ISSN 1343-9499

TOHOKU
MATHEMATICAL
PUBLICATIONS

Number 27

Torsion of elliptic curves over number fields

by

Yasutsugu Fujita

August 2003

Sendai 980-8578, Japan

This series aims to publish material related to the activities of the Mathematical Institute of Tohoku University. This may include:
1. Theses submitted to the Institute by grantees of the degree of Doctor of Science.
2. Proceedings of symposia as well as lecture notes of the Institute.

A primary advantage of the series lies in quick and timely publication. Consequently, some of the material published here may very likely appear elsewhere in final form.

Tohoku Mathematical Publications

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan

TOHOKU
MATHEMATICAL
PUBLICATIONS

Number 27

Torsion of elliptic curves over number fields

by

Yasutsugu FUJITA

August 2003

Sendai 980-8578, Japan

Torsion of elliptic curves over number fields

A thesis presented

by

Yasutsugu Fujita

to

The Mathematical Institute

for the degree of

Doctor of Science

Tohoku University

Sendai, Japan

March 2003

Introduction

Let K be a number field and E an elliptic curve over K. The Mordell-Weil theorem asserts that the group $E(K)$ of K-rational points on E is finitely generated; in particular, the torsion subgroup $E(K)_{\mathrm{tors}}$ of $E(K)$ is finite. In the case where $K = \mathbf{Q}$, the group $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to one of the following fifteen groups:

$$\begin{aligned} &\mathbf{Z}/N\mathbf{Z} && \text{for } N = 1, \ldots, 10, 12, \\ &\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z} && \text{for } N = 1, 2, 3, 4 \end{aligned}$$

(Mazur [13], [14]). For an arbitrary number field K, Merel ([15]) showed that the order $|E(K)_{\mathrm{tors}}|$ of $E(K)_{\mathrm{tors}}$ is bounded above by a constant depending only on the degree of K over $\mathbf{Q}$.

We are interested in determining how $E(K)_{\mathrm{tors}}$ varies as we replace K with an extension L of K, or E with a K-isogenous curve E' to E. More precisely, we study the following two problems on torsion of elliptic curves over a number field:

(1) Classify the torsion subgroup of an elliptic curve over $\mathbf{Q}$ in all elementary abelian 2-extensions of $\mathbf{Q}$, that is, in all number fields of type $(2, \ldots, 2)$.

(2) Examine the order of maximal torsion of an elliptic curve E over a number field K in the K-isogeny class of E.

As to (1), let E be an elliptic curve over $\mathbf{Q}$ and F the maximal elementary abelian 2-extension of $\mathbf{Q}$, that is,

$$F := \mathbf{Q}(\{\sqrt{m}\,;\, m \in \mathbf{Z}\}).$$

Then it is known that one has at most thirty-one possibilities for the torsion subgroup $E(F)_{\mathrm{tors}}$ (Laska and Lorenz [10, Theorem]). However, it is not known whether each type of these thirty-one groups occurs as $E(F)_{\mathrm{tors}}$. In the case where $E(\mathbf{Q})_{\mathrm{tors}}$ is non-cyclic, we may choose a Weierstrass model

$$E : y^2 = x(x + M)(x + N),$$

where M and N are non-zero integers. Then Kwon ([8, Theorem 1]) classified the torsion subgroup of E over all quadratic extensions of $\mathbf{Q}$; Qiu and Zhang ([20, Theorems 3 and 4]) classified the torsion subgroup of E for a certain elliptic curve E with $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ over all elementary abelian 2-extensions of $\mathbf{Q}$; Ohizumi ([17, Theorems 4.1 and 4.2]) classified the torsion subgroup of E for an elliptic curve E with $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ over all bicyclic biquadratic field, that is, over all number fields of type $(2, 2)$. In this thesis, when $E(\mathbf{Q})_{\mathrm{tors}}$ is non-cyclic, we completely determine the torsion subgroup of E over F as well as over all elementary abelian 2-extensions of $\mathbf{Q}$ (Theorems 1 and 2 in Chapter 2).

As to (2), let E be an elliptic curve over a number field K and $\mathcal{C}(E)$ the K-isogeny class of E. Then there exists an elliptic curve $E_0 \in \mathcal{C}(E)$ such that the order $|E_0(K)_{\mathrm{tors}}|$ is maximal in $\mathcal{C}(E)$, that is,

$$|E_0(K)_{\mathrm{tors}}| = \max_{E' \in \mathcal{C}(E)} |E'(K)_{\mathrm{tors}}|,$$

since $\mathcal{C}(E)$ has at most finitely many K-isomorphism classes of elliptic curves over K. Katz ([6]) described the order $|E_0(K)_{\mathrm{tors}}|$ in terms of the reduction $\widetilde{E_\wp}$ of E modulo each prime $\wp$ of K. However, his description depends on the class $\mathcal{C}(E)$ (note that the order of minimal torsion in $\mathcal{C}(E)$ is bounded above by a constant depending only on K in case $\mathrm{End}_K(E) \simeq \mathbf{Z}$; see [22], [16]). For each prime l, we here give a necessary and sufficient condition for the order of the l-primary part $E(K)_{(l)}$ of $E(K)_{\mathrm{tors}}$ being maximal in $\mathcal{C}(E)$ (Theorem 3 in Chapter 3). By making use of it, we can find the order of maximal l-torsion of E over K in $\mathcal{C}(E)$. We also give some sufficient conditions for the order of $E(K)_{(l)}$ being maximal in $\mathcal{C}(E)$ (Proposition 3.1.6 in Chapter 3). Since in general the conditions given in Proposition 3.1.6 are easier to check than the ones in Theorem 3, this proposition is also useful for finding the order of maximal l-torsion in $\mathcal{C}(E)$. Proposition 3.1.6 and Theorem 3 imply several properties concerning the torsion of elliptic curves in their K-isogeny classes.

Acknowledgments

It is a great pleasure of the author to thank Professor Tetsuo Nakamura for his persevering encouragement and helpful advice, without which the present dissertation would never have been written. The author would like to thank Professor Yasuo Morita for his invaluable suggestions and guidance. Thanks also go to Dr. Atsushi Sato for his numerous comments and moral support. Finally, the author is grateful to the staff of the Mathematical Institute of Tohoku University for their encouragement.

Contents

Chapter 1

Elliptic curves

In this chapter, we briefly review some basic properties of elliptic curves, with emphasis on those which are related to Chapter 2 or 3.

1.1 Basic definitions

An elliptic curve E is a smooth projective curve of genus one furnished with a point O on E. The elliptic curve E is said to be defined over the field k if both the curve E and the point O are defined over k. The points on E form an abelian group with the identity element O. If E is defined over a field k, then the group $E(k)$ of k-rational points on E is a subgroup of E.

Every elliptic curve E, defined over a field k, has a plane cubic model of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where the coefficients a_i are in k. Such a model is called a Weierstrass model for E. If further the characteristic $\mathrm{char}(k)$ of k differs from 2 or 3, then E has a Weierstrass model of the form

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

where $A, B \in k$. Given such a model for E, the discriminant Δ and the j-invariant $j(E)$ are given respectively by

$$\Delta = -16(4A^3 + 27B^2), \qquad j(E) = -1728(4A)^3/\Delta.$$

The discriminant Δ does not vanish because of the non-singularity of E. When E_1 and E_2 are elliptic curves defined over a field k, E_1 is isomorphic to E_2 over the algebraic closure $\overline{k}$ of k if and only if $j(E_1) = j(E_2)$.

An isogeny is a non-constant morphism $\phi : E_1 \to E_2$ between elliptic curves satisfying $\phi(O) = O$, which is a group homomorphism. E_1 and E_2 are said to be isogenous if there exists an isogeny ϕ between E_1 and E_2. If E_1, E_2 and ϕ are defined over a field k, then ϕ is said to be a k-isogeny, and E_1 and E_2 are said to be k-isogenous.

Let E be an elliptic curve over a field k. For a positive integer m, is associated the multiplication-by-m map $[m] : E \to E$, which is one of the most important isogenies. Its kernel $E[m]$ is isomorphic to $\mathbf{Z}/m\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$ if the characteristic $\mathrm{char}(k)$ of k is prime to m or $\mathrm{char}(k) = 0$; if $\mathrm{char}(k) = p > 0$, then either $E[p^e]$ is isomorphic to $\mathbf{Z}/p^e\mathbf{Z}$ for all positive integers e or $E[p^e] = 0$ for all positive integers e.

If $\phi : E_1 \to E_2$ is an isogeny of degree $m > 0$, then there exists an isogeny $\hat{\phi} : E_2 \to E_1$ (called the dual isogeny to ϕ) such that $\hat{\phi} \circ \phi = [m]_1$ and $\phi \circ \hat{\phi} = [m]_2$, where $[m]_i$ stands for the multiplication-by-m map on E_i for $i = 1, 2$. We denote by $\mathrm{Hom}(E_1, E_2)$ the group of isogenies between elliptic curves E_1 and E_2 together with the zero map. If $E_1 = E_2 = E$, then we let $\mathrm{End}(E) := \mathrm{Hom}(E, E)$, which is called the endomorphism ring of E. Since for any integer $m \neq 0$ the multiplication-by-m map $[m]$ is non-constant, the group $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbf{Z}$-module. Furthermore, the endomorphism ring $\mathrm{End}(E)$ is isomorphic to $\mathbf{Z}$, to an order in an imaginary quadratic field or to an order in a quaternion algebra ([28, Corollary 9.4, p. 102]). Note that for an elliptic curve over a field k of $\mathrm{char}(k) = 0$, the third possibility can not happen. If $\mathrm{End}(E)$ is isomorphic to an order $\mathcal{O}$ in an imaginary quadratic field, then we say that E has complex multiplication (by $\mathcal{O}$). For a field k, by $\mathrm{Hom}_k(E_1, E_2)$ (resp. $\mathrm{End}_k(E)$) we mean the group (resp. the ring) of those elements in $\mathrm{Hom}(E_1, E_2)$ (resp. $\mathrm{End}(E)$) which are defined over k. If $\mathrm{End}_k(E)$ is isomorphic to an order in an imaginary quadratic field, then we say that E has complex multiplication over k.

1.2 The Tate module

Throughout this section, let k be a field and l a prime number distinct from $\mathrm{char}(k)$. Let E be an elliptic curve over k. The (l-adic) Tate module $T_l(E)$ of E is defined as follows:

$$T_l(E) := \varprojlim E[l^n].$$

Since $E[l^n]$ is isomorphic to $\mathbf{Z}/l^n\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$, it is easy to find that

$$T_l(E) \simeq \mathbf{Z}_l \oplus \mathbf{Z}_l$$

as $\mathbf{Z}_l$-modules. Let G_k denote the Galois group $\mathrm{Gal}(\overline{k}/k)$. Since the action of G_k on each $E[l^n]$ commutes with the multiplication-by-l map, G_k acts continuously on $T_l(E)$. Thus we obtain the l-adic representation (of G_k)

$$\rho_l : \mathrm{G}_k \to \mathrm{Aut}(T_l(E)).$$

Note that if we choose a $\mathbf{Z}_l$-basis of $T_l(E)$, then we have an isomorphism

$$\mathrm{Aut}(T_l(E)) \simeq \mathrm{GL}_2(\mathbf{Z}_l).$$

Let $\boldsymbol{\mu}_{l^n}$ be the group of l^n-th roots of unity. Since G_k also acts continuously on $T_l(\boldsymbol{\mu}) := \varprojlim \boldsymbol{\mu}_{l^n}$, we obtain the l-adic cyclotomic character (of G_k)

$$\chi_l : \mathrm{G}_k \to \mathrm{Aut}(T_l(\boldsymbol{\mu})).$$

Since the Weil pairing

$$e_l : T_l(E) \times T_l(E) \to T_l(\boldsymbol{\mu})$$

is $\mathbf{Z}_l$-bilinear, alternating, non-degenerate and G_k-invariant ([28, Proposition 8.3, p. 99]), we easily see that

$$\det \rho_l = \chi_l \tag{1.2.1}$$

(cf. [32, Section 9]).

Let E_1 and E_2 be elliptic curves over k. Using the fact that $\mathrm{Hom}_k(E_1, E_2)$ is torsion-free, we can show that the natural homomorphism

$$\mathrm{Hom}_k(E_1, E_2) \otimes \mathbf{Z}_l \to \mathrm{Hom}_k(T_l(E_1), T_l(E_2))$$

is injective ([28, Theorem 7.4, p. 92]), where $\mathrm{Hom}_k(T_l(E_1), T_l(E_2))$ denotes the group of those elements in $\mathrm{Hom}(T_l(E_1), T_l(E_2))$ which are defined over k.

Theorem 1.2.1. ([31], [2]) *Let E_1 and E_2 are elliptic curves over k. If k is either a finite field (Tate) or a number field (Faltings), then the map*

$$\mathrm{Hom}_k(E_1, E_2) \otimes \mathbf{Z}_l \to \mathrm{Hom}_k(T_l(E_1), T_l(E_2))$$

is an isomorphism.

If E_1 and E_2 are k-isogenous, then it is easy to find that $T_l(E_1)\otimes\mathbf{Q}_l \simeq T_l(E_2)\otimes\mathbf{Q}_l$ as G_k-modules. The converse holds if k is as in Theorem 1.2.1:

Corollary 1.2.2. *Let E_1 and E_2 are elliptic curves over k. If k is either a finite field or a number field, then the following are equivalent*:

(a) *E_1 and E_2 are k-isogenous.*

(b) *$T_l(E_1) \otimes \mathbf{Q}_l \simeq T_l(E_2) \otimes \mathbf{Q}_l$ as G_k-modules.*

Corollary 1.2.2 follows immediately from Theorem 1.2.1. Note that Theorem 1.2.1 and Corollary 1.2.2 remain valid if we replace "elliptic curves" with "abelian varieties". Concerning the image $\mathrm{Im}\,\rho_l$ of $\rho_l : \mathrm{G}_k \to \mathrm{Aut}(T_l(E))$, the following is known:

Theorem 1.2.3. (Serre [23], [24]) *Let E be an elliptic curve over a number field without complex multiplication. Then $\mathrm{Im}\,\rho_l$ is of finite index in $\mathrm{Aut}(T_l(E))$ for all primes l.*

1.3 Good reduction

Let K be a number field and R the ring of integers of K. Let v be a finite place of K. By K_v, R_v, $\wp_v$ and k_v, we mean the completion of K with respect to v, the ring of integers of K_v, the maximal ideal of R_v and the residue field of R_v, respectively. Let E be an elliptic curve over K. Regarding E as being defined over K_v, we denote by $\widetilde{E_v}$ the reduction of E modulo $\wp_v$. E is said to have good reduction at v if the reduced curve $\widetilde{E_v}$ is non-singular; otherwise, E is said to have bad reduction at v. If E has good reduction at v, then $\widetilde{E_v}$ is an elliptic curve over k_v.

Theorem 1.3.1. (Shafarevich [28, Theorem 6.1, p. 263]) *Let K be a number field. Let S be a finite set of places of K containing the infinite places. Then the set of K-isomorphism classes of elliptic curves over K having good reduction at all places not in S is finite.*

Since K-isogenous elliptic curves have the same set of primes of bad reduction ([25, Corollary 2]), Theorem 1.3.1 implies the following corollaries.

Corollary 1.3.2. *For an elliptic curve E over a number field K, there exist only finitely many K-isomorphism classes of elliptic curves over K which are K-isogenous to E.*

Corollary 1.3.3. (Serre [23, THEOREM, p. IV-9]) *Let E be an elliptic curve over a number field K without complex multiplication over K. Put $\mathrm{G}_K := \mathrm{Gal}(\overline{K}/K)$.*

(a) *$T_l(E)$ is an irreducible G_K-module for all primes l.*

(b) *$E[l]$ is an irreducible G_K-module for all but finitely many primes l.*

Now let us examine the relationship between $E(K)_{\mathrm{tors}}$ and $\widetilde{E_v}(k_v)$. Fix a prime number l. Let $\rho_l : \mathrm{G}_K \to \mathrm{Aut}(T_l(E))$ be the l-adic representation. For a finite place v of K, let F_v denote the Frobenius conjugacy class of v. If l is indivisible by $\wp_v$ and E has good reduction at v, then we have

$$\det(1 - \rho_l(F_v)) = N(\wp_v), \tag{1.3.1}$$

where $N(\wp_v) := |\widetilde{E_v}(k_v)|$ (cf. [23, p. IV-5]).

Theorem 1.3.4. (cf. [6, Appendix]) *Let E be an elliptic curve over a number field K and v a finite place of K. Let e_v denote the absolute ramification index of $\wp_v$ and p_v the prime number divisible by $\wp_v$. If $e_v < p_v - 1$, then the reduction map from $E(K)_{\mathrm{tors}}$ to $\widetilde{E_v}(k_v)$ is an injective homomorphism.*

This shows that

$$N(\wp_v) \equiv 0 \mod |E(K)_{\mathrm{tors}}| \tag{1.3.2}$$

for any place v of K at which E has good reduction and for which $e_v < p_v - 1$.

Remark 1.3.5. The relation (1.3.2) remains valid if we replace E with any K-isogenous curve E' to E, since E and E' have the same primes of good reduction and the same $N(\wp_v)$'s.

1.4 The Mordell-Weil theorem

Theorem 1.4.1 (Mordell-Weil Theorem). *Let E be an elliptic curve over a number field K. Then the group $E(K)$ is finitely generated.*

The proof of this theorem consists of two claims: (i) the weak Mordell-Weil theorem and (ii) the descent.

The claim (i) asserts the following:

Theorem 1.4.2 (Weak Mordell-Weil Theorem). *Let E be an elliptic curve over a number field K. Then the quotient group $E(K)/2E(K)$ is finite.*

This follows from the exact sequence

$$0 \to E(K)/2E(K) \to S^{(2)}(E/K) \to Ш(E/K)[2] \to 0$$

together with the fact that $S^{(2)}(E/K)$ is finite, where $S^{(2)}(E/K)$ is the 2-Selmer group of E over K and $Ш(E/K)[2]$ is the kernel of the multiplication-by-2 map on the Shafarevich-Tate group $Ш(E/K)$ of E over K.

As to the claim (ii), the canonical height plays a crucial role.

Theorem 1.4.3. (cf. [28, Theorem 9.3, p. 229]) *Let E be an elliptic curve over a number field K. There exists a real-valued function $\hat{h}$ on $E(\overline{K})$ (called the canonical height on E) which is a positive semi-definite quadratic form on $E(K)$ with the following properties*:

(a) *For $P \in E(K)$, $\hat{h}(P) = 0$ if and only if P is a torsion point on E.*

(b) *For any constant C, the set $\{P \in E(K)\,;\, \hat{h}(P) \leq C\}$ is finite.*

By making use of Theorems 1.4.2 and 1.4.3, it is easy to prove the Mordell-Weil theorem (see, e.g., [30, Section 18]).

1.5 The Uniform Boundedness Conjecture

Let E be an elliptic curve over a number field K. The Mordell-Weil theorem assures us that the group $E(K)$ is finitely generated; in particular, the torsion subgroup $E(K)_{\mathrm{tors}}$ is finite. As for the l-primary part $E(K)_{(l)}$ of $E(K)_{\mathrm{tors}}$, the following result of Manin has been known.

Theorem 1.5.1. (Manin [11]) *Let K be a number field and l a prime number. There exists a constant $C_{K,l}$ depending only on K and l such that $|E(K)_{(l)}|$ divides $C_{K,l}$ for all elliptic curves E over K.*

In the case where $K = \mathbf{Q}$ or K is a quadratic number field, the possibilities for $E(K)_{\mathrm{tors}}$ are known:

Theorem 1.5.2. (Mazur [13], [14]) *Let E be an elliptic curve over $\mathbf{Q}$. Then the torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to one of the following fifteen groups*:

$$\mathbf{Z}/N\mathbf{Z} \qquad \text{for } N = 1, \ldots, 10, 12,$$
$$\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z} \qquad \text{for } N = 1, 2, 3, 4.$$

Theorem 1.5.3. (Kamienny [4], see also Kenku and Momose [5] and Silverberg [27]) *Let E be an elliptic curve over a quadratic number field K. Then $E(K)_{\mathrm{tors}}$ is isomorphic to one of the following twenty-six groups*:

$$\begin{aligned}
&\mathbf{Z}/N\mathbf{Z} && \text{for } N = 1, \ldots, 16, 18,\\
&\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2N\mathbf{Z} && \text{for } N = 1, \ldots, 6,\\
&\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3N\mathbf{Z} && \text{for } N = 1, 2,\\
&\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}.
\end{aligned}$$

Over an arbitrary number field, Merel settled the so-called Uniform Boundedness Conjecture:

Theorem 1.5.4. (Merel [15]) *Let E be an elliptic curve over a number field K of degree d over $\mathbf{Q}$. Then $|E(K)_{\mathrm{tors}}|$ is bounded above by a constant depending only on d.*

1.6 Complex multiplication

Let K be an imaginary quadratic field and $\mathcal{O}_K$ the ring of integers of K (i.e., the maximal order in K). Denote by h_K the class number of K. Then the number of the isomorphism classes of elliptic curves E over $\mathbf{C}$ with $\mathrm{End}(E) \simeq \mathcal{O}_K$ equals h_K ([26, Proposition 4.10]). Let E be an elliptic curve over $\mathbf{C}$ with $\mathrm{End}(E) \simeq \mathcal{O}_K$. For any field automorphism σ of $\mathbf{C}$, it is clear that $\mathrm{End}(E^\sigma) = \mathrm{End}(E)$ and $j(E^\sigma) = j(E)^\sigma$. Hence $j(E)$ is an algebraic number and $[\mathbf{Q}(j(E)) : \mathbf{Q}] \leq h_K$. More precisely, we have

Theorem 1.6.1. (cf. [1], [26] or [29]) *Let K be an imaginary quadratic field and $\mathcal{O}$ an order in K. Let E be an elliptic curve over $\mathbf{C}$ with complex multiplication by $\mathcal{O}$. Then the following hold.*

(a) *The j-invariant $j(E)$ of E is an algebraic integer.*

(b) *If $\mathcal{O} = \mathcal{O}_K$ is the ring of integers of K, then the field $K(j(E))$ is the Hilbert class field of K (i.e., the maximal unramified abelian extension of K) and $[\mathbf{Q}(j(E)) : \mathbf{Q}] = [K(j(E)) : K] = h_K$.*

Recall that any elliptic curve E over $\mathbf{C}$ has a Weierstrass model

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

where $A, B \in \mathbf{C}$. Given such a model for E, we define the Weber function ϕ_E on E as follows:

$$\phi_E((x,y)) = \begin{cases} (AB/\Delta)x & \text{if } AB \neq 0, \\ (A^2/\Delta)x^2 & \text{if } B = 0, \\ (B/\Delta)x^3 & \text{if } A = 0, \end{cases}$$

where $\Delta = -16(4A^3 + 27B^2) \neq 0$ is the discriminant. Note that ϕ_E is independent of the choice of Weierstrass model.

Theorem 1.6.2. (cf. [1], [26] or [29]) *Let E be an elliptic curve over $\mathbf{C}$ with complex multiplication by the ring of integers $\mathcal{O}_K$ of the imaginary quadratic field K. Let ϕ_E be the Weber function on E. Then the maximal abelian extension of K is obtained by adjoining to K the j-invariant $j(E)$ of E and the values $\phi_E(P)$ for all torsion points P on E.*

Chapter 2

Torsion subgroups of elliptic curves in elementary abelian 2-extensions of Q

Let E be an elliptic curve over $\mathbf{Q}$ and F the maximal elementary abelian 2-extension of $\mathbf{Q}$, that is,

$$F := \mathbf{Q}(\{\sqrt{m}\,;\, m \in \mathbf{Z}\}).$$

It is known that the torsion subgroup $E(F)_{\mathrm{tors}}$ of $E(F)$ is finite (Ribet [21]). More precisely, Laska and Lorenz ([10, Theorem]) showed that there exist at most thirty-one possibilities for $E(F)_{\mathrm{tors}}$ (see also Theorem 2.1.1 below). However, it is not known whether all the groups listed in Theorem 2.1.1 occur as $E(F)_{\mathrm{tors}}$.

Now assume that E has non-cyclic torsion over $\mathbf{Q}$. Then by Mazur's theorem (see Theorem 1.5.2), the group $E(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/m\mathbf{Z}$, 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 $M > N$. We may assume that the greatest common divisor (M, N) of M and N is a square-free integer or $(M, N) = 1$, since for any positive integer d, E is isomorphic over $\mathbf{Q}$ to an elliptic curve E_{d^2} given by

$$E_{d^2} : y^2 = x(x + d^2M)(x + d^2N),$$

by replacing x with x/d^2 and y with y/d^3, respectively. Then by making use of the result of Ono ([18, Theorem 1], see also Theorem 2.1.2 below), Kwon ([8, Theorem

1]) classified the torsion subgroup of E over arbitrary quadratic extension of $\mathbf{Q}$; Qiu and Zhang ([20, Theorems 3 and 4]) classified the torsion subgroup of E for a certain elliptic curve E with $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ over all elementary abelian 2-extensions of $\mathbf{Q}$, that is, over all number fields of type $(2, \ldots, 2)$; Ohizumi ([17, Theorems 4.1 and 4.2]) classified the torsion subgroup of E for an elliptic curve E with $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ over all bicyclic biquadratic fields, that is, over all number fields of type $(2, 2)$.

In this chapter, first we completely determine the structure of the torsion subgroup $E(F)_{\mathrm{tors}}$, when $E(\mathbf{Q})_{\mathrm{tors}}$ is non-cyclic.

Theorem 1. *Let E be an elliptic curve over $\mathbf{Q}$ given by $E : y^2 = x(x+M)(x+N)$, where M and N are integers with $M > N$. Assume that (M, N) is a square-free integer or $(M, N) = 1$. Let $F := \mathbf{Q}(\{\sqrt{m}\,;\, m \in \mathbf{Z}\})$ be the maximal elementary abelian 2-extension of $\mathbf{Q}$. Then $E(F)_{\mathrm{tors}}$ can be classified as follows*:

(a) *If $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, then we have $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$.*

(b) *If $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$, then we have $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$.*

(c) *If $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, then we have $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ or $\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Moreover, we may assume that both M and N are squares. Then $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ if and only if $M - N$ is a square (this is equivalent to the condition that $E_{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$).*

(d) *If $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, then we have $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ or $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. Furthermore, $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all square-free integers D. Otherwise, $E(F)_{\mathrm{tors}}$ can be determined depending only on the type(s) of $E_D(\mathbf{Q})_{\mathrm{tors}}$ (and of $E_{-D}(\mathbf{Q})_{\mathrm{tors}}$ when $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$) for D with $E_D(\mathbf{Q})_{\mathrm{tors}} \not\simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ through the isomorphism $E \simeq E_D$ over F.*

Secondly, by making use of Theorem 1 we classify the torsion subgroup $E(K)_{\mathrm{tors}}$ for all elementary abelian 2-extensions K of $\mathbf{Q}$ (Theorem 2 in Section 2.4). This is a generalization of a result of Kwon ([8, Theorem 1]).

The following notation is in use throughout this chapter. F denotes the maximal elementary abelian 2-extension of $\mathbf{Q}$. If k is an algebraic extension of $\mathbf{Q}$, then we denote by $\mathcal{O}_k$ 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 $\mathbf{Q}$ 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 $E(k)_{\mathrm{tors}}$. For a field k and an element a in k, we denote by $\sqrt{a}$ an element α in the algebraic closure of k satisfying $\alpha^2 = a$. If a is a positive real number, then we take the positive one as $\sqrt{a}$ and we define $\sqrt{-a} = \sqrt{-1}\sqrt{a}$ with the imaginary unit $\sqrt{-1}$ as usual.

2.1 Preliminary results

We begin by stating the result of Laska and Lorenz.

Theorem 2.1.1. ([10, Theorem]) *Let E be an elliptic curve over $\mathbf{Q}$. Then the torsion subgroup $E(F)_{\mathrm{tors}}$ is isomorphic to one of the following thirty-one groups*:

$\mathbf{Z}/2^{a+b}\mathbf{Z} \oplus \mathbf{Z}/2^a\mathbf{Z}$ $(a = 1, 2, 3$ *and* $b = 0, 1, 2, 3)$,
$\mathbf{Z}/2^{a+b}\mathbf{Z} \oplus \mathbf{Z}/2^a\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ $(a = 1, 2, 3$ *and* $b = 0, 1)$,
$\mathbf{Z}/2^a\mathbf{Z} \oplus \mathbf{Z}/2^a\mathbf{Z} \oplus \mathbf{Z}/5\mathbf{Z}$ $(a = 1, 2, 3)$,
$\mathbf{Z}/2^a\mathbf{Z} \oplus \mathbf{Z}/2^a\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ $(a = 1, 2, 3)$

or $\{O\}$, $\mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$, $\mathbf{Z}/5\mathbf{Z}$, $\mathbf{Z}/7\mathbf{Z}$, $\mathbf{Z}/9\mathbf{Z}$, $\mathbf{Z}/15\mathbf{Z}$.

As in [8] or [20], the following result of Ono is a basic tool in this chapter.

Theorem 2.1.2. ([18, Theorem 1]) *Let $E : y^2 = x(x + M)(x + N)$ be an elliptic curve over $\mathbf{Q}$, where M and N are integers. Assume that (M, N) is a square-free integer or $(M, N) = 1$. Then the torsion subgroup $E(\mathbf{Q})_{\mathrm{tors}}$ can be classified as follows*:

(i) *$E(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ 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) *$E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ 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 positive integers with $(u, v) = 1$ and $u^2 + v^2 = w^2$ for some integer w.*

(iii) *$E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ if and only if $M = a^4 + 2a^3b$ and $N = b^4 + 2b^3a$, where a and b are integers with $(a, b) = 1$ and $a/b \notin \{-2, -1, -1/2, 0, 1\}$.*

(iv) *In all other cases, we have $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.*

If we write $E = E(M, N)$, then we see that $E(M, N) \simeq E(-M, N - M) \simeq E(-N, M - N)$ over $\mathbf{Q}$ by replacing x with $x - M$ and $x - N$, respectively. Hence if $E(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ (resp. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$), 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 examining whether a point in E over a field k is divisible by 2 in $E(k)$ (see [3, Theorem 4.1, p. 37] or [7, Theorem 4.2, p. 85], and their proof).

Lemma 2.1.3. *Let k be a field of characteristic not equal to 2 or 3 and E an elliptic curve over k given by*

$$E : y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

with α, β and γ 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. Moreover, if we fix each 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.

2.2 Squares of algebraic integers in F

Let $R := \mathbf{Z}[\{\sqrt{m}\,;\, m \in \mathbf{Z}\}]$, which is a subring of $\mathcal{O}_F$, the ring of algebraic integers in F.

Lemma 2.2.1. *If $a \in \mathcal{O}_F$ is of degree 2^d over $\mathbf{Q}$ for some integer $d \geq 0$, then we have $2^d a \in R$.*

[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 $K_d := \mathbf{Q}(a)$. Then K_d is a number field of type $(2, \ldots, 2)$ of degree 2^d over $\mathbf{Q}$. We may write

$$a = \frac{1}{b}(b_0 + b_1\sqrt{\theta_1} + \cdots + b_m\sqrt{\theta_m})$$

with some integer $m \geq d$, where $b_0 \in \mathbf{Z}$, $b, b_1, \ldots, b_m$ 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 $\left\{1, \sqrt{\theta_{i1}}, \ldots, \sqrt{\theta_{id}}\right\}$ of K_d over $\mathbf{Q}$ such that $\theta_{i1} = \theta_i$ and

$$\theta_{i2}, \ldots, \theta_{id} \in \{\theta_1, \ldots, \check{\theta}_i, \ldots, \theta_m\}.$$

We define the subfield $K_d^{(i)}$ of K_d of degree 2^{d-1} to be $\mathbf{Q}\left(\sqrt{\theta_{i1}}, \sqrt{\theta_{i3}}, \ldots, \sqrt{\theta_{id}}\right)$. Let α_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 α_i, since $(1/b)b_0$, $(1/b)b_i\sqrt{\theta_i} \in K_d^{(i)}$. Then we have $\alpha_i \in K_d^{(i)}$ and we can write

$$a = \alpha_i + \beta_i\sqrt{\theta_{i2}}$$

with some $\beta_i \in K_d^{(i)}$. Let σ be a generator of the Galois group $\mathrm{Gal}(K_d/K_d^{(i)})$. Then we have

$$2\alpha_i = a + a^\sigma \in K_d^{(i)} \cap \mathcal{O}_F.$$

By the assumption of induction, we know that

$$2^d\alpha_i = 2^{d-1}2\alpha_i \in R.$$

Since the terms in the sum $2^d\alpha_i$ are linearly independent over $\mathbf{Z}$, each term in $2^d\alpha_i$ is contained in R. In particular, we have

$$2^d\frac{1}{b}b_0, 2^d\frac{1}{b}b_i\sqrt{\theta_i} \in R.$$

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 2.2.2. *For $a \in \mathcal{O}_F$, 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 we have $a/\sqrt{l^i} \in \mathcal{O}_F$, since $(a/\sqrt{l^i}\,)^2 = a^2/l^i \in \mathcal{O}_F$. By replacing a with $a/\sqrt{l^i}$, it suffices to prove this lemma for $i = 0$.

Let $F' := \mathbf{Q}(\{\sqrt{m}\,;\, m \text{ is an integer indivisible by } l\})$. Since Lemma 2.2.1 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 we have

$$2^{2d}a^2 = (\alpha^2 + \beta^2 l) + 2\alpha\beta\sqrt{l}. \tag{2.2.1}$$

Assume that $\sqrt{l}$ divides a^2 in $\mathcal{O}_F$. The equation (2.2.1) implies that $\sqrt{l}$ divides α^2 in $\mathcal{O}_F$. Lemma 2.2.1 allows us to write

$$\alpha^2 = \frac{1}{2^e}\sqrt{l}\,(\gamma + \delta\sqrt{l})$$

with $\gamma, \delta \in R \cap \mathcal{O}_{F'}$ and some integer $e \geq 0$. Hence we have $2^e\alpha^2 = \gamma\sqrt{l} + \delta l$. 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 we have $2^e\alpha^2 = \delta l$. Since

$$\left(\frac{\sqrt{2^e}}{\sqrt{l}}\,\alpha\right)^2 = \delta \in \mathcal{O}_F,$$

we have $(\sqrt{2^e}/\sqrt{l}\,)\,\alpha \in \mathcal{O}_F$. Therefore, it is easy to see that $\sqrt{l}$ divides α in $\mathcal{O}_F$. It follows from the equation (2.2.1) that l divides $2^{2d}a^2$ in $\mathcal{O}_F$, that is, l divides a^2 in $\mathcal{O}_F$. □

Remark 2.2.3. When $l = 2$, Lemma 2.2.2 does not hold in general. For example, let $a = 1 + \sqrt{-1} + \sqrt{2}$. Then we have

$$\begin{aligned} a^2 &= 2 + 2\sqrt{-1} + 2\sqrt{2}\,(1 + \sqrt{-1}\,) \\ &= 2\sqrt{2}\,\frac{1 + \sqrt{-1}}{\sqrt{2}}\,(1 + \sqrt{2}\,). \end{aligned}$$

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, since

$$\frac{1}{4}a^2 = \frac{1 + \sqrt{-1}}{2} + \frac{1 + \sqrt{-1}}{\sqrt{2}},$$

we must have

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

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

Lemma 2.2.4. ([20, Assertion, p. 166]) *For any $m \in \mathbf{Z}$, $\sqrt{m}$ is a square in F if and only if $|m|$ is a square in $\mathbf{Q}$.*

[Proof] Suppose that $\sqrt{m}$ is a square in F. Then it is not difficult to see that $\sqrt{m}$ can be expressed as follows:

$$\sqrt{m} = c(a + b\sqrt{m})^2,$$

where $c \in \mathbf{Q}$ and $a, b \in \mathbf{Z}$. If m is not a square in $\mathbf{Q}$, then we have $a^2 + b^2 m = 0$, that is, $m = -(a/b)^2$. The converse is obvious. □

2.3 Proof of Theorem 1

We begin by examining the structure of $E(F)_{(2)}$, when $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

Proposition 2.3.1. *Assume that $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Then we have $E(F)_{(2)} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$.*

[Proof] We may assume that $M = u^4$ and $N = v^4$, where u and v are integers with $(u, v) = 1$, $u > v > 0$ and $u^2 + v^2 = w^2$ for some positive integer w.

First, we show that $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Let $P = (x, y) \in E$ be a point of order 4. Then by Lemma 2.1.3, we know that x equals

$$\pm u^2 v^2, \pm u^2 w\sqrt{u^2 - v^2} - u^4 \ \text{ or } \ \pm v^2 w\sqrt{u^2 - v^2} - v^4.$$

Suppose that $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. By Lemma 2.1.3, if x equals any of the above six values, then $x, x + u^4$ and $x + v^4$ must be squares in F. In particular, if $x = u^2 w\sqrt{u^2 - v^2} - u^4$, then

$$x + u^4 = u^2 w\sqrt{u^2 - v^2}$$

must be a square in F. This means that $\sqrt{u^2 - v^2}$ is a square in F. It follows from Lemma 2.2.4 that $u^2 - v^2$ is a square in $\mathbf{Q}$. Thus we have

$$u^4 - v^4 = (u^2 + v^2)(u^2 - v^2) = (wn)^2,$$

where n is an integer with $u^2 - v^2 = n^2$. However, this has no integral solution except $u = v = wn = 0$ (see, for example, Ono [19]). Hence $x + u^4 = u^2 w\sqrt{u^2 - v^2}$ is not a square in F. Therefore, we have $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

Secondly, we show that $E(F) \not\supset \mathbf{Z}/32\mathbf{Z}$. Let $P_3 = (uv(u+v)(v+w), uvw(u+v)(v+w)(w+u))$. Then P_3 is a point of order 8 in $E(\mathbf{Q})$ and $[4]P_3 = (0,0)$. By making use of Lemma 2.1.3, we can find a point $P_4 = (x_4, y_4) \in E(F)$ of order 16 such that $[2]P_4 = P_3$ and

$$x_4 = \sqrt{\xi}\,\eta,$$

where

$$\begin{aligned}
\eta &= \sqrt{\xi} + \sqrt{\eta_1} + \sqrt{\eta_2} + \eta_3, \\
\xi &= uv(u+w)(v+w),\ \eta_1 = uw(u+v)(w+v), \\
\eta_2 &= vw(v+u)(w+u),\ \eta_3 = w(u+v).
\end{aligned}$$

Note that $\xi, \eta_1, \eta_2, \eta_3 \in \mathbf{Z}$ and $\eta \in \mathcal{O}_F$. Since $u^2 + v^2 = w^2$, $(u,v) = 1$ and η is symmetric with respect to u and v, we may assume that

$$u = 2mn,\ v = m^2 - n^2,\ w = m^2 + n^2,$$

where m and n are integers with $(m,n) = 1$, $m > n > 0$ and $m \not\equiv n \pmod 2$. Then we have

$$\begin{aligned}
\sqrt{\xi} &= 2m(m+n)\sqrt{mn(m^2-n^2)}, \\
\eta_1 &= 4m^3n(m^2+n^2)(m^2+2mn-n^2), \\
\eta_2 &= (m+n)^2(m^4-n^4)(m^2+2mn-n^2), \\
\eta_3 &= (m^2+n^2)(m^2+2mn-n^2).
\end{aligned}$$

We see that none of ξ, η_1 and η_2 is not a square in $\mathbf{Q}$ by making use of $(u,v) = 1$ and $u^2 + v^2 = w^2$ (see [8, p. 157]). We need the following lemma.

Lemma 2.3.2. *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 $\mathcal{O}_F$.*

[Proof of Lemma 2.3.2] 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' and 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 does not occur, 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 Lemma 2.3.2, it suffices to show that $\sqrt{l}$ does not divide η in $\mathcal{O}_F$.

(i) Assume that l divides m. Since l divides η_1, it follows from Lemma 2.2.1 that $\sqrt{l}$ divides η in $\mathcal{O}_F$ if and only if l divides both η_2 and η_3 in $\mathbf{Z}$. However, this implies that l divides n, which contradicts $(m,n)=1$. Hence $\sqrt{l}$ does not divide η in $\mathcal{O}_F$.

(ii) Assume that l divides n. Since l divides η_1, we see that $\sqrt{l}$ does not divide η in $\mathcal{O}_F$ in the same way as (i).

(iii) Assume that l divides $m-n$. Since l divides η_2, it follows from Lemma 2.2.1 that $\sqrt{l}$ divides η in $\mathcal{O}_F$ if and only if l divides both η_1 and η_3 in $\mathbf{Z}$. Since

$$\eta_3 = w(u+v) = \{(m-n)^2+2mn\}\{(m-n)(m+n)+2mn\},$$

we see that l divides η_3 if and only if l divides $2mn$. However, since l is odd and $(m,n)=(m-n,m)=(m-n,n)=1$, we know that l does not divide $2mn$. Hence $\sqrt{l}$ does not divide η in $\mathcal{O}_F$.

(iv) Assume that l divides $m+n$. Since l divides η_2, we see that $\sqrt{l}$ does not divide η in $\mathcal{O}_F$ in the same way as (iii).

(i), (ii), (iii) and (iv) imply that $\sqrt{l}$ does not divide η in $\mathcal{O}_F$. This completes the proof of the lemma. □

Now comparing Lemma 2.2.2 with Lemma 2.3.2, we easily see that x_4 is not a square in $\mathcal{O}_F$, that is, in F. It follows from Lemma 2.1.3 that P_4 is not in $2E(F)$.

By making use of Lemma 2.1.3, we can find a point $P_4' = (x_4', y_4') \in E(F)$ of order 16 such that $[2]P_4' = P_3 + Q_1 = P_3'$ and

$$x_4' = \sqrt{uv(u+w)(v-w)}\,\big\{\sqrt{uw(u-v)(w-v)} + \sqrt{vw(v-u)(w+u)} + \sqrt{uv(u+w)(v-w)} + w(u-v)\big\},$$

where $P_3' = (uv(u+w)(v-w), uvw(u-v)(v-w)(w+u))$ and $Q_1 = (-u^4, 0)$. Since x_4' is obtained by substituting $-v$ into v in x_4, it is easy to see that x_4' is not a square in F. Hence we know by Lemma 2.1.3 that $P_4' \notin 2E(F)$. Put $Q_2 := P_4' - P_4 \in E(F)$. Then we have $[2]Q_2 = P_3' - P_3 = Q_1$. Suppose that there exists a point $P \in E(F)$ of order 32. Then we have

$$[2]P = [a]P_4 + [b]Q_2$$

for some integers $a \in \{1,3,5,7,9,11,13,15\}$ and $b \in \{0,1,2,3\}$, since $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. 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 we have

$$[2](P+Q) = P_4 \text{ or } P_4'.$$

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, we obtain $E(F) \not\supset \mathbf{Z}/32\mathbf{Z}$.

Now we know that $E(F) \supset \langle Q_2 \rangle \oplus \langle P_4 \rangle \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. Consequently, we have $E(F)_{(2)} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. □

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

$$E(F)_{(2')} := \bigcup_{n:\mathrm{odd}} \{P \in E(F)\,;\, [n]P = O\}.$$

We can easily determine the structure of $E(F)_{(2')}$ by making use of Theorem 2.1.1 and Theorem 1 (ii) in [8], which implies that $E(\mathbf{Q}(\sqrt{D})) \not\supset \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$ for all square-free integers D.

Proposition 2.3.3. *Assume that* $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$. *Then we have* $E(F)_{(2')} \simeq \mathbf{Z}/3\mathbf{Z}$.

[Proof] It suffices to show that $E(F) \not\supset \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$, since Theorem 2.1.1 implies that $E(F) \not\supset \mathbf{Z}/6p\mathbf{Z}$ for any prime $p \neq 2$. Since (M, N) is a square-free integer or $(M, N) = 1$, there exist integers a and b with $(a, b) = 1$ such that $M = a^4 + 2a^3b$ and $N = b^4 + 2b^3a$ by Theorem 2.1.2 (iii). Let $P_0 = (x_0, y_0)$ be a point of order 3 in E. By the triplication formula, x_0 is a root of the equation

$$3x^4 + 4(M+N)x^3 + 6MNx^2 - M^2N^2 = 0.$$

Since there exists a point $P_1 = (a^2b^2, a^2b^2(a+b)^2) \in E(\mathbf{Q})$ of order 3, by making use of $M = a^4 + 2a^3b$ and $N = b^4 + 2b^3a$ we see that the left hand side of this equation has the following decomposition:

$$\begin{aligned} &3x^4 + 4(M+N)x^3 + 6MNx^2 - M^2N^2 \\ &\qquad = (x - a^2b^2)\{3x^3 + (a+2b)(b+2a)(2a^2 - ab + 2b^2)x^2 \\ &\qquad\qquad + a^2b^2(a+2b)^2(b+2a)^2x + a^4b^4(a+2b)^2(b+2a)^2\}. \end{aligned}$$

We denote by $f(x)$ the expression in the brace in this decomposition. If $E(F) \supset \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$, then $f(x)$ must be decomposed as a product of linear polynomials in F. Since the Galois group $\mathrm{Gal}(F/\mathbf{Q})$ has no element of order 3, there exists $\alpha \in \mathbf{Q}$ such that $f(\alpha) = 0$. Let D be the square-free part of $\alpha(\alpha + M)(\alpha + N)$ and let $\beta := \sqrt{\alpha(\alpha + M)(\alpha + N)}$. Then the point $P_2 = (\alpha, \beta)$ is of order 3 in $E(\mathbf{Q}(\sqrt{D}\,))$ and P_1 and P_2 generate $E[3]$. Hence we have $E(\mathbf{Q}(\sqrt{D}\,)) \supset E[3]$, which contradicts Theorem 1 (iii) in [8]. Therefore, we have $E(F) \not\supset \mathbf{Z}/3\mathbf{Z} \oplus \mathbf{Z}/3\mathbf{Z}$. □

In order to examine the structure of $E(F)_{(2)}$, we need the following elementary lemma.

Lemma 2.3.4. *Let $\alpha, \beta \in \mathbf{Q}$ and let γ 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 $\mathbf{Q}$.*

[Proof] If $\alpha + \beta\sqrt{\gamma}$ is a square in F, then it can be expressed as follows:

$$\alpha + \beta\sqrt{\gamma} = c(a + b\sqrt{\gamma}\,)^2,$$

where $c \in \mathbf{Q}$ and $a, b \in \mathbf{Z}$. This means that

$$\begin{cases} c(a^2 + b^2\gamma) = \alpha, \\ 2abc = \beta. \end{cases}$$

Then we see that $4(a^2c)^2 - 4\alpha(a^2c) + \beta^2\gamma = 0$. Hence we have

$$a^2c = \frac{\alpha \pm \sqrt{\alpha^2 - \beta^2\gamma}}{2} \in \mathbf{Q}.$$

Therefore, we obtain $\sqrt{\alpha^2 - \beta^2\gamma} \in \mathbf{Q}$. □

Since we have $E_D(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all square-free integers D by Theorem 2 (ii) in [8], it suffices to show the following.

Proposition 2.3.5. *Assume that $E(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ and $E_D(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all square-free integers D. Then we have $E(F)_{(2)} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.*

[Proof] By Lemma 2.1.3, the x-coordinate of a point P of order 4 on E equals one of the following:

$$\pm\sqrt{MN},\ -M \pm \sqrt{M(M-N)},\ -N \pm \sqrt{N(N-M)}.$$

Suppose that $E(F) \supset \mathbf{Z}/8\mathbf{Z}$. By Lemma 2.1.3, there exists a point $P = (x, y)$ of order 4 on $E(F)$ such that x, $x + M$ and $x + N$ are all squares in F.

Suppose that $x = \pm\sqrt{MN}$. By Lemma 2.2.4, $|MN|$ is a square in $\mathbf{Q}$. Hence, we may assume that $M = d_1^2 D$ and $N = \pm d_2^2 D$ for some square-free integer D (or $D = 1$) and some relatively prime integers d_1 and d_2. If $M = d_1^2 D$ and $N = d_2^2 D$, then the D-quadratic twist E_D of E is given by

$$E_D : y^2 = x\{x + (d_1 D)^2\}\{x + (d_2 D)^2\}.$$

Hence we have $E_D(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, which contradicts the assumption. Therefore, assume that $M = d_1^2 D$ and $N = -d_2^2 D$. Then we have

$$x + M = \pm d_1 d_2 D\sqrt{-1} + d_1^2 D.$$

By Lemma 2.3.4, if $x + M$ is a square in F, then we have $\sqrt{(d_1^2 D)^2 + (d_1 d_2 D)^2} \in \mathbf{Q}$, that is, $\sqrt{d_1^2 + d_2^2} \in \mathbf{Q}$. However, since the D-quadratic twist E_D of $E = E(M, N)$ is isomorphic over $\mathbf{Q}$ to an elliptic curve $E' = E_D(-N, M - N)$ given by

$$E' : y^2 = x\{x + (d_2 D)^2\}\{x + (d_1^2 + d_2^2)D^2\},$$

we must have $E_D(\mathbf{Q}) \simeq E'(\mathbf{Q}) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ by Theorem 2.1.2 (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 respectively M, N and x with $-M, N - M$ and $x + M$ (resp. with $-N, M - N$ and $x + N$) in the above argument. Therefore, we have $E(F) \not\supset \mathbf{Z}/8\mathbf{Z}$. Since it is clear that $E(F) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, we obtain the proposition. □

When $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, the structure of $E(F)_{(2)}$ depends on whether $E_{-1}(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$. Note that in this case $E_{-1}(\mathbf{Q})_{\mathrm{tors}}$ is isomorphic to either $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ (see [8, Theorem 2 (iii)]).

Proposition 2.3.6. *Assume that* $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. *If* $E_{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$, *then we have* $E(F)_{(2)} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. *Otherwise, we have* $E(F)_{(2)} \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

[Proof] We may assume that $M = s^2$ and $N = t^2$, where s and t are integers with $(s, t) = 1$ and $s > t > 0$. Then we have

$$E(\mathbf{Q})_{\mathrm{tors}} = \langle P_2 \rangle \oplus \langle Q_1 \rangle \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z},$$

where $P_2 = (st, st(s+t))$ and $Q_1 = (-s^2, 0)$. Note that $[2]P_2 = (0,0)$. By Lemma 2.1.3, we see that $E(F) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ and that 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

$$x(P_3) = st + s\sqrt{t(s+t)} + t\sqrt{s(s+t)} + (s+t)\sqrt{st},$$

$$x(Q_2) = -s^2 + s\sqrt{s^2 - t^2}.$$

Now we show that $P_3 \notin 2E(F)$. 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 2.2.4, st is a square in $\mathbf{Q}$. This means that there exist positive integers u and v such that $s = u^2$ and $t = v^2$ because of $(s,t) = 1$. Thus we have

$$\begin{aligned} x(P_3) + M &= u^2v^2 + u^2v\sqrt{u^2+v^2} + uv^2\sqrt{u^2+v^2} + (u^2+v^2)uv + u^4 \\ &= u(u+v)\sqrt{u^2+v^2}(v + \sqrt{u^2+v^2}\,). \end{aligned}$$

Since $(u,v) = 1$, we have $(v, u^2+v^2) = 1$. Note that by Theorem 2.1.2 (ii), u^2+v^2 is not a square in $\mathbf{Q}$, since $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. 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 we have

$$x(P_3) + M = uw(u+v)(2w + v\sqrt{2}\,).$$

Since $x(P_3) + M$ is a square in F, we can express $2w + v\sqrt{2}$ as follows:

$$2w + v\sqrt{2} = c(a + b\sqrt{2}\,)^2,$$

where $c \in \mathbf{Q}$ and $a, b \in \mathbf{Z}$ with $(a,b) = 1$. Then we have $c(a^2+2b^2) = 2w$ and $2abc = v$, which mean 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 the assumption that $(a,b) = 1$. 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 $\mathcal{O}_F$ because of $(v, u^2+v^2) = 1$ and Lemma 2.2.1. 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 $\mathcal{O}_F$, which contradicts Lemma 2.2.2. It follows that $x(P_3) + M$ is not a square in F. Therefore, from Lemma 2.1.3 we obtain $P_3 \notin 2E(F)$.

Case 1. $E_{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

In this case, by Theorem 2 (iii) in [8], $s^2 - t^2$ is not a square in $\mathbf{Q}$. Suppose that $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, that is, $Q_2 \in 2E(F)$. Then by Lemma 2.1.3, $x(Q_2)$, $x(Q_2)+M$ and $x(Q_2)+N$ are all squares in F. Since $x(Q_2)+M = s\sqrt{s^2-t^2}$, Lemma 2.2.4 implies that $x(Q_2) + M$ is a square in F if and only if $s^2 - t^2$ is a square in $\mathbf{Q}$, which contradicts the assumption. Hence we obtain $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. By making use of Lemma 2.1.3, we can find a point $P_3' \in E(F)$ of order 8 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 the expression $x(P_3)$, it is easy to see that $x(P_3') + M$ is not a square in F. Hence we know by Lemma 2.1.3 that $P_3' \notin 2E(F)$. Put $Q_2' := P_3' - P_3 \in E(F)$. Then we have $[2]Q_2' = P_2' - P_2 = Q_1$. Suppose that there exists a point $P \in E(F)$ of order 16. Then we have

$$[2]P = [a]P_3 + [b]Q_2'$$

for some integers $a \in \{1, 3, 5, 7\}$ and $b \in \{0, 1, 2, 3\}$, since $E(F) \not\supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Now we define a point $Q \in \langle P_3 \rangle \oplus \langle Q_2' \rangle$ as follows:

$$Q := \begin{cases} -\left[(a-1)/2\right] P_3 - \left[b/2\right] Q_2' & \text{if } b = 0, 2, \\ -\left[(a-1)/2\right] P_3 - \left[(b-1)/2\right] Q_2' & \text{if } b = 1, 3. \end{cases}$$

Then we have

$$[2](P + Q) = P_3 \text{ or } P_3'.$$

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, we obtain $E(F) \not\supset \mathbf{Z}/16\mathbf{Z}$. Consequently, we have $E(F)_{(2)} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

Case 2. $E_{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

In this case, by Theorem 2 (iii) in [8], $s^2 - t^2 = r^2$ for some positive integer r. Then we have $x(Q_2) = s(r-s)$. By Lemma 2.1.3, we know that there exists a point Q_3 of order 8 in $E(F)$ such that $[2]Q_3 = Q_2$ and

$$x(Q_3) = s\sqrt{r(r-s)} + (s-r)\sqrt{-rs} + r\sqrt{s(s-r)} + s(r-s).$$

Note that $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Thus we have

$$\begin{aligned} x(Q_3) + M &= s\sqrt{r(r-s)} + (s-r)\sqrt{-rs} + r\sqrt{s(s-r)} + rs \\ &= \sqrt{-rs}\left\{\frac{1}{\sqrt{2}}(\sqrt{s} - \sqrt{-r} + \sqrt{s-r}\,)\right\}^2. \end{aligned}$$

If $r = (r')^2$ and $s = (s')^2$ for some integers r' and s', then we must have $(s')^4 - (r')^4 = t^2$, which has no integral solution except $s' = r' = t = 0$. Hence rs is not a square in $\mathbf{Q}$ because of $(r, s) = 1$. It follows from Lemma 2.2.4 that $x(Q_3) + M$ is not a square in F. Therefore by Lemma 2.1.3, we have $Q_3 \notin 2E(F)$.

We show that $E(F) \not\supset \mathbf{Z}/16\mathbf{Z}$. By making use of Lemma 2.1.3, we can find a point $R_3 \in E(F)$ of order 8 such that $[2]R_3 = R_2$ and

$$\begin{aligned} x(R_3) = \sqrt{rt}\,\frac{1+\sqrt{-1}}{\sqrt{2}}&\left\{\frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}}\right\}^2 \\ &+ t\sqrt{r}\left\{\frac{1+\sqrt{-1}}{\sqrt{2}}\right\}^2 \frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} \\ &+ r\sqrt{t}\,\frac{1+\sqrt{-1}}{\sqrt{2}}\,\frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} + t(r\sqrt{-1} - t), \end{aligned}$$

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

$$\begin{aligned} x(R_3) + N = \sqrt{rt}\,\frac{1+\sqrt{-1}}{\sqrt{2}}&\left\{\frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} + \sqrt{r}\right\} \\ &\times \left\{\frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} + \sqrt{t}\,\frac{1+\sqrt{-1}}{\sqrt{2}}\right\}. \end{aligned}$$

Put

$$A := \frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} + \sqrt{r}$$

and

$$B := \frac{\sqrt{r+s}+\sqrt{r-s}}{\sqrt{2}} + \sqrt{t}\,\frac{1+\sqrt{-1}}{\sqrt{2}}.$$

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 F, that is, a square in $\mathcal{O}_F$.

First, suppose that there exists an odd prime l which divides the square-free part of t. Since $r < s$, $\sqrt{r+s}$ and $\sqrt{r-s}$ are linearly independent over $\mathbf{Z}$, and it is clear that l does not divide $(r+s, r-s)$. Hence by Lemma 2.2.1, $\sqrt{l}$ does not divide $\sqrt{r+s} + \sqrt{r-s}$ in $\mathcal{O}_F$, which means that $\sqrt{l}$ does not divide B in $\mathcal{O}_F$. If $\sqrt{r+s}$, $\sqrt{r-s}$ and $\sqrt{2r}$ are linearly indenpendent over $\mathbf{Z}$, then it is clear that

$\sqrt{l}$ does not divide A in $\mathcal{O}_F$ because of $(l, 2r) = 1$ and Lemma 2.2.1. Otherwise, the square-free part of $r + s$ equals that of $2r$, which is either 1 or 2, since either $r = 2mn$, $t = m^2 - n^2$, $s = m^2 + n^2$ or $r = m^2 - n^2$, $t = 2mn$, $s = m^2 + n^2$ for some relatively prime integers m and n. Then the square-free part of $r - s$ is either -1 or -2. Thus A can be expressed as follows:

$$A = a_0 + a_1\sqrt{-1} + a_2\sqrt{2} + a_3\sqrt{-2},$$

where a_0, a_1, a_2 and a_3 are integers. Hence by Lemma 2.2.1, there exists an integer i such that A is divisible not by $l^i\sqrt{l}$, but by l^i in $\mathcal{O}_F$. Therefore, for some integer e, $x(R_3) + N$ is divisible not by l^{e+1}, but by $l^e\sqrt{l}$ in $\mathcal{O}_F$. It follows from Lemma 2.2.2 that $x(R_3) + N$ is not a square in $\mathcal{O}_F$, which contradicts the assumption. Therefore, we see that 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. We easily see that $\sqrt{p}$ does not divide A in $\mathcal{O}_F$ in the same way as above. Since either $t = (t')^2$ or $t = 2(t')^2$ and either $r = 2mn$, $t = m^2 - n^2$, $s = m^2 + n^2$ or $r = m^2 - n^2$, $t = 2mn$, $s = m^2 + n^2$ for some relatively prime integers m and n, we can express B as follows:

$$B = a_0 + a_1\sqrt{-1} + a_2\sqrt{2} + a_3\sqrt{-2},$$

where a_0, a_1, a_2 and a_3 are integers. Hence by Lemma 2.2.1, there exists an integer i such that B is divisible not by $p^i\sqrt{p}$, but by p^i in $\mathcal{O}_F$. Therefore, for some integer e, $x(R_3) + N$ is divisible not by p^{e+1}, but by $p^e\sqrt{p}$ in $\mathcal{O}_F$. It follows from Lemma 2.2.2 that $x(R_3) + N$ is not a square in $\mathcal{O}_F$, which contradicts the assumption. Therefore, we see that either $r = (r')^2$ or $r = 2(r')^2$ for some integer r'. Accordingly, there exist three possibilities for r and t as follows:

(1) $r = (r')^2$, $t = (t')^2$;
(2) $r = 2(r')^2$, $t = (t')^2$;
(3) $r = (r')^2$, $t = 2(t')^2$.

If (1) occurred, then we would have $(r')^4 + (t')^4 = s^2$, which has no integral solution except $r' = t' = s = 0$. Hence (1) does not occur. If (2) occurred, then

$$r = 2mn,\ t = m^2 - n^2,\ s = m^2 + n^2$$

for some relatively prime integers m and n. Since $r = 2(r')^2$, there would exist integers m' and n' such that $m = (m')^2$ and $n = (n')^2$. Hence $(t')^2 = t = (m')^4 - (n')^4$,

which has no integral solution except $t' = m' = n' = 0$. Therefore, (2) does not occur. By replacing r, r' and t, t' with t, t' and r, r', respectively, we easily see that (3) does not occur. Consequently, $x(R_3) + N$ is not a square in F. By Lemma 2.1.3, we see that $R_3 \notin 2E(F)$.

Now let P_4, Q_4, R_4 be points of order 16 in E respectively such that

$$[2]P_4 = P_3,\ [2]Q_4 = Q_3,\ [2]R_4 = R_3,$$

and put

$$\begin{aligned}\mathcal{P} &:= \{P_4 + P\,;\, P \in E[8]\},\\ \mathcal{Q} &:= \{Q_4 + P\,;\, P \in E[8]\},\\ \mathcal{R} &:= \{R_4 + P\,;\, P \in E[8]\}.\end{aligned}$$

Then it is obvious that

$$E[16] = E[8] \sqcup \mathcal{P} \sqcup \mathcal{Q} \sqcup \mathcal{R}.$$

Since P_4, Q_4, R_4 can not be in $E(F)$, we obtain $E(F) \not\supset \mathbf{Z}/16\mathbf{Z}$. It follows that $E(F)_{(2)} \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. This completes the proof of Proposition 2.3.6. □

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

Proposition 2.3.7. ([20, Theorem 2 and Remark 2]) *Let E be an elliptic curve over $\mathbf{Q}$. Assume that $E(\mathbf{Q})_{\mathrm{tors}} = E(\mathbf{Q})_{(2)}$ and $E_D(\mathbf{Q})_{\mathrm{tors}} = E_D(\mathbf{Q})_{(2)}$ for all square-free integers D. Then we have $E(F)_{\mathrm{tors}} = E(F)_{(2)}$.*

Remark 2.3.8. Although Theorem 2 and Remark 2 in [20] 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 $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$, then we have $E_D(\mathbf{Q})_{\mathrm{tors}} = E_D(\mathbf{Q})_{(2)}$ for all square-free integers D ([8, Theorem 2]), (a) follows from Propositions 2.3.1 and 2.3.7, and (c) follows from Propositions 2.3.6 and 2.3.7 (note that by Theorem 2 (iii) in [8], $M - N$ is a square if and only if $E_{-1}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$). We obtain (b) just by combining Propositions 2.3.5 and 2.3.3. As for (d), if $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all D, then we obtain $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ from Propositions 2.3.5 and 2.3.7; if $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ (resp. $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$)

for some D, then we know from (a) (resp. (b)) that $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ (resp. $\mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$), since E is isomorphic to E_D over F for all square-free integers D; if $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ and $E_{-D}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ (resp. $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$) for some D, then we know from (c) that $E(F)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ (resp. $\mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$), since $E \simeq E_D$ over F. This completes the proof of Theorem 1. □

2.4 Theorem 2: A result in number fields of type $(2, \ldots, 2)$

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

Case 1. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

We may assume that $M = u^4$ and $N = v^4$, where u and v are integers with $(u, v) = 1$, $u > v > 0$ and $u^2 + v^2 = w^2$ for some positive integer w.

(I) By Lemma 2.1.3, $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ 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 $\sqrt{u^2 - v^2} \in K$. Therefore, $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ if and only if $\sqrt{-1}, \sqrt{u^2 - v^2} \in K$.

(II) We give a necessary and sufficient condition on which $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. Let $P_3 = (uv(u+w)(v+w), uvw(u+v)(v+w)(w+u)) \in E(\mathbf{Q})$ and $P_3' = P_3 + Q_1 \in E(\mathbf{Q})$, where $Q_1 = (-u^4, 0)$. Then P_3 and P_3' are of order 8 and $x(P_3') = uv(u+w)(v-w)$. Assume that $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. Then it is easy to see that either P_3 or P_3' is contained in $2E(K)$. By Lemma 2.1.3, this is equivalent to the condition that either $\sqrt{uv(u+w)(v+w)}, \sqrt{uw(u+v)(w+v)} \in K$ or $\sqrt{uv(u+w)(v-w)}, \sqrt{uw(u-v)(w-v)} \in K$. On account of (I), we obtain the following:

$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ if and only if either $\sqrt{-1} \notin K$ or $\sqrt{u^2 - v^2} \notin K$
and either $\sqrt{uv(u+w)(v+w)}, \sqrt{uw(u+v)(w+v)} \in K$
or $\sqrt{uv(u+w)(v-w)}, \sqrt{uw(u-v)(w-v)} \in K$.

(III) Assume that $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$. By Theorem 1 (a), there exists a point $P_4 \in E(F)$ of order 16 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 $[2]Q_2 = Q_1 = (-u^4, 0)$. Suppose that $P_4 \notin E(K)$. Then it is not difficult to see 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 we have $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, which contradicts Theorem 1 (a). Therefore, we must have $P_4 \in E(K)$. On account of (I) and (II), we obtain the following:

$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ if and only if

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

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

Case 2. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$.

By Theorem 1 (b), we may pay attention only to the 2-primary part of $E(K)_{\mathrm{tors}}$.

(I) By Lemma 2.1.3, $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ 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 2.1.3 and Theorem 1 (b), $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ if and only if $\sqrt{-1}, \sqrt{M}, \sqrt{N}, \sqrt{M-N} \in K$.

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

Case 3. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

We may assume that $M = s^2$ and $N = t^2$, where s and t are integers with $(s,t) = 1$ and $s > t > 0$. Put $r := \sqrt{s^2 - t^2}$.

(I) By Lemma 2.1.3, $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if $\sqrt{-s^2}$, $r\sqrt{-1} \in K$, namely, $\sqrt{-1}$, $r \in K$.

(II) Assume that $E(K) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. 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 $E(K) \supset \mathbf{Z}/8\mathbf{Z}$ if and only if either $P_2 \in 2E(K)$ or $P_2' \in 2E(K)$. By Lemma 2.1.3, this is equivalent to the condition that either $\sqrt{st}, \sqrt{s(s+t)}, \sqrt{t(s+t)} \in K$ or $\sqrt{-st}, \sqrt{s(s-t)}, \sqrt{t(t-s)} \in K$, that is, 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:

$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ if and only if either $\sqrt{-1} \notin K$ or $r \notin K$

and either $\sqrt{st}, \sqrt{s(s+t)} \in K$ or $\sqrt{-st}, \sqrt{s(s-t)} \in K$.

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

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 $[2]P_2 = P_1 = (0,0)$, $[2]Q_2 = Q_1 = (-s^2, 0)$ and $[2]R_2 = R_1 = (-t^2, 0)$. Then it is obvious that $E(K) \supset \mathbf{Z}/8\mathbf{Z}$ if and only if P_2, Q_2 or R_2 is contained in $2E(K)$. By Lemma 2.1.3, this is equivalent to the condition that

$$\begin{aligned} & \sqrt{st}, \sqrt{s(s+t)}, \sqrt{t(s+t)} \in K, \\ & \sqrt{s(r-s)}, \sqrt{rs}, \sqrt{r(-r+s)} \in K \\ \text{or} \quad & \sqrt{t(-t+r\sqrt{-1}\,)}, \sqrt{r(r+t\sqrt{-1}\,)}, \sqrt{rt\sqrt{-1}} \in K. \end{aligned}$$

Since

$$\begin{aligned} \sqrt{r(r+t\sqrt{-1}\,)} &= \pm\frac{\sqrt{2r}}{2}\left(\sqrt{r+s} + \sqrt{r-s}\right), \\ \sqrt{rt\sqrt{-1}} &= \pm\frac{\sqrt{2rt}}{2}(1+\sqrt{-1}\,) \\ \text{and} \quad t(-t+r\sqrt{-1}\,) &= \frac{1}{r^2}\left\{r(r+t\sqrt{-1}\,)\right\}\left\{rt\sqrt{-1}\right\}, \end{aligned}$$

the third condition can be replaced with the condition that

$$\sqrt{2rt}, \sqrt{2r(r+s)}, \sqrt{2r(r-s)} \in K$$

(note that $\sqrt{-1} \in K$ because of the assumption that $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$). Furthermore, since

$$\sqrt{2r(r-s)} = \frac{2rt\sqrt{-1}}{\sqrt{2r(r+s)}},$$

we see that $\sqrt{2r(r-s)} \in K$ if and only if $\sqrt{2r(r+s)} \in K$. Similarly, we see that $\sqrt{s(r-s)} \in K$ if and only if $\sqrt{s(r+s)} \in K$. Hence, $E(K) \supset \mathbf{Z}/8\mathbf{Z}$ 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 $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$). On account of (I), we obtain the following:

$E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ if and only if $\sqrt{-1}, r \in K$ and
$\sqrt{st}, \sqrt{s(s+t)} \in K$, $\sqrt{rs}, \sqrt{s(r+s)} \in K$ or $\sqrt{2rt}, \sqrt{2r(r+s)} \in K$.

(IV) We easily see that $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ 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 occurs only if $r \in \mathbf{Q}$.

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

Case 4. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

If $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ (resp. $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$) 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 $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ for some D, assume that $\sqrt{D} \notin K$; in the case where $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq E_{-D}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ for some D, assume that $\sqrt{D} \notin K$ and $\sqrt{-D} \notin K$.

Case 4.1. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ for some square-free integer D.
We may assume that $M = D(u')^4$ and $N = D(v')^4$, where u' and v' are positive integers with $(u', v') = 1$ such that $(u')^2 + (v')^2$ is a square. By Lemma 2.1.3, it is clear that $E(K) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ because of $\sqrt{D} \notin K$.

(I) By Lemma 2.1.3, $E(K) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if either $\sqrt{-D}$, $\sqrt{-D\{(u')^4 - (v')^4\}} \in K$ or $\sqrt{-D}, \sqrt{-D\{(v')^4 - (u')^4\}} \in K$, 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 $E(K) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. 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 $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, which contradicts Theorem 1 (a). Therefore, we obtain the following:

$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if
$\sqrt{-D} \in K$ and either $\sqrt{(u')^2 - (v')^2} \in K$ or $\sqrt{(v')^2 - (u')^2} \in K$.

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

Case 4.2. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ for some square-free integer D.

We may assume that $M = D(s')^2$ and $N = D(t')^2$, where s' and t' are positive integers with $(s', t') = 1$. By Lemma 2.1.3, it is clear that $E(K) \not\supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ because of $\sqrt{D} \notin K$.

(I) By Lemma 2.1.3, $E(K) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ 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 $\sqrt{(s')^2 - (t')^2} \in K$ or $\sqrt{(t')^2 - (s')^2} \in K$. Suppose that $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. Then, since $P_1 = (0, 0) \notin 2E(K)$, 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 $E(F) \supset \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$. It follows from Theorem 1 (c) that $E_{-D}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

Hence by assumption we have $\sqrt{-D} \notin K$, which contradicts the assumption that $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z} \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$. Therefore, we obtain the following:

$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if
$$\sqrt{-D} \in K \text{ and either } \sqrt{(s')^2 - (t')^2} \in K \text{ or } \sqrt{(t')^2 - (s')^2} \in K.$$

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

Case 4.3. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ or $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ for all square-free integers D.

Assume that $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ for some D. Then by Theorem 1 (b) we know that $E(F)_{(2')} \simeq E_D(F)_{(2')} \simeq \mathbf{Z}/3\mathbf{Z}$, and by Theorem 2.1.2 (iii) we know that the points of order 3 in $E(F)$ can be written as $(Da^2b^2, \pm D\sqrt{D}a^2b^2(a+b)^2)$ with some integers a and b. It follows from $\sqrt{D} \notin K$ that $E(K)_{(2')} = \{O\}$. Therefore, this case can be treated just as the case where $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all square-free integers D. Thus from Lemma 2.1.3, we easily obtain the following:

(I) $E(K) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ 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) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ if and only if $\sqrt{-1}, \sqrt{M}, \sqrt{N}, \sqrt{M-N} \in K$.

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

To sum up, we obtain the following.

Theorem 2. *Let E be an elliptic curve over $\mathbf{Q}$ given by $y^2 = x(x+M)(x+N)$, where M and N are integers with $M > N$. Assume that (M, N) is a square-free integer or $(M, N) = 1$. Let K be a number field of type $(2, \ldots, 2)$. Then $E(K)_{\mathrm{tors}}$ can be classified as follows*:

Case 1. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

We may assume that $M = u^4$ and $N = v^4$, where u and v are integers with $(u, v) = 1$, $u > v > 0$ and $u^2 + v^2 = w^2$ for some positive integer w.

(I) *$E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ if and only if $\sqrt{-1}, \sqrt{u^2 - v^2} \in K$.*

(II) *$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ if and only if either $\sqrt{-1} \notin K$ or $\sqrt{u^2 - v^2} \notin K$ and either $\sqrt{uv(u+w)(v+w)}, \sqrt{uw(u+v)(w+v)} \in K$ or $\sqrt{uv(u+w)(v-w)}$, $\sqrt{uw(u-v)(w-v)} \in K$.*

(III) *$E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$ if and only if $\sqrt{-1}, \sqrt{u^2 - v^2}, \sqrt{uv(u+w)(v+w)}$, $\sqrt{uw(u+v)(w+v)} \in K$.*

(IV) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$.

Case 2. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$.

(I) $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ *if and only if one of the following conditions holds*:

(i) $\sqrt{M}, \sqrt{N} \in K$,
(ii) $\sqrt{-M}, \sqrt{-M+N} \in K$,
(iii) $\sqrt{-N}, \sqrt{-N+M} \in K$.

(II) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$ *if and only if* $\sqrt{-1}, \sqrt{M}, \sqrt{N}, \sqrt{M-N} \in K$.

(III) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$.

Case 3. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

We may assume that $M = s^2$ *and* $N = t^2$, *where* s *and* t *are integers with* $(s,t) = 1$ *and* $s > t > 0$. *Put* $r := \sqrt{s^2 - t^2}$.

(I) $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *if and only if* $\sqrt{-1}, r \in K$.

(II) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ *if and only if either* $\sqrt{-1} \notin K$ *or* $r \notin K$ *and either* $\sqrt{st}, \sqrt{s(s+t)} \in K$ *or* $\sqrt{-st}, \sqrt{s(s-t)} \in K$.

(III) $E(K) \supset \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ *if and only if* $\sqrt{-1}, r \in K$ *and one of the following conditions holds*:

(i) $\sqrt{st}, \sqrt{s(s+t)} \in K$,
(ii) $\sqrt{rs}, \sqrt{s(r+s)} \in K$,
(iii) $\sqrt{2rt}, \sqrt{2r(r+s)} \in K$.

(IV) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ *if and only if* $\sqrt{-1}$, $r, \sqrt{rs}, \sqrt{st}, \sqrt{s(r+s)}, \sqrt{s(s+t)} \in K$.

Note that this case occurs only if $r \in \mathbf{Q}$.

(V) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$.

Case 4. $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

If $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ (*resp.* $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$, $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$) *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* $E_D(\mathbf{Q})_{\mathrm{tors}} \not\simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ *for some* D, *assume that* $\sqrt{D} \notin K$ (*in the case where* $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq E_{-D}(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *for some* D, *assume that* $\sqrt{D} \notin K$ *and* $\sqrt{-D} \notin K$).

Case 4.1. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$ *for some square-free integer* D.

We may assume that $M = D(u')^4$ *and* $N = D(v')^4$, *where* u' *and* v' *are positive integers with* $(u', v') = 1$ *such that* $(u')^2 + (v')^2$ *is a square.*

(I) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *if and only if* $\sqrt{-D} \in K$ *and either* $\sqrt{(u')^2 - (v')^2} \in K$ *or* $\sqrt{(v')^2 - (u')^2} \in K$.

(II) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Case 4.2. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *for some square-free integer* D.

We may assume that $M = D(s')^2$ *and* $N = D(t')^2$, *where* s' *and* t' *are positive integers with* $(s', t') = 1$.

(I) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *if and only if* $\sqrt{-D} \in K$ *and either* $\sqrt{(s')^2 - (t')^2} \in K$ *or* $\sqrt{(t')^2 - (s')^2} \in K$.

(II) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Case 4.3. $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ *or* $\mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/6\mathbf{Z}$ *for all square-free integers* D.

(I) $E(K) \supset \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *if and only if one of the following conditions holds*:

(i) $\sqrt{M}, \sqrt{N} \in K$,

(ii) $\sqrt{-M}, \sqrt{-M+N} \in K$,

(iii) $\sqrt{-N}, \sqrt{-N+M} \in K$.

(II) $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/4\mathbf{Z}$ *if and only if* $\sqrt{-1}, \sqrt{M}, \sqrt{N}, \sqrt{M-N} \in K$.

(III) *In all other cases,* $E(K)_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$.

Remark 2.4.1. The result of Qiu and Zhang ([20, Theorem 4]) is a part of Case 4.3 in Theorem 2. In fact, in Theorem 4 in [20], they classified $E(K)_{\mathrm{tors}}$ on the assumption that

$$M \text{ and } N \text{ are square-free integers, not equal to } \pm 1, \text{ with } (M, N) = 1,$$

which implies that $E(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ and $E_D(\mathbf{Q})_{\mathrm{tors}} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$ for all square-free integers D ([20, Lemma 2]).

Let G be one of those groups which appear in Theorem 2. Let 2^d denote the minimal degree over $\mathbf{Q}$ of those number fields K of type $(2, \ldots, 2)$ for which there exists an elliptic curve E over $\mathbf{Q}$ such that $E(K)_{\mathrm{tors}} \simeq G$. Close examination of each condition given in Theorem 2 showed the following:

- If $G \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/16\mathbf{Z}$, then we have $d = 4$.
- If $G \simeq \mathbf{Z}/4\mathbf{Z} \oplus \mathbf{Z}/12\mathbf{Z}$, then we have $d = 3$.

- If $G \simeq \mathbf{Z}/8\mathbf{Z} \oplus \mathbf{Z}/8\mathbf{Z}$, then we have $d = 4$.
- In all other cases, we have $d \leq 2$.

In particular, it is easy to see that Theorem 2 and the above imply Theorem 3 in [20] and Theorems 4.1 and 4.2 in [17], which are stated for $d = 2$.

Chapter 3

Maximal l-torsion of elliptic curves in isogeny classes

Let K be a number field. Merel proved the Uniform Boundedness Conjecture, which asserts that there exists a constant B, depending only on the degree of K over $\mathbf{Q}$, such that for any elliptic curve E over K the order $|E(K)_{\mathrm{tors}}|$ of the torsion subgroup of $E(K)$ is less than B (see Theorem 1.5.4). Before that, Ross ([22, Theorem 1]) gave an upper bound for $\min_{E' \in \mathcal{C}(E)} |E'(K)_{\mathrm{tors}}|$ assuming $\mathrm{End}_K(E) \simeq \mathbf{Z}$, where $\mathcal{C}(E)$ denotes the K-isogeny class of E. More precisely, he showed that there exists a constant C, divisible only by those primes dividing the number $w(K)$ of roots of unity in K, such that for any elliptic curve E over K with $\mathrm{End}_K(E) \simeq \mathbf{Z}$ there exists an elliptic curve E' in $\mathcal{C}(E)$ such that $|E'(K)_{\mathrm{tors}}|$ divides C (see also Nakamura [16, Theorem 1]). On the other hand, Katz ([6, Theorem 1(bis)]) described $\max_{E' \in \mathcal{C}(E)} |E'(K)_{\mathrm{tors}}|$ (without the extra assumption) in terms of the reduction $\widetilde{E_\wp}$ of E modulo each prime $\wp$ of K, although his description depends on the K-isogeny class under consideration.

Fix a prime number l. In this chapter, we give a necessary and sufficient condition for the order of the l-primary part $E(K)_{(l)}$ of $E(K)_{\mathrm{tors}}$ being maximal in $\mathcal{C}(E)$.

Theorem 3. *Let K be a number field, E an elliptic curve over K and l a prime number. Then we have $|E(K)_{(l)}| = \max_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$ if and only if for any K-isogeny f of degree l from E to an elliptic curve E' over K, we have $|E(K)_{(l)}| \geq |E'(K)_{(l)}|$.*

Note that for any K-isogeny $f : E \to E'$ of degree l, we have

$$|E'(K)_{\mathrm{tors}}| = \frac{1}{l}|E(K)_{\mathrm{tors}}|, \ |E(K)_{\mathrm{tors}}| \quad \text{or} \quad l|E(K)_{\mathrm{tors}}|$$

and that E has at most $l+1$ K-isogenies of degree l up to K-isomorphisms. It is also to be noted that even if we have $|E(K)_{(l)}| \leq |E'(K)_{(l)}|$ for any K-isogeny $f : E \to E'$ of degree l, $|E(K)_{(l)}|$ does not necessarily equal $\min_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$ in general (see Example 3.2.5).

Theorem 3 allows us to find $l^M := \max_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$ by composing K-isogenies of degree l because of the finiteness of K-isomorphism classes of elliptic curves in $\mathcal{C}(E)$. Before making use of Theorem 3, it is often a shorter way to find l^M that one checks conditions (sufficient for $|E(K)_{(l)}|$ being maximal in $\mathcal{C}(E)$) given in Proposition 3.1.6. We also make use of Proposition 3.1.6 in order to prove Theorem 3. Furthermore, we show that Proposition 3.1.6 and Theorem 3 imply several properties concerning the torsion of elliptic curves in their K-isogeny classes (see Corollaries 3.1.8, 3.1.10, 3.1.11, 3.1.12 and 3.2.3).

We now fix notation. Let K be a number field and $\overline{K}$ the algebraic closure of K. Denote by G_K the Galois group $\mathrm{Gal}(\overline{K}/K)$ of $\overline{K}$ over K. Let E be an elliptic curve over K. Fix a prime number l. Denote by $E(K)_{(l)}$ the l-primary part of $E(K)_{\mathrm{tors}}$ and by $T_l(E)$ the l-adic Tate module of E. Denote also by $w_l(K)$ the number of l-power-th roots of unity in K and let n be an integer such that $l^n = w_l(K)$. Furthermore, let $\mathcal{C}(E)$ be the K-isogeny class of E, and let M and m be integers such that $l^M = \max_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$ and $l^m = \min_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$, respectively.

3.1 Sufficient conditions for E having maximal l-torsion

In this section, we give some sufficient conditions for $|E(K)_{(l)}| = l^M$. Note that the section is also in a preparatory step of the proof of Theorem 3.

Throughout the section, we assume that $E(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^t\mathbf{Z}$ for some integers $s \geq t \geq 0$. For all integers $i > 0$, we identify $T_l(E)/l^iT_l(E)$ with $E[l^i]$. Now choose a basis $\{x, y\}$ for $T_l(E)$ such that $x \bmod l^s$, $y \bmod l^t \in E(K)$; if $t = 0$ (resp. $s = 0$), then take y (resp. x) arbitrarily as long as $\{x, y\}$ is a basis for $T_l(E)$. Let ρ_l be the l-adic representation attached to $\{x, y\}$. Then we have

$$\rho_l(\mathrm{G}_K) \subset \begin{pmatrix} 1 + l^s\mathbf{Z}_l & l^t\mathbf{Z}_l \\ l^s\mathbf{Z}_l & 1 + l^t\mathbf{Z}_l \end{pmatrix}.$$

For $\sigma \in \mathrm{G}_K$, we put

$$\rho_l(\sigma) := \begin{pmatrix} 1 + l^s a_\sigma & l^t b_\sigma \\ l^s c_\sigma & 1 + l^t d_\sigma \end{pmatrix}$$

with a_σ, b_σ, c_σ and d_σ in $\mathbf{Z}_l$. It occurs neither that $a_\sigma \equiv c_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ nor that $b_\sigma \equiv d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, since $E(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^t\mathbf{Z}$. On account of the Tchebotarev density theorem ([9, Theorem 10, p. 169]), the equations (1.3.1), (1.3.2) and Remark 1.3.5 in Chapter 1 imply that

$$\det(1 - \rho_l(\sigma)) \equiv 0 \pmod{l^M} \qquad \text{for all } \sigma \in \mathrm{G}_K \tag{3.1.1}$$

(see [6, Introduction]). We separate the possibilities of ρ_l into four cases.

Case 1. Either $a_\sigma \equiv b_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ or $c_\sigma \equiv d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$.

In this case, it is obvious from the fact (3.1.1) that $s + t < M$. More precisely, if $c_\sigma \equiv d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, put $E_1 := E/\langle x \bmod l \rangle$. Then there exists a K-isogeny $f_1 : E \to E_1$ of degree l and $|E_1(K)_{(l)}| = l^{s+t+1}$. Similarly, if $a_\sigma \equiv b_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, put $E_2 := E/\langle y \bmod l \rangle$. Then there exists a K-isogeny $f_2 : E \to E_2$ of degree l and $|E_2(K)_{(l)}| = l^{s+t+1}$.

Case 2. Either $a_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ or $d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, and there exist $\tau, \tau' \in \mathrm{G}_K$ such that b_τ, $c_{\tau'} \in \mathbf{Z}_l^\times$.

Lemma 3.1.1. *In Case 2, we have $s + t = M$.*

[Proof] Suppose that $s + t < M$. Then the fact (3.1.1) implies that

$$a_\tau d_\tau - b_\tau c_\tau \equiv a_{\tau'} d_{\tau'} - b_{\tau'} c_{\tau'} \equiv 0 \pmod{l^{M-(s+t)}}. \tag{3.1.2}$$

If either $c_\tau \in \mathbf{Z}_l^\times$ or $b_{\tau'} \in \mathbf{Z}_l^\times$, then the equation (3.1.2) would not hold. Thus we may assume that $c_\tau \equiv b_{\tau'} \equiv 0 \pmod{l}$. Now we have

$$\rho_l(\tau\tau') = \begin{pmatrix} 1 + l^s(a_\tau + a_{\tau'} + l^t b_\tau c_{\tau'} + l^s a_\tau a_{\tau'}) & l^t(b_\tau + b_{\tau'} + l^t b_\tau d_{\tau'} + l^s a_\tau b_{\tau'}) \\ l^s(c_\tau + c_{\tau'} + l^t d_\tau c_{\tau'} + l^s c_\tau a_{\tau'}) & 1 + l^t(d_\tau + d_{\tau'} + l^t d_\tau d_{\tau'} + l^s c_\tau b_{\tau'}) \end{pmatrix}.$$

If $t > 0$, then we have

$$\det(1 - \rho_l(\tau\tau')) \equiv -l^{s+t} b_\tau c_{\tau'} \pmod{l^{s+t+1}},$$

since $(a_\tau + a_{\tau'})(d_\tau + d_{\tau'}) \equiv c_\tau \equiv b_{\tau'} \equiv 0 \pmod{l}$ by assumption. Hence $b_\tau, c_{\tau'} \in \mathbf{Z}_l^\times$ implies that

$$\det(1 - \rho_l(\tau\tau')) \not\equiv 0 \pmod{l^{s+t+1}},$$

which contradicts the fact (3.1.1) and the assumption $s+t < M$. Therefore $s+t = M$. If $t = 0$, then by assumption we have

$$\begin{aligned}\det(1 - \rho_l(\tau\tau')) &\equiv l^s\{b_\tau c_{\tau'}(d_\tau + d_{\tau'} + d_\tau d_{\tau'}) - b_\tau c_{\tau'}(1 + d_\tau)(1 + d_{\tau'})\} \\ &= -l^s b_\tau c_{\tau'} \not\equiv 0 \pmod{l^{s+1}},\end{aligned}$$

which contradicts the fact (3.1.1) and the assumption $s = s + t < M$. Therefore $s + t = M$. This completes the proof of the lemma. □

Case 3. Either $b_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ or $c_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, and there exist $\tau, \tau' \in \mathrm{G}_K$ such that a_τ, $d_{\tau'} \in \mathbf{Z}_l^\times$.

Lemma 3.1.2. *In Case* 3 *we have* $s + t = M$.

We omit the proof, since we can prove this lemma in a fashion similar to the proof of Lemma 3.1.1.

Case 4. There exist $\tau_1, \tau_2, \tau_3, \tau_4 \in \mathrm{G}_K$ such that $a_{\tau_1}, b_{\tau_2}, c_{\tau_3}, d_{\tau_4} \in \mathbf{Z}_l^\times$.

We examine this case more precisely.

(i) $s < n$.

In this case, we have $s = t$ and for all $\sigma \in G_K$

$$a_\sigma + d_\sigma + l^s(a_\sigma d_\sigma - b_\sigma c_\sigma) \equiv 0 \pmod{l^{n-s}}, \tag{3.1.3}$$

since $\det \rho_l(\sigma) \equiv 1 \pmod{l^n}$ for all $\sigma \in \mathrm{G}_K$ (see the equation (1.2.1)).

Lemma 3.1.3. *In the case* (i) *of Case* 4, *we have* $s + t = M$.

[Proof] Suppose that there exists an elliptic curve $E' \in \mathcal{C}(E)$ such that $E'(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^w\mathbf{Z}$, where v and w are integers with $v + w = M > s + t = 2s$ and $v \geq w \geq 0$. Choose a basis $\{x', y'\}$ for $T_l(E')$ such that $x' \bmod l^v$, $y' \bmod l^w \in E'(K)$; if $w = 0$, then take y' arbitrarily as long as $\{x', y'\}$ is a basis for $T_l(E)$. Then the l-adic representation ρ_l' attached to $\{x', y'\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho_l'(\sigma) = \begin{pmatrix} 1 + l^v a_\sigma' & l^w b_\sigma' \\ l^v c_\sigma' & 1 + l^w d_\sigma' \end{pmatrix} \in \begin{pmatrix} 1 + l^v\mathbf{Z}_l & l^w\mathbf{Z}_l \\ l^v\mathbf{Z}_l & 1 + l^w\mathbf{Z}_l \end{pmatrix}$$

with $a'_\sigma, b'_\sigma, c'_\sigma$ and d'_σ in $\mathbf{Z}_l$. Since $T_l(E) \otimes \mathbf{Q}_l \simeq T_l(E') \otimes \mathbf{Q}_l$ as G_K-modules, we may assume that there exists a matrix $U = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ in $M_2(\mathbf{Z}_l) \cap \mathrm{GL}_2(\mathbf{Q}_l)$ such that $(x'\ y') = (x\ y)U$ and that at least one of the elements $\alpha, \beta, \gamma, \delta$ is in $\mathbf{Z}_l^\times$ (note that the matrix representation attached to $\{x', y'\}$ coincides with the one attached to $\{lx', ly'\}$). Now we have $\rho_l(\sigma)U = U\rho'_l(\sigma)$ for all $\sigma \in \mathrm{G}_K$, that is, for all $\sigma \in \mathrm{G}_K$,

$$\begin{cases} (l^s a_\sigma - l^v a'_\sigma)\alpha + l^s b_\sigma \gamma - l^v c'_\sigma \beta & = 0, \quad (3.1.4a) \\ (l^s a_\sigma - l^w d'_\sigma)\beta + l^s b_\sigma \delta - l^w b'_\sigma \alpha & = 0, \quad (3.1.4b) \\ (l^s d_\sigma - l^v a'_\sigma)\gamma + l^s c_\sigma \alpha - l^v c'_\sigma \delta & = 0, \quad (3.1.4c) \\ (l^s d_\sigma - l^w d'_\sigma)\delta + l^s c_\sigma \beta - l^w b'_\sigma \gamma & = 0. \quad (3.1.4d) \end{cases}$$

Note that for all $\sigma \in \mathrm{G}_K$,

$$l^w d'_\sigma \equiv l^s(a_\sigma + d_\sigma) + l^{2s}(a_\sigma d_\sigma - b_\sigma c_\sigma) - l^v a'_\sigma \pmod{l^M} \quad (3.1.5)$$

because of $\det \rho_l(\sigma) = \det \rho'_l(\sigma)$. Since $v \geq w$, we have $v > s$. The equations (3.1.4a) and (3.1.4c) imply that

$$a_\sigma \alpha + b_\sigma \gamma \equiv c_\sigma \alpha + d_\sigma \gamma \equiv 0 \pmod{l^{v-s}}$$

for all $\sigma \in \mathrm{G}_K$. If $\alpha, \gamma \in \mathbf{Z}_l^\times$, then the point

$$x + \frac{\gamma}{\alpha} y \mod l^v$$

of order l^v would be in $E(K)$, which contradicts the assumption. Hence either α or γ is divisible by l, and both are divisible by l. Therefore we have

$$\alpha \equiv \gamma \equiv 0 \pmod{l^{v-s}}.$$

Now by the assumption $2s < M$, we have $a_\sigma d_\sigma - b_\sigma c_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, since $\det(1 - \rho_l(\sigma)) = l^{2s}(a_\sigma d_\sigma - b_\sigma c_\sigma) \equiv 0 \pmod{l^M}$ for all $\sigma \in \mathrm{G}_K$. Hence by the equation (3.1.3) we have $a_\sigma + d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$. Since it follows from the equation (3.1.5) that $l^w d'_\sigma \equiv 0 \pmod{l^{s+1}}$ for all $\sigma \in \mathrm{G}_K$, the equations (3.1.4b), (3.1.4d) and $v + w - s > s$ imply that

$$a_\sigma \beta + b_\sigma \delta \equiv c_\sigma \beta + d_\sigma \delta \equiv 0 \pmod{l}$$

for all $\sigma \in \mathrm{G}_K$. For the same reason as above, we have $\beta \equiv \delta \equiv 0 \pmod{l}$, which contradicts the assumption that at least one of $\alpha, \beta, \gamma, \delta$ is in $\mathbf{Z}_l^\times$. Therefore, we have $s + t = 2s = M$. □

(ii) $s \geq n$.

In this case, we have $(s \geq) t = n$, since $\det \rho_l(\sigma) \equiv 1 \pmod{l^n}$ for all $\sigma \in \mathrm{G}_K$.

Lemma 3.1.4. *In the case* (ii) *of Case* 4*, assume further that there exists* $u \in \mathbf{Z}_l^\times$ *such that either*

$$a_\sigma + ub_\sigma \equiv 0 \pmod{l} \qquad \text{for all } \sigma \in \mathrm{G}_K$$

or

$$c_\sigma + ud_\sigma \equiv 0 \pmod{l} \qquad \text{for all } \sigma \in \mathrm{G}_K\,.$$

Then we have $s + t = M$*.*

[Proof] Let

$$U := \begin{pmatrix} 1 & 0 \\ l^{s-n}u & 1 \end{pmatrix}.$$

Then for all $\sigma \in \mathrm{G}_K$,

$$\begin{aligned} \rho_l'(\sigma) &:= U^{-1}\rho_l(\sigma)U \\ &= \begin{pmatrix} 1 + l^s(a_\sigma + ub_\sigma) & l^n b_\sigma \\ l^s(c_\sigma + ud_\sigma) - l^{2s-n}u(a_\sigma + ub_\sigma) & 1 + l^n d_\sigma - l^s u b_\sigma \end{pmatrix} \end{aligned}$$

Assume that $a_\sigma + ub_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$. Since $E(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$ and $s \geq n$, there exists $\tau \in \mathrm{G}_K$ such that $c_\tau + ud_\tau \in \mathbf{Z}_l^\times$. Hence by the assumption given in Case 4, we may write

$$\rho_l'(\sigma) = \begin{pmatrix} 1 + l^{s+1}a_\sigma' & l^n b_\sigma' \\ l^s c_\sigma' & 1 + l^n d_\sigma' \end{pmatrix} \in \begin{pmatrix} 1 + l^{s+1}\mathbf{Z}_l & l^n\mathbf{Z}_l \\ l^s\mathbf{Z}_l & 1 + l^n\mathbf{Z}_l \end{pmatrix}$$

for all $\sigma \in \mathrm{G}_K$, where there exist $\tau, \tau' \in \mathrm{G}_K$ such that $b_\tau', c_{\tau'}' \in \mathbf{Z}_l^\times$. Therefore, it follows from Lemma 3.1.1 that $s + t = s + n = M$.

We can also show that $s + t = M$ when $c_\sigma + ud_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ in the same way as above. □

Remark 3.1.5. In the case (ii) of Case 4, if the assumption given in Lemma 3.1.4 is not satisfied, that is, if for each $u \in \mathbf{Z}_l^\times$ there exist $\tau, \tau' \in \mathrm{G}_K$ such that $a_\tau + ub_\tau, c_{\tau'} + ud_{\tau'} \in \mathbf{Z}_l^\times$, then $s + t = M$ does not hold in general. We treat this case in Section 3.2.

Recall that $E(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^t\mathbf{Z}$ with integers $s \geq t \geq 0$. We now define two points P and Q in E depending on s and t as follows:

- $s \geq t > 0$. P and Q are points of order l^s and l^t, respectively, satisfying $E(K)_{(l)} = \langle P \rangle \oplus \langle Q \rangle$.

- $s > t = 0$. P is a K-rational point of order l^s, and if E has a K-rational subgroup Γ of order l which is not contained in $\langle P \rangle$, then Q is a point with $\langle Q \rangle = \Gamma$; otherwise, Q is the identity element O.
- $s = t = 0$. Q is O, and if E has a K-rational subgroup Γ of order l, then P is a point with $\langle P \rangle = \Gamma$; otherwise, P is O.

Putting $s' := \max\{s, 1\}$ and $t' := \max\{t, 1\}$, we further define two elliptic curves K-isogenous to E as follows:

$$E_1 := E/\langle [l^{s'-1}]P \rangle,\ E_2 := E/\langle [l^{t'-1}]Q \rangle.$$

Note that the G_K-stable subgroups $\langle [l^{s'-1}]P \rangle$ and $\langle [l^{t'-1}]Q \rangle$ are of order l if $P \neq O$ and $Q \neq O$.

With the above notation, the lemmas sum up to the following.

Proposition 3.1.6.

(a) *If $s = t < n$, then we have $s + t = M$.*

(b) *If $t < n$ and $|E_1(K)_{(l)}| = l^{s+t}$, then we have $s + t = M$.*

(c) *In the case where $t = n$, if $|E_1(K)_{(l)}| = l^{s+t}$, then we have $s + t = M$; if $|E_2(K)_{(l)}| = l^{s+t}$ and $Q \neq O$, then we have $s + t = M$.*

[Proof] If $P = Q = O$, then it is easy to find that $|E(K)_{(l)}| = l^{s+t} = 1$, since E has no K-isogeny of l-power-th degree. Hence we may assume that $P \neq O$.

(a) Since $s = t$, there exists a basis $\{x, y\}$ for $T_l(E)$ such that the l-adic representation ρ_l attached to $\{x, y\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho_l(\sigma) = \begin{pmatrix} 1 + l^s a_\sigma & l^s b_\sigma \\ l^s c_\sigma & 1 + l^s d_\sigma \end{pmatrix} \in \begin{pmatrix} 1 + l^s \mathbf{Z}_l & l^s \mathbf{Z}_l \\ l^s \mathbf{Z}_l & 1 + l^s \mathbf{Z}_l \end{pmatrix}.$$

Since $s < n$ and $\det \rho_l(\sigma) \equiv 1 \pmod{l^n}$ for all $\sigma \in \mathrm{G}_K$, this is in Case 2, in Case 3 or in the case (i) of Case 4. Thus Lemma 3.1.1, 3.1.2 or 3.1.3 implies that $s + t = M$.

(b) Since $t < n$, there exists a basis $\{x, y\}$ for $T_l(E)$ such that the l-adic representation ρ_l attached to $\{x, y\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho_l(\sigma) = \begin{pmatrix} 1 + l^s a_\sigma & l^t b_\sigma \\ l^s c_\sigma & 1 + l^n d_\sigma \end{pmatrix} \in \begin{pmatrix} 1 + l^s \mathbf{Z}_l & l^t \mathbf{Z}_l \\ l^s \mathbf{Z}_l & 1 + l^n \mathbf{Z}_l \end{pmatrix},$$

where there exists $\tau \in \mathrm{G}_K$ such that $b_\tau \in \mathbf{Z}_l^\times$. Then we may choose a basis $\{x_1, y_1\}$ for $T_l(E_1)$ such that $(x_1\ y_1) = (x\ y)U$, where $U = \left(\begin{smallmatrix} 1 & 0 \\ 0 & l \end{smallmatrix}\right)$, and the l-adic representation $\rho_{1,l}$ attached to $\{x_1, y_1\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho_{1,l}(\sigma) = U^{-1}\rho_l(\sigma)U = \begin{pmatrix} 1 + l^s a_\sigma & l^{t+1}b_\sigma \\ l^{s-1}c_\sigma & 1 + l^n d_\sigma \end{pmatrix}.$$

Hence if $|E_1(K)_{(l)}| = l^{s+t}$, then there exists $\tau' \in \mathrm{G}_K$ such that $c_{\tau'} \in \mathbf{Z}_l^\times$. It follows from $t < n$ and Lemma 3.1.1 that $s + t = M$.

(c) We may take $\{x, y\}$, ρ_l and $\{x_1, y_1\}$, $\rho_{1,l}$ as in the proof of (b). First, assume that $|E_1(K)_{(l)}| = l^{s+t}$. Since $t = n$, it is easy to see that $\{x_1 \bmod l^{s-1}, y_1 \bmod l^{n+1}\}$, $\{x_1 \bmod l^s, y_1 \bmod l^n\}$ or $\{x_1 + l^{s-n-1}uy_1 \bmod l^s, y_1 \bmod l^n\}$ (for some $u \in \mathbf{Z}_l^\times$) is a basis for $E_1(K)_{(l)}$ (note that the first possibility occurs only if $s = n$, since $\det \rho_{1,l}(\sigma) \equiv 1 \bmod l^n$ for all $\sigma \in \mathrm{G}_K$), namely, that $d_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, $c_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ or there exists $u \in \mathbf{Z}_l^\times$ such that $c_\sigma + ud_\sigma$ for all $\sigma \in \mathrm{G}_K$. Hence it follows from Lemma 3.1.1, 3.1.2 or 3.1.4 that $s+t = M$. Secondly, assume that $|E_2(K)_{(l)}| = l^{s+t}$ and $Q \neq O$. In the same way as above, we can show that $a_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, $b_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$ or there exists $u \in \mathbf{Z}_l^\times$ such that $a_\sigma + ub_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$. Hence it follows from Lemma 3.1.1, 3.1.2 or 3.1.4 that $s + t = M$. □

Remark 3.1.7.

(i) In Case 1, we have either $E_1(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^{t+1}\mathbf{Z}$ or $E_2(K)_{(l)} \simeq \mathbf{Z}/l^{s+1}\mathbf{Z}$ $\oplus \mathbf{Z}/l^t\mathbf{Z}$.

(ii) Proposition 3.1.6 (a) implies that if $E(K)_{(l)} = \{O\}$ and $n > 0$, then $M = 0$. This is also deduced from the properties of the Weil pairing (see [22, Proposition 2]).

Corollary 3.1.8. *Let*

$$v := \max\{N \in \mathbf{Z} \mid E'(K) \supset \mathbf{Z}/l^N\mathbf{Z},\ E' \in \mathcal{C}(E)\}.$$

Then there exists an elliptic curve E' in $\mathcal{C}(E)$ such that

$$E'(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^{M-v}\mathbf{Z}.$$

[Proof] We may assume that $v > 0$. Let

$$w := \max\{N \in \mathbf{Z} \mid E'(K) \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^N\mathbf{Z},\ E' \in \mathcal{C}(E)\}.$$

It suffices to show that $v+w=M$. If $w=n$, then it is obvious that $v+w=M$. Assume that $w<n$. If $v=w$, then we have $M=2v=v+w$ by Proposition 3.1.6 (a). If $v>w$, let E_0 be an elliptic curve in $\mathcal{C}(E)$ such that

$$E_0(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^w\mathbf{Z}$$

and let P_0 be a point in $E_0(K)$ of order l^v. Putting $E_1 := E_0/\langle [l^{v-1}]P_0 \rangle$, we have

$$E_1(K)_{(l)} \simeq \mathbf{Z}/l^{v-1}\mathbf{Z} \oplus \mathbf{Z}/l^{w+1}\mathbf{Z}$$

by the maximality of w and the assumption $w<n$. Therefore, we obtain $v+w=M$ from Proposition 3.1.6 (b). □

Remark 3.1.9. Let $M_{\mathrm{tors}} := \max_{E' \in \mathcal{C}(E)} |E'(K)_{\mathrm{tors}}|$ and $v_{\mathrm{tors}} := \max\{N \in \mathbf{Z} \mid E'(K) \supset \mathbf{Z}/N\mathbf{Z},\ E' \in \mathcal{C}(E)\}$. Applying Corollary 3.1.8 for each l, we see that there exists $E' \in \mathcal{C}(E)$ such that

$$E'(K)_{\mathrm{tors}} \simeq \mathbf{Z}/v_{\mathrm{tors}}\mathbf{Z} \oplus \mathbf{Z}/w_{\mathrm{tors}}\mathbf{Z},$$

where $w_{\mathrm{tors}} := M_{\mathrm{tors}}/v_{\mathrm{tors}}$.

If $s<n$, then we obtain an upper bound for M.

Corollary 3.1.10. *If $s<n$, then we have $M \leq 2s < 2n$.*

[Proof] If $t=s$, then we obtain $M=2s$ from Proposition 3.1.6 (a). Assume that $t<s$. Let $P \in E(K)$ be a point of order l^s and let $E_1 := E/\langle [l^{s-1}]P \rangle$. Then we have $|E_1(K)_{(l)}| \geq l^{s+t}$.

If $|E_1(K)_{(l)}| = l^{s+t}$, then we obtain $M = s+t < 2s$ from Proposition 3.1.6 (b). Suppose that $|E_1(K)_{(l)}| > l^{s+t}$. Then we have $E_1(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^{t+1}\mathbf{Z}$. If $t+1=s$, then we obtain $M=2s$ from Proposition 3.1.6 (a). If $t+1<s$, let $P' \in E'(K)$ be a point of order l^s and let $E_1'(K) := E_1/\langle [l^{s-1}]P' \rangle$. If $|E_1'(K)_{(l)}| = l^{s+t+1}$, then we obtain $M = s+t+1 < 2s$ from Proposition 3.1.6 (a). If $|E_1'(K)_{(l)}| > l^{s+t+1}$, repeat this process, and we will eventually find $E' \in \mathcal{C}(E)$ such that $E'(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^{t_0}\mathbf{Z}$ with $t \leq t_0 \leq s$ and $s+t_0=M$. □

Recall that m is an integer such that $l^m = \min_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$.

Corollary 3.1.11. *Assume that $T_l(E)$ is an irreducible G_K-module and that $E(K) \supset \mathbf{Z}/l^{2n+1}\mathbf{Z}$. Then we have $m=n$.*

[Proof] It follows from Lemma 2 in [16] that $m \leq n$. On the other hand, we have $m \geq n$ by Corollary 3.1.10. □

Note that if $\mathrm{End}_K(E) \simeq \mathbf{Z}$, then $T_l(E)$ is an irreducible G_K-module for all primes l (see Corollary 1.3.3 (a)).

Corollary 3.1.12. *There exists an elliptic curve E' in $\mathcal{C}(E)$ such that $E'(K)_{(l)} \simeq \mathbf{Z}/l^m\mathbf{Z}$.*

[Proof] Suppose that there exists $E_0 \in \mathcal{C}(E)$ such that

$$E_0(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^t\mathbf{Z}$$

and

$$T_l(E) = \mathbf{Z}_l\, x \oplus \mathbf{Z}_l\, y,$$

where $x \bmod l^s$, $y \bmod l^t \in E_0(K)$ and $s + t = m$ with $s \geq t > 0$. Then the l-adic representation ρ_l attached to $\{x, y\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho_l(\sigma) = \begin{pmatrix} 1 + l^s a_\sigma & l^t b_\sigma \\ l^s c_\sigma & 1 + l^t d_\sigma \end{pmatrix} \in \begin{pmatrix} 1 + l^s\mathbf{Z}_l & l^t\mathbf{Z}_l \\ l^s\mathbf{Z}_l & 1 + l^t\mathbf{Z}_l \end{pmatrix}.$$

If $b_\sigma \equiv c_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$, then there exist $\tau, \tau' \in \mathrm{G}_K$ such that $a_\tau, d_{\tau'} \in \mathbf{Z}_l^\times$. It follows from Proposition 3.1.6 (c) that $m = s+t = M$. Hence taking any $E' \in \mathcal{C}(E)$ with $E'(K)_{(l)}$ cyclic (see [16, Lemma 1]), we have $E'(K)_{(l)} \simeq \mathbf{Z}/l^m\mathbf{Z}$.

If there exists $\tau \in \mathrm{G}_K$ such that c_τ (resp. b_τ) $\in \mathbf{Z}_l^\times$, put $E' := E_0/\Gamma$ with $\Gamma := \langle x \bmod l^s \rangle$ (resp. $\langle y \bmod l^t \rangle$). It is obvious that $E'(K)_{(l)}$ is cyclic and $|E'(K)_{(l)}| \leq l^{s+t} = l^m$, that is, $E'(K)_{(l)} \simeq \mathbf{Z}/l^m\mathbf{Z}$. □

Remark 3.1.13.

(i) If $T_l(E)$ is an irreducible G_K-module, then Corollary 3.1.12 is a part of Lemma 3 in [16].

(ii) Let $m_{\mathrm{tors}} := \min_{E' \in \mathcal{C}(E)} |E'(K)_{\mathrm{tors}}|$. Applying Corollary 3.1.12 for each l, we see that there exists $E' \in \mathcal{C}(E)$ such that $E'(K)_{\mathrm{tors}} \simeq \mathbf{Z}/m_{\mathrm{tors}}\mathbf{Z}$.

3.2 Proof of Theorem 3

Assume still that $E(K)_{(l)} \simeq \mathbf{Z}/l^s\mathbf{Z} \oplus \mathbf{Z}/l^t\mathbf{Z}$ with integers $s \geq t \geq 0$. As in Section 3.1, choose a basis $\{x, y\}$ for $T_l(E)$ such that the l-adic representation ρ_l attached

to $\{x, y\}$ has the form:
for $\sigma \in \mathrm{G}_K$,

$$\rho_l(\sigma) = \begin{pmatrix} 1 + l^s a_\sigma & l^t b_\sigma \\ l^s c_\sigma & 1 + l^t d_\sigma \end{pmatrix}$$

with a_σ, b_σ, c_σ and d_σ in $\mathbf{Z}_l$. In this section, we consider the case with which we did not deal in Section 3.1 (note that it is contained in the case (ii) of Case 4). It is easy to see that the case where $s = 0$ is either in Case 1 or in the case where the assumption given in Proposition 3.1.6 (a) or (c) is satisfied. Hence, it remains to consider the case satisfying the following conditions:
(1) $s > 0$ and $t = n$;
(2) There exist $\tau_1, \tau_2, \tau_3, \tau_4 \in \mathrm{G}_K$ such that $a_{\tau_1}, b_{\tau_2}, c_{\tau_3}, d_{\tau_4} \in \mathbf{Z}_l^\times$;
(3) For each $u \in \mathbf{Z}_l^\times$, there exist $\tau, \tau' \in \mathrm{G}_K$ such that $a_\tau + ub_\tau, c_{\tau'} + ud_{\tau'} \in \mathbf{Z}_l^\times$.

Lemma 3.2.1. *Assume* (1), (2) *and* (3). *For* $u \in \mathbf{Z}_l^\times$, *put*

$$E^u := E/\langle ux + y \mod l \rangle.$$

Then we have $s + t < M$ *if and only if there exists* $u \in \mathbf{Z}_l^\times$ *such that* $E^u \in \mathcal{C}(E)$ *and* $|E^u(K)_{(l)}| = l^{s+t+1}$. *Note that the* G_K*-stable subgroups* $\langle ux + y \bmod l \rangle$ *are of order* l.

[Proof] It suffices to prove that if $s + t < M$, then there exists $u \in \mathbf{Z}_l^\times$ such that $E^u \in \mathcal{C}(E)$ and $|E^u(K)_{(l)}| = l^{s+t+1}$. Assume that $s+t = s+n < M$. Let $v := M-n$. Suppose that there exists $E' \in \mathcal{C}(E)$ such that $E'(K)_{(l)} \simeq \mathbf{Z}/l^{v'}\mathbf{Z} \oplus \mathbf{Z}/l^{w'}\mathbf{Z}$, where v' and w' are integers with $v' + w' = M$ and $v' \geq w' \geq 0$. If $w' < n$, put $E'' := E'/\langle x \mod l^{n-w'} \rangle$. Then we have

$$E''(K)_{(l)} \simeq \mathbf{Z}/l^v\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z},$$

since $v = M - n = v' + w' - n$. Hence we may assume that $v' = v$ and $w' = n$ by replacing E' with E'', if necessary. Let Γ be a cyclic G_K-stable subgroup of E such that $E' = E/\Gamma$.

Suppose that $\Gamma = \langle x + l^i uy \bmod l^r \rangle$ with $u \in \mathbf{Z}_l$ and some positive integers i and r. We may choose a basis $\{x', y'\}$ for $T_l(E')$ such that

$$(x'\ y') = (x\ y)U, \quad \text{where } U = \begin{pmatrix} 1 & 0 \\ l^i u & l^r \end{pmatrix}.$$

Then the l-adic representation ρ'_l attached to $\{x', y'\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\begin{aligned}\rho'_l(\sigma) &= U^{-1}\rho_l(\sigma)U \\ &= \begin{pmatrix} 1 + l^{n+i}ub_\sigma + l^s a_\sigma & l^{n+r}b_\sigma \\ l^{n+i-r}u(d_\sigma - l^i u b_\sigma) + l^{s-r}(c_\sigma - l^i u a_\sigma) & 1 + l^n(d_\sigma - l^i u b_\sigma) \end{pmatrix}.\end{aligned}$$

Since $y' \bmod l^n \in E'(K)$ and $E'(K) \supset \mathbf{Z}/l^n\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$, we must have $x' \bmod l^n \in E'(K)$, that is, for all $\sigma \in \mathrm{G}_K$ the $(2,1)$-component of the matrix $\rho'_l(\sigma)$ must be congruent with 0 modulo l^n. However, $E'(K) \supset \mathbf{Z}/l^{s+1}\mathbf{Z}$ implies that there exist $u_0 \in \mathbf{Z}_l$ and an integer $i_0 \geq 0$ such that $x' + l^{i_0}u_0 y' \bmod l^{s+1} \in E'(K)$, which does not occur, since for each $u' \in \mathbf{Z}_l$ there exists $\tau \in \mathrm{G}_K$ such that $c_\tau + u' d_\tau \in \mathbf{Z}_l^\times$ by assumption.

Suppose that $\Gamma = \langle l^i u x + y \bmod l^r \rangle$ with $u \in \mathbf{Z}_l$ and some positive integers i and r. We may choose a basis $\{x', y'\}$ for $T_l(E')$ such that

$$(x'\ y') = (x\ y)U, \quad \text{where } U = \begin{pmatrix} l^r & l^i u \\ 0 & 1 \end{pmatrix}.$$

Then the l-adic representation ρ'_l attached to $\{x', y'\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho'_l(\sigma) = \begin{pmatrix} 1 + l^s(a_\sigma - l^i u c_\sigma) & l^{n-r}(b_\sigma - l^i u d_\sigma) + l^{s+i-r}u(a_\sigma - l^i u c_\sigma) \\ l^{s+r}c_\sigma & 1 + l^n(d_\sigma + l^{s+i-n}u c_\sigma) \end{pmatrix}.$$

Since $x' \bmod l^n \in E'(K)$ and $E'(K) \supset \mathbf{Z}/l^n\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}$, we must have $y' \bmod l^n \in E'(K)$, that is, for all $\sigma \in \mathrm{G}_K$ the $(1,2)$-component of $\rho'_l(\sigma)$ must be congruent with 0 modulo l^n, which contradicts the assumption that there exists $\tau \in \mathrm{G}_K$ such that $b_\tau \in \mathbf{Z}_l^\times$.

Therefore, we may assume that $\Gamma = \langle ux + y \bmod l^r \rangle$ with $u \in \mathbf{Z}_l^\times$ and some positive integer r. When we choose a basis $\{x', y'\}$ for $T_l(E')$ such that

$$(x'\ y') = (x\ y)U, \quad \text{where } U = \begin{pmatrix} l^r & u \\ 0 & 1 \end{pmatrix},$$

the l-adic representation attached to $\{x', y'\}$ has the form:
for all $\sigma \in \mathrm{G}_K$,

$$\rho'_l(\sigma) = \begin{pmatrix} 1 + l^s(a_\sigma - u c_\sigma) & l^{n-r}(b_\sigma - u d_\sigma) + l^{s-r}u(a_\sigma - u c_\sigma) \\ l^{s+r}c_\sigma & 1 + l^n(d_\sigma + l^{s-n}u c_\sigma) \end{pmatrix}.$$

Note that the $(1,2)$-component of $\rho'_l(\sigma)$ is congruent with 0 modulo l^n for all $\sigma \in \mathrm{G}_K$, and that there exists $\tau \in \mathrm{G}_K$ such that $d_\tau + l^{s-n}uc_\tau \in \mathbf{Z}_l^\times$ by assumption. If there exists $\tau' \in \mathrm{G}_K$ such that $a_{\tau'} - uc_{\tau'} \in \mathbf{Z}_l^\times$, then Lemma 3.1.2 and $r > 0$ imply that $s + n = M$, which contradicts the assumption. Hence we have $a_\sigma - uc_\sigma \equiv 0 \pmod{l}$ for all $\sigma \in \mathrm{G}_K$. Therefore, when we put

$$E^u := E/\Gamma^u \quad \text{with} \quad \Gamma^u := \langle ux + y \mod l \rangle,$$

we see that

$$E^u(K)_{(l)} \simeq \mathbf{Z}/l^{s+1}\mathbf{Z} \oplus \mathbf{Z}/l^n\mathbf{Z}.$$

It is clear that $|\Gamma^u| = l$. This completes the proof of the lemma. □

Recall that $s' := \max\{s, 1\}$ and $t' := \max\{t, 1\}$; P and Q are points, more or less, of order l^s and l^t, respectively, satisfying $E(K)_{(l)} = \langle P \rangle \oplus \langle Q \rangle$ (see Section 3.1); $E_1 := E/\langle [l^{s'-1}]P \rangle$ and $E_2 := E/\langle [l^{t'-1}]Q \rangle$. We reformulate Lemma 3.2.1 in terms of these symbols.

Proposition 3.2.2. *Assume that $t = n$, $|E_1(K)_{(l)}| < l^{s+t}$ and either $|E_2(K)_{(l)}| < l^{s+t}$ or $Q = O$. For an integer u with $1 \le u \le l-1$, put*

$$E^u := E/\langle [l^{s'-1}u]P + [l^{t'-1}]Q \rangle.$$

Then we have $s + t < M$ if and only if there exists u such that $|E^u(K)_{(l)}| = l^{s+t+1}$. Note that the G_K-stable subgroups $\langle [l^{s'-1}u]P + [l^{t'-1}]Q \rangle$ are of order l.

[Proof] It is easy to find that the assumptions imply the conditions (1), (2) and (3). It follows immediately from the definitions of s', t' and P, Q that

$$ux + y \mod l = [l^{s'-1}u]P + [l^{t'-1}]Q.$$

Therefore, we obtain the proposition as a corollary of Lemma 3.2.1. □

Now Theorem 3 follows from Propositions 3.1.6 and 3.2.2.

[Proof of Theorem 3] It suffices to show that if $|E'(K)_{(l)}| \le |E(K)_{(l)}|$ for any K-isogeny f of degree l from E to an elliptic curve E' in $\mathcal{C}(E)$, then $|E(K)_{(l)}| = \max_{E \in \mathcal{C}(E)} |E'(K)_{(l)}|$. In Case 1, we have already seen that there exists a K-isogeny $f : E \to E'$ of degree l such that $|E'(K)_{(l)}| = l^{s+t+1}$. Next, in the case where there exist P, Q such that E and P, Q satisfy the assumption given in Proposition 3.1.6 (a), (b) or (c), $E(K)$ already has maximal l-torsion in $\mathcal{C}(E)$. Hence we may only

examine the case where the assumptions given in Proposition 3.2.2 are satisfied. Therefore, Theorem 3 follows from Proposition 3.2.2. □

The following corollary is obtained immediately from Theorem 3.

Corollary 3.2.3. *Let $|E(K)_{(l)}| = l^N$ for some integer N with $N < M$. Then there exists a K-isogeny f from E to an elliptic curve E' in $\mathcal{C}(E)$ such that $|E'(K)_{(l)}| = l^M$ and* $\mathrm{Ker}\, f = \mathbf{Z}/l^{M-N}\mathbf{Z}$.

[Proof] By Theorem 3, there exist $E' \in \mathcal{C}(E)$ and $f : E \to E'$ such that $|E'(K)_{(l)}| = l^M$ and $\deg f = l^{M-N}$. The cyclicity of $\mathrm{Ker}\, f$ follows from Lemma 6.2 in [12], which asserts that any K-isogeny of minimal degree between elliptic curves over K has a cyclic kernel. □

Remark 3.2.4. Let $M_{\mathrm{tors}} := \max_{E' \in \mathcal{C}(E)} |E(K)_{\mathrm{tors}}|$. Applying Corollary 3.2.3 for each l, we see that if we put $D := M_{\mathrm{tors}}/|E(K)_{\mathrm{tors}}|$, then there exist $E' \in \mathcal{C}(E)$ and a K-isogeny $f : E \to E'$ such that $|E'(K)_{\mathrm{tors}}| = M_{\mathrm{tors}}$ and $\mathrm{Ker}\, f \simeq \mathbf{Z}/D\mathbf{Z}$.

The following example shows that even if we have $|E(K)_{(l)}| \leq |E'(K)_{(l)}|$ for any K-isogeny $f : E \to E'$ of degree l, $|E(K)_{(l)}|$ does not necessarily equal $\min_{E' \in \mathcal{C}(E)} |E'(K)_{(l)}|$ in general.

Example 3.2.5. Let E be an elliptic curve given by

$$E : y^2 = x(x^2 + 4).$$

Then

$$E(\mathbf{Q})_{(2)} = \{O, (0,0), (2, \pm 4)\} \simeq \mathbf{Z}/4\mathbf{Z}.$$

Let $K = \mathbf{Q}$ and $l = 2$. Put $E_1 := E/\langle (0,0) \rangle$. Then $E_1 \in \mathcal{C}(E)$ and E_1 is given by

$$E_1 : y^2 = x(x^2 - 1).$$

Thus we have

$$E_1(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}$$

(which means that $M = 2$ by Proposition 3.1.6 (b)). Put $E_2 := E/\langle (2,4) \rangle$. Then $E_2 \in \mathcal{C}(E)$ and E_2 is given by

$$E_2 : y^2 = x(x^2 - 6x + 1).$$

Since we see that

$$E_2(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z},$$

we obtain $m = 1$ from Proposition 3.1.6 (a). On the other hand, it follows from

$$E[2] = \{O, (0,0), (\pm 2\sqrt{-1}, 0)\}$$

that the only $\mathrm{G}_{\mathbf{Q}}$-stable subgroup of order 2 of E is $\langle (0,0) \rangle$. Therefore, for every elliptic curve E' over $\mathbf{Q}$ which has a $\mathbf{Q}$-isogeny of degree 2 to E, we have $|E'(\mathbf{Q})_{(2)}| = 4 > 2^m = 2$.

We conclude this chapter by taking some examples, in which we find "M" (and "m").

Example 3.2.6. Let $l = 2$, $K = \mathbf{Q}$ and

$$E : y^2 = x(x-2)(x-8).$$

Then we have

$$E(\mathbf{Q})_{(2)} = \{O, (0,0), (2,0), (8,0)\} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

Put $E_1 := E/\langle (0,0) \rangle$. Then E_1 is given by

$$E_1 : y^2 = x(x-2)(x+16).$$

Thus we have

$$E_1(\mathbf{Q})_{(2)} \simeq \mathbf{Z}/2\mathbf{Z} \oplus \mathbf{Z}/2\mathbf{Z}.$$

Therefore, we obtain $M = 2$ from Proposition 3.1.6 (c). On the other hand, put $E_2 := E/\langle (2,0) \rangle$. Then E_2 is given by

$$E_2 : y^2 = x(x^2 + 2x + 4).$$

Thus we have

$$E_2(\mathbf{Q}) \simeq \mathbf{Z}/2\mathbf{Z}.$$

Therefore, since $n = 1 > 0$, we obtain $m = 1$ from Proposition 3.1.6 (a).

Example 3.2.7. Let $l = 3$, $K = \mathbf{Q}$ and

$$E : y^2 = x^3 + 4.$$

Then we have

$$E(\mathbf{Q})_{(3)} = \{O, (0, \pm 2)\} \simeq \mathbf{Z}/3\mathbf{Z}.$$

Put $E_1 := E/\langle(0,2)\rangle$. Then E_1 is given by

$$E_1 : y^2 = x^3 - 108.$$

Thus we have

$$E_1(\mathbf{Q})_{(3)} = \{O\},$$

which means that $m = 0$. Since

$$E[3] = \{O, (0, \pm 2), (\theta, \pm 2\sqrt{-3}), (\omega\theta, \pm 2\sqrt{-3}), (\omega^2\theta, \pm 2\sqrt{-3})\},$$

where $\theta := -2\sqrt[3]{2}$ and $\omega := (-1+\sqrt{-3})/2$, we see that the only $G_{\mathbf{Q}}$-stable subgroup of order 3 of E is $\langle(0,2)\rangle = \langle(0,-2)\rangle$. Therefore, we obtain $M = 1$ from Theorem 3.

Example 3.2.8. Let $l = 2$, $K = \mathbf{Q}(\sqrt{-1})$ and

$$E : y^2 = x(x^2 - 2\sqrt{-1}x - 3).$$

Then we have

$$E(K)_{(2)} = \{O, (0,0)\} \simeq \mathbf{Z}/2\mathbf{Z}.$$

Hence, since $n = 2 > 0$, we obtain $m = 1$ from Proposition 3.1.6 (a). Put $E_1 := E/\langle(0,0)\rangle$. Then E_1 is given by

$$E_1 : y^2 = x(x^2 + 4\sqrt{-1}x + 8).$$

Thus we have

$$E_1(K)_{(2)} \simeq \mathbf{Z}/2\mathbf{Z}.$$

Therefore, we obtain $M = 1$ from Proposition 3.1.6 (b).

Bibliography

[1] A. Borel, S. Cowla, C. S. Herz, K. Iwasawa and J.-P. Serre, *Seminar on Complex Multiplication*, Lecture Notes in Math. 21, Springer-Verlag, Berlin, 1966.

[2] G. Faltings, Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, Invent. Math. 73 (1983), 349–366.

[3] N. Husemöller, *Elliptic Curves*, Springer-Verlag, New York, 1987.

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

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

[6] N. M. Katz, Galois properties of torsion points on abelian varieties, Invent. Math. 62 (1981), 481–502.

[7] A. W. Knapp, *Elliptic Curves*, Princeton Univ. Press, Princeton, NJ, 1992.

[8] S. Kwon, Torsion subgroups of elliptic curves over quadratic extensions, J. Number Theory 62 (1997), 144–162.

[9] S. Lang, *Algebraic Number Theory*, Springer-Verlag, New York, 1986.

[10] M. Laska and M. Lorenz, Rational points on elliptic curves over $\mathbf{Q}$ in elementary abelian 2-extensions of $\mathbf{Q}$, J. Reine Angew Math. 355 (1985), 163–172.

[11] Yu. I. Manin, The p-torsion of elliptic curves is uniformly bounded, Math. USSR-Izvestija 3 (1969), 433–438.

[12] D. W. Masser and G. Wüstholz, Estimating isogenies on elliptic curves, Invent. Math. 100 (1990), 1–24.

[13] B. Mazur, Modular curves and the Eisenstein ideal, Inst. Hautes Études Sci. Publ. Math. 47 (1977), 33–186.

[14] B. Mazur, Rational isogenies of prime degree, Invent. Math. 44 (1978), 129–162.

[15] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Invent. Math. 124 (1996), 437–449.

[16] T. Nakamura, Cyclic torsion of elliptic curves, Proc. Amer. Math. Soc. 127 (1999), 1589–1595.

[17] K. Ohizumi, Rational torsion points of elliptic curves and certain quartic extensions (Japanese), Master's Thesis submitted to Tohoku University, 2001 (March).

[18] K. Ono, Euler's concordant forms, Acta Arith. 78 (1996), 101–123.

[19] T. Ono, *Variations on a Theme of Euler*, Plenum Press, New York, 1994.

[20] D. Qiu and X. Zhang, Elliptic curves and their torsion subgroups over number fields of type $(2, 2, \ldots, 2)$, Sci. China Ser. A 44 (2001), 159–167.

[21] K. A. Ribet, Torsion points of abelian varieties in cyclotomic extensions (Appendix to N. M. Katz and S. Lang, Finiteness theorems in geometric classfield theory), L'Enseignement Math. 27 (1981), 315–319.

[22] R. Ross, Minimal torsion in isogeny classes of elliptic curves, Trans. Amer. Math. Soc. 344 (1994), 203–215.

[23] J.-P. Serre, *Abelian l-adic Representations and Elliptic Curves*, Benjamin, New York, 1968.

[24] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. 15 (1972), 259–331.

[25] J.-P. Serre and J. Tate, Good reduction of abelian varieties, Ann. of Math. 68 (1968), 492–517.

[26] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Forms*, Princeton Univ. Press, Princeton, NJ, 1971.

[27] A. Silverberg, Points of finite order on abelian varieties, in *p-adic Methods in Number Theory and Algebraic Geometry*, 175–193, Contemp. Math. 133, Amer. Math. Soc., Providence, RI, 1992.

[28] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1986.

[29] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, New York, 1994.

[30] J. H. Silverman, A survey of the arithmetic theory of elliptic curves, in *Modular Forms and Fermat's Last Theorem*, G. Cornell, J. H. Silverman and G. Stevens ed., Springer-Verlag, 1997, 17–40.

[31] J. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966), 134–144.

[32] J. Tate, The arithmetic of elliptic curves, Invent. Math. 23 (1974), 179–206.

Tohoku Mathematical Publications

No.1 Hitoshi Furuhata: *Isometric pluriharmonic immersions of Kähler manifolds into semi-Euclidean spaces*, 1995.

No.2 Tomokuni Takahashi: *Certain algebraic surfaces of general type with irregularity one and their canonical mappings*, 1996.

No.3 Takeshi Ikeda: *Coset constructions of conformal blocks*, 1996.

No.4 Masami Fujimori: *Integral and rational points on algebraic curves of certain types and their Jacobian varieties over number fields*, 1997.

No.5 Hisatoshi Ikai: *Some prehomogeneous representations defined by cubic forms*, 1997.

No.6 Setsuro Fujiié: *Solutions ramifiées des problèmes de Cauchy caractéristiques et fonctions hypergéométriques à deux variables*, 1997.

No.7 Miho Tanigaki: *Saturation of the approximation by spectral decompositions associated with the Schrödinger operator*, 1998.

No.8 Y. Nishiura, I. Takagi and E. Yanagida: *Proceedings of the International Conference on Asymptotics in Nonlinear Diffusive Systems — towards the Understanding of Singularities in Dissipative Structures —*, 1998.

No.9 Hideaki Izumi: *Non-commutative L^p-spaces constructed by the complex interpolation method*, 1998.

No.10 Youngho Jang: *Non-Archimedean quantum mechanics*, 1998.

No.11 Kazuhiro Horihata: *The evolution of harmonic maps*, 1999.

No.12 Tatsuya Tate: *Asymptotic behavior of eigenfunctions and eigenvalues for ergodic and periodic systems*, 1999.

No.13 Kazuya Matsumi: *Arithmetic of three-dimensional complete regular local rings of positive characteristics*, 1999.

No.14 Tetsuya Taniguchi: *Non-isotropic harmonic tori in complex projective spaces and configurations of points on Riemann surfaces*, 1999.

No.15 Taishi Shimoda: *Hypoellipticity of second order differential operators with sign-changing principal symbols*, 2000.

No.16 Tatsuo Konno: *On the infinitesimal isometries of fiber bundles*, 2000.

No.17 Takeshi Yamazaki: *Model-theoretic studies on subsystems of second order arithmetic*, 2000.

No.18 Daishi Watabe: *Dirichlet problem at infinity for harmonic maps*, 2000.

No.19 Tetsuya Kikuchi: *Studies on commuting difference systems arising from solvable lattice models*, 2000.

No.20 Seiki Nishikawa: *Proceedings of the Fifth Pacific Rim Geometry Conference*, 2001.

No.21 Mizuho Ishizaka: *Monodromies of hyperelliptic families of genus three curves*, 2001.

No.22 Keisuke Ueno: *Constructions of harmonic maps between Hadamard manifolds*, 2001.

No.23 Hiroshi Sato: *Studies on toric Fano varieties*, 2002.

No.24 Hiroyuki Kamada: *Self-dual Kähler metrics of neutral signature on complex surfaces*, 2002.

No.25 Reika Fukuizumi: *Stability and instability of standing waves for nonlinear Schrödinger equations*, 2003.

No.26 Tôru Nakajima: *Stability and singularities of harmonic maps into spheres*, 2003.

No.27 Yasutsugu Fujita: *Torsion of elliptic curves over number fields*, 2003.

Tohoku Mathematical Publications

Mathematical Institute
Tohoku University
Sendai 980-8578, Japan