}_{11}$ over a quadratic field K are induced by solutions over K of the equation,

$$X_1(11) : y^2 - y = x^3 - x^2$$

where the cusps are those points whose x-cordinates satisfy the equation

$$x(x-1)(x^5 - 18x^4 + 35x^3 - 16x^2 - 2x + 1) = 0.$$

We see that $X_1(11)$ is an elliptic curve given by $[0, -1, -1, 0, 0]$.

- First, consider $K = \mathbb{Q}(\sqrt{2})$. In this case, we compute in MAGMA that rank of $X_1(11)(\mathbb{Q}(\sqrt{2}))$ is 1. Therefore, $\mathbb{Z}_{11}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}(\sqrt{2})$. Using the non-torsion point $(\frac{1}{2}, \frac{1}{4}(2+\sqrt{2})$, we obtain explicitly the curve

  $$y^2 + \frac{1}{8}(3-\sqrt{2})xy + \frac{1}{128}\sqrt{2}y = x^3 + \frac{1}{64}\sqrt{2}x^2$$

  where $(0,0)$ is a point of order 11.

- Now consider $K = \mathbb{Q}(\sqrt{5})$. In this case the rank of $X_1(11)(\mathbb{Q}(\sqrt{5}))$ is 0 and the torsion group is $\mathbb{Z}_5$. Following [5], we note that

  $$X_1(11)(\mathbb{Q}(\sqrt{5})) = \{O, (0,0), (0,1), (1,0), (1,1)\}$$

  We see that all the torsion points corresponds to $x = 0$ or $x = 1$, and hence they are cusps. Therefore, $\mathbb{Z}_{11}$ cannot occur as a torsion over the quadratic field $\mathbb{Q}(\sqrt{5})$.

5. The Torsion $\mathbb{Z}_{13}$

Elliptic curves with torsion $\mathbb{Z}_{13}$ over a quadratic field K are induced by solutions over K of the equation [12],

$$X_1(13) : y^2 = x^6 - 2x^5 + x^4 - 2x^3 + 6x^2 - 4x + 1$$

where the cusps satisfy

$$x(x-1)(x^3 - 4x^2 + x + 1) = 0.$$

We see that $X_1(13)$ is a hyperelliptic curve. As the points of a hyperelliptic curve have no group structure, it is more convenient to study its Jacobian variety. This case follows from [5], but for the sake of completeness we reproduce the main points here.

Let J_1 be the Jacobian of the curve C_1, $C_1^{(d)}$ the quadratic twist of C_1 by d and $J_1^{(d)}$ the Jacobian of $C_1^{(d)}$. In MAGMA [2] there is an implementation of 2-descent on Jacobians (the Rank Bounds function, see [13] for the algorithm), but unfortunately only over $\mathbb{Q}$. We find via 2-descent, that rank $(J_1(13)(\mathbb{Q}(\sqrt{d}))) = 0$ for $d = 2, 5$. Further, we compute that $(J_1(13)(\mathbb{Q}(\sqrt{d})))_{\text{tors}}$ is isomorphic to $\mathbb{Z}_{21}$ for these two values of d. All these points on $\mathbb{Z}_{21}$ are generated by the cusps of $X_1(13)$. Hence $\mathbb{Z}_{13}$ cannot occur as a torsion over these quadratic fields.

6. The Torsion $\mathbb{Z}_{14}$

Elliptic curves with torsion $\mathbb{Z}_{14}$ over a quadratic field K are induced by solutions over K of the equation (see [12]),

$$X_1(14) : y^2 + xy + y = x^3 - x$$

where the cusps satisfy

$$x(x-1)(x+1)(x^3 - 9x^2 - x + 1)(x^3 - 2x^2 - x + 1) = 0.$$

We see that $X_1(14)$ is an elliptic curve given by $[1, 0, 1, -1, 0]$.

- The rank of $X_1(14)(K)$ is 0 for $K = \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$. Also, $(X_1(14)(K))_{\text{tors}} \cong \mathbb{Z}_6$ in both the cases. Since the points in $\mathbb{Z}_6$ corresponds to $x = 0, 1$ or -1, all the torsion points are cusps. As a result, $\mathbb{Z}_{14}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$.

7. The torsion $\mathbb{Z}_{15}$

Elliptic curves with torsion $\mathbb{Z}_{15}$ over a quadratic field K are induced by solutions over K of the equation (see [12]),

$$X_1(15) : y^2 + xy + y = x^3 + x^2$$

where the cusps satisfy

$$x(x+1)(x^4 + 3x^3 + 4x^2 + 2x + 1)(x^4 - 7x^3 - 6x^2 + 2x + 1) = 0.$$

We see that $X_1(15)$ is an elliptic curve given by $[1, 1, 1, 0, 0]$.

- The rank of $X_1(15)$ over $\mathbb{Q}(\sqrt{2})$ is 0 and the torsion subgroup is $\mathbb{Z}_4$. All the torsion point correspond to cusps, and hence $\mathbb{Z}_{15}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$.

- The rank of $X_1(15)$ over $\mathbb{Q}(\sqrt{5})$ is 0 and the torsion subgroup is $\mathbb{Z}_8$. From a non-cuspidal point on it, one can obtain an elliptic curve (see [5])

$$y^2 = x^3 + (281880\sqrt{5} - 630315)xy + 328392630 - 146861640\sqrt{5},$$

with a point $(264\sqrt{5} - 585, 5076\sqrt{5} - 11340)$ of order 15.

8. The Torsion $\mathbb{Z}_{16}$

Elliptic curves with torsion $\mathbb{Z}_{16}$ over a quadratic field K are induced by solutions over K of the equation (see [12]),

$$X_1(16) : y^2 = x(x^2 + 1)(x^2 + 2x - 1)$$

where the cusps satisfy

$$x(x - 1)(x + 1)(x^2 - 2x - 1)(x^2 + 2x - 1) = 0.$$

We see that $X_1(16)$ is a hyperelliptic curve. Proceeding as in the case of $X_1(13)$, one can compute that for $d = 2, 5$

$$\begin{aligned}
&\text{rank } (J_1(16)(\mathbb{Q}(\sqrt{d}))) = 0,\\
&(J_1(16)(\mathbb{Q}(\sqrt{2})))_{\text{tors}} = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{10},\\
&(J_1(16)(\mathbb{Q}(\sqrt{5})))_{\text{tors}} = \mathbb{Z}_2 \oplus \mathbb{Z}_{10}.
\end{aligned}$$

Since all these torsion points are induced by the cusps of $X_1(16)$, so $\mathbb{Z}_{16}$ cannot appear as torsion over these two fields.

9. The Torsion $\mathbb{Z}_{18}$

Elliptic curves with torsion $\mathbb{Z}_{18}$ over a quadratic field K are induced by solutions over K of the equation (see [12]),

$$X_1(18) : y^2 = x^6 + 2x^5 + 5x^4 + 10x^3 + 10x^2 + 4x + 1$$

where the cusps satisfy

$$x(x + 1)(x^2 + x + 1)(x^2 - 3x - 1) = 0.$$

We see that $X_1(18)$ is a hyperelliptic curve. Since the prime 3 remains prime in $\mathbb{Q}(\sqrt{2})$, so by proposition $2.4(i)$ in [8], we see that $\mathbb{Z}_{18}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$. On the other hand, as 5 ramifies in $\mathbb{Q}(\sqrt{5})$, so by proposition $2.4(iii)$ in [8], we see that $\mathbb{Z}_{18}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{5})$.

10. The Torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$

Elliptic curves with torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$ over a quadratic field K are induced by solutions over K of the equation [12],

$$X_1(2,10) : y^2 = x^3 + x^2 - x$$

where the cusps satisfy

$$x(x^2-1)(x^2-4x-1)(x^2+x-1) = 0.$$

We see that $X_1(2,10)$ is an elliptic curve given by $[0,1,0,-1,0]$.

- The rank of $X_1(2,10)$ over $\mathbb{Q}(\sqrt{2})$ is 0 and the torsion subgroup is $\mathbb{Z}_6$. We easily verify that all the torsion points correspond to cusps and hence $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{2})$.
- The rank of the curve over the quadratic fields $\mathbb{Q}(\sqrt{5})$ is 0 and the torsion subgroup is $\mathbb{Z}_2 \oplus \mathbb{Z}_6$. All the torsion points correspond to cusps and hence $\mathbb{Z}_2 \oplus \mathbb{Z}_{10}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{5})$.

11. The Torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$

Elliptic curves with torsion $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$ over a quadratic field K are induced by solutions over K of the equation,

$$X_1(2,12) : y^2 = x^3 - x^2 + x$$

where the cusps satisfy

$$x(x-1)(2x-1)(2x^2-x+1)(3x^2-3x-1)(6x^2-6x-1) = 0.$$

We see that $X_1(2,12)$ is an elliptic curve given by $[0,-1,0,1,0]$.

The rank of $X_1(2,12)$ over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{5})$ are 0 and the torsion subgroup is $\mathbb{Z}_4$. All the torsion points correspond to cusps, and hence $\mathbb{Z}_2 \oplus \mathbb{Z}_{12}$ can not appear as torsion over these quadratic fields.

Acknowledgement

I am extremely grateful to my mentor Prof. Anupam Saikia and Prof. Filip Najman for their guidance and motivating e-mail responses during the preparation of this manuscript. I would like to thank the anonymous referee for his/her valuable comments.

REFERENCES

1. H. Baziz, Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points, *Math. Computation*, **79**(272) (2010), 2371-2386.
2. W. Bosma and J. Cannon, Handbook of Magma functions, available online at *archive.msri.org/about/computing/docs/magma*.
3. W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system I: The user language, *J. Symbolic Comput.*, **24** (1997), 235-265.
4. S. Kamienny, Torsion points on elliptic curves and q-coefficients of modular forms, *Invent. Math.*, **109**(2) (1992), 221-229.
5. S. Kamienny and F. Najman, Torsion groups of elliptic curves over Quadratic fields, *Acta Arithmetica*, **152** (2012), 291-305.
6. J. Silverman, Arithmetic of elliptic curves, second edition, GTM-106, Springer, (2008).
7. B. Mazur, Modular curves and Eisenstein ideal, Publications Mathématiques de *I'I.H.É.S.*, Tome **47** (1977), 33-186.
8. M. A. Kenku and F. Momose, Torsion points on elliptic curves defined over quadratic fields, *Nagoya Math. J.*, **109** (1988), 125-149.
9. F. Najmam, Torsion of elliptic curves over quadratic cyclotomic field, *Math. Journal of Okayama University*, **53** (2011), 75-82.
10. F. Najman, Complete classification of torsion of elliptic curves over quadratic cyclotomic field, *Journal of Number Theory*, **130** (2010), 1964-1968.
11. E-mail correspondence with Dr. Filip Najman.
12. F. Rabarison, Structure de torsion des courbes elliptiques definies sur les corps de nombres quadratiques, *Acta Arithmetica*, **144**(1) (2010), 17-52.
13. M. Stoll, Implementing 2-descent on Jacobians of hyperelliptic curves of genus two II, *Acta Arithmatica*, **98** (2001), 245-277.
14. F. Diamond and J Shurman, *A first course in modular forms*, GTM-228, Springer, USA (2005).
15. M. Chou, Torsion of rational elliptic curves over quartic Gaolis number fields, *Journal of Number Theory*, **160** (2016), 603-628.