COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 61, No. 1 2012

ed. RIKKYO UNIV/MATH
IKEBUKURO TOKYO
171–8501 JAPAN

# Torsion Points of Elliptic Curves with Bad Reduction at Some Primes

by

Masaya YASUDA

(Received July 30, 2010)
(Revised April 17, 2012)

**Abstract.** Let $E$ be an elliptic curve over a number field $K$. For a prime $p$, the $p$-torsion points of $E$ are the points of finite order $p$ in the Mordell-Weil group $E(K)$. In this paper, we show that $E$ has no $p$-torsion points if $E$ has bad reduction at some primes.

## 1. Introduction

For a prime $p$, the $p$-torsion points of an elliptic curve $E$ over a number field $K$ are the points of finite order $p$ in the Mordell-Weil group $E(K)$. A. Ogg [9] conjectured which groups can be torsion subgroups of elliptic curves over $\mathbb{Q}$. In his papers [7, 8], Mazur proved Ogg's conjecture and showed that any elliptic curve over $\mathbb{Q}$ cannot have $p$-torsion points for the primes $p \geq 11$. In the case where $K$ is a quadratic field, Kenku-Momose [6] and Kamienny [5] classified the possible torsion subgroups of elliptic curves over $K$ and showed that any elliptic curve over $K$ cannot have $p$-torsion points for the primes $p \geq 17$. In this paper, we study the $p$-torsion points of elliptic curves over a number field $K$ that have bad reduction at some primes. We shall first prove the following result which is concerned with the $p$-torsion points of elliptic curves over $\mathbb{Q}$ for $p = 5$ and 7.

THEOREM 1.1. *Let $p = 5$ or 7. Let $E$ be an elliptic curve over $\mathbb{Q}$ with bad reduction only at the primes $\ell \neq p$ with $\ell \not\equiv \pm 1 \bmod p$. Then $E$ has no $p$-torsion points.*

Let $\mathcal{E}$ denote the Néron model of $E$ over $\mathbb{Z}$ and $\mathcal{E}[p]$ the kernel of multiplication by $p$. We give two proofs of Theorem 1.1. The main idea of the first proof is to examine the finite flat group scheme $\mathcal{E}[p]$ over the ring $\mathbb{Z}[1/N]$, where $N$ is the product of the primes at which $E$ has bad reduction. On the other hand, the main idea of the second proof is to study the extension $\mathbb{Q}(E[p])$ of $\mathbb{Q}$, where $\mathbb{Q}(E[p])$ is the field generated by the points of the $p$-torsion subgroup $E[p]$.

Based on the idea of the first proof of Theorem 1.1, we studied the $p$-torsion points of elliptic curves over certain number fields with good reduction everywhere [16]. On the other hand, we can apply the idea of the second proof of Theorem 1.1 to the case where $K$ is a number field. Our result is the following which extends [16, Theorem 3.8] to the case where $E$ has bad reduction at some primes.

2000 *Mathematics Subject Classification*. Primary 14H52; Secondary 14G05.

THEOREM 1.2. *Let $K$ be a number field and $p \geq 5$ a prime number. Suppose that $p$ does not divide the class number of $K(\zeta_p)$ and the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p-1$ for all primes $\mathfrak{p}$ of $K$ over $p$. Let $E$ be an elliptic curve over $K$ with bad reduction only at the primes $\mathfrak{l}$ of $K$ over the primes $\ell \neq p$ with $\ell^f \not\equiv \pm 1 \bmod p$, where $f$ is the residue degree of $\mathfrak{l}$. Then $E$ has no $p$-torsion points.*

**Acknowledgment.** I would like to thank the reviewers for giving me useful comments. Especially, I would like to thank the reviewer who gave me the idea of the second proof of Theorem 1.1.

NOTATION. The symbols $\mathbb{Z}$, and $\mathbb{Q}$ denote, respectively, the ring of rational 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 $\mathbb{Q}_p$. If $G$ is a group scheme over a ring $R$, and $n \in \mathbb{Z}$, we write $G[n]$ for the kernel of multiplication $[n]_G : G \to G$.

## 2. The first proof of Theorem 1.1

We begin with the following lemma:

LEMMA 2.1. *Let $E$ be an elliptic curve over a number field $K$. Suppose $E$ has a $p$-torsion point for $p \geq 5$. Let $\mathfrak{q}$ be a prime of $K$ with $\mathfrak{q} \nmid p$. Then $E$ has semistable reduction at $\mathfrak{q}$.*

*Proof.* See the proof of [1, Lemma 1.3]. □

Let $p \geq 5$ be a prime number and $N$ a square-free integer with $p \nmid N$. Let $E$ be an elliptic curve over $\mathbb{Q}$. Assume that $E$ has bad reduction only at the primes dividing $N$ and $E$ has a $p$-torsion point $P$. Using the Weil-pairing $e_p : E[p] \times E[p] \to \mu_p$, we define a map $E[p] \to \mu_p$ by $Q \mapsto e_p(P, Q)$. Since the point $P$ is rational over $\mathbb{Q}$, this map gives an exact sequence

$$0 \to \mathbb{Z}/p\mathbb{Z} \to E[p] \to \mu_p \to 0 \tag{1}$$

of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. Let $\mathcal{E}$ be the Néron model of $E$ over $\mathbb{Z}$. By Lemma 2.1 and A. Grothendieck's semistable reduction Theorem [3, Exp. IX, (3.5.3)], we see that $\mathcal{E}[p]$ is a finite flat group scheme over $\mathbb{Z}[1/N]$. By [8, §3, Step 1], we have $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$ where $\mathbb{Z}/p\mathbb{Z}$ is the constant group scheme generated by the point $P$.

LEMMA 2.2. *The exact sequence* (1) *of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$*-modules induces an exact sequence*

$$0 \to \mathbb{Z}/p\mathbb{Z} \to \mathcal{E}[p] \to \mu_p \to 0$$

*of finite flat group schemes over* $\mathbb{Z}[1/N]$, *where* $\mathbb{Z}/p\mathbb{Z}$ (*resp.* $\mu_p$) *is a constant* (*resp. diagonalizable* ) *group scheme over* $\mathbb{Z}[1/N]$.

*Proof.* Let $G$ be a finite flat group scheme over the ring $\mathbb{Z}[1/N]$ defined by coker $(\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{E}[p])$. It suffices to show that the group scheme $G$ is isomorphic to the diagonalizable group scheme $\mu_p$ over $\mathbb{Z}[1/N]$. Since the group scheme $G$ is étale over $\mathbb{Z}[1/pN]$, we can consider the group scheme $G$ over $\mathbb{Z}[1/pN]$ in terms of Galois modules, and hence $G$ is isomorphic to the diagonalizable scheme $\mu_p$ over $\mathbb{Z}[1/pN]$ by the exact sequence (1). Next we consider the group scheme $G$ over the ring $\mathbb{Z}_p$. Since the group scheme over $\mathbb{Z}_p$ is uniquely determined up to isomorphism by the isomorphism type over $\mathbb{Q}_p$ (see [14]), the group scheme $G$ is isomorphic to the diagonalizable group scheme $\mu_p$ over $\mathbb{Z}_p$. This completes the proof by [10, Proposition 2.3]. □

Let $\mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ be the group of extensions of $\mu_p$ by $\mathbb{Z}/p\mathbb{Z}$ over $\mathbb{Z}[1/N]$. By Lemma 2.2, we have $\mathcal{E}[p] \in \mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$. In the case where $N = \ell$ is a prime with $\ell \neq p$, Schoof classified the group $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ [11, Corollary 4.2]. We give the following result needed later.

PROPOSITION 2.3. *Let $p \geq 5$ be a prime number and $N$ a product of primes $\ell \neq p$ with $\ell \not\equiv \pm 1 \bmod p$. Then the group $\mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ is trivial.*

*Proof.* The idea is based on the proof of [11, Corollary 4.2]. Let $\zeta_p$ be a primitive $p$-th root of unity. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and let $\omega : \Delta \to \mathbb{F}_p^*$ denote the cyclotomic character defined by $\sigma(\zeta_p) = \zeta^{\omega(\sigma)}$ for every $\sigma \in \Delta$. For any $\mathbb{F}_p[\Delta]$-module $M$, let $M_{\omega^i}$ denote the $\omega^i$-eigenspace of $M$. By a similar proof of [11, Proposition 4.1], we get an exact sequence

$$\begin{aligned}(2)\qquad 0 \to \mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) &\to \left(\mathbb{Z}[1/pN, \zeta_p]^* / \left(\mathbb{Z}[1/pN, \zeta_p]^*\right)^p\right)_{\omega^2} \\ &\to \left(\mathbb{Q}_p(\zeta_p)^* / \left(\mathbb{Q}_p(\zeta_p)^*\right)^p\right)_{\omega^2}.\end{aligned}$$

We compute the group in the middle of the exact sequence (2). By the proof of [11, Corollary 4.2], we get the following exact sequence of $\omega^2$-eigenspaces:

$$\begin{aligned}(3)\qquad 0 &\to \left(\mathbb{Z}[1/p, \zeta_p]^* / \left(\mathbb{Z}[1/p, \zeta_p]^*\right)^p\right)_{\omega^2} \\ &\to \left(\mathbb{Z}[1/pN, \zeta_p]^* / \left(\mathbb{Z}[1/pN, \zeta_p]^*\right)^p\right)_{\omega^2} \to \left(\bigoplus_{\mathfrak{l}|N} \mathbb{F}_p\right)_{\omega^2} \to 0,\end{aligned}$$

where $\mathfrak{l}$ runs over the set of the primes of $\mathbb{Z}[\zeta_p]$ that lie over $N$. We identify the Galois group $\Delta$ with $\mathbb{F}_p^*$ via the cyclotomic character $\omega$. By [15, Theorem 8.13], the $\mathbb{F}_p[\Delta]$-module $\mathbb{Z}[1/p, \zeta_p]^*/(\mathbb{Z}[1/p, \zeta_p]^*)^p$ is isomorphic to $\mu_p \times \mathbb{F}_p[\Delta/\langle -1\rangle]$. So its $\omega^2$-eigenspace has $\mathbb{F}_p$-dimension 1. The module $\bigoplus_{\mathfrak{l}|N} \mathbb{F}_p$ is a permutation module isomorphic to $\bigoplus_{\ell|N} \mathbb{F}_p[\Delta/\langle\ell\rangle]$, where $\ell$ runs over the set of the primes dividing $N$. The $\omega^2$-eigenspace of $\mathbb{F}_p[\Delta/\langle\ell\rangle]$ is trivial for which $\omega^2(\ell) \neq 1$. By assumption, the $\omega^2$-eigenspace of $\bigoplus_{\ell|N} \mathbb{F}_p[\Delta/\langle\ell\rangle]$ is trivial. This shows that the group in the middle of the exact sequence (3) has dimension 1 over $\mathbb{F}_p$.

Since $p \geq 5$, the $\omega^2$-eigenspace of $\mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$ has dimension 1. By [15, Theorem 8.25], the $\omega^2$-eigenspace of the cyclotomic units is equal to the $\omega^2$-eigenspace of the local units. Therefore the $\omega^2$-eigenspace of the cyclotomic units in $\mathbb{Z}[1/p, \zeta_p]^*$ maps surjectively onto the $\omega^2$-eigenspace of $\mathbb{Q}_p(\zeta_p)^*/(\mathbb{Q}_p(\zeta_p)^*)^p$. It follows that the rightmost arrow in the exact sequence (2) is surjective. This completes the proof. □

Here we prove Theorem 1.1. The idea is based on the proof of [8, §3] or [16, Theorem 3.8]. Let $p = 5$ or 7. Let $E$ be an elliptic curve over $\mathbb{Q}$ as in Theorem 1.1. Suppose $E$ has a $p$-torsion point. Set $E_1 = E$. Since the exact sequence (1) of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules is split by Lemma 2.2 and Proposition 2.3, there exists an elliptic curve $E_2$ over $\mathbb{Q}$ and a $\mathbb{Q}$-isogeny $E_1 \to E_2$ with kernel $\mu_p$. Then the image of the Galois submodule $\mathbb{Z}/p\mathbb{Z}$ gives a point of order $p$ in $E_2$. Continuing in this fashion, we obtain a sequence of $\mathbb{Q}$-isogenies

$$E_1 \to E_2 \to \cdots ,$$

where each isogeny has kernel $\mu_p$. By Shafarevich's Theorem [12, Chapter IX, Theorem 6.1], we see that $E_i \simeq E_j$ for some $i < j$. Composing our $\mathbb{Q}$-isogenies gives an endomorphism $f : E_i \to E_i$ defined over $\mathbb{Q}$. If $P_i \in E_i(\mathbb{Q})$ is the image of $P \in E(\mathbb{Q})$, then by construction $P_i \notin \ker f$. Since $\deg f$ is a power of $p$, we see that $f$ is a non-scalar endomorphism. Therefore the elliptic curve $E_i$ has complex multiplication. But this contradicts to Lemma 2.1 (see [12, Chapter VII, Proposition 5.4]). This completes the proof of Theorem 1.1. □

## 3. The second proof of Theorem 1.1

Let $E$ be an elliptic curve over $\mathbb{Q}$ with a $p$-torsion point $R$ for $p = 5$ or 7. To prove Theorem 1.1, it suffices to show that $E$ has bad reduction at $p$, or a prime $\ell \equiv \pm 1 \bmod p$. We note that $E$ is isogeneous to an elliptic curve $E'$ over $\mathbb{Q}$ with a $p$-torsion point such that $\mathbb{Q}(E'[p])$ is a ramified extension of $\mathbb{Q}(\zeta_p)$ of degree $p$ (see the last paragraph of §2). Since both $E$ and $E'$ have bad reduction at same primes, we may assume that $F = \mathbb{Q}(E[p])$ is a ramified extension of $K = \mathbb{Q}(\zeta_p)$ of degree $p$.

Since $K$ has class number 1, the extension $F/K$ is ramified at some prime over a prime $\ell$. By the proof of [8, §3, Step 3], we have $\mathbb{Q}_p(E[p]) = \mathbb{Q}_p(\zeta_p)$ if $E$ has good reduction at $p$. Hence we may assume $\ell \neq p$. By the criterion of Néron-Ogg-Shafarevich [12, Chapter VII, Theorem 7.1], we see that $\ell$ is a prime of bad reduction for $E$. Since $E$ has semistable reduction at $\ell$ by Lemma 2.1, there exists an extension of $M$ of degree 1 or 2 over $\mathbb{Q}_\ell$ such that $E$ is isomorphic to the Tate curve $E_q$ over $M$, where $q$ is the Tate parameter (see [13, Chapter V] for details). By the theory of Tate curves, we have

$$\phi : E(\overline{\mathbb{Q}}_\ell) \simeq \overline{\mathbb{Q}}_\ell^*/q^{\mathbb{Z}} .$$

With the identification $\phi$, we clearly have

$$\phi : E[p] \simeq (\zeta_p^{\mathbb{Z}} \cdot Q^{\mathbb{Z}})/q^{\mathbb{Z}} ,$$

where $Q = q^{1/p} \in \overline{\mathbb{Q}}_\ell$ is a fixed $p$-th root of $q$. Hence we have $M(E[p]) = M(q^{1/p}, \zeta_p)$. Since $M(E[p])$ is a ramified extension of $M(\zeta_p)$ of degree $p$, we see that $q^{1/p}\zeta_p^i \notin M$ for any $i$. On the other hand, we have $\zeta_p \in M$ since $R$ is defined over $M$. Therefore we have $[\mathbb{Q}_\ell(\zeta_p) : \mathbb{Q}_\ell] = 1$ or 2, which means $\ell \equiv \pm 1 \bmod p$. This completes the proof of Theorem 1.1. □

*Proof of Theorem* 1.2. By a similar argument of the second proof of Theorem 1.1, we can prove Theorem 1.2. Let $p \geq 5$ be a prime number and $K$ a number field with the following conditions:

(a) $p$ does not divide the class number of $K(\zeta_p)$,

(b) the ramification index $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p-1$ for all primes $\mathfrak{p}$ of $K$ over $p$.

Let $E$ be an elliptic curve over $K$ with a $p$-torsion point. By a similar argument as above, we may assume that $L = K(E[p])$ is a ramified extension of $M = K(\zeta_p)$ of degree $p$. By the assumption (a), the extension $L/M$ is ramified at some prime over a prime $\mathfrak{l}$ of $M$. Let $\mathfrak{p}$ be a prime of $K$ over $p$ and let $K_{\mathfrak{p}}$ denote the completion of $K$ at $\mathfrak{p}$. By the assumption (b), we note that any finite flat group scheme over $K_{\mathfrak{p}}$ of $p$-power order admits a prolongation over the ring of integers of $K_{\mathfrak{p}}$ (see [2, Théoreme 3.3.3]). Therefore it follows from the proof of [8, §3, Step 3] that we have $K_{\mathfrak{p}}(E[p]) = K_{\mathfrak{p}}(\zeta_p)$ if $E$ has good reduction at $\mathfrak{p}$. Hence we may assume $\mathfrak{l} \nmid p$. Let $\ell$ be the prime number with $\mathfrak{l} \mid \ell$. By a similar argument as above, we have $[K_{\mathfrak{l}}(\zeta_p), K_{\mathfrak{l}}] = 1$ or 2, which means $\ell^f \equiv \pm 1 \bmod p$ where $f$ is the residue degree of $\mathfrak{l}$. This completes the proof of Theorem 1.2. □

REMARK. By Theorem 1.2 or [16, Theorem 3.8], we obtain the following results on the class number of $K(\zeta_p)$.

- Set $K = \mathbb{Q}(\sqrt{26})$ and $p = 5$. Let
$$E : y^2 + (1-\epsilon)xy - \epsilon y = x^3 - \epsilon x^2$$
be an elliptic curve over $K$, where $\epsilon = 5 + \sqrt{26}$ is the fundamental unit of $K$. Since the discriminant $\Delta(E)$ is equal to $-\epsilon^6$, we see that $E$ has good reduction everywhere. Since $E$ has a $p$-torsion point $(0, 0)$, it follows from Theorem 1.2 or [16, Theorem 3.8] that the class number of $K(\zeta_p)$ is divisible by 5. In fact, the class number of $K(\zeta_p)$ is equal to 40.
- Set $K = \mathbb{Q}(\sqrt{37})$ and $p = 5$. Let
$$E : y^2 - \epsilon y = x^3 + \frac{3\epsilon + 1}{2}x^2 + \frac{11\epsilon + 1}{2}x$$
be an elliptic curve over $K$ with good reduction everywhere, where $\epsilon = 6 + \sqrt{37}$ is the fundamental unit of $K$ (see [4]). Since $E$ has a $p$-torsion point $(0, 0)$, it follows from Theorem 1.2 or [16, Theorem 3.8] that the class number of $K(\zeta_p)$ is divisible by 5. In fact, the class number of $K(\zeta_p)$ is equal to 5.

## 4. The primes at which elliptic curves with a $p$-torsion point have bad reduction

For $p = 5$ or 7, let $E$ be an elliptic curve over $\mathbb{Q}$ with a $p$-torsion point. Theorem 1.1 shows that $E$ has bad reduction at $p$, or a prime $\ell \neq p$ with $\ell \equiv \pm 1 \bmod p$. In this section, we give some examples of the primes at which $E$ has bad reduction.

For $p = 5$, we see that the elliptic curve $E$ is isomorphic to an elliptic curve defined by the equation
$$E_\lambda^{(5)} : y^2 + (1-\lambda)xy - \lambda y = x^3 - \lambda x^2.$$
The discriminant of $E_\lambda^{(5)}$ is $\Delta(E_\lambda^{(5)}) = \lambda^5(\lambda^2 - 11\lambda - 1)$. With $\lambda \in \mathbb{Q}\setminus\{0\}$, the elliptic curve $E_\lambda^{(5)}$ has a 5-torsion point $(0, 0)$. For $p = 7$, we see that the elliptic curve $E$ is isomorphic

to an elliptic curve defined by the equation

$$E_\lambda^{(7)} : y^2 + (1 + \lambda - \lambda^2)xy + (\lambda^2 - \lambda^3)y = x^3 + (\lambda^2 - \lambda^3)x^2.$$

The discriminant of $E_\lambda^{(7)}$ is $\Delta(E_\lambda^{(7)}) = \lambda^7(\lambda-1)^7(\lambda^3 - 8\lambda^2 + 5\lambda + 1)$. With $\lambda \in \mathbb{Q} \setminus \{0, 1\}$, the elliptic curve $E_\lambda^{(7)}$ has a 7-torsion point $(0, 0)$. In the following table, we list the primes at which $E_\lambda^{(p)}$ has bad reduction for $p = 5, 7$ and some $\lambda$.

TABLE 1. The primes at which $E_\lambda^{(p)}$ has bad reduction for $p = 5, 7$ and $\lambda = 1, 2, \cdots, 10$

| $\lambda$ | The primes $\ell$ at which $E_\lambda^{(p)}$ has bad reduction | | The primes $\ell$ satisfying $\ell = p$ or $\ell \equiv \pm 1 \bmod p$ | |
|---|---|---|---|---|
| | $p = 5$ | $p = 7$ | $p = 5$ | $p = 7$ |
| 1 | 11 | — | 11 | — |
| 2 | 2, 19 | 2, 13 | 19 | 13 |
| 3 | 3, 5 | 2, 3, 29 | 5 | 29 |
| 4 | 2, 29 | 2, 3, 43 | 29 | 43 |
| 5 | 5, 31 | 2, 5, 7 | 5, 31 | 7 |
| 6 | 2, 5, 31 | 2, 3, 5, 41 | 31 | 41 |
| 7 | 7, 29 | 2, 3, 7, 13 | 29 | 7, 13 |
| 8 | 2, 5 | 2, 7, 41 | 5 | 7, 41 |
| 9 | 3, 19 | 2, 3, 127 | 19 | 127 |
| 10 | 2, 5, 11 | 2, 3, 5, 251 | 5, 11 | 251 |

## References

[1] T. A. Fisher, *On* 5 *and* 7 *descents for elliptic curves*, PhD Thesis, The University of Cambridge (2000).

[2] J. -M. Fontaine, Groupes $p$-divisible sur les corps locaux, Astérisque **47–48**, Soc. Math. France, Paris (1977).

[3] A. Grothendieck, *Modèles de Néron et monodromie*, Exp IX in Groupes de monodromie en géométrie algébrique, SGA 7, Part I, Lecture Notes in Mathematics **288** (1971) Springer-Verlag, New-York.

[4] T. Kagawa, *Elliptic curves with everywhere good reduction over real quadratic fields*, PhD Thesis, Waseda University (1998).

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

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

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

[8] B. Mazur, *Rational points on modular curves*, in Modular Functions of one Variable V, Lecture Notes in Math. **601** (1977), 107–148.

[9] A. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27.

[10] R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Annalen, **325** (2003), 413–448.

[11] R. Schoof, *Semi-stable abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only*, Composito Math. **141** (2005), 847–868.

[12] J. H. Silverman, The arithmetic of elliptic curves, Graduate Texts in Math. **106**, Springer-Verlag, Berlin-Heidelberg-New York, 1994.
[13] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Graduate Texts in Math. **151**, Springer-Verlag, Berlin-Heidelberg-New York, 1994.
[14] J. Tate, Finite flat group schemes, Modular forms and Fermat's last theorem, Springer-Verlag, Berlin-Heidelberg-New York, 1997, 121–154.
[15] L.C. Washington, Introduction to cyclotomic fields, Graduate Texts in Math. **83**, Springer-Verlag, Berlin Heidelberg New York, 1982.
[16] M. Yasuda, *Torsion points of elliptic curves with good reduction*, Kodai Math. J. **31** (2008), 385–403.

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