ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 48, Number 8, 2018

TORSION OF ELLIPTIC CURVES OVER IMAGINARY QUADRATIC FIELDS OF CLASS NUMBER 1

NABA KANTA SARMA AND ANUPAM SAIKIA

ABSTRACT. Filip Najman examined the possibilities for the group of torsion points on elliptic curves over the number fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$ in [**10, 11**]. In this article, we study the possible torsion structures of elliptic curves over the remaining imaginary quadratic fields of class numbers 1, i.e., over the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$.

1. Introduction. Around 1908, Henri Poincaré showed that the set $E(K)$ of K-rational points on a given elliptic curve E over a given field K, together with a specified base point O, can be given the structure of an abelian group in the projective setting using a chord-tangent law. He further conjectured that the group $E(\mathbb{Q})$ is finitely generated, and it was proven in the affirmative in 1922 by Louis Mordell. Later, André Weil generalized this result for abelian varieties over algebraic number fields. Barry Mazur [**9**] proved the following deep theorem which lists all of the possibilities for the torsion subgroup of $E(\mathbb{Q})$.

Theorem 1.1. *Let E be any elliptic curve over $\mathbb{Q}$. Then, $E(\mathbb{Q})_{\mathrm{tors}}$ must be one of the following* 15 *groups*:

$$\begin{aligned} &\mathbb{Z}/N\mathbb{Z}, \quad 1 \leq N \leq 12,\ N \neq 11,\\ &\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, \quad 1 \leq N \leq 4. \end{aligned}$$

Subsequently, several mathematicians worked on the possible torsion groups that can appear over quadratic extensions of $\mathbb{Q}$, culminating in the following theorem.

2010 AMS *Mathematics subject classification.* Primary 11G05, Secondary 11G18.

Keywords and phrases. Elliptic curve, torsion subgroup, cusp.

Received by the editors on February 1, 2018, and in revised form on May 21, 2018.

DOI:10.1216/RMJ-2018-48-8-2689

Theorem 1.2 ([**6, 8**]). *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*:

$$\begin{aligned}
&\mathbb{Z}/N\mathbb{Z}, && 1 \le N \le 18,\ N \ne 17,\\
&\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2N\mathbb{Z}, && 1 \le N \le 6,\\
&\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3N\mathbb{Z}, && 1 \le N \le 2,\\
&\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.
\end{aligned}$$

In 2010, Najman [**10, 11**] took a different approach by fixing a quadratic extension K of $\mathbb{Q}$ and then looking for possible torsion structures over K. He found all of the possible torsion subgroups for the quadratic fields $\mathbb{Q}(\sqrt{-1})$ and $\mathbb{Q}(\sqrt{-3})$.

Theorem 1.3 ([**11**]). *Let E be an elliptic curve defined over $\mathbb{Q}(\sqrt{-1})$. Then, $E(\mathbb{Q}(\sqrt{-1}))_{\text{tors}}$ is either one of the groups from Mazur's theorem or $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.*

Theorem 1.4 ([**11**]). *Let E be an elliptic curve defined over $\mathbb{Q}(\sqrt{-3})$. Then, $E(\mathbb{Q}(\sqrt{-3}))_{\text{tors}}$ is either one of the groups from Mazur's theorem or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$.*

In 2012, Kamienny and Najman [**7**] outlined an approach that can be used to study the possible torsion structure over a quadratic field. In this paper, we follow that approach to determine the possible torsion structures over the remaining imaginary quadratic fields of class number 1, namely, over the fields $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$.

2. Statement of the main result.

When we consider the possibilities for the torsion subgroup of an elliptic curve over an imaginary quadratic field of class number 1, we may not realize all the groups listed in Theorem 1.2. This paper determines those exceptional groups which cannot be realized as a torsion group of elliptic curves over imaginary quadratic fields of class number 1. The main result of this paper can be summarized in the following theorem:

Theorem 2.1. *Let E be an elliptic curve over an imaginary quadratic number field K of class number* 1*. Then, as K varies, $E(K)_{\mathrm{tors}}$ is isomorphic to one of the groups appearing in Theorem* 1.2*, excluding the groups $\mathbb{Z}/13\mathbb{Z}$, $\mathbb{Z}/16\mathbb{Z}$ and $\mathbb{Z}/18\mathbb{Z}$.*

3. Background.

3.1. Elliptic curve and its quadratic twist. An elliptic curve is a smooth projective variety of genus 1 with a specified base point O. An elliptic curve over K can be represented by a Weierstrass equation of the form:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_i \in K. \tag{3.1}$$

If $\mathrm{char}(K) \neq 2, 3$, we can use the substitution

$$x \longrightarrow \frac{1}{36}(x - 3a_1^2 - 12a_2), \qquad y \longrightarrow \frac{1}{216}(y - a_1x - a_3) \tag{3.2}$$

to reduce the equation to the short Weierstrass form

$$y^2 = x^3 + Ax + B,$$

where A and B are given by

$$\begin{aligned} A &= -27a_1^4 - 216a_1^2a_2 - 432a_2^2 + 648a_1a_3 + 1296a_4, \\ B &= 54a_1^6 + 648a_1^4a_2 + 2592a_1^2a_2^2 - 1944a_1^3a_3 + 3456a_2^3 - 3888a_1^2a_4 \\ &\quad - 7776a_1a_2a_3 + 11664a_3^2 - 15552a_2a_4 + 46656a_6. \end{aligned}$$

The d-quadratic twist of an elliptic curve in short Weierstrass form is defined by the equation

$$E^{(d)} : y^2 = x^3 + d^2Ax + d^3B.$$

3.2. Division polynomials. Let E be an elliptic curve over a field K defined by the short Weierstrass equation

$$E : y^2 = x^3 + Ax + B.$$

We define the division polynomials **[15]** $\psi_n \in \mathbb{Z}[x, y, A, B]$ by

$$\begin{aligned} &\psi_0 = 0, \qquad \psi_1 = 1, \qquad \psi_2 = 2y, \\ &\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2, \end{aligned}$$

$$\begin{aligned}\psi_4 &= 4y(x^6+5Ax^4+20Bx^3-5A^2x^2-4ABx-8B^2-A^3),\\ \psi_{2n+1} &= \psi_{n+2}\psi_n^3-\psi_{n-1}\psi_{n+1}^3 \quad \text{for } n\geq 2,\\ \psi_{2n} &= (2y)^{-1}\psi_n[\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2] \quad \text{for } n\geq 3.\end{aligned}$$

We also define the polynomials

$$\begin{aligned}\phi_n &= x\psi_n^2-\psi_{n+1}\psi_{n-1},\\ \omega_n &= (4y)^{-1}(\psi_{n+2}\psi_{n-1}^2-\psi_{n-2}\psi_{n+1}^2).\end{aligned}$$

Division polynomials are related to torsion points by the following theorem.

Theorem 3.1. *Consider the elliptic curve*

$$y^2 = x^3+Ax+B,$$

defined over a number field K. Let $P=(x,y)$ be a point on the curve, and let n be a positive integer. Then,

$$nP = \left(\frac{\phi_n(x)}{\psi_n^2(x)}, \frac{\omega_n(x,y)}{\psi_n^3(x,y)}\right).$$

3.3. The modular curves $X_1(N)$ and $X_1(M,N)$. For positive integers M and N with $M \mid N$, consider the congruence subgroup $\Gamma_1(M,N)$ of $\mathrm{SL}(2,\mathbb{Z})$ defined by

$$\Gamma_1(M,N) := \left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix} : \begin{pmatrix} a & b\\ c & d\end{pmatrix} \equiv \begin{pmatrix} 1 & *\\ 0 & 1\end{pmatrix} \mathrm{mod}(N),\ M \mid b.\right\}$$

When $M=1$, we denote the subgroup $\Gamma_1(1,N)$ simply by $\Gamma_1(N)$. Such a subgroup acts on the upper half plane $\mathbb{H}$ by fractional linear transformations, as follows:

$$\gamma(\tau) := \frac{a\tau+b}{c\tau+d}, \quad \tau\in\mathbb{H}, \qquad \gamma = \begin{pmatrix} a & b\\ c & d\end{pmatrix} \in \Gamma_1(M,N).$$

The set of orbits of this action by $\Gamma_1(M,N)$ (respectively $\Gamma_1(N)$) is denoted by $Y_1(M,N)$ (respectively $Y_1(N)$) and can be given the structure of a non-compact Riemann surface. We can compactify it by adjoining cusps with appropriate local coordinate charts to obtain a compact Riemann surface, which we denote by $X_1(M,N)$ (respectively $X_1(N)$).

The modular curve $Y_1(N)$ parameterizes isomorphism classes of complex elliptic curves E with a point of order N. Since a modular curve has the structure of a compact Riemann surface, it can be interpreted as a non-singular irreducible projective algebraic curve $\mathcal{C}$. Equivalently, the field of rational functions on $\mathcal{C}$ is isomorphic to the field of meromorphic functions on the modular curve. Hence, the homogeneous polynomials defining $\mathcal{C}$ are often referred to as defining equations of the corresponding modular curve. It turns out that the modular curve $X_1(M,N)$ is defined over $\mathbb{Q}(\zeta_M)$, where ζ_M is the Mth primitive root of unity. The details can be found in [**5**].

3.4. Defining equations for modular curves. Nice models for the modular curves $X_1(N)$ and $X_1(2,N)$ that we require can be found in [**1, 13**]. For example, the defining equation for the modular curve $X_1(11)$ is given by

$$X_1(11) : y^2 - y \ = \ x^3 - x, \tag{3.3}$$

where the cusps are given by

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

Except for the cusps, each solution of (3.3) corresponds to a point on $Y_1(11)$, and hence to an isomorphism class of elliptic curves with a torsion point of order 11. Note that equation (3.3) represents an elliptic curve. Similarly, the defining equations for the modular curves $X_1(14)$, $X_1(15)$, $X_1(2,10)$ and $X_1(2,12)$ indicate that they are all elliptic curves, while the defining equations for the modular curves $X_1(13)$, $X_1(16)$ and $X_1(18)$ indicate that these are hyperelliptic curves.

4. Key steps. We adopt the following steps in determining the torsion subgroup over a quadratic field $K = \mathbb{Q}(\sqrt{d})$ [**7**].

- If $X_1(M,N)$ is an elliptic curve E, then we compute its rank over K. In MAGMA, one can compute the rank of any elliptic curve $\mathbb{Q}$, but not over K. However, the rank of a rational elliptic curve E over a quadratic field $K = \mathbb{Q}(\sqrt{d})$ can be computed using the relation

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

where $E^{(d)}$ denote the quadratic twist of E [**14,** Example 10.16].

(a) If the rank over K is positive, then there will be infinitely many distinct points on $Y_1(M, N)$, and hence, there will be infinitely many non-isomorphic elliptic curves with torsion $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ over K.

(b) If the rank of E over K is zero, we proceed to compute the torsion subgroup of $E(K)$. As in the case of computation of rank, in MAGMA, we can compute the torsion subgroup over Q only. Having computed the torsion subgroups of the elliptic curves E and its d-quadratic twist $E^{(d)}$ over $\mathbb{Q}$, the torsion subgroup of E over $K = \mathbb{Q}(\sqrt{d})$ can be computed using the relation

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

when n is odd [**4**]. To compute the even torsion over K, we use the division polynomials introduced in subsection 3.2.

Having found the torsion subgroup over K, one must check whether all of the torsion points are cusps. If not, then there will be finitely many explicitly computable elliptic curves with torsion subgroup $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. On the other hand, if all of the torsion points are cusps, then $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ cannot appear as a torsion group for any elliptic curve over K.

• If $X_1(M, N)$ is a hyperelliptic curve, namely, $X_1(13)$, $X_1(16)$ or $X_1(18)$, then there are only finitely many K-rational points, by a renowned result of Faltings. In order to find all of these points, we study the Jacobian of $X_1(M, N)$. Note that the set of K-rational points on a hyperelliptic curve does not have any natural group structure like those on an elliptic curve. In MAGMA, we can compute the rank of the Jacobian over $\mathbb{Q}$ using 2-descent on Jacobians by using the relation [**11,** Lemma 3]

$$\operatorname{rank}(J(\mathbb{Q}(\sqrt{d}))) = \operatorname{rank}(J(\mathbb{Q})) + \operatorname{rank}(J^{(d)}(\mathbb{Q})),$$

where $J^{(d)}$ denotes the quadratic twist of J by d.

(a) If the rank of the Jacobian is zero, we 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 no such point is found, then $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ cannot appear as a torsion group for any elliptic curve over K.

(b) If the rank is positive, we can apply Chabauty's method (if the rank is one) or other similar methods. However, this case does not arise in our subsequent discussion.

- Having found a K-rational point on $Y_1(M,N)$, we can construct [**13**] elliptic curves with torsion $\mathbb{Z}/M\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$ over K.

5. Known results over imaginary quadratic fields so far. We first state certain known results that we use in the sequel.

- The groups $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ can occur as torsion of elliptic curves over the quadratic field $\mathbb{Q}(\sqrt{-3})$ only [**8**].

- The group $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ can occur as torsion of elliptic curves over the quadratic field $\mathbb{Q}(\sqrt{-1})$ only [**8**].

- Let E be an elliptic curve over an imaginary quadratic field K. Then, $E(K)_{\text{tors}}$ cannot be $\mathbb{Z}/13\mathbb{Z}$ or $\mathbb{Z}/18\mathbb{Z}$ [**3**].

Note that the torsion groups appearing in Mazur's theorem will appear over any number field. Thus, we are left to examine the additional 11 torsion structures mentioned in Theorem 1.2:

$$\mathbb{Z}/11\mathbb{Z},\ \mathbb{Z}/13\mathbb{Z},\ \mathbb{Z}/14\mathbb{Z},\ \mathbb{Z}/15\mathbb{Z},\ \mathbb{Z}/16\mathbb{Z},\ \mathbb{Z}/18\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z},\ \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \text{ and } \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}.$$

Using the above results, our study is further reduced to the torsion groups:

$$\mathbb{Z}/11\mathbb{Z},\ \mathbb{Z}/14\mathbb{Z},\ \mathbb{Z}/15\mathbb{Z},\ \mathbb{Z}/16\mathbb{Z},\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z} \text{ and } \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}.$$

For our computations, we used the version of MAGMA freely available at `www.magma.maths.usyd.edu/calc`.

6. Proof of the main result. We prove the main theorem in a series of lemmas.

Lemma 6.1. *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathbb{Z}/11\mathbb{Z}$ *appears as torsion of elliptic curves are* $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-19})$ *and* $\mathbb{Q}(\sqrt{-43})$.

Proof. By **[13]**, elliptic curves with torsion $\mathbb{Z}/11\mathbb{Z}$ 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-coordinates 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. By (3.2), the equation for $X_1(11)$ can be reduced to the short Weierstrass form

$$y^2 = x^3 - 432x + 8208.$$

- Consider first the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2})$. In this case, we compute that the rank of $X_1(11)(\mathbb{Q})$ is 0, while the rank of the quadratic twist $X_1(11)^{(-2)}(\mathbb{Q})$ is 1. Therefore,

$$\operatorname{rank}(X_1(11)(\mathbb{Q}(\sqrt{-2})) = 0 + 1 = 1.$$

Hence, $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over $\mathbb{Q}(\sqrt{-2})$. Using the non-torsion point $(2 + \sqrt{-2}, -1 - 2\sqrt{-2})$, we obtain the curve

$$y^2 + (15 - 8\sqrt{-2})xy + 4(33 + 39\sqrt{-2})y = x^3 + 54(2 + \sqrt{-2})x^2,$$

which has $(0, 0)$ as a point of order 11. In a similar way, we find that the rank of $X_1(11)$ over each of the fields $\mathbb{Q}(\sqrt{-7}), \mathbb{Q}(\sqrt{-19})$ and $\mathbb{Q}(\sqrt{-43})$ is 1, and hence, $\mathbb{Z}/11\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these imaginary quadratic fields of class number 1.

- Next, consider the field $K = \mathbb{Q}(\sqrt{-11})$. In this case, the rank of $X_1(11)(\mathbb{Q})$ and $X_1(11)^{(-11)}(\mathbb{Q})$ are both 0. Therefore,

$$\operatorname{rank}(X_1(11)(\mathbb{Q}(\sqrt{-11})) = 0 + 0 = 0.$$

We then compute

$$(X_1(11)(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/5\mathbb{Z}, \qquad (X_1(11)^{(-11)}(\mathbb{Q}))_{\text{tors}} \cong \{O\}.$$

The n-torsion of $X_1(11)(\mathbb{Q}(\sqrt{-11}))$ for odd n is determined by the above computation. To compute the 2-torsion, we note that points of order 2 correspond to $y = 0$ in the short Weierstrass equation $y^2 = f(x)$. In this case, as noted above, $f(x) = x^3 - 432x + 8208$.

We find that $f(x)$ is irreducible over $\mathbb{Q}$, and hence over all quadratic extensions of $\mathbb{Q}$. This ensures that $X_1(11)$ does not have 2-torsion over $K = \mathbb{Q}(\sqrt{-11})$. As a result,

$$X_1(11)(\mathbb{Q}(\sqrt{-11})) \cong \mathbb{Z}/5\mathbb{Z} \cong \{O, (0,0), (0,1), (1,0), (1,1)\}.$$

We see that all of these torsion points correspond to $x = 0$ or 1, and hence, are cusps of $X_1(11)$. Therefore, $\mathbb{Z}/11\mathbb{Z}$ cannot occur as torsion over the quadratic field $\mathbb{Q}(\sqrt{-11})$. Exactly the same arguments show that $\mathbb{Z}/11\mathbb{Z}$ cannot occur as torsion over the quadratic fields $\mathbb{Q}(\sqrt{-67})$ and $\mathbb{Q}(\sqrt{-163})$. □

Lemma 6.2. *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathbb{Z}/14\mathbb{Z}$ *appears as a torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$.

Proof. By **[13]**, elliptic curves with torsion $\mathbb{Z}/14\mathbb{Z}$ over a quadratic field K are induced by solutions over K of the equation

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

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, which can be reduced to the short Weierstrass form

$$y^2 = x^3 - 675x + 13662.$$

- Consider first the imaginary quadratic field $K = \mathbb{Q}(\sqrt{d})$, where $d = -11$, -43, -67 or -163. In each of these cases, we compute that the rank of $X_1(14)\,(\mathbb{Q})$ is 0, while the rank of $X_1(14)^{(d)}(\mathbb{Q})$ is 1. Therefore,

$$\operatorname{rank}(X_1(14)(\mathbb{Q}(\sqrt{d})) = 0 + 1 = 1.$$

Hence, $\mathbb{Z}/14\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$ for $d = -11$, -43, -67 or -163.

- We compute that the rank of $X_1(14)\,(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -2$, -7 or -19. Also, we compute that, in each of these cases,

$$(X_1(14)(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}, \qquad (X_1(11)^{(d)}(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}.$$

We next note that complete 2-torsion is contained in $X_1(14)$ $(\mathbb{Q}(\sqrt{d}))$ if and only if the 2-division polynomial splits over it. From the short Weierstrass form above, we note that $x^3-675x+13662$ splits only over $\mathbb{Q}(\sqrt{-7})$. This shows that

$$\begin{aligned}(X_1(14)(\mathbb{Q}(\sqrt{-7})))_{\text{tors}} &\cong \mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/6\mathbb{Z},\\ (X_1(14)(\mathbb{Q}(\sqrt{d})))_{\text{tors}} &\cong \mathbb{Z}/6\mathbb{Z} \quad \text{for } d=-2,\ -19.\end{aligned}$$

All of the points in $\mathbb{Z}/6\mathbb{Z}$ correspond to $x=0$ or 1, and hence, are cusps. As seen in [**7**], non-cuspidal torsion points in $X_1(14)$ $(\mathbb{Q}(\sqrt{-7})$ induce the curve

$$y^2+\frac{63+\sqrt{-7}}{56}xy+\frac{11+\sqrt{-7}}{112}y=x^3+\frac{11+\sqrt{-7}}{112}x^2,$$

where $(0,0)$ is a point of order 14. Thus, $\mathbb{Z}/14\mathbb{Z}$ appears as torsion over $\mathbb{Q}(\sqrt{-7})$ for finitely many elliptic curves defined over the field. Moreover, $\mathbb{Z}/14\mathbb{Z}$ does not appear as a torsion over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-19})$. □

Lemma 6.3. *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathbb{Z}/15\mathbb{Z}$ *appears as a torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-7})$, $\mathbb{Q}(\sqrt{-11})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$

Proof. By [**13**], elliptic curves with torsion $\mathbb{Z}/15\mathbb{Z}$ over a quadratic field K are induced by solutions over K of the equation

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

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, which can be reduced to the short Weierstrass form

$$y^2=x^3-27x+8694.$$

- Consider first the imaginary quadratic field $K=\mathbb{Q}(\sqrt{d})$, where $d=-7$, -11, -43, -67 or -163. In each of these cases, we compute that the rank of $X_1(15)(\mathbb{Q})$ is 0, while the rank of $X_1(15)^{(d)}(\mathbb{Q})$ is 1. Therefore,

$$\operatorname{rank}(X_1(15)(\mathbb{Q}(\sqrt{d}))=0+1=1.$$

Hence, $\mathbb{Z}/15\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$, where $d = -7$, -11, -43, -67 or -163.

- We compute that the rank of $X_1(15)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -2$ and -19. Also, we compute that, in each of these cases,

$$(X_1(15)(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}, \qquad (X_1(11)^{(d)}(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}.$$

From the short Weierstrass form above, we note that $x^3 - 27x + 8694$ splits only over $\mathbb{Q}(\sqrt{-15})$. Hence, in each case, we obtain

$$(X_1(15)(\mathbb{Q}(\sqrt{d})))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}.$$

Clearly, all of these points in $\mathbb{Z}/4\mathbb{Z}$ corresponds to $x = 0$ or 1, and hence are cusps. Hence, $\mathbb{Z}/15\mathbb{Z}$ cannot appear as torsion over $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-19})$. □

Lemma 6.4. *The only imaginary quadratic field of class number* 1 *over which the group* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ *appears as a torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-2})$, $\mathbb{Q}(\sqrt{-11})$ *and* $\mathbb{Q}(\sqrt{-19})$.

Proof. By **[13]**, elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ over a quadratic field K are induced by solutions over K of the equation

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

where the cusps satisfy

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

We see that $X_1(2, 10)$ is an elliptic curve.

- We compute that the rank of $X_1(2, 10)(\mathbb{Q})$ is 0, while the rank of $X_1(15)^{(d)}(\mathbb{Q})$ is 1 for $d = -2$, -11 and -19. Thus, for these values of d, the rank of $X_1(2, 10)(\mathbb{Q}(\sqrt{d})$ is 1, and hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$.

- We compute that the rank of $X_1(2, 10)(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -7$, -43, -67 and -163. Also, we compute that, in each of these cases,

$$(X_1(2, 10)(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}, \qquad (X_1(2, 10)^{(d)}(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}.$$

We observe that the polynomial $x^3 + x^2 - x$ splits only over $\mathbb{Q}(\sqrt{5})$. Hence, in each case, we obtain

$$(X_1(2,10)(\mathbb{Q}(\sqrt{d})))_{\text{tors}} \cong \mathbb{Z}/6\mathbb{Z}.$$

We find that these points in $\mathbb{Z}/6\mathbb{Z}$ correspond to $x = 0, -1$ or 1, and hence are cusps. Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot appear as torsion over any of these fields. □

Lemma 6.5. *The only imaginary quadratic fields of class number* 1 *over which the group* $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ *appears as a torsion subgroup of elliptic curves are* $\mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$ *and* $\mathbb{Q}(\sqrt{-163})$.

Proof. By **[13]**, elliptic curves with torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ 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.

• We compute that the rank of $X_1(2,12)(\mathbb{Q})$ is 0, while the rank of $X_1(2,12)^{(d)}(\mathbb{Q})$ is 1 for $d = -19$, -43, -67 or -163. Therefore, the rank of $X_1(2,12)(\mathbb{Q}(\sqrt{d})$ is 1, and hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ appears as a torsion subgroup for infinitely many isomorphism classes of elliptic curves over each of these fields $\mathbb{Q}(\sqrt{d})$ for $d = -19$, -43, -67 or -163.

• We compute that the rank of $X_1(2,12)$ $(\mathbb{Q}(\sqrt{d}))$ is 0 for $d = -2$, -7 and -11. Also, we compute that, in each of these cases,

$$(X_1(2,12)(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}, \qquad (X_1(11)^{(d)}(\mathbb{Q}))_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z}.$$

We observe that the polynomial $x^3 - x^2 + x$ splits only over $\mathbb{Q}(\sqrt{-3})$. Hence, for $d = -2$ or -7, we obtain

$$(X_1(2,12)(\mathbb{Q}(\sqrt{d})))_{\text{tors}} \cong \mathbb{Z}/4\mathbb{Z}.$$

These points in $\mathbb{Z}_4$ correspond to $x = 0$ or 1, and hence are cusps of $X_1(2,12)$. Hence, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ cannot appear as torsion over any of these fields. □

Lemma 6.6. *The group $\mathbb{Z}/16\mathbb{Z}$ cannot appear as a torsion subgroup of elliptic curves over any imaginary quadratic field of class number* 1.

Proof. By [**13**], elliptic curves with torsion $\mathbb{Z}/16\mathbb{Z}$ over a quadratic field K are induced by solutions over K of the equation,

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

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. As the points of a hyperelliptic curve have no group structure, we make use of the Jacobian of $X_1(16)$. Let J be the Jacobian of $X_1(16)$. For $d \in \{-2, -7, -11, -19, -43, -67, -163\}$, let $X_1(16)^{(d)}$ denote the quadratic twist of $X_1(16)$ by d. Let $J^{(d)}$ be the Jacobian of $X_1(16)^{(d)}$. We compute that rank $(J(\mathbb{Q})) = 0$ and rank $(J^{(d)}(\mathbb{Q})) = 0$. Thus, we obtain, as in [**11,** Lemma 3],

$$\text{rank}(J(Q(\sqrt{d}))) = \text{rank}(J(Q) + \text{rank}(J^{(d)}(Q)) = 0 + 0 = 0$$

for each $d \in \{-2, -7, -11, -19, -43, -67, -163\}$. We next compute that

$$(J_1(\mathbb{Q}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

The discriminant of the $X_1(16)$ is -2^{19}; thus, 2 is the only rational prime with bad reduction. Since 3 splits into $Q(\sqrt{-2})$, hence, the prime-to-3 part of $(J(Q(\sqrt{-2})))_{\text{tors}}$ injects into $J(\mathbb{F}_3)$ and, since the rational prime 5 remains inert in $Q(\sqrt{-2})$, hence, the prime-to-5-part of $(J(Q(\sqrt{-2})))_{\text{tors}}$ injects into $J(\mathbb{F}_{5^2})$. Since $|J(\mathbb{F}_3)| = 20$ and $|J(\mathbb{F}_{5^2})| = 40$, we see that

$$|(J(Q(\sqrt{-2})))_{\text{tors}}| \leq 20.$$

Therefore, it follows that

$$(J_1(\mathbb{Q}(\sqrt{-2})))_{\text{tors}} = (J_1(\mathbb{Q}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}.$$

Similar arguments with different primes of good reduction lead to

$$(J_1(\mathbb{Q}(\sqrt{d})))_{\text{tors}} = (J_1(\mathbb{Q}))_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$$

for each $d \in \{-7, -11, -19, -43, -67, -163\}$. In MAGMA, we check that all these torsion points are induced by the cusps of $X_1(16)$. As a result, $\mathbb{Z}/16\mathbb{Z}$ cannot appear as torsion of elliptic curves over any of these fields. □

The main theorem now follows from Lemmas 6.1–6.6, together with Theorems 1.3 and 1.4.

Acknowledgments. We are extremely grateful to Prof. Filip Najman for his valuable comments and suggestions during the preparation of this manuscript.

REFERENCES

1. H. Baziz, *Equations for the modular curve $X_1(N)$ and models of elliptic curves with torsion points*, Math. Comp. **79** (2010), 2371–2386.

2. W. Bosma, J. Cannon, C. Fieker and A. Steel, *Handbook of Magma functions*, Version 2.19, `https://www.math.uzh.ch/sepp/magma-2.19.8-cr/Handbook`, 2013.

3. J. Bosman, P. Bruin, A. Dujella and F. Najman, *Ranks of elliptic curves with prescribed torsion over number fields*, IMRN (2014), 2885–2923.

4. M. Chou, *Torsion of rational elliptic curves over quartic Galois number fields*, J. Num. Th. **160** (2016), 603–628.

5. F. Diamond and J. Shurman, *A first course in modular forms*, Springer, New York, 2005.

6. S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.

7. S. Kamienny and F. Najman, *Torsion groups of elliptic curves over quadratic fields*, Acta Arith. **152** (2012), 291–305.

8. M.A. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

9. B. Mazur, *Modular curves and Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

10. F. Najmam, *Torsion of elliptic curves over quadratic cyclotomic field*, Math. J. Okayama Univ. **53** (2011), 75–82.

11. ———, *Complete classification of torsion of elliptic curves over quadratic cyclotomic field*, J. Num. Th. **130** (2010), 1964–1968.

12. ———, personal correspondence, 2015.

13. F. Rabarison, *Structure de torsion des courbes elliptiques definies sur les corps de nombres quadratiques*, Acta Arith. **144** (2010), 17–52.

14. J. Silverman, *Arithmetic of elliptic curves*, Springer, New York, 2008.

15. L. Washington, *Elliptic curves*, CRC Press, Boca Raton, 1992.

Indian Institute of Technology, Department of Mathematics, Guwahati, Guwahati 781039, Assam, India and Assam University, Department of Mathematics, Silchar, Cachar-788011, Assam, India
Email address: **naba.sarma@iitg.ac.in, naba.sarma@iitg.ernet.in**

Indian Institute of Technology, Department of Mathematics, Guwahati, Guwahati 781039, Assam, India
Email address: **a.saikia@iitg.ac.in, a.saikia@iitg.ernet.in**