Torsion subgroups of elliptic curves with non-cyclic torsion over $\mathbb{Q}$ in elementary abelian 2-extensions of $\mathbb{Q}$

by

YASUTSUGU FUJITA (Sendai)

1. Introduction. Let $E$ be an elliptic curve over $\mathbb{Q}$ and $F$ the maximal elementary abelian 2-extension of $\mathbb{Q}$, that is, $F := \mathbb{Q}(\{\sqrt{m}; m \in \mathbb{Z}\})$. It is known that the torsion subgroup $E(F)_{\text{tors}}$ of $E(F)$ is finite (Ribet [8]). More precisely, Laska and Lorenz showed that there exist at most thirty-one possibilities for $E(F)_{\text{tors}}$ (see [3, Theorem] or Theorem 2.1). However, it is not known whether all the groups listed in Theorem 2.1 can happen as $E(F)_{\text{tors}}$.

Now assume that $E$ has non-cyclic torsion over $\mathbb{Q}$; then by Mazur’s theorem ([4]), the group $E(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$, where $m = 2, 4, 6$ or 8. Such an elliptic curve has a Weierstrass model $E : y^2 = x(x + M)(x + N)$, where $M$ and $N$ are non-zero integers with $M > N$. Further we may assume that the greatest common divisor $(M, N)$ of $M$ and $N$ is a square-free integer or 1, since for any positive integer $d$, $E$ is isomorphic over $\mathbb{Q}$ to an elliptic curve $E_{d^2}$ given by $y^2 = x(x + d^2M)(x + d^2N)$ by replacing $x$ with $x/d^2$ and $y$ with $y/d^3$, respectively. Then using the result of Ono ([6, Main Theorem 1], see also Theorem 2.2), Kwon classified the torsion subgroup of $E$ over all quadratic fields ([2, Theorem 1]); Qiu and Zhang classified the torsion subgroup of $E$ for a certain elliptic curve $E$ with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ over all elementary abelian 2-extensions of $\mathbb{Q}$, i.e., over all number fields of type $(2, \ldots, 2)$ ([7, Theorems 3 and 4]); Ohizumi classified the torsion subgroup of $E$ for an elliptic curve $E$ with $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ over all bicyclic biquadratic fields, i.e., over all number fields of type $(2, 2)$ ([5, Main Theorems 4.1 and 4.2]).

In this paper, first we completely determine the structure of the torsion subgroup $E(F)_{\text{tors}}$ when $E(\mathbb{Q})_{\text{tors}}$ is non-cyclic:

**Theorem 1.** Let $E$ be an elliptic curve over $\mathbb{Q}$ given by the equation $y^2 = x(x + M)(x + N)$, where $M$ and $N$ are integers with $M > N$. Assume

2000 Mathematics Subject Classification: Primary 11G05.
that \((M, N)\) is a square-free integer or 1. Let \(F := \mathbb{Q}(\{\sqrt{m}; m \in \mathbb{Z}\})\) be the maximal elementary abelian 2-extension of \(\mathbb{Q}\). Then \(E(F)_{\text{tors}}\) can be classified as follows:

(a) If \(E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\), then \(E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}\).
(b) If \(E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}\), then \(E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}\).
(c) If \(E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\), then \(E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\) or \(\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\). In this case, we may assume that both \(M\) and \(N\) are squares. Then \(E(F)_{\text{tors}} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\) if and only if \(M - N\) is a square (this is equivalent to the condition that \(E_{-1}(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\)).
(d) If \(E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\), then \(E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\), \(\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\) or \(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\) for all square-free integers \(D\). Otherwise, \(E(F)_{\text{tors}}\) can be determined depending only on the type(s) of \(E_D(\mathbb{Q})_{\text{tors}}\) (and of \(E_{-D}(\mathbb{Q})_{\text{tors}}\) when \(E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\)) for \(D\) with \(E_D(\mathbb{Q})_{\text{tors}} \not\simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}\) through the isomorphism \(E \simeq E_D\) over \(F\).

Secondly, using Theorem 1 we classify the torsion subgroup \(E(K)_{\text{tors}}\) for all elementary abelian 2-extensions \(K\) of \(\mathbb{Q}\) (Section 5). This is a generalization of the result of Kwon ([2, Theorem 1]).

The following notation is in force throughout this paper. \(F\) denotes the maximal elementary abelian 2-extension of \(\mathbb{Q}\). If \(k\) is an algebraic extension of \(\mathbb{Q}\), then we denote by \(O_k\) the ring of algebraic integers in \(k\). For integers \(M\) and \(N\), we denote by \((M, N)\) the greatest common divisor of \(M\) and \(N\). For a square-free integer \(D\), we define the \(D\)-quadratic twist \(E_D\) of an elliptic curve \(E : y^2 = x(x + M)(x + N)\) over \(\mathbb{Q}\) by \(E_D : y^2 = x(x + DM)(x + DN)\). Given a Weierstrass model for \(E\), we often denote by \(x(P)\) the \(x\)-coordinate of a point \(P\) on \(E\). If \(A\) is an abelian group, then we denote by \(A[n]\) the subgroup of \(A\) annihilated by \(n\). For a prime number \(l\) and an elliptic curve \(E\) over a field \(k\), we denote by \(E(k)_{(l)}\) the \(l\)-primary part of \(E(k)_{\text{tors}}\). For a field \(k\) and an element \(a\) in \(k\), we mean by \(\sqrt{a}\) an element \(\alpha\) in the algebraic closure of \(k\) satisfying \(\alpha^2 = a\). If \(a\) is a positive real number, then we take the positive root as \(\sqrt{a}\) and we define \(\sqrt{-a} = \sqrt{-1} \sqrt{a}\) with the imaginary unit \(\sqrt{-1}\), as usual.

**Acknowledgments.** We would like to thank Professor Tetsuo Nakamura for his helpful comments and suggestions.

**2. Preliminary results.** We begin by stating the result of Laska and Lorenz:

**Theorem 2.1** ([3, Theorem]). Let \(E\) be an elliptic curve over \(\mathbb{Q}\). Then the torsion subgroup \(E(F)_{\text{tors}}\) is isomorphic to one of the following thirty-one
groups:
\[ \mathbb{Z}/2^{a+b}\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \quad (a = 1, 2, 3 \text{ and } b = 0, 1, 2, 3), \]
\[ \mathbb{Z}/2^{a+b}\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad (a = 1, 2, 3 \text{ and } b = 0, 1), \]
\[ \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/5\mathbb{Z} \quad (a = 1, 2, 3), \]
\[ \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/2^a\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \quad (a = 1, 2, 3) \]
or \{O\}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}, \mathbb{Z}/9\mathbb{Z}, \mathbb{Z}/15\mathbb{Z}.

Just as in [2] or [7], the result of Ono is a basic tool in this paper:

**Theorem 2.2** ([6, Main Theorem 1]). Let \( E : y^2 = x(x + M)(x + N) \) be an elliptic curve over \( \mathbb{Q} \), where \( M \) and \( N \) are integers. Assume that \((M, N)\) is a square-free integer or 1. Then the torsion subgroup \( E(\mathbb{Q})_{\text{tors}} \) can be classified as follows:

(i) \( E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) if and only if \( M \) and \( N \) are both squares, or \(-M\) and \(-M + N\) are both squares, or \(-N\) and \(-N + M\) are both squares.

(ii) \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) if and only if \( M = u^4 \) and \( N = v^4 \), or \(-M = u^4 \) and \(-M + N = v^4 \), or \(-N = u^4 \) and \(-N + M = v^4 \), where \( u \) and \( v \) are relatively prime positive integers with \( u^2 + v^2 = w^2 \) for some integer \( w \).

(iii) \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \) if and only if \( M = a^4 + 2a^3b \) and \( N = b^4 + 2b^3a \), where \( a \) and \( b \) are relatively prime integers with \( a/b \not\in \{-2, -1, -1/2, 0, 1\} \).

(iv) In all other cases, \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \).

If we write \( E = E(M, N) \), then we obtain \( E(M, N) \simeq E(-M, N - M) \simeq E(-N, M - N) \) over \( \mathbb{Q} \) by replacing \( x \) with \( x - M \) and \( x - N \). Hence, if \( E(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) (resp. \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \)), then we can assume that \( M \) and \( N \) are both squares (resp. \( M = u^4 \) and \( N = v^4 \)) by changing \( x \)-coordinates suitably.

The following lemma is useful for finding whether a point on \( E \) over a field \( k \) is divisible by 2 in \( E(k) \) (see [1, Theorem 4.2, p. 85] and its proof):

**Lemma 2.3.** Let \( k \) be a field of characteristic not equal to 2 or 3, and \( E \) an elliptic curve over \( k \) given by \( y^2 = (x - \alpha)(x - \beta)(x - \gamma) \) with \( \alpha, \beta, \gamma \) in \( k \). For \( P = (x, y) \in E(k) \), there exists a \( k \)-rational point \( Q = (x', y') \) on \( E \) such that \([2]Q = P \) if and only if \( x - \alpha, x - \beta \) and \( x - \gamma \) are all squares in \( k \). In this case, if we fix the sign of \( \sqrt{x - \alpha}, \sqrt{x - \beta} \) and \( \sqrt{x - \gamma} \), then \( x' \) equals one of the following:

\[ \sqrt{x - \alpha} \sqrt{x - \beta} \pm \sqrt{x - \alpha} \sqrt{x - \gamma} \pm \sqrt{x - \beta} \sqrt{x - \gamma} + x \]
or
\[-\sqrt{x - \alpha} \sqrt{x - \beta} \pm \sqrt{x - \alpha} \sqrt{x - \gamma} \mp \sqrt{x - \beta} \sqrt{x - \gamma} + x,\]
where the signs are taken simultaneously.

Using Theorem 2.2 and Lemma 2.3, Kwon classified the torsion subgroup of \( E = E(M, N) \) over all quadratic fields ([2, Theorem 1]) and the torsion subgroup of \( E_D \) for all square-free integers \( D \):

**THEOREM 2.4 ([2, Theorem 2]).** Let \( E : y^2 = x(x + M)(x + N) \) be an elliptic curve over \( \mathbb{Q} \), where \( M \) and \( N \) are integers.

(i) If \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \), then \( E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) for all square-free integers \( D \).

(ii) If \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \), then \( E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) for all square-free integers \( D \).

(iii) If \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \), we may assume that \( M = s^2 \) and \( N = t^2 \) for some integers \( s \) and \( t \). If \( D = -1 \) and \( s^2 - t^2 = \pm r^2 \) for some integer \( r \), then \( E_D(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \). In all other cases, \( E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \).

(iv) If \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \), then \( E_D(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) for only finitely many \( D \) and \( E_D(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) for almost all \( D \).

The following proposition is classical (see, e.g., [1, III.1]).

**PROPOSITION 2.5.** Any integral solution \((x, y, z)\) of \( X^4 \pm Y^4 = Z^2 \) satisfies \( xyz = 0 \).

3. **Squares of algebraic integers in \( F \).** Let \( R := \mathbb{Z}[(\sqrt{m}; m \in \mathbb{Z})] \); it is a subring of \( \mathcal{O}_F \).

**LEMMA 3.1.** If \( a \in \mathcal{O}_F \) is of degree \( 2^d \) over \( \mathbb{Q} \) for some integer \( d \geq 0 \), then \( 2^d a \in R \).

**Proof.** We prove this lemma by induction on \( d \). It is obvious that the lemma holds for \( d = 0, 1 \).

Assume that \( d \geq 2 \). Let \( K_d := \mathbb{Q}(a) \). Then \( K_d \) is a number field of type \((2, \ldots, 2)\) of degree \( 2^d \) over \( \mathbb{Q} \). We may write

\[ a = \frac{1}{b} \left( b_0 + b_1 \sqrt{\theta_1} + \cdots + b_m \sqrt{\theta_m} \right) \]

with some integer \( m \geq d \), where \( b_0, b_1, \ldots, b_m \) are non-zero integers and \( \theta_1, \ldots, \theta_m \) are distinct square-free integers. For each \( i \) with \( 1 \leq i \leq m \), we may choose a basis \( \{1, \sqrt{\theta_{i1}}, \ldots, \sqrt{\theta_{i1d}}\} \) of \( K_d \) over \( \mathbb{Q} \) such that \( \theta_{i1} = \theta_i \) and \( \theta_{i2}, \ldots, \theta_{id} \in \{\theta_1, \ldots, \hat{\theta_i}, \ldots, \theta_m\} \). We define the subfield \( K_d^{(i)} \) of \( K_d \) of degree \( 2^{d-1} \) to be \( \mathbb{Q} \left( \sqrt{\theta_{i1}}, \sqrt{\theta_{i2}}, \ldots, \sqrt{\theta_{id}} \right) \). Let \( \alpha_i \) be the sum of the elements
in the set
\[ \left\{ \frac{1}{b} b_0, \frac{1}{b} b_1 \sqrt{\theta_1}, \ldots, \frac{1}{b} b_m \sqrt{\theta_m} \right\} \cap K_d^{(i)}. \]

Note that the terms \((1/b)b_0\) and \((1/b)b_i \sqrt{\theta_i}\) appear in the sum \(\alpha_i\), since \((1/b)b_0, (1/b)b_i \sqrt{\theta_i} \in K_d^{(i)}\). Then \(\alpha_i \in K_d^{(i)}\) and we can write \(a = \alpha_i + \beta_i \sqrt{\theta_i} \sqrt{\theta_i}\) with some \(\beta_i \in K_d^{(i)}\). Let \(\sigma\) be a generator of the Galois group \(\text{Gal}(K_d/K_d^{(i)})\). Then \(2\alpha_i = a + a^\sigma \in K_d^{(i)} \cap \mathcal{O}_F\). By the inductive assumption, \(2^d\alpha_i = 2^{d-1}2\alpha_i \in R\). Since the terms in the sum \(2^d\alpha_i\) are linearly independent over \(\mathbb{Z}\), each term in \(2^d\alpha_i\) is contained in \(R\); in particular, \(2^d(1/b)b_0, 2^d(1/b)b_i \sqrt{\theta_i} \in R\). Since this holds for each \(i\) with \(1 \leq i \leq m\), we obtain
\[
2^d a = 2^d \frac{1}{b} b_0 + 2^d \frac{1}{b} b_1 \sqrt{\theta_1} + \cdots + 2^d \frac{1}{b} b_m \sqrt{\theta_m} \in R.
\]

This completes the proof of the lemma. ■

We need the following lemmas in order to verify that a certain element in \(F\) is not a square in \(F\).

**Lemma 3.2.** Let \(a \in \mathcal{O}_F\), an odd prime \(l\) and an integer \(i \geq 0\), if \(l^i \sqrt{l}\) divides \(a^2\) in \(\mathcal{O}_F\), then so does \(l^{i+1}\).

**Proof.** If \(l^i \sqrt{l}\) divides \(a^2\) in \(\mathcal{O}_F\), then \(a/\sqrt{l} \in \mathcal{O}_F\), since \((a/\sqrt{l})^2 = a^2/l^i \in \mathcal{O}_F\). By replacing \(a\) with \(a/\sqrt{l}\), it suffices to prove the assertion for \(i = 0\).

Let \(F' := \mathbb{Q}(\{\sqrt{m}; m \text{ is an integer indivisible by } l\})\). Since Lemma 3.1 implies that \(2^d a \in R\) for some integer \(d \geq 0\), we may write \(2^d a = \alpha + \beta \sqrt{l}\) with \(\alpha, \beta \in R \cap \mathcal{O}_{F'}\). Thus
\[
(3.1) \quad 2^{2d} a^2 = (\alpha^2 + \beta^2 l) + 2\alpha\beta \sqrt{l}.
\]

Assume that \(\sqrt{l}\) divides \(a^2\) in \(\mathcal{O}_F\). The equation (3.1) implies that \(\sqrt{l}\) divides \(\alpha^2 \in \mathcal{O}_F\). Lemma 3.1 allows us to write \(\alpha^2 = \sqrt{l} (\gamma + \delta \sqrt{l})/2^e\) with \(\gamma, \delta \in R \cap \mathcal{O}_{F'}\) and some integer \(e \geq 0\). Hence \(2^e \alpha^2 = \gamma \sqrt{l} + \delta l\). However, \(\alpha^2 \in \mathcal{O}_{F'}\), together with the linear independence of 1 and \(\sqrt{l}\) over \(\mathcal{O}_{F'}\), implies that \(\gamma = 0\). Hence \(2^e \alpha^2 = \delta l\). Since \((\sqrt{2^e} \alpha/\sqrt{l})^2 = \delta \in \mathcal{O}_F\), we have \((\sqrt{2^e} \alpha/\sqrt{l}) \alpha \in \mathcal{O}_F\). Hence it is easy to find that \(\sqrt{l}\) divides \(\alpha\) in \(\mathcal{O}_F\). It follows from (3.1) that \(l\) divides \(2^{2d} a^2\) in \(\mathcal{O}_F\), that is, \(l\) divides \(a^2\) in \(\mathcal{O}_F\). ■

**Remark 3.3.** When \(l = 2\), Lemma 3.2 does not hold in general. For example, let \(a = 1 + \sqrt{-1} + \sqrt{2}\). Then
\[
a^2 = 2\sqrt{2} \frac{1 + \sqrt{-1}}{\sqrt{2}} (1 + \sqrt{2}).
\]

Since \((1 + \sqrt{-1})/\sqrt{2} \in \mathcal{O}_F\), it is obvious that \(2\sqrt{2}\) divides \(a^2\) in \(\mathcal{O}_F\). Suppose
that 4 divides \( a^2 \) in \( \mathcal{O}_F \). Then we must have

\[
\frac{1 + \sqrt{-1}}{2} \in \mathcal{O}_F \cap \mathbb{Q}(\sqrt{-1}) = \mathcal{O}_{\mathbb{Q}(\sqrt{-1})},
\]

since \( a^2/4 = (1 + \sqrt{-1})/2 + (1 + \sqrt{-1})/\sqrt{2} \), which contradicts the fact that \( \mathcal{O}_{\mathbb{Q}(\sqrt{-1})} \subset R \). It follows that \( a^2 \) is divisible not by 4 but by \( 2\sqrt{2} \) in \( \mathcal{O}_F \).

**Lemma 3.4 ([7, Assertion, p. 166]).** For any \( m \in \mathbb{Z} \), \( \sqrt{m} \) is a square in \( F \) if and only if \( |m| \) is a square in \( \mathbb{Q} \).

**Proof.** Suppose that \( \sqrt{m} \) is a square in \( F \). Then it is not difficult to find that it can be expressed as \( \sqrt{m} = c(a + b\sqrt{m})^2 \), where \( c \in \mathbb{Q} \) and \( a, b \in \mathbb{Z} \). If \( m \) is not a square in \( \mathbb{Q} \), then \( a^2 + b^2 m = 0 \), that is, \( m = -(a/b)^2 \). The converse obviously holds. \( \blacksquare \)

4. **Proof of Theorem 1.** We begin by examining the structure of \( E(F)(2) \) when \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \).

**Proposition 4.1.** Assume that \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). Then \( E(F)(2) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \).

**Proof.** We may assume that \( M = u^4 \) and \( N = v^4 \), where \( u \) and \( v \) are relatively prime integers with \( u > v > 0 \) and \( u^2 + v^2 = w^2 \) for some integer \( w > 0 \).

First, we show that \( E(F) \not\supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). By Lemma 2.3, we can find a point \( P = (x, y) \) of order 4 on \( E \) such that \( x = u^2 w\sqrt{u^2 - v^2} - u^4 \). Suppose that \( E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). Then by Lemma 2.3, \( x + u^4 = u^2 w\sqrt{u^2 - v^2} \) must be a square in \( F \). This means that \( \sqrt{u^2 - v^2} \) is a square in \( F \). It follows from Lemma 3.4 that \( u^2 - v^2 \) is a square in \( \mathbb{Q} \), which contradicts Proposition 2.5 and the assumption \( u^2 + v^2 = w^2 \). Hence \( x + u^4 = u^2 w\sqrt{u^2 - v^2} \) is not a square in \( F \). Therefore, \( E(F) \not\supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \).

Secondly, we show that \( E(F) \not\supset \mathbb{Z}/32\mathbb{Z} \). Let

\[
P_3 = (uv(u + w)(v + w), uwv(u + v)(v + w)(w + u)).
\]

Then \( P_3 \) is a point of order 8 in \( E(\mathbb{Q}) \) and \( [4]P_3 = (0, 0) \). Using Lemma 2.3, we can find a point \( P_4 = (x_4, y_4) \) of order 16 in \( E(F) \) such that \( [2]P_4 = P_3 \) and \( x_4 = \sqrt[3]{\xi} \eta \), where

\[
\begin{align*}
\eta &= \sqrt[3]{\xi} + \sqrt[3]{\eta_1} + \sqrt[3]{\eta_2} + \eta_3, \\
\xi &= uv(u + w)(v + w), \quad \eta_1 = uw(u + v)(w + v), \\
\eta_2 &= vw(v + u)(w + u), \quad \eta_3 = w(u + v).
\end{align*}
\]

Note that \( \xi, \eta_1, \eta_2, \eta_3 \in \mathbb{Z} \) and \( \eta \in \mathcal{O}_F \). Since \( u^2 + v^2 = w^2 \), \( (u, v) = 1 \) and \( \eta \) is symmetric with respect to \( u, v \), we may assume that \( u = 2mn, v = m^2 - n^2, w = m^2 + n^2 \), where \( m \) and \( n \) are relatively prime integers with \( m > n > 0 \).
and $m \not\equiv n \pmod{2}$. Then
\[
\sqrt{\xi} = 2m(m+n)\sqrt{mn(m^2-n^2)},
\]
\[
\eta_1 = 4m^3n(m^2+n^2)(m^2+2mn-n^2),
\]
\[
\eta_2 = (m+n)^2(m^4-n^4)(m^2+2mn-n^2),
\]
\[
\eta_3 = (m^2+n^2)(m^2+2mn-n^2).
\]
We see that none of $\xi$, $\eta_1$ and $\eta_2$ is a square in $\mathbb{Q}$ by using $(u,v) = 1$ and $u^2 + v^2 = w^2$ (see [2, p. 157]). We need the following lemma:

**Lemma 4.2.** There exists an odd prime $l$ and an integer $i \geq 0$ such that $x_4$ is divisible not by $l^{i+1}$ but by $l^i\sqrt{l}$ in $O_F$.

**Proof of Lemma 4.2.** Suppose that the square-free part of $mn(m^2-n^2)$ is 2. Then both $m+n$ and $m-n$ are squares and either $m = 2(m')^2, n = (n')^2$ or $m = (m')^2, n = 2(n')^2$ for some integers $m', n'$, since any two of $m, n, m+n, m-n$ are relatively prime. If $m = 2(m')^2$ and $n = (n')^2$, then both $2(m')^2 + (n')^2$ and $2(m')^2 - (n')^2$ must be squares, which cannot happen, since either $2(m')^2 + (n')^2$ or $2(m')^2 - (n')^2$ is congruent with 2 or 3 modulo 4. If $m = (m')^2$ and $n = 2(n')^2$, then both $(m')^2 + 2(n')^2$ and $(m')^2 - 2(n')^2$ must be squares, which contradicts the fact that 2 is not a congruent number. Hence there exists an odd prime $l$ which divides the square-free part of $mn(m^2-n^2)$. In order to prove the lemma, it suffices to show that $\sqrt{l}$ does not divide $\eta$ in $O_F$.

Suppose that $\sqrt{l}$ divides $\eta$ in $O_F$. Since $l$ divides either $\eta_1$ or $\eta_2$, Lemma 3.1 implies that $l$ divides $\eta_3$. Hence, it is easy to see that $l$ divides both $mn$ and $m^2-n^2$, which contradicts $(m,n) = 1$. Therefore, $\sqrt{l}$ does not divide $\eta$ in $O_F$. This completes the proof of the lemma. 

Now comparing Lemma 3.2 with Lemma 4.2, we easily find that $x_4$ is not a square in $O_F$. It follows from Lemma 2.3 that $P_4 \not\in 2E(F)$.

Next, using Lemma 2.3 we can find a point $P'_4 = (x'_4, y'_4)$ of order 16 in $E(F)$ such that $[2]P'_4 = P_3 + Q_1 = P'_3$ and
\[
x'_4 = \sqrt{uw(u+w)(v-w)}\{\sqrt{uw(u-v)(w-v)} + \sqrt{uv(v-u)(w+u)} \\
+ \sqrt{uw(u+w)(v-w)} + w(u-v)\},
\]
where $P'_3 = (uw(u+w)(v-w), uvw(u-v)(w+u))$ and $Q_1 = (-u^4, 0)$. Since $x'_4$ is obtained by substituting $-v$ into $v$ in $x_4$, it is easy to show that $x'_4$ is not a square in $F$. It follows from Lemma 2.3 that $P'_4 \not\in 2E(F)$. Put $Q_2 := P'_4 - P_4 \in E(F)$. Then $[2]Q_2 = P'_3 - P_3 = Q_1$. Note that $Q_2$ is not a multiple of $P_4$, since $Q_1$ would then be a multiple of $[8]P_4 = (0, 0)$. Suppose that there exists a point $P$ of order 32 in $E(F)$. Then $[2]P = [a]P_4 + [b]Q_2$ for some integers $a \in \{1, 3, 5, 7, 9, 11, 13, 15\}$ and $b \in \{0, 1, 2, 3\}$, since $E(F) \not\subseteq$
Let \( \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). Now we define a point \( Q \in \langle P_4 \rangle \oplus \langle Q_2 \rangle \) as follows:

\[
Q := \begin{cases} 
-[(a - 1)/2]P_4 - [b/2]Q_2 & \text{if } b = 0, 2, \\
-[(a - 1)/2]P_4 - [(b - 1)/2]Q_2 & \text{if } b = 1, 3.
\end{cases}
\]

Then \( [2](P + Q) = P_4 \) or \( P_4 \). Since \( P + Q \in E(F) \), we must have either \( P_4 \in 2E(F) \) or \( P_4' \in 2E(F) \), which is a contradiction. Therefore, \( E(F) \not\supset \mathbb{Z}/32\mathbb{Z} \). Consequently, \( E(F)_{(2)} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \), which completes the proof of Proposition 4.1.

When \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \), we define \( E(F)_{(2')} \) as follows:

\[
E(F)_{(2')} := \{ P \in E(F); [n]P = O \text{ for some odd integer } n \}.
\]

We can easily determine the structure of \( E(F)_{(2')} \) using Theorem 2.1 and Theorem 1(ii) in [2], which implies that \( E(\mathbb{Q}(\sqrt{D})) \not\supset \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \) for all square-free integers \( D \).

**PROPOSITION 4.3.** Assume that \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \). Then \( E(F)_{(2')} \simeq \mathbb{Z}/3\mathbb{Z} \).

**Proof.** It suffices to show that \( E(F) \not\supset \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \), since Theorem 2.1 implies that \( E(F) \not\supset \mathbb{Z}/6\mathbb{Z} \) for any odd prime \( p \). By the tripling formula, the \( x \)-coordinates of points of order 3 on \( E \) are the roots of some equation of degree 4 with coefficients in \( \mathbb{Q} \). Assume that \( E(\mathbb{Q}) \supset \mathbb{Z}/3\mathbb{Z} \). Then one of the roots is the \( x \)-coordinate of a point \( P_1 \) of order 3 in \( E(\mathbb{Q}) \). Hence, if \( E(F) \supset \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \), then some polynomial \( g(x) \) of degree 3 with coefficients in \( \mathbb{Q} \) must be decomposed as a product of linear polynomials in \( F \). Since the Galois group \( \text{Gal}(F/\mathbb{Q}) \) has no element of order 3, there exists \( \alpha \in \mathbb{Q} \) such that \( g(\alpha) = 0 \). Let \( E \) be given by \( y^2 = f(x) \), let \( D \) be the square-free part of \( f(\alpha) \) and put \( \beta := \sqrt{f(\alpha)} \). Then the point \( P_2 = (\alpha, \beta) \) is of order 3 in \( E(\mathbb{Q}(\sqrt{D})) \), and \( P_1 \) and \( P_2 \) generate \( E[3] \). Hence \( E(\mathbb{Q}(\sqrt{D})) \supset E[3] \), which contradicts Theorem 1(ii) in [2]. Therefore, \( E(F) \not\supset \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z} \).

In order to determine the structure of \( E(F)_{(2)} \), we need an elementary lemma:

**LEMMA 4.4.** Let \( \alpha, \beta \in \mathbb{Q} \) and let \( \gamma \) be a square-free integer. If \( \alpha + \beta \sqrt{\gamma} \) is a square in \( F \), then \( \alpha^2 - \beta^2 \gamma \) is a square in \( \mathbb{Q} \).

**Proof.** If \( \alpha + \beta \sqrt{\gamma} \) is a square in \( F \), then it can be expressed as \( \alpha + \beta \sqrt{\gamma} = c(a + b\sqrt{\gamma})^2 \), where \( c \in \mathbb{Q} \) and \( a, b \in \mathbb{Z} \). This means that \( c(a^2 + b^2\gamma) = \alpha \) and \( 2abc = \beta \). Then \( 4(a^2c)^2 - 4\alpha(a^2c) + \beta^2\gamma = 0 \). Hence

\[
a^2c = \frac{\alpha \pm \sqrt{\alpha^2 - \beta^2\gamma}}{2} \in \mathbb{Q}.
\]

Therefore, \( \sqrt{\alpha^2 - \beta^2\gamma} \in \mathbb{Q} \).
Since we have $E_D(\mathbb{Q})_{(2)} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for all square-free integers $D$ by Theorem 2.4(ii), it suffices to show the following.

**Proposition 4.5.** Assume that $E(\mathbb{Q})_{(2)} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $E_D(\mathbb{Q})_{(2)} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for all square-free integers $D$. Then $E(F)_{(2)} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

**Proof.** By Lemma 2.3, the $x$-coordinate of a point $P$ of order 4 on $E$ equals one of $\pm \sqrt{MN}, -M \pm \sqrt{M(M-N)}, -N \pm \sqrt{N(N-M)}$. Suppose that $E(F) \supset \mathbb{Z}/8\mathbb{Z}$. By Lemma 2.3, there exists a point $P = (x, y)$ of order 4 in $E(F)$ such that $x$, $x + m$ and $x + n$ are all squares in $F$.

Suppose that $x = \pm \sqrt{MN}$. By Lemma 3.4, $|MN|$ is a square in $\mathbb{Q}$. Hence, we may assume that $M = d_1^2D, N = \pm d_2^2D$ for some $D$, a square-free integer, or 1, and some relatively prime integers $d_1, d_2$. If $M = d_1^2D, N = d_2^2D$, then the $D$-quadratic twist $E_D$ of $E$ is given by $y^2 = x(x + (d_1D)^2).$ Hence by Theorem 2.2(ii) we have $E_D(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, which contradicts the assumption. Therefore assume that $M = d_1^2D, N = -d_2^2D$. Then $x + m = \pm d_1d_2D \sqrt{-1} = d_1D$. By Lemma 4.4, if $x + m$ is a square in $F$, then $\sqrt{(d_1^2D)^2 + (d_1d_2D)^2} \in \mathbb{Q}$, that is, $\sqrt{d_1^2 + d_2^2} \in \mathbb{Q}$. However, since the $D$-quadratic twist $E_D$ of $E = E(M, N)$ is isomorphic over $\mathbb{Q}$ to an elliptic curve $E = E_D(-N, M-N)$ given by $y^2 = x(x + (d_2D)^2)\{x + (d_1^2 + d_2^2)D^2\}$, we must have $E_D(\mathbb{Q}) \simeq E'(\mathbb{Q}) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ by Theorem 2.2(i), which contradicts the assumption.

If $x = -M \pm \sqrt{M(M-N)}$ (resp. $x = -N \pm \sqrt{N(N-M)}$), then we also arrive at a contradiction by replacing $M, N$ and $x$ with $-M, N-M$ and $x + M$ (resp. with $-N, M-N$ and $x + N$) in the above argument. Therefore, $E(F) \not\supset \mathbb{Z}/8\mathbb{Z}$. Since it is clear that $E(F) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, we obtain the assertion. 

When $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$, the structure of $E(F)_{(2)}$ depends on whether $E_{-1}(\mathbb{Q})_{\text{tors}}$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Note that in this case $E_{-1}(\mathbb{Q})_{\text{tors}}$ is isomorphic to either $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ (see Theorem 2.4(iii)).

**Proposition 4.6.** Assume that $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. If $E_{-1}(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, then $E(F)_{(2)} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Otherwise, $E(F)_{(2)} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

**Proof.** We may assume that $M = s^2$ and $N = t^2$, where $s$ and $t$ are relatively prime integers with $s > t > 0$. Then

$$E(\mathbb{Q})_{\text{tors}} = (Q_1) \oplus (P_2) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z},$$

where $P_2 = (st, st(s+t))$ and $Q_1 = (-s^2, 0)$. Note that $[2]P_2 = (0, 0)$. By Lemma 2.3, $E(F) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ and there exist points $P_3$ and $Q_2$ of order 8 and order 4, respectively, in $E(F)$ such that $[2]P_3 = P_2$, $[2]Q_2 = Q_1$ and $x(P_3) = st + s\sqrt{t(s+t)} + t\sqrt{s(s+t)} + (s+t)\sqrt{st}$, $x(Q_2) = -s^2 + s\sqrt{s^2 - t^2}$. 


Suppose that \( P_3 \in 2E(F) \). Since
\[
x(P_3) = \sqrt{st}\left\{ \frac{1}{\sqrt{2}} (\sqrt{s} + \sqrt{t} + \sqrt{s+t}) \right\}^2,
\]
we see that \( x(P_3) \) is a square in \( F \) if and only if \( \sqrt{st} \) is a square in \( F \); hence by Lemma 3.4, \( st \) is a square in \( \mathbb{Q} \). This means that there exist positive integers \( u, v \) such that \( s = u^2, t = v^2 \), since \( (s, t) = 1 \). Thus
\[
x(P_3) + M = u^2v^2 + u^2v\sqrt{u^2 + v^2} + uv^2\sqrt{u^2 + v^2} + (u^2 + v^2)uv + u^4
\]
\[
= u(u+v)\sqrt{u^2 + v^2}(v + \sqrt{u^2 + v^2}).
\]
Since \((u, v) = 1\), we have \((v, u^2 + v^2) = 1\). Note that by Theorem 2.2(ii), \( u^2 + v^2 \) is not a square in \( \mathbb{Q} \), since \( E(Q)_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \). Suppose that the square-free part of \( u^2 + v^2 \) is 2. If we write \( u^2 + v^2 = 2w^2 \) with some integer \( w > 0 \), then \( x(P_3) + M = uw(u+v)(2w+v\sqrt{2}) \). Since \( x(P_3) + M \) is a square in \( F \), we can write \( 2w + v\sqrt{2} = c(a+b\sqrt{2}) \), where \( c \in \mathbb{Q} \) and \( a, b \in \mathbb{Z} \) with \((a, b) = 1\). Then \( c(a^2 + 2b^2) = 2w \) and \( 2abc = v \), which means that \( v(a^2 + 2b^2) = 4abw \). Since \( v \) is odd because of \( u^2 + v^2 = 2w^2 \), we must have \( a^2 + 2b^2 \equiv 0 \pmod{4} \), that is, \( a \equiv b \equiv 0 \pmod{2} \), which contradicts \((a, b) = 1\). Therefore there exists an odd prime \( l \) which divides the square-free part of \( u^2 + v^2 \). However for such a prime \( l \), \( \sqrt{l} \) does not divide \( v + \sqrt{u^2 + v^2} \) in \( O_F \) because of \((v, u^2 + v^2) = 1\) and Lemma 3.1; hence there exists an integer \( i \) such that \( x(P_3) + M \) is divisible not by \( l^{i+1} \) but by \( l^i \sqrt{l} \) in \( O_F \), which contradicts Lemma 3.2. It follows that \( x(P_3) + M \) is not a square in \( F \), and from Lemma 2.3 that \( P_3 \notin 2E(F) \).

**Case 1:** \( E_{-1}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \). In this case, by Theorem 2.4(iii), \( s^2 - t^2 \) is not a square in \( \mathbb{Q} \). Suppose that \( E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \), that is, \( Q_2 \in 2E(F) \). Then by Lemma 2.3, \( x(Q_2) \), \( x(Q_2) + M \) and \( x(Q_2) + N \) are all squares in \( F \). Since \( x(Q_2) + M = s\sqrt{s^2 - t^2} \), Lemma 3.4 implies that \( x(Q_2) + M \) is a square in \( F \) if and only if \( s^2 - t^2 \) is a square in \( \mathbb{Q} \), which contradicts the assumption. Hence \( E(F) \not\cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). Using Lemma 2.3, we can find a point \( P'_3 \) of order 8 in \( E(F) \) such that \( [2]P'_3 = P_2 + Q_1 = P'_2 \) and \( x(P'_3) = -st + s\sqrt{-t(s-t) - t\sqrt{s(s-t)} + (s-t)\sqrt{-st}} \), where \( P'_2 = (-st, -st(s-t)) \). Since \( x(P'_3) \) is obtained by substituting \(-t \) into \( t \) in \( x(P_3) \), it is easy to see that \( x(P'_3) + M \) is not a square in \( F \). It follows from Lemma 2.3 that \( P'_3 \notin 2E(F) \). Put \( Q'_2 := P'_3 - P_3 \in E(F) \). Then \( [2]Q'_2 = P'_2 - P_2 = Q_1 \). Suppose that there exists a point \( P \) of order 16 in \( E(F) \). Then \( [2]P = [a]P_3 + [b]Q_2 \) for some integers \( a \in \{1, 3, 5, 7\} \) and \( b \in \{0, 1, 2, 3\} \), since \( E(F) \not\cong \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). Now we define a point \( Q \in \langle P_3 \rangle \oplus \langle Q'_2 \rangle \) as follows:

\[
Q := \begin{cases} 
-[(a-1)/2]P_3 - [b/2]Q'_2 & \text{if } b = 0, 2, \\
-[(a-1)/2]P_3 - [(b-1)/2]Q'_2 & \text{if } b = 1, 3.
\end{cases}
\]
Then \([2](P + Q) = P_3\) or \(P_3'\). Since \(P + Q \in E(F)\), we must have either \(P_3 \in 2E(F)\) or \(P_3' \in 2E(F)\), which is a contradiction. Therefore, \(E(F) \not\cong \mathbb{Z}/16\mathbb{Z}\). Consequently, \(E(F)(2) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\).

**Case 2**: \(E_{-1}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}\). In this case, by Theorem 2.4(iii), \(s^2 - t^2 = r^2\) for some integer \(r > 0\). Then \(x(Q_2) = s(r - s)\). By Lemma 2.3, \(E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}\). In fact, there exists a point \(Q_3\) of order 8 in \(E(F)\) such that \([2]Q_3 = Q_2\) and \(x(Q_3) = s\sqrt{r(r - s) + (s - r)\sqrt{-r^2 + r\sqrt{s(s - r) + s(r - s)}}}\). Thus

\[
x(Q_3) + M = \sqrt{-rs} \left\{ \frac{1}{\sqrt{2}} (\sqrt{s - \sqrt{-r}} + \sqrt{s - r}) \right\}^2.
\]

However, by Proposition 2.5 and \((r, s) = 1\) it is easy to see that \(rs\) is not a square in \(\mathbb{Q}\). It follows from Lemma 3.4 that \(x(Q_3) + M\) is not a square in \(F\), and from Lemma 2.3 that \(Q_3 \not\in 2E(F)\).

Next, we show that \(E(F) \not\cong \mathbb{Z}/16\mathbb{Z}\). Using Lemma 2.3, we can find a point \(R_3\) of order 8 in \(E(F)\) such that \([2]R_3 = R_2\) and

\[
x(R_3) = \sqrt{rt} \frac{1 + \sqrt{-1}}{\sqrt{2}} \left\{ \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} \right\}^2 + t\sqrt{r} \left\{ \frac{1 + \sqrt{-1}}{\sqrt{2}} \right\}^2 \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + r\sqrt{t} \frac{1 + \sqrt{-1}}{\sqrt{2}} \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + t(r\sqrt{-1} - t),
\]

where \(R_2 = (t(r\sqrt{-1} - t), rt(r\sqrt{-1} - t))\) and \([2]R_2 = (-t^2, 0)\). Then we have

\[
x(R_3) + N = \sqrt{rt} \frac{1 + \sqrt{-1}}{\sqrt{2}} \left\{ \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + \sqrt{r} \right\} \times \left\{ \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + \sqrt{t} \frac{1 + \sqrt{-1}}{\sqrt{2}} \right\}.
\]

Put

\[
A := \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + \sqrt{r}, \quad B := \frac{\sqrt{r + s} + \sqrt{r - s}}{\sqrt{2}} + \sqrt{t} \frac{1 + \sqrt{-1}}{\sqrt{2}}.
\]

Note that \(A, B, x(R_3) + N \in \mathcal{O}_F\) and that both \(A\) and \(B\) divide \(x(R_3) + N\) in \(\mathcal{O}_F\). Suppose that \(x(R_3) + N\) is a square in \(\mathcal{O}_F\).

First, suppose that there exists an odd prime \(\ell\) which divides the square-free part of \(t\). Since \(r < s\), \(\sqrt{r + s}\) and \(\sqrt{r - s}\) are linearly independent over \(\mathbb{Z}\); and since \((r + s, r - s)\) divides \((2r, 2s) = 2\), \(l\) does not divide \((r + s, r - s)\). Hence by Lemma 3.1, \(\sqrt{\ell}\) does not divide \(\sqrt{r + s} + \sqrt{r - s}\) in \(\mathcal{O}_F\), which means that \(\sqrt{\ell}\) does not divide \(B\) in \(\mathcal{O}_F\). If \(\sqrt{r + s}, \sqrt{r - s}\) and \(\sqrt{2}r\) are linearly independent over \(\mathbb{Z}\), then it is clear that \(\sqrt{\ell}\) does not divide \(A\).
in \( \mathcal{O}_F \) because of \((l, 2r) = 1\) and Lemma 3.1. Otherwise, the square-free part of \( r + s \) equals that of \( 2r \); it is either 1 or 2, since \( s = m^2 + n^2 \) and \( r = 2mn \) or \( m^2 - n^2 \) for some relatively prime integers \( m, n \). Then the square-free part of \( r - s \) is either \(-1\) or \(-2\). Thus \( A \) can be expressed as 

\[
A = a_0 + a_1\sqrt{-1} + a_2\sqrt{2} + a_3\sqrt{-2}
\]

with integers \( a_0, a_1, a_2, a_3 \). Hence by Lemma 3.1 there exists an integer \( i \) such that \( A \) is divisible not by \( l^i \sqrt{i} \) but by \( l^{i+1} \) in \( \mathcal{O}_F \). Therefore for some integer \( e \), \( x(R_3) + N \) is divisible not by \( l^{e+1} \) but by \( l^{e+1} \sqrt{i} \) in \( \mathcal{O}_F \). It follows from Lemma 3.2 that \( x(R_3) + N \) is not a square in \( \mathcal{O}_F \), which contradicts the assumption. Therefore, either \( t = (t')^2 \) or \( t = 2(t')^2 \) for some integer \( t' \).

Secondly, suppose that there exists an odd prime \( p \) which divides the square-free part of \( r \). In the same way as above, we easily see that \( \sqrt{p} \) does not divide \( A \) in \( \mathcal{O}_F \), that \( B \) can be expressed as 

\[
B = a_0 + a_1\sqrt{-1} + a_2\sqrt{2} + a_3\sqrt{-2}
\]

with integers \( a_0, a_1, a_2, a_3 \) (since either \( t = (t')^2 \) or \( t = 2(t')^2 \)) and that \( x(R_3) + N \) is not a square in \( \mathcal{O}_F \), which contradicts the assumption. Therefore, either \( r = (r')^2 \) or \( r = 2(r')^2 \) for some integer \( r' \). It follows that \( r = (r')^2 \) and \( t = (t')^2 \), \( r = 2(r')^2 \) and \( t = (t')^2 \) or \( r = (r')^2 \) and \( t = 2(t')^2 \). It is not difficult to see that none of these cases happens because of Proposition 2.5. It follows that \( x(R_3) + N \) is not a square in \( F \), and from Lemma 2.3 that \( R_3 \not\in 2E(F) \).

Now let \( P_4, Q_4, R_4 \) be points of order 16 on \( E \) such that \([2]P_4 = P_3\), \([2]Q_4 = Q_3\), \([2]R_4 = R_3\), and put \( \mathcal{P} := \{P_4 + P; P \in E[8]\}, \mathcal{Q} := \{Q_4 + P; P \in E[8]\}, \mathcal{R} := \{R_4 + P; P \in E[8]\} \). Then it is obvious that \( E[16] = E[8] \cup \mathcal{P} \cup \mathcal{Q} \cup \mathcal{R} \). Since \( P_4, Q_4, R_4 \) cannot be in \( E(F) \), we obtain \( E(F) \not\subset \mathbb{Z}/16\mathbb{Z} \). Consequently, \( E(F)_{(2)} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). This completes the proof of Proposition 4.6.

In order to prove Theorem 1, we need one more proposition due to Qiu and Zhang.

**Proposition 4.7** ([7, Theorem 2 and Remark 2]). Let \( E \) be an elliptic curve over \( \mathbb{Q} \). Assume that \( E(\mathbb{Q})_{\text{tors}} = E(\mathbb{Q})_{(2)} \) and \( E_D(\mathbb{Q})_{\text{tors}} = E_D(\mathbb{Q})_{(2)} \) for all square-free integers \( D \). Then \( E(F)_{\text{tors}} = E(F)_{(2)} \).

**Remark 4.8.** Although Theorem 2 and Remark 2 in [7] are expressed in terms of a number field \( K \) of type \((2, \ldots, 2)\) instead of \( F \), it is clear that they are also valid for \( F \).

Now all we have to do is put the propositions together.

**Proof of Theorem 1.** Since if \( E(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) or \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \), then \( E_D(\mathbb{Q})_{\text{tors}} = E_D(\mathbb{Q})_{(2)} \) for all square-free integers \( D \) by Theorem 2.4, (a) follows from Propositions 4.1 and 4.7; (c) follows from Propositions 4.6 and 4.7 (note that by Theorem 2.4(iii), \( M - N \) is a square if and only if \( E_{-1}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \)). We obtain (b) just by combining Propositions...
4.5 and 4.3. In (d), if \( E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) for all \( D \), then \( E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) from Propositions 4.5 and 4.7; if \( E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) (resp. \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z} \)) for some \( D \), then (a) (resp. (b)) shows that \( E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \) (resp. \( \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z} \)) through the isomorphism \( E \simeq E_D \) over \( F \); if \( E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \) and \( E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \) (resp. \( \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z} \)) for some \( D \), then (c) shows that \( E(F)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) (resp. \( \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \)). This completes the proof of Theorem 1.

5. A classification over number fields of type \((2, \ldots, 2)\). Let \( E : y^2 = x(x + M)(x + N) \) be an elliptic curve over \( \mathbb{Q} \), where \( M \) and \( N \) are integers with \( M > N \) such that \((M, N)\) is a square-free integer or 1. Let \( K \) be a number field of type \((2, \ldots, 2)\). It is not difficult to determine the structure of \( E(K)_{\text{tors}} \) because of Theorem 1.

Case 1: \( E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \). We may assume that \( M = u^4 \) and \( N = v^4 \), where \( u \) and \( v \) are relatively prime integers with \( u > v > 0 \) and \( u^2 + v^2 = w^2 \) for some integer \( w > 0 \).

(I) By Lemma 2.3, \( E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) if and only if \( \sqrt{-1}, \sqrt{u^4 - v^4} \in K \). Since \( u^4 - v^4 = w^2(u^2 - v^2) \), we see that \( \sqrt{u^4 - v^4} \in K \) if and only if \( \sqrt{u^2 - v^2} \in K \). Hence, \( E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \) if and only if \( \sqrt{-1}, \sqrt{u^2 - v^2} \in K \).

(II) We find a necessary and sufficient condition for \( E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \). Let \( P_3 = (uw(u + w)(v + w), uw(u + v)(v + w)(w + u)) \in E(\mathbb{Q}) \) and \( P'_3 = P_3 + Q_1 \in E(\mathbb{Q}) \), where \( Q_1 = (-u^4, 0) \). Then \( P_3 \) and \( P'_3 \) are of order 8 and \( x(P'_3) = uw(u+w)(v-w) \). Assume that \( E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \). Then it is easy to see that either \( P_3 \) or \( P'_3 \) is contained in \( 2E(K) \). By Lemma 2.3, this is equivalent to the condition that either

\[
\sqrt{uw(u+w)(v+w)}, \sqrt{uw(u+v)(w+v)} \in K
\]

or

\[
\sqrt{uw(u+w)(v-w)}, \sqrt{uw(u-v)(w-v)} \in K.
\]

On account of (I), we obtain the following: \( E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \) if and only if either \( \sqrt{-1} \notin K \) or \( \sqrt{u^2 - v^2} \notin K \) and either

\[
\sqrt{uw(u+w)(v+w)}, \sqrt{uw(u+v)(w+v)} \in K
\]

or

\[
\sqrt{uw(u+w)(v-w)}, \sqrt{uw(u-v)(w-v)} \in K.
\]

(III) Assume that \( E(K)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z} \). By Theorem 1(a), there exists a point \( P_3 \) of order 16 in \( E(F) \) such that \( [2]P_4 = P_3 \). Let \( P''_3 := P_3 + Q_2 \), where \( Q_2 \) is a point of order 4 in \( E(K) \) such that \( [2]Q_2 = Q_1 \). If \( P_4 \notin E(K) \), then it is not difficult to find that there exists a point \( P''_4 \in E(K) \) (of order 16) such that \( [2]P''_4 = P''_3 \). However since \( [2](P''_4 - P_4) = P''_3 - P_3 = Q_2 \), we have \( Q_2 \in 2E(F) \). Hence \( E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z} \), which contradicts...
Theorem 1(a). Therefore we must have $P_4 \in E(K)$. On account of (I) and (II), we obtain the following: $E(K)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$ if and only if

$$\sqrt{-1}, \sqrt{u^2 - v^2}, \sqrt{uv(u + w)(v + w)}, \sqrt{uv(u + v)(w + v)} \in K.$$ 

(IV) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ from Theorem 1(a).

CASE 2: $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$. By Theorem 1(b), we may restrict ourselves to the 2-primary part of $E(K)_{\text{tors}}$.

(I) By Lemma 2.3, $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ if and only if $\sqrt{M}, \sqrt{N} \in K$, $\sqrt{-M}, \sqrt{-M + N} \in K$ or $\sqrt{-N}, \sqrt{-N - M} \in K$.

(II) By Lemma 2.3 and Theorem 1(b), $E(K)_{\text{tors}} \simeq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$ if and only if $\sqrt{-1}, \sqrt{M}, \sqrt{N}, \sqrt{-M - N} \in K$.

(III) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ from Theorem 1(b).

CASE 3: $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. We may assume that $M = s^2$ and $N = t^2$, where $s$ and $t$ are relatively prime integers with $s > t > 0$. Put $r := \sqrt{s^2 - t^2}$.

(I) By Lemma 2.3, $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if $\sqrt{-s^2}, r\sqrt{-1} \in K$, namely, $\sqrt{-1}, r \in K$.

(II) Assume that $E(K) \not\supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Let $P_1 = (0, 0), Q_1 = (-s^2, 0), P_2 = (st, st(s + t))$ and $P_2' = (-st, st(t - s))$, where $[2]P_2 = P_1$ and $P_2 + Q_1 = P_2'$. Then $E(K) \supset \mathbb{Z}/8\mathbb{Z}$ if and only if either $P_2 \in 2E(K)$ or $P_2' \in 2E(K)$.

By Lemma 2.3, this is equivalent to the condition that either $\sqrt{st}, \sqrt{s(s + t)} \in K$ or $\sqrt{-st}, \sqrt{s(s - t)} \in K$. On account of (I), we obtain the following: $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ if and only if either $\sqrt{-1} \not\in K$ or $r \not\in K$ and either $\sqrt{st}, \sqrt{s(s + t)} \in K$ or $\sqrt{-st}, \sqrt{s(s - t)} \in K$.

(III) We find a necessary and sufficient condition on which $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Assume that $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$.

Let $P_2 = (st, st(s + t)), Q_2 = (s(r - s), rs(r - s)\sqrt{-1})$ and $R_2 = (t(r\sqrt{-1}-t), rt(r\sqrt{-1}-t))$, where $[2]P_2 = P_1$, $[2]Q_2 = Q_1$ and $[2]R_2 = R_1 = (-t^2, 0)$. Then it is obvious that $E(K) \supset \mathbb{Z}/8\mathbb{Z}$ if and only if $P_2, Q_2$ or $R_2$ is contained in $2E(K)$. By Lemma 2.3, this is equivalent to the condition that $\sqrt{st}, \sqrt{s(s + t)} \in K$, $\sqrt{s(r - s)}, \sqrt{rs} \in K$ or $\sqrt{r(t + \sqrt{-1})}, \sqrt{rt\sqrt{-1}} \in K$ (note that $\sqrt{-1} \in K$ by the assumption that $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$). Since

$$\sqrt{r(t + \sqrt{-1})} = \pm \frac{\sqrt{2r}}{2} (\sqrt{r + s + \sqrt{r - s}})$$

and

$$\sqrt{rt\sqrt{-1}} = \pm \frac{\sqrt{2rt}}{2} (1 + \sqrt{-1}),$$
the third condition can be replaced with $\sqrt{2rt}, \sqrt{2r(r+s)}, \sqrt{2r(r-s)} \in K$. Further, since $\sqrt{2r(r-s)} = 2rt\sqrt{-1}/\sqrt{2r(r+s)}$, we see that $\sqrt{2r(r-s)} \in K$ if and only if $\sqrt{2r(r+s)} \in K$. Similarly we find that $\sqrt{s(r+s)} \in K$ if and only if $\sqrt{s(r-s)} \in K$. Hence $E(K) \supset \mathbb{Z}/8\mathbb{Z}$ if and only if $\sqrt{st}, \sqrt{s(s+t)} \in K$, $\sqrt{rs}, \sqrt{s(r+s)} \in K$ or $\sqrt{2rt}, \sqrt{2r(r+s)} \in K$ (on the assumption that $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$). On account of (I), we obtain the following: $E(K) \supset \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ if and only if $\sqrt{-1}, r \in K$ and

$$\sqrt{st}, \sqrt{s(s+t)} \in K, \sqrt{rs}, \sqrt{s(r+s)} \in K \text{ or } \sqrt{2rt}, \sqrt{2r(r+s)} \in K.$$

(IV) We easily see that $E(K)_{\text{tors}} \simeq \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ if and only if $\sqrt{-1}, r, \sqrt{st}, \sqrt{s(s+t)}, \sqrt{rs}, \sqrt{s(r+s)}, \sqrt{2rt}, \sqrt{2r(r+s)} \in K$, that is,

$$\sqrt{-1}, r, \sqrt{rs}, \sqrt{st}, \sqrt{s(r+s)}, \sqrt{s(s+t)} \in K.$$

Note that this case can occur only if $r \in \mathbb{Q}$.

(V) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ from Theorem 1(c).

**Case 4:** $E(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. If $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ (resp. $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$) and $\sqrt{D} \in K$ for some square-free integer $D$, then we may consider ourselves to be in Case 1 (resp. Case 2, Case 3) through the isomorphism $E \simeq E_D$ over $F$. Hence in the case where $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ for some $D$, assume that $\sqrt{D} \notin K$; in the case where $E_D(\mathbb{Q})_{\text{tors}} \simeq E_{-D}(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ for some $D$, assume that $\sqrt{-D} \notin K$ and $\sqrt{-D} \notin K$.

**Case 4.1:** $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$ for some square-free integer $D$. We may assume that $M = D(u'')^4$ and $N = D(v'')^4$, where $u'$ and $v'$ are relatively prime positive integers such that $(u'')^2 + (v'')^2$ is a square. By Lemma 2.3, it is clear that $E(K) \not\supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ because of $\sqrt{D} \notin K$.

(I) By Lemma 2.3, $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if either $\sqrt{-D}$, $\sqrt{-D\{(u'')^4 - (v'')^4\}} \in K$ or $\sqrt{-D}, \sqrt{-D\{(u'')^4 - (v'')^4\}} \in K$, that is, $\sqrt{-D} \in K$ and either $\sqrt{(u'')^2 - (v'')^2} \in K$ or $\sqrt{(v'')^2 - (u'')^2} \in K$. Suppose that $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then since $P_1 = (0,0) \notin 2E(K)$, either $Q_1 = (-D(u'')^4,0)$ or $R_1 = (-D(v'')^4,0)$ is contained in $4E(K)$; hence $P_1 \in 4E(F)$ implies that $E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$, which contradicts Theorem 1(a). Therefore we obtain the following: $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if $\sqrt{-D} \in K$ and either

$$\sqrt{(u'')^2 - (v'')^2} \in K \text{ or } \sqrt{(v'')^2 - (u'')^2} \in K.$$

(II) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

**Case 4.2:** $E_D(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ for some square-free integer $D$. We may assume that $M = D(s')^2$ and $N = D(t')^2$, where $s'$ and $t'$ are relatively
prime positive integers. By Lemma 2.3, it is clear that $E(K) \not\subseteq \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ because of $\sqrt{D} \notin K$.

(I) By Lemma 2.3, $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if either $\sqrt{-D}$, $\sqrt{-D}\{(s')^2 - (t')^2\} \in K$ or $\sqrt{-D}, \sqrt{-D}\{(t')^2 - (s')^2\} \in K$, that is, $\sqrt{-D} \in K$ and either $(s')^2 - (t')^2 \in K$ or $(t')^2 - (s')^2 \in K$. Suppose that $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$. Then since $P_1 = (0,0) \not\in 2E(K)$, either $Q_1 = (-D(s')^2,0)$ or $R_1 = (-D(t')^2,0)$ is contained in $4E(K)$; hence $P_1 \in 4E(F)$ implies that $E(F) \supset \mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.

Therefore we obtain the following: $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. Hence by assumption we must have $\sqrt{-D} \notin K$, which is a contradiction. Therefore we obtain the following: $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Let $d_2$ be an integer such that $[K: \mathbb{Q}] = 2^d$. Then we write $K = K_d$.

Remark 5.1. The result of Qiu and Zhang ([7, Theorem 4]) is contained in Case 4.3. In fact, in Theorem 4 in [7], they classified $E(K)_{\text{tors}}$ on the assumption that $M$ and $N$ are relatively prime square-free integers, not equal to $\pm 1$, which implies that $E(Q)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $E(D)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for all square-free integers $D$. From Lemma 2.3 we easily get the following:

(II) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Case 4.3: $E_D(Q)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ for all square-free integers $D$. Assume that $E_D(Q)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ for some $D$. Then by Theorem 1(b) we know that $E(F)_{(2)} \simeq E_D(F)_{(2)} \simeq \mathbb{Z}/3\mathbb{Z}$, and by Theorem 2.2(iii) we may assume that the points of order 3 in $E(F)$ are $(Da^2b^2, \pm D\sqrt{D}a^2b^2(a+b)^2)$ with some integers $a, b$. It follows from $\sqrt{-D} \notin K$ that $E(K)_{(2)} = \{O\}$. Therefore this case can be treated just as the case where $E_D(Q)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for all square-free integers $D$. Thus from Lemma 2.3 we easily get the following:

(II) $E(K) \supset \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$ if and only if $\sqrt{M}, \sqrt{N} \in K$, $\sqrt{-M}, \sqrt{-M+N} \in K$.

(III) In all other cases, we obtain $E(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$.

Remark 5.1. The result of Qiu and Zhang ([7, Theorem 4]) is contained in Case 4.3. In fact, in Theorem 4 in [7], they classified $E(K)_{\text{tors}}$ on the assumption that $M$ and $N$ are relatively prime square-free integers, not equal to $\pm 1$, which implies that $E(Q)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $E(D)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ for all square-free integers $D$. ([7, Lemma 2]).

Let $d$ be an integer such that $[K: \mathbb{Q}] = 2^d$. Then we write $K = K_d$. We conclude this paper to give the minimal $d_m$ for which each type above can be realized as $E(K_{d_m})_{\text{tors}}$ with some $E$ and some $K_{d_m}$. Close examination will show the following:

- In Case 1, we have $d_m = 4$ for the type $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/16\mathbb{Z}$.
- In Case 2, we have $d_m = 3$ for the type $\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}$.
- In Case 3, we have $d_m = 4$ for the type $\mathbb{Z}/8\mathbb{Z} \oplus \mathbb{Z}/8\mathbb{Z}$.
- For all other types, we have $d_m = 2$. 
It is easy to see that this and the classification in this section together imply Theorem 3 in [7] and Main Theorems 4.1 and 4.2 in [5], which are stated for $K_2$.

References


Mathematical Institute
Tohoku University
Sendai 980-8578, Japan
E-mail: fyasut@yahoo.co.jp

Received on 10.12.2002
and in revised form on 28.1.2004 (4421)