Bull. Korean Math. Soc. **50** (2013), No. 1, pp. 83–96
http://dx.doi.org/10.4134/BKMS.2013.50.1.083

TORSION POINTS OF ELLIPTIC CURVES WITH BAD REDUCTION AT SOME PRIMES II

Masaya Yasuda

Abstract. Let K be a number field and fix a prime number p. For any set S of primes of K, we here say that an elliptic curve E over K has S-reduction if E has bad reduction only at the primes of S. There exists the set $B_{K,p}$ of primes of K satisfying that any elliptic curve over K with $B_{K,p}$-reduction has no p-torsion points under certain conditions. The first aim of this paper is to construct elliptic curves over K with $B_{K,p}$-reduction and a p-torsion point. The action of the absolute Galois group on the p-torsion subgroup of E gives its associated Galois representation $\overline{\rho}_{E,p}$ modulo p. We also study the irreducibility and surjectivity of $\overline{\rho}_{E,p}$ for semistable elliptic curves with $B_{K,p}$-reduction.

1. Introduction

Let E be an elliptic curve over a number field K. For a prime number p, the p-torsion points of E are the points of finite order p in the Mordell-Weil group $E(K)$. In [14], we studied the existence of a p-torsion points of E which has bad reduction only at some primes, and showed the following [14, Theorem 1.2]. Let ζ_p denote a fixed primitive p-th root of unity.

Theorem 1.1. *Let K be a number field. Let $p \geq 5$ be a prime number such that the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p. Set*

$$B_{K,p} = \{\mathfrak{q} : \textit{prime of } K \textit{ over a prime } \ell \mid \ell \neq p \textit{ and } \ell^f \not\equiv \pm 1 \bmod p\},$$

where f is the residue degree of $\mathfrak{q}$. Let E be an elliptic curve over K with $B_{K,p}$-reduction. If p does not divide the class number $h_{K(\zeta_p)}$ of $K(\zeta_p)$, then E has no p-torsion points.

Fix a prime number $p \geq 5$ with $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p. It follows by Theorem 1.1 that $h_{K(\zeta_p)}$ is divisible by p if there exists E over K with $B_{K,p}$-reduction and a p-torsion point. The motivation of this paper arises from the question whether we can construct such pairs (E, K). We here focus

Received April 25, 2011; Revised May 7, 2012.
2010 *Mathematics Subject Classification.* Primary 14H52; Secondary 14G05.
Key words and phrases. reduction of elliptic curves, torsion points, Galois representation.

on the case where K is a quadratic field. Kamienny [2] and Kenku-Momose [3] classified the possible torsion subgroups of elliptic curves over quadratic fields K, and showed that any elliptic curve over K cannot have p-torsion points for the primes $p \geq 17$. Hence it is sufficient to consider the cases $p = 5, 7, 11$ and 13. In the cases $p = 5$ and 7, we construct such pairs (E, K) using Kubert's parametrization [5, Table 3] for an infinite family of elliptic curves with a p-torsion point. Furthermore, we list such pairs (E, K) and their $h_{K(\zeta_p)}$. For the cases $p = 11$ and 13, Jeon, Kim and Lee [1] gave an infinite family of elliptic curves E over quadratic fields K with a p-torsion point. On the contrary to the cases $p = 5$ and 7, we show that an elliptic curve from the family given by Jeon, Kim and Lee cannot have $B_{K,p}$-reduction with very high probability.

Let G_K denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. The action of G_K on the p-torsion subgroup $E[p]$ gives its associated Galois representation

$$\overline{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p)$$

modulo p. We also study the irreducibility and surjectivity of $\overline{\rho}_{E,p}$ for semistable elliptic curves E with $B_{K,p}$-reduction. Using a part of Serre's results [11], Mazur [7] studied the surjectivity of $\overline{\rho}_{E,p}$ for semistable elliptic curves E over $\mathbb{Q}$. Furthermore, Kraus [4] extended Mazur's work to the case where K is a quadratic field. We then focus on the case where K is a cubic field. We mainly consider the irreducibility of $\overline{\rho}_{E,p}$. If $\overline{\rho}_{E,p}$ is reducible, then we have

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix},$$

where $\phi_i : G_K \to \mathbb{F}_p^\times$ is a character for $i = 1, 2$. For semistable elliptic curves E with good reduction at the primes of K over p, we show that each ϕ_i has a structure of an $\mathcal{O}_K$-group scheme of order p, where $\mathcal{O}_K$ is the ring of integers of K. Our main idea is to classify the structure of $\mathcal{O}_K$-group schemes of order p for cubic fields K and show that either of ϕ_i is a trivial character under certain conditions. We obtain the following result on the irreducibility of $\overline{\rho}_{E,p}$.

Theorem 1.2. *Let p be an odd prime number. Let K be a cubic field with $\gcd(p-1, h_K^+) = 1$, where h_K^+ is the narrow class number of K. Suppose that $p \nmid h_{K(\zeta_p)}$ and $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p. Let E be a semistable elliptic curve over K with $B_{K,p}$-reduction. If p satisfies either of the following conditions, then $\overline{\rho}_{E,p}$ is irreducible.*

(A) *p is prime in $\mathcal{O}_K$.*
(B) *In the case where K is a totally real cubic field, we have $p \nmid \mathrm{Nm}_{K/\mathbb{Q}}(u^2-1)$ or $\mathrm{Nm}_{K/\mathbb{Q}}(v^2-1)$, where u, v are two independent fundamental units of K and $\mathrm{Nm}_{K/\mathbb{Q}}$ denotes the norm map. In the case where K is a complex cubic field, we have $p \nmid \mathrm{Nm}_{K/\mathbb{Q}}(u-1)$, where u is a fundamental unit of K such that $u > 0$ with respect to the only one real place of K.*

Notation. The symbols $\mathbb{Z}$, and $\mathbb{Q}$ denote, respectively, the ring of integers, and the field of rational numbers. For a prime p, the finite field with p elements

is denoted by $\mathbb{F}_p$. We denote the p-adic integers and the p-adic number field by $\mathbb{Z}_p$ and $\mathbb{Q}_p$. Let $\mathcal{O}_K$ denote the ring of integers of a number field K. For a prime $\mathfrak{p}$ of K, let $\mathcal{O}_\mathfrak{p}$ denote the completion of $\mathcal{O}_K$ at $\mathfrak{p}$, $k_\mathfrak{p}$ its residue field, and $K_\mathfrak{p}$ the field of fractions of $\mathcal{O}_\mathfrak{p}$.

2. Preliminaries

In this section, we consider the property of elliptic curves with $B_{K,p}$-reduction and a p-torsion point. We also review families of elliptic curves with a p-torsion point.

2.1. Elliptic curves with $B_{K,p}$-reduction and a p-torsion point

Let K be a number field. Fix a prime number $p \geq 5$ with $e_\mathfrak{p} < p-1$ for the primes $\mathfrak{p}$ of K over p. If there exists an elliptic curve with $B_{K,p}$-reduction and a p-torsion point, it follows by Theorem 1.1 that $p \mid h_{K(\zeta_p)}$ and hence $A_{K(\zeta_p)} \neq 0$, where A_F denotes the p-part of the ideal class group of a number field F. Furthermore, we can see the following property.

Let E be an elliptic curve over K with $B_{K,p}$-reduction and a p-torsion point P. Using the Weil-pairing $e_p : E[p] \times E[p] \to \mu_p$, we define a map $\psi : E[p] \to \mu_p$ by $Q \mapsto e_p(P,Q)$, where μ_p denotes the set of the p-th root of unity. Since the point P is rational over K, this map gives an exact sequence

$$0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E[p] \xrightarrow{\psi} \mu_p \longrightarrow 0 \tag{1}$$

of G_K-modules, where $\mathbb{Z}/p\mathbb{Z}$ denotes the constant G_K-module generated by P. Let $L = K(E[p])$ denote the field generated by the points of $E[p]$. By [14, Poof of Theorem 1.2], we may assume that L is an unramified extension of $K(\zeta_p)$ of degree p. The representation $\overline{\rho}_{E,p}$ induces the representation

$$\rho : \mathrm{Gal}(L/K) \to \mathrm{GL}_2(\mathbb{F}_p).$$

We note that ρ is faithful and of the form $\left(\begin{smallmatrix} 1 & * \\ 0 & \omega \end{smallmatrix}\right)$ by the exact sequence (1) where

$$\omega : \Delta \to \mathbb{F}_p^\times, \quad \Delta = \mathrm{Gal}(K(\zeta_p)/K)$$

denotes the cyclotomic character defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$ for every $\sigma \in \Delta$. We see that ρ does not split by the assumption $L \neq K(\zeta_p)$, and hence the group $\mathrm{Gal}(L/K(\zeta_p))$ is isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of all matrices of the form $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ under the representation ρ. We now consider the action of Δ on $\mathrm{Gal}(L/K(\zeta_p))$ by conjugation in $\mathrm{Gal}(L/K)$. Consider Δ as a subgroup of $\mathbb{F}_p^\times$ under the cyclotomic character ω and fix $a \in \Delta \subset \mathbb{F}_p^\times$. Since conjugating $\left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)$ by $a \in \mathbb{F}_p^\times$ gives $\left(\begin{smallmatrix} 1 & k/a \\ 0 & 1 \end{smallmatrix}\right)$, we see that $a \in \Delta \subset \mathbb{F}_p^\times$ acts on $\mathrm{Gal}(L/K(\zeta_p))$ as multiplication by a^{-1}. Then we have $A_{K(\zeta_p)}^{\omega^{-1}} \neq 0$, where R^{ω^i} denotes the ω^i-eigenspace of a $\mathbb{Z}_p[\Delta]$-module R as in the notation of [13, §6.3].

2.2. Families of elliptic curves with a p-torsion point

2.2.1. The cases $p = 5$ and 7. Let E be an elliptic curve over a number field K with a p-torsion point P. The following result is well-known ([5, 12] for details): For $p = 5$, there exists a unique $t \in K \setminus \{0\}$ such that E is isomorphic to an elliptic curve defined by the equation

$$E_t^{(5)} : y^2 + (1-t)xy - ty = x^3 - tx^2$$

and the 5-torsion point P corresponds to $(0, 0)$ under the isomorphism. The discriminant of $E_t^{(5)}$ is

$$\Delta(E_t^{(5)}) = t^5(t^2 - 11t - 1). \tag{2}$$

Similarly, for $p = 7$, there exists a unique $t \in K\setminus\{0, 1\}$ such that E is isomorphic to an elliptic curve defined by the equation

$$E_t^{(7)} : y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2$$

and the 7-torsion point P corresponds to $(0, 0)$ under the isomorphism. The discriminant of $E_t^{(7)}$ is

$$\Delta(E_t^{(7)}) = t^7(t-1)^7(t^3 - 8t^2 + 5t + 1). \tag{3}$$

2.2.2. The cases $p = 11$ and 13. For $p = 11$ and 13, Jeon, Kim and Lee gave an infinite family of elliptic curves $E_t^{(p)}, t \in \mathbb{Q}$ over quadratic fields $\mathbb{Q}(\sqrt{d_p})$ having a p-torsion point as follows (see [1, Section 3] for details): For $p = 11$, set

$$\begin{cases} b_{11} &= -\frac{1}{4}t(t-1)(t^2 + 1 - \sqrt{d_{11}})(t^3 + t - 2 - t\sqrt{d_{11}}), \\ c_{11} &= \frac{1}{2}t(t-1)(t^2 + 1 - \sqrt{d_{11}}), \\ d_{11} &= t^4 + 2t^2 - 4t + 1. \end{cases}$$

On the other hand, for $p = 13$, set

$$\begin{cases} b_{13} &= -\frac{t(t^4-t^2+t+1-(t-1)\sqrt{d_{13}})(t^3+t^2+1-\sqrt{d_{13}})(t^4+t^3+t+2-t\sqrt{d_{13}})}{4(t^3+t^2-1-\sqrt{d_{13}})}, \\ c_{13} &= -\frac{t(t^3+t^2+1-\sqrt{d_{13}})(t^4-t^2+t+1-(t-1)\sqrt{d_{13}})}{2(t^3+t^2-1-\sqrt{d_{13}})}, \\ d_{13} &= t^6 + 2t^5 + t^4 + 2t^3 + 6t^2 + 4t + 1. \end{cases}$$

Let $p = 11$ or 13. Let $E_t^{(p)}$ be an elliptic curve over a quadratic field $\mathbb{Q}(\sqrt{d_p})$ defined by the equation

$$E_t^{(p)} : y^2 + (1 - c_p)xy - b_p y = x^3 - b_p x^2$$

with $t \in \mathbb{Q}$. Then $E_t^{(p)}$ has a p-torsion point $(0, 0)$.

3. A construction of elliptic curves with $B_{K,p}$-reduction and a p-torsion point (quadratic field case)

Throughout this section, let K be a quadratic field.

3.1. The cases $p = 5$ and 7

In this subsection, we construct pairs (E, K), where E is an elliptic curve over K with $B_{K,p}$-reduction and a p-torsion point. To construct such pairs, we give the following result:

Proposition 3.1. *Let $p = 5$ or 7. Let $E = E_t^{(p)}, t \in \mathcal{O}_K$ be an elliptic curve over defined as in §2.2.1. Suppose that E has $B_{K,p}$-reduction. Then we have*

$$\begin{cases} t^2 - 11t - 1 \in \mathcal{O}_K^\times & \text{if } p = 5, \\ t^3 - 8t^2 + 5t + 1 \in \mathcal{O}_K^\times & \text{if } p = 7. \end{cases}$$

Proof. For simplicity, we only consider the case $p = 7$. Assume $t^3-8t^2+5t+1 \notin \mathcal{O}_K^\times$. Then there exists a prime ℓ dividing $t^3-8t^2+5t+1 \in \mathcal{O}_K$. By the equation (3), the elliptic curve E has bad reduction at some prime $\mathfrak{q}$ of K over ℓ. Since E has $B_{K,p}$-reduction, we may assume $\ell \neq 7$. We note that the solutions of the equation

$$X^3 - 8X^2 + 5X + 1 = 0$$

define the extension field $K(\zeta_7 + \zeta_7^{-1})$ over K. Now we consider the following diagram:

$$\begin{array}{ccc} \mathrm{Gal}(K(\zeta_7)/K) & \overset{\omega}{\hookrightarrow} & (\mathbb{Z}/7\mathbb{Z})^\times \\ \sigma \downarrow & & \downarrow \\ \mathrm{Gal}(K(\zeta_7 + \zeta_7^{-1})/K) & \hookrightarrow & (\mathbb{Z}/7\mathbb{Z})^\times/\{\pm 1\}, \end{array}$$

where ω is the cyclotomic character defined as in §2.1 and σ is the restriction map. Let $s \in \mathrm{Gal}(K(\zeta_7)/K)$ denote the Frobenius map satisfying

$$\mathrm{Gal}(K_\mathfrak{q}(\zeta_7)/K_\mathfrak{q}) = \langle s \rangle.$$

Note that we have $\omega(s) = \ell^f \in (\mathbb{Z}/7\mathbb{Z})^\times$, where f denotes the residue degree of $\mathfrak{q}$. Then we can see the following:

$$\begin{aligned} & X^3 - 8X^2 + 5X + 1 = 0 \bmod \mathfrak{q} \text{ has a solution } t \in \mathcal{O}_K, \\ \Longrightarrow\ & X^3 - 8X^2 + 5X + 1 = 0 \text{ has a solution } t' \in \mathcal{O}_\mathfrak{q} \text{ (by Hensel's lemma)}, \\ \Longrightarrow\ & \sigma(s) = 1 \in \mathrm{Gal}(K(\zeta_7 + \zeta_7^{-1})/K) \Longleftrightarrow \ell^f \equiv \pm 1 \bmod 7. \end{aligned}$$

This is a contradiction to the fact that E has $B_{K,p}$-reduction. This completes the proof of Proposition 3.1. □

We can apply Proposition 3.1 to construct pairs (E, K) as follows: Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field, where m is a square-free integer. Set $t = a + b\sqrt{m} \in \mathcal{O}_K$ with $2a, 2b \in \mathbb{Z}$. Let $0 \neq u = a^2 - mb^2 \in \mathbb{Z}$ denote the norm of $t \in \mathcal{O}_K$.

3.1.1. The case $p = 5$. By Proposition 3.1, consider the condition

$$t^2 - 11t - 1 \in \mathcal{O}_K^\times \Longleftrightarrow \mathrm{Nm}_{K/\mathbb{Q}}(t^2 - 11t - 1) = \pm 1. \tag{4}$$

Since we have

$$\mathrm{Nm}_{K/\mathbb{Q}}(t^2 - 11t - 1) = -4a^2 - 22(u-1)a + u^2 + 123u + 1,$$

we see that the condition (4) is equivalent to the condition

$$X^2 + 11(u-1)X - u^2 - 123u - 1 = \pm 1 \tag{5}$$

with $X = 2a \in \mathbb{Z}$. Note that the equation (5) can be transformed to the Pell equation

$$A^2 - 5B^2 = \pm 4 \tag{6}$$

with $A = 2X + 11(u-1) \in \mathbb{Z}$ and $B = 5(u+1) \in \mathbb{Z}$. Let $\epsilon = \frac{1+\sqrt{5}}{2}$ be a fundamental unit of $\mathbb{Q}(\sqrt{5})$. It is well known that the integer solutions of the Pell equation (6) are given by the elements $\pm\epsilon^n$ for $n = 0, 1, 2, \ldots$. Since $B \in 5\mathbb{Z}$, we note that the solutions of the equation (5) corresponds to the elements $\pm\epsilon^{5n}$ for $n = 0, 1, 2, \ldots$. For example, we have that an integer solution $(A, B) = (-11, -5)$ of the Pell equation (6) corresponds the element $-\epsilon^5 = -\frac{11+5\sqrt{5}}{2}$. Therefore we see that a pair $(X, u) = (11, -2)$ satisfies the condition (5).

A computation shows that only the pairs

$$\begin{aligned}(X,u) = {} & (10,-1),(12,-1),(11,-2),(22,-2),(12,10),(-111,10),(10,-12),\\ & (133,-12),(22,121),(-1342,121),(0,-123),(1364,-123)\end{aligned}$$

satisfy the condition (5) with $|u| < 1000$. For each pair (X, u), we compute a solution (a, b, m) and check whether the elliptic curve $E_t^{(5)},\ t = a + b\sqrt{m}$ over $K = \mathbb{Q}(\sqrt{m})$ has $B_{K,5}$-reduction as follows:

- For $(X, u) = (10, -1)$, we have a solution $(a, b, m) = (5, 1, 26)$. We see that the elliptic curve $E_t^{(5)},\ t = a+b\sqrt{m}$ has good reduction everywhere over $K = \mathbb{Q}(\sqrt{26})$. Therefore $E_t^{(5)}$ has $B_{K,5}$-reduction.
- For $(X, u) = (11, -2)$, we have a solution $(a, b, m) = \left(\frac{11}{2}, \frac{1}{2}, 129\right)$. We see that the elliptic curve $E_t^{(5)},\ t = a+b\sqrt{m}$ has bad reduction only at the primes of $K = \mathbb{Q}(\sqrt{129})$ over 2. Therefore $E_t^{(5)}$ has $B_{K,5}$-reduction.
- For $(X, u) = (12, 10)$, we have a solution $(a, b, m) = (6, 1, 26)$. Since the elliptic curve $E_t^{(5)},\ t = a + b\sqrt{m}$ has bad reduction at the primes of $K = \mathbb{Q}(\sqrt{26})$ over 5, the elliptic curve $E_t^{(5)}$ does not have $B_{K,5}$-reduction.

In Table 1, we list the triples (a, b, m) such that the elliptic curve $E_t^{(5)},\ t = a+b\sqrt{m}$ over $K = \mathbb{Q}(\sqrt{m})$ has $B_{K,5}$-reduction. Furthermore, for each (a, b, m), we also list $h_{K(\zeta_5)}$ which is computed by using PARI/GP Version 2.4.1 [10]. We note that $h_{K(\zeta_5)}$ is divisible by 5.

3.1.2. The case $p = 7$. As in the case $p = 5$, consider the condition

$$t^3 - 8t^2 + 5t + 1 \in \mathcal{O}_K^\times \Longleftrightarrow \mathrm{Nm}_{K/\mathbb{Q}}(t^3 - 8t^2 + 5t + 1) = \pm 1 \tag{7}$$

TABLE 1. List of the triples (a, b, m) with $|u| < 1000$ such that $E_t^{(5)},\ t = a + b\sqrt{m}$ over $K = \mathbb{Q}(\sqrt{m})$ has $B_{K,5}$-reduction $(u = a^2 - mb^2)$

(X, u)	(a, b, m)	$h_{K(\zeta_5)}$
$(10, -1)$	$(5, 1, 26)$	40
$(12, -1)$	$(6, 1, 37)$	5
$(11, -2)$	$(\frac{11}{2}, \frac{1}{2}, 129)$	10
$(22, -2)$	$(11, 1, 123)$	160
$(10, -12)$	$(5, 1, 37)$	5
$(133, -12)$	$(\frac{133}{2}, \frac{1}{2}, 17737)$	307125
$(-1342, 121)$	$(-671, 1, 450120)$	320
$(0, -123)$	$(0, 1, 123)$	160
$(1364, -123)$	$(682, 1, 465247)$	461194240

TABLE 2. List of the triples (a, b, m) with $|u| < 1000$ such that $E_t^{(7)},\ t = a + b\sqrt{m}$ over $K = \mathbb{Q}(\sqrt{m})$ has $B_{K,7}$-reduction $(u = a^2 - mb^2)$

(X, u)	(a, b, m)	$h_{K(\zeta_7)}$
$(6, -1)$	$(3, 1, 10)$	28
$(7, -2)$	$(\frac{7}{2}, \frac{1}{2}, 57)$	56
$(8, 5)$	$(4, 1, 11)$	28

by Proposition 3.1. A computation shows that $\mathrm{Nm}_{K/\mathbb{Q}}(t^3 - 8t^2 + 5t + 1)$ is equal to

$$8a^3 + (20u - 32)a^2 + (-16u^2 - 86u + 10)a + (u^3 + 54u^2 + 4u + 1).$$

Therefore the condition (7) is equivalent to the condition

$$X^2 + (5u - 8)X^2 + (-8u^2 - 43u + 5)X + (u^3 + 54u^2 + 4u + 1) = \pm 1 \tag{8}$$

with $X = 2a \in \mathbb{Z}$. We see that only the pairs

$$(X, u) = (2, 1), (6, -1), (7, -1), (7, -2), (8, 5), (8, 6), (9, 7)$$

satisfy the condition (8) with $|u| < 1000$. As in the case $p = 5$, in Table 2, we list the triples (a, b, m) such that the elliptic curve $E_t^{(7)},\ t = a + b\sqrt{m}$ over $K = \mathbb{Q}(\sqrt{m})$ has $B_{K,7}$-reduction. We note that $h_{K(\zeta_7)}$ is divisible by 7.

Remark. The equation (8) defines a nonsingular projective curve C of genus 1. It follows from Siegel's Theorem that the set $C(\mathbb{Z})$ of the integer solutions is finite. Therefore, unlike the case $p = 5$, there are only finitely many solutions $(X, u) \in \mathbb{Z}^2$ of the equation (8).

3.2. The cases $p = 11$ and 13

In this subsection, we consider whether we can construct pairs (E, K), where $E = E_t^{(p)}$ is an elliptic curve over K defined as in §2.2.2 such that E has $B_{K,p}$-reduction.

3.2.1. The case $p = 11$. Let $E = E_t^{(11)}$, $t \in \mathbb{Z}$ be an elliptic curve over $K = \mathbb{Q}(\sqrt{d_{11}})$ defined as in §2.2.2. A computation shows that the discriminant of E is equal to

$$\Delta(E) = -\frac{t^3 + t - 2 - t\sqrt{d_{11}}}{2} \cdot b_{11}^3 \cdot T,$$

where

$$\begin{aligned} T = & -t^3(t^9 + 5t^8 + 6t^7 + 3t^6 - 14t^5 - 14t^4 + t^3 + 11t^2 - 1) \\ & + t^3(t^7 + 5t^6 + 5t^5 - 9t^3 - 6t^2 + 2t + 1)\sqrt{d_{11}} \in \mathcal{O}_K. \end{aligned}$$

Furthermore, we have $\mathrm{Nm}_{K/\mathbb{Q}}(T) = -4t^{10} \cdot (t^5 - t^4 - 15t^3 + 14t^2 + 3t - 1)$. Let $F = t^5 - t^4 - 15t^3 + 14t^2 + 3t - 1 \in \mathbb{Z}$. Since $\Delta(E) \neq 0$, we see $F \neq \pm 1$. Therefore there exists a prime ℓ with $\ell \mid F$, and hence the elliptic curve E has bad reduction at some prime $\mathfrak{q}$ of K over ℓ. We note that the solutions of the equation

$$X^5 - X^4 - 15X^3 + 14X^2 + 3X - 1 = 0$$

define the extension field $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ over $\mathbb{Q}$. By a similar argument of the proof of Proposition 3.1, we have $\ell \equiv \pm 1 \bmod 11$ if $\ell \neq 11$. Therefore we have the following:

Proposition 3.2. *Let $E = E_t^{(11)}$, $t \in \mathbb{Z}$ be an elliptic curve over $K = \mathbb{Q}(\sqrt{d_{11}})$ defined as in §2.2.2. Then E does not have $B_{K,11}$-reduction.*

3.2.2. The case $p = 13$. Let $E = E_t^{(13)}$, $t \in \mathbb{Z}$ be an elliptic curve over $K = \mathbb{Q}(\sqrt{d_{13}})$ defined as in §2.2.2. A computation shows that the discriminant of E is equal to

$$\Delta(E) = \frac{t^4 + t^3 + t + 2 - t\sqrt{d_{13}}}{2} \cdot b_{13}^3 \cdot T,$$

where $T \in \mathcal{O}_K$ satisfies $\mathrm{Nm}_{K/\mathbb{Q}}(T) = 4t^6 \cdot (t+1)^3 \cdot (t^3 + 4t^2 + t - 1)$. Let $F = t^3 + 4t^2 + t - 1 \in \mathbb{Z}$. Since $\Delta(E) \neq 0$, we see $F \neq \pm 1$. Therefore there exists a prime ℓ with $\ell \mid F$, and hence the elliptic curve E has bad reduction at some prime $\mathfrak{q}$ of K over ℓ. Let L be the splitting field of the equation

$$X^3 + 4X^2 + X - 1 = 0.$$

Then L is a subfield of $\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1})$ with $[\mathbb{Q}(\zeta_{13} + \zeta_{13}^{-1}) : L] = 2$. By a similar argument of the proof of Proposition 3.1, we have $\ell^2 \equiv \pm 1 \bmod 13$ if $\ell \neq 13$. If there exists a prime $\ell \neq 13$ such that $\ell \mid F$ and the residue degree of K over ℓ is equal to 2, then the elliptic curve E does not have $B_{K,13}$-reduction. Hence

we conclude that an elliptic curve $E_t^{(13)},\ t \in \mathbb{Z}$ does not have $B_{K,13}$-reduction with very high probability.

4. Mod p Galois representations

In this section, we consider the irreducibility and surjectivity of $\overline{\rho}_{E,p}$ for semistable elliptic curves E over a number field K with $\mathfrak{q} \in B_{K,p}$-reduction.

4.1. Classification of $\mathcal{O}_K$-group schemes of order p

Let K be a number field. Fix a prime number p. We shall review the classification of $\mathcal{O}_K$-group schemes of order p due to Oort and Tate [9]. Let M be the set of non-generic points of $\mathrm{Spec}(\mathcal{O}_K)$, and let M_p denote the set of $\mathfrak{p} \in M$ such that $\mathfrak{p}$ divides p. Let F denote the functor which associates with each commutative ring R with unity the set $F(R)$ of isomorphism classes of R-group schemes of order p. Then Oort and Tate showed that the square

$$\begin{array}{ccc} F(\mathcal{O}_K) & \to & \prod_{\mathfrak{p}\in M} F(\mathcal{O}_\mathfrak{p}) \\ \downarrow & & \downarrow \\ F(K) & \to & \prod_{\mathfrak{p}\in M} F(K_\mathfrak{p}) \end{array}$$

is Cartesian (see [9, Lemma 4]). Let C_K denote the idèle class group of K. Using class field theory, there are canonical bijections

$$\begin{aligned} F(K) &\simeq \mathrm{Hom}_{\mathrm{cont}}(C_K, \mathbb{F}_p^\times), \\ F(K_\mathfrak{p}) &\simeq \mathrm{Hom}_{\mathrm{cont}}(K_\mathfrak{p}^\times, \mathbb{F}_p^\times)\ (\mathfrak{p} \in M), \text{ and} \\ F(\mathcal{O}_\mathfrak{p}) &\simeq \mathrm{Hom}_{\mathrm{cont}}(K_\mathfrak{p}^\times/U_\mathfrak{p}, \mathbb{F}_p^\times)\ (\mathfrak{p} \in M \setminus M_p), \end{aligned}$$

where $\mathrm{Hom}_{\mathrm{cont}}$ denotes the set of the continuous homomorphisms and $U_\mathfrak{p}$ is the group of units in $\mathcal{O}_\mathfrak{p}$ (see [9, Lemma 6]). Via these bijections, the arrows in the above diagram are induced by the canonical homomorphisms $K_\mathfrak{p}^\times \to C_K$ and $K_\mathfrak{p}^\times \to K_\mathfrak{p}^\times/U_\mathfrak{p}$.

For an $\mathcal{O}_K$-group scheme G of order p, we denote by $\psi^G \in \mathrm{Hom}_{\mathrm{cont}}(C_K, \mathbb{F}_p^\times)$ the idèle character determined by $G \otimes K$, and by $\psi_\mathfrak{p}^G$ the corresponding character of $K_\mathfrak{p}^\times$ for $\mathfrak{p} \in M$. For each $\mathfrak{p} \in M_p$, we let $n_\mathfrak{p}^G = v_\mathfrak{p}(a)$, where $v_\mathfrak{p}$ is the normalized discrete valuation of $K_\mathfrak{p}$ and a is the element of $\mathcal{O}_\mathfrak{p}$ such that $G \otimes \mathcal{O}_\mathfrak{p} \simeq G_{a,b}$ in the notation of [9]. Note that $n_\mathfrak{p}^G$ is uniquely determined by G. Oort and Tate showed the following [9, Theorem 3]:

Theorem 4.1 (Oort-Tate)**.** *The map $G \mapsto (\psi^G, (n_\mathfrak{p}^G)_{\mathfrak{p}\in M_p})$ gives a bijection between the isomorphism classes of $\mathcal{O}_K$-group schemes of order p and the systems $(\psi, (n_\mathfrak{p})_{\mathfrak{p}\in M_p})$ consisting of a continuous homomorphism $\psi : C_K \to \mathbb{F}_p^\times$ and for each $\mathfrak{p} \in M_p$ an integer $n_\mathfrak{p}$ with $0 \le n_\mathfrak{p} \le e_\mathfrak{p}$, which satisfy the following conditions*:

(A) *For $\mathfrak{p} \in M \setminus M_p$, ψ is unramified at $\mathfrak{p}$, i.e., $\psi_\mathfrak{p}(U_\mathfrak{p}) = 1$,*
(B) *For $\mathfrak{p} \in M_p$, $\psi_\mathfrak{p}(u) = (\mathrm{Nm}_{k_\mathfrak{p}/\mathbb{F}_p}(\overline{u}))^{-n_\mathfrak{p}},\ \forall u \in U_\mathfrak{p}$, where $u \mapsto \overline{u}$ denotes the residue class map.*

Here $\psi_{\mathfrak{p}} : K_{\mathfrak{p}}^{\times} \to \mathbb{F}_p^{\times}$ denotes the local character induced by ψ via the canonical map $K_{\mathfrak{p}}^{\times} \to C_K$.

For a given family $(n_{\mathfrak{p}})_{\mathfrak{p}\in M_p}$, there is no idèle class character ψ satisfying the conditions (A) and (B) of Theorem 4.1, or the set of all idèle characters is a principal homogeneous space under the group of homomorphisms of the narrow class group of K into $\mathbb{F}_p^{\times}$. Therefore, if the narrow class number h_K^+ of K is prime to $(p-1)$, there is at most one ψ for a given family $(n_{\mathfrak{p}})_{\mathfrak{p}\in M_p}$. Furthermore, for an $\mathcal{O}_K$-group scheme G of order p corresponding to $(n_{\mathfrak{p}})_{\mathfrak{p}\in M_p}$, the Cartier dual of G corresponds to $(e_{\mathfrak{p}} - n_{\mathfrak{p}})_{\mathfrak{p}\in M_p}$.

4.2. Irreducibility and surjectivity of $\overline{\rho}_{E,p}$

Let p be a prime number. Let E be an elliptic curve over a number field K. If the representation $\overline{\rho}_{E,p}$ is reducible, then we have

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \phi_1 & * \\ 0 & \phi_2 \end{pmatrix}, \ \phi_i : G_K \to \mathbb{F}_p^{\times}, \ i = 1, 2. \tag{9}$$

We note that each character ϕ_i induces $\overline{\phi}_i : \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \mathbb{F}_p^{\times}$, where K^{ab} is the maximal abelian extension field of K.

Proposition 4.2. *Assume that E is a semistable elliptic curve with good reduction at the primes of K over p. Then each character ϕ_i gives an $\mathcal{O}_K$-group scheme G of order p with $\psi^G = \overline{\phi}_i \circ \sigma_K$, where $\sigma_K : C_K \to \mathrm{Gal}(K^{\mathrm{ab}}/K)$ is the reciprocity map.*

Proof. Since E has good reduction at the primes $\mathfrak{p}$ of K over p, the p-torsion subgroup $E[p]$ is an $\mathcal{O}_{\mathfrak{p}}$-group scheme. Therefore it follows that ϕ_i has a structure of an $\mathcal{O}_{\mathfrak{p}}$-group scheme of order p. Let S_E denote the set of the primes of K at which E has bad reduction. Let $\mathfrak{q}$ be a prime of K with $\mathfrak{q} \nmid p$.

- In the case $\mathfrak{q} \notin S_E$, the representation $\overline{\rho}_{E,p}$ is unramified at $\mathfrak{q}$ by the criterion of Néron-Ogg-Shafarevich (see [12, Chapter VII, Theorem 7.1]). Hence ϕ_i is unramified at $\mathfrak{q}$.
- In the case $\mathfrak{q} \in S_E$, there exists an unramified extension field L over $K_{\mathfrak{q}}$ of degree 1 or 2 such that E is isomorphic to the Tate curve E_q over L, where q is the Tate parameter (see [11, §1.12]). By the theory of Tate curves, we have $E(L) \simeq \overline{L}^{\times}/q^{\mathbb{Z}}$. With this identification, we clearly have $E[p] \simeq (\zeta_p \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}}$, where $Q = q^{1/p} \in \overline{L}$ is a fixed p-th root of q. Therefore the representation $\overline{\rho}_{E,p}$ restricted to $\mathrm{Gal}(\overline{L}/L)$ has the form $\left(\begin{smallmatrix} 1 & * \\ 0 & \chi \end{smallmatrix}\right)$, where χ is the cyclotomic character. Hence it follows that ϕ_i is unramified at $\mathfrak{q}$.

The above argument shows that ϕ_i is unramified at the primes $\mathfrak{q}$ of K with $\mathfrak{q} \nmid p$. Therefore we can see that the character $\overline{\phi}_i \circ \sigma_K$ satisfies the conditions (A) and (B) of Theorem 4.1. This completes the proof. □

Let K be a cubic field. We next consider the structure of $\mathcal{O}_K$-group schemes of order p. Our result is as follows:

Proposition 4.3. *Let p be an odd prime number. Let K be a cubic field with $\gcd(p-1, h_K^+) = 1$. If p satisfies either the condition* (A) *or* (B) *of Theorem 1.2, then the only $\mathcal{O}_K$-group schemes of order p are $\mathbb{Z}/p\mathbb{Z}$ and μ_p, where $\mathbb{Z}/p\mathbb{Z}$ (resp. μ_p) is a constant (resp. diagonalizable) group scheme.*

Proof. In the case where p is prime in $\mathcal{O}_K$, this is prove by Oort-Tate [9]. We next consider the case where p is not prime in $\mathcal{O}_K$. For simplicity, we only consider the case where K is a complex number field. Assume $p \nmid \mathrm{Nm}_{K/\mathbb{Q}}(u-1)$, where u is a fundamental unit of K such that $u > 0$ with respect to the only one real place of K.

The basic idea is based on [4]. We first consider the case $p\mathcal{O}_K = \mathfrak{p}_1^2\mathfrak{p}_2$, where $\mathfrak{p}_1, \mathfrak{p}_2$ are the primes of K over p. For the family $(n_{\mathfrak{p}_1}, n_{\mathfrak{p}_2}) = (1, 0)$, we assume that there is an idèle class character $\psi : C_K \to \mathbb{F}_p^\times$ satisfying the conditions (A) and (B) of Theorem 4.1. According to class field theory, there is a modulus of the form $\mathfrak{m} = \infty \cdot \mathfrak{p}_1$ such that ψ induces a surjective homomorphism $\overline{\psi} : C_m \to \mathbb{F}_p^\times$, where $C_\mathfrak{m}$ is the ray class group of K modulus $\mathfrak{m}$. Let C_∞ be the narrow class group of K. There is an exact sequence [8]

$$1 \to U^+/U_{\mathfrak{m},1} \to (\mathcal{O}_K/\mathfrak{p}_1)^\times \to C_\mathfrak{m} \to C_\infty \to 1,$$

where U^+ is the group of totally positive units of K and $U_{\mathfrak{m},1}$ is the subgroup of the elements of U^+ which are congruent to 1 modulo $\mathfrak{p}_1$. Since $\gcd(p-1, h_K^+) = 1$, we see that a composition of the following maps

$$\Phi : (\mathcal{O}_K/\mathfrak{p}_1)^\times \to C_\mathfrak{m} \xrightarrow{\overline{\psi}} \mathbb{F}_p^\times$$

is an isomorphism. Since $u \in U^+$ and the image of U^+ is in the kernel of the isomorphism Φ, we have $u - 1 \in \mathfrak{p}_1$. This is a contradiction to the condition $p \nmid \mathrm{Nm}_{K/\mathbb{Q}}(u-1)$. Therefore there is no idèle character ψ satisfying the conditions (A) and (B) of Theorem 4.1 for the family $(n_{\mathfrak{p}_1}, n_{\mathfrak{p}_2}) = (1, 0)$. Furthermore, considering the Cartier dual, the same result holds for the family $(n_{\mathfrak{p}_1}, n_{\mathfrak{p}_2}) = (1, 1)$. A similar argument shows that there is no idèle class character for families $(n_{\mathfrak{p}_1}, n_{\mathfrak{p}_2}) = (0, 1)$, $(2, 0)$. Therefore the only $\mathcal{O}_K$-group schemes of order p are $\mathbb{Z}/p\mathbb{Z}$ and μ_p by Theorem 4.1.

In the case where $p\mathcal{O}_K = \mathfrak{p}^3$, $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ or $\mathfrak{p}_1\mathfrak{p}_2$, a similar argument as above shows the same result. This completes the proof. □

We note that Theorem 1.1 holds for the primes $p \geq 3$ when E is restricted to be semistable. Combining Propositions 4.2 and 4.3 with Theorem 1.1, we can prove Theorem 1.2 as follows:

Proof of Theorem 1.2. The idea is based on the proof of [7, Theorem 4] or [4, Théorème]. Suppose that $\overline{\rho}_{E,p}$ is reducible. Then $\overline{\rho}_{E,p}$ has the form (9). Since $\phi_1 \cdot \phi_2 = \chi$, it follows from Propositions 4.2 and 4.3 that either of ϕ_i is a trivial character. Hence we see that E or $E' = E/\mu_p$ has a p-torsion point. Since E

and E' have bad reduction at same primes, this is a contradiction to Theorem 1.1. This completes the proof of Theorem 1.2. □

Example. Let K be a cubic field with $h_K^+ = 1$. Let E be an elliptic curve over K with everywhere good reduction. By Theorem 1.2, we obtain the following results on the irreducibility of $\overline{\rho}_{E,p}$:

- Let $K = \mathbb{Q}[x]/(f(x))$ be a complex cubic field defined by $f(x) = x^3 + x - 1$. We have that the element $x \in \mathcal{O}_K$ is a fundamental unit of K with $x > 0$ and $\mathrm{Nm}_{K/\mathbb{Q}}(x-1) = 1$. We also have $3\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $f_1 = 1$ and $f_2 = 2$, where f_i is the residue degree of $\mathfrak{p}_i$. Since $\sharp E(k_{\mathfrak{p}_1}) \leq 3+1+2\sqrt{3} < 8$, the elliptic curve E has no p-torsion points for the primes $p \geq 11$. By a similar argument of the proof of Theorem 1.2, we see that $\overline{\rho}_{E,p}$ is irreducible for the primes $p \geq 11$. Furthermore, since $h_{K(\zeta_p)} = 1$ for $p = 3, 5$ and 7, it follows from Theorem 1.2 that $\overline{\rho}_{E,p}$ is irreducible for $p = 3, 5$ and 7. Therefore we have that $\overline{\rho}_{E,p}$ is irreducible for the primes $p \geq 3$.
- Let $K = \mathbb{Q}[x]/(f(x))$ be a totally real cubic field defined by $f(x) = x^3 - x^2 - 3x - 1$. We have that elements $x, x^2 - 2x \in \mathcal{O}_K$ are two independent fundamental units of K with $\mathrm{Nm}_{K/\mathbb{Q}}(x^2 - 1) = 4$ and $\mathrm{Nm}_{K/\mathbb{Q}}((x^2-2x)^2 - 1) = 16$. We also have $2\mathcal{O}_K = \mathfrak{p}^3$. Since $\sharp E(k_{\mathfrak{p}}) \leq 2 + 1 + 2\sqrt{2} < 7$, the elliptic curve E has no p-torsion points for the primes $p \geq 7$. By a similar argument of the proof of Theorem 1.2, we see that $\overline{\rho}_{E,p}$ is irreducible for the primes $p \geq 7$. Furthermore, since $h_{K(\zeta_3)} = 1$ and $h_{K(\zeta_5)} = 2$, it follows from Theorem 1.2 that $\overline{\rho}_{E,p}$ is irreducible for $p = 3$ and 5. Therefore we have that $\overline{\rho}_{E,p}$ is irreducible for the primes $p \geq 3$.

We give the following result mainly due to Serre [11]:

Proposition 4.4. *Let K be a number field with $h_K^+ = 1$ and let D_K denote the discriminant of K. Let E be a semistable elliptic curve over K with the j-invariant j_E. Let p be a prime such that $p \nmid D_K$. If $p = 2, 3$ or 5, suppose $p \nmid v(j_E)$ for some $v \in S_E$, where S_E is the set of the finite places v at which E has bad reduction. If $\overline{\rho}_{E,p}$ is irreducible, then $\overline{\rho}_{E,p}$ is surjective.*

Proof. See the proof of [11, Proposition 21] or [4, §3]. □

Combining the above result with Theorem 1.2, we obtain the following result on the surjectivity of $\overline{\rho}_{E,p}$.

Theorem 4.5. *Let K be a cubic field with $h_K^+ = 1$ and let D_K denote the discriminant of K. Let p be an odd prime number such that $p \nmid D_K$. Suppose that $p \nmid h_{K(\zeta_p)}$ and $e_{\mathfrak{p}} < p - 1$ for the primes $\mathfrak{p}$ of K over p. Let E be a semistable elliptic curve over K with $B_{K,p}$-reduction. If $p = 3$ or 5, suppose $p \nmid v(j_E)$ for some $v \in S_E$. If p satisfies either the condition* (A) *or* (B) *of Theorem 1.2, then $\overline{\rho}_{E,p}$ is surjective.*

Remark. In the case where $K = \mathbb{Q}$ or K is a quadratic field, we can show similar results of Theorems 1.2 and 4.5 (see also [4] in the case where K is a quadratic field). However, in general, it does not hold in the case $[K : \mathbb{Q}] \geq 4$.

4.3. $K(\zeta_p)$-rational points of order p

Let K be a number field. Let E be an elliptic curve over K with a p-torsion point. There exist an elliptic curve E^* over K and a K-isogeny $E \to E^*$ with kernel $\mathbb{Z}/p\mathbb{Z}$. By the exact sequence (1), we have $\mu_p \subset E^*$ and hence E^* has a $K(\zeta_p)$-rational point of order p. For an elliptic curve E over K with $B_{K,p}$-reduction, we here consider the existence of a $K(\zeta_p)$-rational point of E of order p. By Theorem 1.2, we obtain the following result (cf. Theorem 1.1):

Proposition 4.6. *Let p be an odd prime number. Let K be a cubic field with $\gcd(p-1, h_K^+) = 1$. Suppose that $p \nmid K(\zeta_p)$ and $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p. Let E be a semistable elliptic curve over K with $B_{K,p}$-reduction. If p satisfies either* (A) *or* (B) *of Theorem 1.2, then E has no $K(\zeta_p)$-rational points of order p.*

Proof. Suppose that E has a $K(\zeta_p)$-rational point of order p. Set $L = K(E[p])$ and $M = K(\zeta_p)$. Let G be a simple subgroup of $E[p]$ as a $\mathrm{Gal}(L/K)$-module. Set $S_p = \mathrm{Gal}(L/M)$. We may assume that S_p is non-trivial. Then the order of S_p is equal to p. Since $S_p \triangleleft \mathrm{Gal}(L/K)$, we see that the set $G(\overline{K})^{S_p}$ of the S_p-fixed points is a $\mathrm{Gal}(L/K)$-submodule of $G(\overline{K})$. Since $\sharp G(\overline{K}) \equiv \sharp G(\overline{K})^{S_p} \bmod p$, the group $G(\overline{K})^{S_p}$ is non-trivial, and hence $G(\overline{K}) = G(\overline{K})^{S_p}$ because G is simple. Then $G(\overline{K})$ is a $\mathrm{Gal}(M/K)$-module. Since the group $\mathrm{Gal}(M/K)$ has exponent dividing $p-1$, the $\mathbb{F}_p[\mathrm{Gal}(M/K)]$-module $G(\overline{K})$ is a product of 1-dimensional eigenspaces. Since G is simple, there is only one such eigenspace, and hence G has order p. Therefore the representation $\overline{\rho}_{E,p}$ is reducible. But this contradicts to Theorem 1.2. This completes the proof of Proposition 4.6. □

References

[1] D. Jeon, C. H. Kim, and Y. Lee, *Families of elliptic curves over quartic number fields with prescribed torsion subgroups*, Math. Comp. **80** (2011), no. 276, 2395–2410.

[2] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), no. 2, 221–229.

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

[4] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, J. Number Theory **60** (1996), no. 2, 245–253.

[5] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. (3) **33** (1976), no. 2, 193–237.

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

[7] ———, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), no. 2, 129–162.

[8] J. Neukirch, *Algebraic Number Theory*, Grudlehren der Mathematischen Wisenshaften, vol. 322, Springer-Verlag, Berlin-Heidelberg New York, 1999.

[9] Oort and Tate, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. **3** (1970), 1–21.
[10] The PARI Group, Bordeaux, *PARI/GP*, available from `http://pari.math.u-bordeaux.fr/doc.html`.
[11] J.-P. Serre, *Propriétés galoisiennes des points d'ortre fini des courbes elliptiques*, Invent. Math. **15** (1972), no. 4, 259–331.
[12] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Math. **106**, Springer-Verlag, Berlin-Heidelberg New York, 1994.
[13] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Math. **83**, Springer-Verlag, Berlin-Heidelberg New York, 1982.
[14] M. Yasuda, *Torsion points of elliptic curves with bad reduction at some primes*, to appear in Commentarii Math. Univ. St. Pauli.

Fujitsu Laboratories Ltd.
4-1-1, Kamikodanaka, Nakahara-ku, Kawasaki
211-8588, Japan
E-mail address: `myasuda@labs.fujitsu.com`