数理解析研究所講究録
第2012巻 2016年 41-65

Relation between torsion points and reduction of elliptic curves over number fields

Masaya Yasuda
Institute of Mathematics for Industry,
Kyushu University

Abstract

This is a summary of our previous work on relation between torsion points and bad reduction primes of an elliptic curve E over a number field. We mainly introduce some results on the non-existence of a torsion points of E of prime order p if E has bad reduction only at certain primes related with p.

1 Introduction

Let E be an elliptic curve over a number field K. For a prime p, the K-rational p-torsion points of E are the points of exact order p in the Mordell-Weil group $E(K)$. In 1975, A. Ogg [Ogg75] first conjectured which groups can be $\mathbb{Q}$-rational torsion subgroups of an elliptic curve over $\mathbb{Q}$. In 1977, Mazur [Maz77, Maz78] proved Ogg's conjecture and showed that any elliptic curve over $\mathbb{Q}$ cannot have a $\mathbb{Q}$-rational p-torsion point for the primes $p \geq 11$. For quadratic fields, Kamienny [Kam92] and Kenku-Momose [KM88] classified the possible torsion subgroups and showed that any elliptic curve over a quadratic field K has no K-rational p-torsion points for the primes $p \geq 17$. For cubic fields, Parent [Par00, Par03] proved the same result on the non-existence of p-torsion points as in the case of quadratic fields. Moreover, it was announced at the 2010 Algorithmic Number Theory Symposium (ANTS-IX) [Sto10] that Kamienny, Stein and Stoll proved that 17 is the largest prime dividing the order of the K-rational torsion subgroup of an elliptic curve over any quartic field K.

In addition to the above development on classification of possible p-torsion points, the notion of *reduction* plays an important role in the theory of elliptic

curves. In this paper, we are interested in relation between the (non-)existence of a K-rational p-torsion point of E and the primes at which E has bad reduction. To investigate the relation, it is helpful to study the ramification of the extension $K(E[p])$ over $K(\zeta_p)$, where let $K(E[p])$ denote the field generated by the p-torsion subgroup $E[p]$ and ζ_p a fixed primitive p-th root of unity. Note that this extension gives a Kummer extension of degree dividing p if E has a K-rational p-torsion point. Then the motivation of this paper is to study the relation among the following three mathematical objects:

1. (Non-)existence of a K-rational p-torsion point of E
2. The primes of K at which E has bad reduction
3. Ramification of the extension $K(E[p])$ over $K(\zeta_p)$

Agashe [Aga08] studied a part of the above relations. Specifically, he showed that if an elliptic curve over $\mathbb{Q}$ of square-free conductor N (namely, a semi-stable elliptic curve) has a $\mathbb{Q}$-rational p-torsion point for $p \geq 5$, then p divides either $6N$ or the order of the cuspidal subgroup of $J_0(N)(\mathbb{C})$, where let $J_0(N)$ denote the Jacobian variety determined by the congruence subgroup $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$. T. Takagi [Tak12] gave an explicit formula for the order of cuspidal subgroups, and he combined his result with Agashe's one to obtain a non-existence result of a $\mathbb{Q}$-rational p-torsion point of semi-stable elliptic curves over $\mathbb{Q}$ with certain conductor N. This paper basically gives a summary of the author's previous work [Yas08, Yas12a, Yas13a, Yas13b]. Especially, in this paper, we introduce an extension of Agashe-Takagi's non-existence result.

Notation The symbols $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote, respectively, the ring of integers, the field of rational numbers, the field of real numbers, and the field of complex numbers. For a prime p, the finite field with p elements is denoted by $\mathbb{F}_p$. Let ζ_p denote a fixed primitive p-th root of unity, and μ_p the set of p-th roots of unity. By $\mathbb{Z}_p$ and $\mathbb{Q}_p$, we denote the p-adic integers and the p-adic rational numbers, respectively. For a number field K, let $\mathcal{O}_K$ denote its ring of integers, and U_K the group of units in the ring $\mathcal{O}_K$. For a prime $\mathfrak{p}$ of K, let $\mathcal{O}_\mathfrak{p}$ be the completion of the ring $\mathcal{O}_K$ at $\mathfrak{p}$, and $U_\mathfrak{p}$ denote the group of units in $\mathcal{O}_\mathfrak{p}$. We also define a filtration $\{U_\mathfrak{p}^{(i)}\}_{i\geq 1}$ of the group $U_\mathfrak{p}$ given by $U_\mathfrak{p}^{(i)} = 1+\mathfrak{p}^i$ (e.g. see [Ser79, Chapter IV]), and we have $\mathcal{O}_\mathfrak{p} \supset U_\mathfrak{p} \supset U_\mathfrak{p}^{(1)} \supset \cdots \supset U_\mathfrak{p}^{(i)} \supset \cdots$. We denote by $e_\mathfrak{p}$ and $f_\mathfrak{p}$ the ramification index and the residue degree of $\mathfrak{p}$, respectively. Let $v_\mathfrak{p}$ be the normalized discrete valuation determined by $\mathfrak{p}$ (then we have $v_\mathfrak{p}(p) = e_\mathfrak{p}$).

2 Preliminaries

In this section, we give some basic results on elliptic curves, which shall be needed for our later discussions.

2.1 Elliptic curves with a p-torsion point

Given a number field K and a prime number p, fix an elliptic curve E over K having a K-rational p-torsion point P. Using the Weil-pairing

$$e_p : E[p] \times E[p] \longrightarrow \mu_p,$$

we can define a map $\psi : E[p] \longrightarrow \mu_p$ by $Q \longmapsto e_p(P, Q)$. Let G_K denote the absolute Galois group $\mathrm{Gal}(\overline{K}/K)$. Since the point P is rational over K, the map ψ gives an exact sequence of G_K-modules

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

where $\mathbb{Z}/p\mathbb{Z}$ is the constant G_K-module generated by P. Take $Q \in E[p]$ satisfying $e_p(P, Q) = \zeta_p$, and then the set $\{P, Q\}$ forms a basis of $E[p]$ as an $\mathbb{F}_p$-vector space.

Lemma 2.1. *Let $L = K(E[p])$ denote the extension field over K generated by the p-torsion points of E. Then L contains the field $F = K(\zeta_p)$.*

Proof. Since $\sigma(\zeta_p) = e_p(\sigma(P), \sigma(Q)) = e_p(P, Q) = \zeta_p$ for any element $\sigma \in \mathrm{Gal}(\overline{K}/L)$, the element ζ_p is stable under the Galois group $\mathrm{Gal}(\overline{K}/L)$. Then L contains ζ_p, and hence we have $F \subseteq L$. □

The action of G_K on $E[p]$ gives its associated Galois modulo p representation

$$\overline{\rho}_{E,p} : G_K \longrightarrow \mathrm{Aut}(E[p]) \simeq \mathrm{GL}_2(\mathbb{F}_p). \tag{2}$$

Given an element $\tau \in G_K$, we have $\overline{\rho}_{E,p}(\tau) \begin{pmatrix} P \\ Q \end{pmatrix} = \begin{pmatrix} \tau(P) \\ \tau(Q) \end{pmatrix}$. This representation induces the faithful representation $\rho : \mathrm{Gal}(L/K) \longrightarrow \mathrm{GL}_2(\mathbb{F}_p)$. By the exact sequence (1), the representation ρ has the form $\begin{pmatrix} 1 & * \\ 0 & \omega \end{pmatrix}$, where we let

$$\omega : \Delta = \mathrm{Gal}(F/K) \longrightarrow \mathbb{F}_p^{\times} \tag{3}$$

denote the cyclotomic character defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$ for every $\sigma \in \Delta$.

Proposition 2.2. *The field L is a Kummer extension over F of degree either 1 or p.*

Proof. The group $\mathrm{Gal}(L/F)$ is isomorphic to the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of all matrices of the form $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ under ρ. Therefore the field L is an extension field over F of degree dividing p, and hence L/F is a Kummer extension. □

We further consider the action of Δ on $\mathrm{Gal}(L/F)$ by conjugation in $\mathrm{Gal}(L/K)$. Let us consider Δ as a subgroup of $\mathbb{F}_p^\times$ under the cyclotomic character ω. Fix $a \in \Delta \subset \mathbb{F}_p^\times$. Since conjugating $\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ by $a \in \mathbb{F}_p^\times$ gives $\begin{pmatrix} 1 & k/a \\ 0 & 1 \end{pmatrix}$, we see that $a \in \Delta \subset \mathbb{F}_p^\times$ acts on $\mathrm{Gal}(L/F)$ as multiplication by a^{-1}. Then we can obtain the following result on the p-part of the ideal class group of F:

Proposition 2.3. *Let A_F denote the p-part of the ideal class group of F. If the extension L/F is non-trivial and unramified, then $A_F^{\omega^{-1}} \neq 0$, where let R^{ω^i} denote the ω^i-eigenspace of a $\mathbb{Z}_p[\Delta]$-module R.*

2.2 Families of elliptic curves with a p-torsion point

Here we give some facts on elliptic curves having a K-rational p-torsion point only for $p = 5$ and 7. Let E be an elliptic curve over a number field K with a K-rational p-torsion point P. For $p = 5$ and 7, there exists an element $t \in K$ such that E is isomorphic to the elliptic curve given by the Weierstrass equation

$$E_t^{(5)} : y^2 + (1-t)xy - ty = x^3 - tx^2 \text{ (if } p = 5), \text{ or} \tag{4}$$

$$E_t^{(7)} : y^2 + (1+t-t^2)xy + (t^2-t^3)y = x^3 + (t^2-t^3)x^2 \text{ (if } p = 7), \tag{5}$$

where the point $P \in E$ corresponds to $(0,0) \in E_t^{(p)}$ (see [Kub76, Table 3] or [Sil86, Appendix C] for details). Then the discriminant of $E_t^{(p)}$ is given by

$$\Delta(E_t^{(p)}) = \begin{cases} t^5 \cdot Q_5(t) & \text{for } p = 5, \\ t^7(t-1)^7 \cdot Q_7(t) & \text{for } p = 7, \end{cases}$$

where we set

$$\begin{cases} Q_5(X) = X^2 - 11X - 1, \\ Q_7(X) = X^3 - 8X^2 + 5X + 1. \end{cases}$$

2.2.1 Modular Interpretation

For an odd prime number p, let $X_1(p)$ denote the modular curve associated to the congruence subgroup $\Gamma_1(p) \subset \mathrm{SL}_2(\mathbb{Z})$. According to [Sil86, Appendix C], the modular curve $X_1(p)$ is a smooth projective curve over $\mathbb{Q}$, and it has $(p-1)$ cusps. More specifically, only half of the cusps are defined over $\mathbb{Q}$, but the other $\frac{1}{2}(p-1)$ cusps are defined over the maximal real subfield $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$ of $\mathbb{Q}(\zeta_p)$. In terms of modular curves, one elliptic curve over K having a K-rational p-torsion point corresponds to one K-rational point of $X_1(p)$. In particular, the curve $X_1(p)$ is isomorphic to the projective line $\mathbb{P}^1$ for cases $p = 5$ and 7. In the two cases, each point $[t, 1] \in \mathbb{P}^1$ maps to the pair $(E_t^{(p)}, P) \in X_1(p)$ defined over the function field $\mathbb{Q}(t)$ where P is the K-rational p-torsion point $(0, 0)$ of $E_t^{(p)}$ (in this setting, we consider t as an indeterminate element), namely, we have the correspondence

$$\mathbb{P}^1 \ni [t, 1] \longmapsto (E_t^{(p)}, P) \in X_1(p). \tag{6}$$

Furthermore, the result in [Fis00, Chapter 1] tells us that we have

$$(E_t^{(5)}, 2P) \simeq (E_{-1/t}^{(5)}, P) \text{ and } (E_t^{(7)}, 2P) \simeq (E_{(t-1)/t}^{(7)}, P). \tag{7}$$

From the correspondence (6), the cusps of the curve $X_1(p)$ correspond to the values t satisfying either $\Delta(E_t^{(p)}) = 0$ or $t = \infty$. Therefore all the cusps of $X_1(p)$ for $p = 5$ and 7 are computable and shown in the below table:

Table 1: The cusps of $X_1(p)$ for $p = 5$ and 7

p	Cusps defined over $\mathbb{Q}$	Cusps defined over $\mathbb{Q}(\zeta_p) \cap \mathbb{R}$
5	$t = 0, \infty$	the roots of $Q_5(X) = 0$ (α_5, β_5 defined below)
7	$t = 0, 1, \infty$	the roots of $Q_7(X) = 0$ ($\alpha_7, \beta_7, \gamma_7$ defined below)

2.2.2 Verdure's Kummer generators

For any Kummer extension $L/K(\zeta_p)$ of degree p, there exists an element $\kappa \in L$ satisfying both $\kappa^p = a \in K(\zeta_p)$ and $L = K(\zeta_p, \kappa) = K\left(\zeta_p, \sqrt[p]{a}\right)$.

Definition 2.4. We call such an element $\kappa \in L$ (resp. $\kappa^p = a \in K(\zeta_p)$) a *Kummer element* (resp. *Kummer generator*) for the extension $L/K(\zeta_p)$.

Given an elliptic curve E over K having a K-rational p-torsion point, Verdure [Ver06] directly computed Kummer generators for the extension $L = K(E[p])$ over $F = K(\zeta_p)$ in cases $p = 3, 5$ and 7. His main idea for obtaining such a Kummer generator is to make use of Lagrange resolvents for the p-th division polynomial associated to E. For explicit Kummer generators obtained by Verdure, let us give the roots of the equation $Q_p(X) = 0$ for $p = 5$ and 7.

- The case $p = 5$

$$\begin{cases} Q_5(X) &= (X - \alpha_5)(X - \beta_5), \\ \alpha_5 &= 8 + 5\zeta_5 + 5\zeta_5^4, \\ \beta_5 &= 3 - 5\zeta_5 - 5\zeta_5^4. \end{cases}$$

- The case $p = 7$

$$\begin{cases} Q_7(X) &= (X - \alpha_7)(X - \beta_7)(X - \gamma_7), \\ \alpha_7 &= 1 - 2\zeta_7 - 3\zeta_7^2 - 3\zeta_7^5 - 2\zeta_7^6, \\ \beta_7 &= 1 - 2\zeta_7^2 - 3\zeta_7^3 - 3\zeta_7^4 - 2\zeta_7^5, \\ \gamma_7 &= 1 - 3\zeta_7 - 2\zeta_7^3 - 2\zeta_7^4 - 3\zeta_7^6. \end{cases}$$

Then we are ready to introduce explicit Kummer generators directly computed by Verdure (note that in [Ver06, Theorem 5 and 6] he merely gives a criterion to decide whether all the p-torsion points are rational or not):

Proposition 2.5 (see Theorem 5 and 6 of [Ver06]). *Let K be the function field $\mathbb{Q}(t)$ of variable t. For $p = 5$, set*

$$a_5(t) = \frac{t - \alpha_5}{t - \beta_5} \in K(\zeta_5).$$

For $p = 7$, set

$$a_7(t) = \frac{(t - \alpha_7)(t - \beta_7)^2}{(t - \gamma_7)^3} \in K(\zeta_7).$$

Then, for $E = E_t^{(p)}$, the element $a_p(t)$ gives a Kummer generator for the extension $L = K(E[p])$ over $F = K(\zeta_p)$, namely, we have $L = F\left(\sqrt[p]{a_p(t)}\right)$.

Proof. See the computational results in the proof of [Ver06, Theorem 5 and 6] for details. Note that all the computations in [Ver06] are performed using the software package *MAGMA* for arithmetic computations. Here we give only a

sketch of his strategy; Let $L = K(E[p])$ and $F = K(\zeta_p)$. By factoring the p-th division polynomial associated to E into the product of irreducible polynomials, we first find a point $Q \in E[p]$ such that $\{P, Q\}$ forms a basis of $E[p]$ as an $\mathbb{F}_p$-vector space, where $P = (0, 0)$ denotes the p-torsion point of E. Next we find a generator σ in the group $\mathrm{Gal}(L/F)$ satisfying $\sigma(Q) = Q + P$ (see also [Ver06, Corollary 3]). Then, for a fixed number $i \in \{1, 2, \ldots, p-1\}$, we compute

$$\kappa = \sum_{k=0}^{p-1} \zeta_p^{ik} \sigma^k(x_Q) = \sum_{k=0}^{p-1} \zeta_p^{ik} x_{Q+kP} \in L,$$

where x_R denotes the x-coordinate of a point R of E. Specifically, in the proof of [Ver06, Theorem 5 and 6], Verdure takes $i = 1$ for $p = 5$ and $i = 3$ for $p = 7$. By the above construction, the element κ clearly satisfies

$$\sigma(\kappa) = \sum_{k=0}^{p-1} \zeta_p^{ik} x_{Q+(k+1)P} = \zeta_p^{-i} \sum_{k=0}^{p-1} \zeta_p^{i(k+1)} x_{Q+(k+1)P} = \zeta_p^{-i} \kappa.$$

Therefore we have $\sigma(\kappa^p) = \kappa^p$ and hence $\kappa^p \in F$, which can give a Kummer generator for the extension L/F. □

3 Non-existence of a rational p-torsion point

Given a number field K and a prime number $p \geq 5$, we study the relation between the non-existence of a K-rational p-torsion point of E over K and the primes at which E has bad reduction.

Definition 3.1. For any set S of primes of K, we say that an elliptic curve E over K has *S-reduction* if E has bad reduction only at the primes of S, in other words, if E has good reduction outside the primes of S.

In the below, we first give a main result (cf. [Yas08, Theorem 0.1] for a result on p-torsion points of an elliptic curve with everywhere good reduction):

Theorem 3.2 (Theorem 1.2 of [Yas12a]). *Let K be a number field having a real place. Let $p \geq 5$ be a prime number such that $e_{\mathfrak{p}} < p - 1$ for the primes $\mathfrak{p}$ of K over p. Set*

$$S_{K,p} = \{\mathfrak{q} : \text{prime of } K \text{ over a prime } \ell \mid \ell \neq p \text{ and } \ell^{f_{\mathfrak{q}}} \not\equiv \pm 1 \bmod p\}.$$

Let E be an elliptic curve over K with $S_{K,p}$-reduction. If p does not divide the class number h_F of $F = K(\zeta_p)$, then E has no K-rational p-torsion points.

The result of Theorem 3.2 in the case $K = \mathbb{Q}$ shows the following result:

Theorem 3.3 (The case $K = \mathbb{Q}$ of Theorem 3.2). *Let $p = 5$ or 7. Let E be an elliptic curve over $\mathbb{Q}$. If E has bad reduction only at the primes $\ell \not\equiv 0, \pm 1 \bmod p$, then E has no $\mathbb{Q}$-rational p-torsion points.*

The result of Theorem 3.3 includes Agashe-Takagi's non-existence result [Aga08, Tak12], which enforces us to restrict the case where E is semi-stable (see also Remark 3.7 below). Here we begin to prove Theorem 3.3. Specifically, we present the following two ways to prove Theorem 3.3:

1. Let E be an elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational p-torsion point. The first way is to examine the finite flat group scheme generated by the p-torsion subgroup $E[p]$ over the ring $\mathbb{Z}[1/N]$, where N is the product of the primes at which E has bad reduction. This proof mainly relies on a part of Schoof's papers [Sch03, Sch05].

2. In contrast, given an elliptic curve E over $\mathbb{Q}$ with a $\mathbb{Q}$-rational p-torsion point, the second way is to study the ramified primes of the Kummer extension $L = \mathbb{Q}(E[p])$ over $F = \mathbb{Q}(\zeta_p)$. In particular, we make use of the theory of Tate curves to study such the ramification.

Compared to Agashe-Takagi's way, our proofs are so elementary and fundamental that it does not require any knowledge about modular curves and forms.

3.1 The first proof of Theorem 3.3

Here we give the first proof of Theorem 3.3, which basically taken from [Yas12a, Section 2]. Let us start with the following well-known lemma:

Lemma 3.4. *Let E be an elliptic curve over a number field K. Suppose E has a K-rational p-torsion point for $p \geq 5$. Let $\mathfrak{q}$ be a prime of K with $\mathfrak{q} \nmid p$. Then E has semi-stable reduction at $\mathfrak{q}$.*

Proof. See the proof of [Fis00, Lemma 1.3] for details. Here we only consider the case $K = \mathbb{Q}$; Suppose E has additive reduction at a prime $q \neq p$. Consider the filtration $E(\mathbb{Q}_q) \supset E_0(\mathbb{Q}_q) \supset E_1(\mathbb{Q}_q)$ as described in [Sil86, Chapter VII]. By the theory of formal groups, the multiplication by p is invertible on the group $E_1(\mathbb{Q}_q)$. The additive reduction tells us $E_0(\mathbb{Q}_q)/E_1(\mathbb{Q}_q) \simeq \mathbb{F}_q^+$ and the Tamagawa number $[E(\mathbb{Q}_q) : E_1(\mathbb{Q}_q)]$ is at most 4. Therefore the p-torsion subgroup $E(\mathbb{Q}_q)[p]$ is trivial. This gives a contradiction to the assumption that E has a $\mathbb{Q}$-rational p-torsion point. This completes the proof. □

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 $\mathbb{Q}$-rational p-torsion point P. Let $\mathcal{E}$ be the Néron model of E over $\mathbb{Z}$. By Lemma 3.4 and Grothendieck's semi-stable reduction [Gro71, Theorem in Exp. IX], we see that $\mathcal{E}[p]$ is a finite flat group scheme over the ring $\mathbb{Z}[1/N]$, where let $G[p]$ denote the kernel of multiplication by p for a group scheme G. By [Maz77, Step 1 in Section 3], we have $\mathbb{Z}/p\mathbb{Z} \subset \mathcal{E}$, where $\mathbb{Z}/p\mathbb{Z}$ denotes the constant group scheme over $\mathbb{Z}[1/N]$ generated by the point P.

Lemma 3.5. *The exact sequence* (1) *of* $G_{\mathbb{Q}}$*-modules induces an exact sequence*

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

of finite flat group schemes over $\mathbb{Z}[1/N]$*, where* $\mathbb{Z}/p\mathbb{Z}$ *(resp.* μ_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 $\operatorname{coker}\left(\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathcal{E}[p]\right)$. It suffices to show that G is isomorphic to the diagonalizable group scheme μ_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 μ_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 any group scheme over $\mathbb{Z}_p$ is uniquely determined up to isomorphism by its isomorphism type over $\mathbb{Q}_p$ (e.g., see [Tat97]), the group scheme G is isomorphic to the diagonalizable group scheme μ_p over $\mathbb{Z}_p$. This shows that G is isomorphic to μ_p over $\mathbb{Z}[1/N]$ by [Sch03, Proposition 2.3]. □

Let $\mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ denote the group of extensions of μ_p by $\mathbb{Z}/p\mathbb{Z}$ over the ring $\mathbb{Z}[1/N]$. By the above lemma, we clearly 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 clarified the group $\mathrm{Ext}^1_{\mathbb{Z}[1/\ell]}(\mu_p, \mathbb{Z}/p\mathbb{Z})$ [Sch05, Corollary 4.2]. Based on [Sch05, Corollary 4.2], we shall give a key result to prove Theorem 3.3 as follows:

Proposition 3.6. *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 [Sch05, Corollary 4.2]. Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and let $\omega : \Delta \longrightarrow \mathbb{F}_p^{\times}$ denote the cyclotomic character (3). For any $\mathbb{F}_p[\Delta]$-module M, let M^{ω^i} denote the ω^i-eigenspace of M as in Proposition

2.3. By a similar proof of [Sch05, Proposition 4.1], we get an exact sequence

$$0 \longrightarrow \mathrm{Ext}^1_{\mathbb{Z}[1/N]}(\mu_p, \mathbb{Z}/p\mathbb{Z}) \longrightarrow \left(\mathbb{Z}[1/pN, \zeta_p]^\times / \left(\mathbb{Z}[1/pN, \zeta_p]^\times\right)^p\right)^{\omega^2} \longrightarrow \left(\mathbb{Q}_p(\zeta_p)^\times / \left(\mathbb{Q}_p(\zeta_p)^\times\right)^p\right)^{\omega^2}. \quad (8)$$

We shall compute the group in the middle of the exact sequence (8). By the proof of [Sch05, Corollary 4.2], we get the following exact sequence of ω^2-eigenspaces

$$0 \longrightarrow \left(\mathbb{Z}[1/p, \zeta_p]^\times / \left(\mathbb{Z}[1/p, \zeta_p]^\times\right)^p\right)^{\omega^2} \longrightarrow \left(\mathbb{Z}[1/pN, \zeta_p]^\times / \left(\mathbb{Z}[1/pN, \zeta_p]^\times\right)^p\right)^{\omega^2} \longrightarrow \left(\bigoplus_{\mathfrak{l}|N} \mathbb{F}_p\right)^{\omega^2} \longrightarrow 0, \quad (9)$$

where $\mathfrak{l}$ runs over the set of the primes of $\mathbb{Z}[\zeta_p]$ lying over N. We identify the Galois group Δ with $\mathbb{F}_p^\times$ via the cyclotomic character ω. By [Was82, Theorem 8.13], the $\mathbb{F}_p[\Delta]$-module $\mathbb{Z}[1/p, \zeta_p]^\times/(\mathbb{Z}[1/p, \zeta_p]^\times)^p$ is isomorphic to $\mu_p \times \mathbb{F}_p[\Delta/\langle -1\rangle]$. So its ω^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 ℓ runs over the set of the primes dividing N. The ω^2-eigenspace of $\mathbb{F}_p[\Delta/\langle\ell\rangle]$ is trivial for which $\omega^2(\ell) \neq 1$. By assumption, the ω^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 sequence (9) has dimension 1 over $\mathbb{F}_p$. Furthermore, since $p \geq 5$, the ω^2-eigenspace of $\mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$ has dimension 1. By [Was82, Theorem 8.25], the ω^2-eigenspace of the cyclotomic units is equal to the ω^2-eigenspace of the local units. Therefore the ω^2-eigenspace of the cyclotomic units in $\mathbb{Z}[1/p, \zeta_p]^\times$ maps surjectively onto the ω^2-eigenspace of $\mathbb{Q}_p(\zeta_p)^\times/(\mathbb{Q}_p(\zeta_p)^\times)^p$. It follows that the rightmost arrow in the sequence (8) is surjective. This completes the proof. □

Here we are ready to prove Theorem 3.3. The idea is mainly based on the proof of [Maz77, Section 3]. Let $p = 5$ or 7. Let E be an elliptic curve over $\mathbb{Q}$ as in Theorem 3.3. Suppose E has a $\mathbb{Q}$-rational p-torsion point P. Set $E_1 = E$. Since the exact sequence (1) of $G_\mathbb{Q}$-modules is split by Lemma 3.5 and Proposition 3.6, there exists an elliptic curve E_2 over $\mathbb{Q}$ and a $\mathbb{Q}$-isogeny $E_1 \longrightarrow E_2$ with kernel μ_p. Then the image of the Galois submodule $\mathbb{Z}/p\mathbb{Z}$ of $E_1[p]$ gives a $\mathbb{Q}$-rational p-torsion point in the elliptic curve E_2. Continuing in this fashion, we obtain a sequence of $\mathbb{Q}$-isogenies $E_1 \longrightarrow E_2 \longrightarrow \cdots$, where each isogeny has kernel μ_p and each curve E_i has a $\mathbb{Q}$-rational p-torsion point. By Shafarevich's Theorem [Sil86, Theorem 6.1], we see that $E_{i_0} \simeq E_{j_0}$ for some

$i_0 < j_0$. Composing the above $\mathbb{Q}$-isogenies gives an endomorphism $f : E_{i_0} \longrightarrow E_{i_0}$ defined over $\mathbb{Q}$. If $P_{i_0} \in E_{i_0}(\mathbb{Q})$ is the image of the starting p-torsion point $P \in E(\mathbb{Q})$, then by construction we have $P_{i_0} \notin \ker f$. Since $\deg f$ is a power of p, we see that f is a non-scalar endomorphism. Therefore the elliptic curve E_{i_0} has complex multiplication. But this contradicts to Lemma 3.4 since any elliptic curve with complex multiplication cannot have semi-stable reduction (e.g., see [Sil86, Proposition 5.4 and 5.5] and [Sil94, Corollary 6.4])[1]. This completes the first proof of Theorem 3.3. □

3.2 The second proof of Theorem 3.3

Here we give the second proof of Theorem 3.3, which is taken from [Yas12a, Section 3]. Let E be an elliptic curve over $\mathbb{Q}$ with a $\mathbb{Q}$-rational p-torsion point P for $p = 5$ or 7. To prove Theorem 3.3, 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 $\mathbb{Q}$-rational p-torsion point such that $\mathbb{Q}(E'[p])$ is a ramified extension of $\mathbb{Q}(\zeta_p)$ of degree p. Since both E and E' have bad reduction at the same primes, we may assume that $L = \mathbb{Q}(E[p])$ is a ramified Kummer extension of $F = \mathbb{Q}(\zeta_p)$ of degree p.

Since the cyclotomic field F has class number 1, the extension L/F is ramified at some primes over a prime ℓ. By the proof of [Maz77, Step 3 in Section 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 [Sil86, Theorem 7.1], we see that ℓ is a prime of bad reduction for E. Since E has semi-stable reduction at ℓ by Lemma 3.4, 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 denotes the Tate parameter (e.g., [Sil94, Chapter V] for details). By the theory of Tate curves, we have

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

With this ϕ, we also have $\phi : E[p] \simeq (\zeta_p^{\mathbb{Z}} \cdot R^{\mathbb{Z}})/q^{\mathbb{Z}}$, where $R = q^{1/p} \in \overline{\mathbb{Q}}_\ell$ is a fixed primitive p-th root of q. Then 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 the p-torsion point P is defined over M. Therefore we have $[\mathbb{Q}_\ell(\zeta_p) : \mathbb{Q}_\ell] = 1$ or 2, which means $\ell \equiv \pm 1 \bmod p$. □

[1] In order to lead this contradiction, we further need the well-known fact proved by Tate [Tat74] that there is no elliptic curve over $\mathbb{Q}$ with good reduction everywhere. In other words, any elliptic curve over $\mathbb{Q}$ with complex multiplication has always bad reduction somewhere.

Remark 3.7. Here we briefly introduce the key result in Agashe-Takagi's way [Aga08, Tak12] to prove Theorem 3.3 under the condition that E has semi-stable. The key in their proof is the result of Theorem 1.1 proved by Agashe [Aga08]. For the sake of simplicity, we here give an *informal* statement of his result (see [Aga08, Theorem 1.1] for details): "Given an elliptic curve E over $\mathbb{Q}$ of square-free conductor N. Let r be a prime dividing the order of the $\mathbb{Q}$-rational torsion subgroup $E(\mathbb{Q})_{\mathrm{tor}}$. Then the prime r divides either $6N$ or the order of the cuspidal subgroup C, where C is defined as the group of zero divisors on the modular curve $X_0(N)(\mathbb{C})$ that supported on the cusps." Compared to our two proofs, his proof is considerably tricky and it requires a lot of knowledge about the theory of modular forms. However, his proof is important in the literature, and it gives an interesting relation among torsion subgroups and cuspidal subgroups. In other words, the (non-)existence of a rational torsion point of an elliptic curve may be explained in terms of cuspidal subgroups. In fact, as mentioned in [Aga08, Section 1], he suspects $E(\mathbb{Q})_{\mathrm{tor}} \subseteq C$ as long as N is square-free. In particular, when N is prime, Mazur [Maz77] proved that $C = J_0(N)(\mathbb{Q})$ and hence the above relation holds in this case.

3.3 Proof of Theorem 3.2

By a similar argument of the second proof of Theorem 3.3, we can prove the result of Theorem 3.2 as a generalization of Theorem 3.3 for a general number field K. Let $p \geq 5$ be a prime number and K a number field such that the following two conditions are satisfied:

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

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

Let E be an elliptic curve over K with a K-rational p-torsion point. By a similar argument as in Section 3.2, we may assume that $L = K(E[p])$ is a ramified extension over F of degree p. By the assumption (a), the extension L/F is ramified at some primes over a prime $\mathfrak{q}$ of K. Let $\mathfrak{p}$ be a prime of K over p. By the assumption (b), any finite flat group scheme over $K_{\mathfrak{p}}$ of p-power order admits a prolongation over the ring of integers of $K_{\mathfrak{p}}$ [Fon77, Théoreme 3.3.3]. Therefore it follows from the proof of [Maz77, Step 3 in Section 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 $\mathfrak{q} \nmid p$. Let ℓ be the prime number satisfying $\mathfrak{q} \mid \ell$. By a similar argument as in the previous subsection, we have $[K_{\mathfrak{q}}(\zeta_p) : K_{\mathfrak{q}}] = 1$ or 2, which means $\ell^{f_{\mathfrak{q}}} \equiv \pm 1 \bmod p$. □

4 Elliptic curves having both $S_{K,p}$-reduction and a p-torsion point

Given a prime number $p \geq 5$ and a number field K such that $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p. Set $F = K(\zeta_p)$. It follows from Theorem 3.2 that the class number h_F of F is divisible by p if there exists an elliptic curve E over K having both $S_{K,p}$-reduction and a K-rational p-torsion point. This means that *the existence of such a pair (E, K) tells us the p-divisibility of the class number h_F* (note that there exist no such elliptic curves over $\mathbb{Q}$ since the class number of $\mathbb{Q}(\zeta_p)$ is equal to 1 for $p = 5$ and 7). Here we give several examples of such pairs (E, K) only for $p = 5$ and 7. Our strategy to construct such pairs is to start with taking an elliptic curve $E = E_t^{(p)}$ for $p = 5$ or 7, which has a K-rational p-torsion point $P = (0, 0)$.

Proposition 4.1. *Let $p = 5$ or 7. Let $E = E_t^{(p)}, t \in \mathcal{O}_K$ be an elliptic curve over K defined as in Section 2.2. Assume that the Weierstrass equation (4) (resp. the equation (5)) for E in the case $p = 5$ (resp. the case $p = 7$) is minimal. If E has $S_{K,p}$-reduction, then $Q_p(t) \in U_K$ where the polynomial $Q_p(X) \in \mathbb{Z}[X]$ is already defined in Subsection 2.2.*

Proof. We consider only the case $p = 7$. Assume that $Q_7(t) \notin U_K$ and E has $S_{K,p}$-reduction. Then there exists a prime ℓ dividing the value $Q_7(t) = t^3 - 8t^2 + 5t + 1 \in \mathcal{O}_K$. Since ℓ divides the minimal discriminant $\Delta(E) = t^7(t-1)^7 \cdot Q_7(t)$ of E, the curve E has bad reduction at a certain prime $\mathfrak{q}$ of K over ℓ (it requires the assumption that $\Delta(E)$ is minimal). Since E has $S_{K,p}$-reduction, we may assume $\ell \neq 7$. The solutions of the equation $Q_7(X) = X^3 - 8X^2 + 5X + 1 = 0$ define the extension field $K(\zeta_7 + \zeta_7^{-1})$ over K. Now consider the 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 by (3) 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 $\omega(s) = \ell^{f_{\mathfrak{q}}} \in (\mathbb{Z}/7\mathbb{Z})^\times$. Then we obtain

$$\begin{aligned} & Q_7(X) \equiv 0 \bmod \mathfrak{q} \text{ has a solution } X = t \in \mathcal{O}_K, \\ \Longrightarrow\ & Q_7(X) = 0 \text{ has a solution } X = t' \in \mathcal{O}_{\mathfrak{q}} \text{ by Hensel's lemma}, \\ \Longrightarrow\ & \sigma(s) = 1 \in \mathrm{Gal}(K(\zeta_7+\zeta_7^{-1})/K) \Longleftrightarrow \ell^{f_{\mathfrak{q}}} \equiv \pm 1 \bmod 7. \end{aligned}$$

This is a contradiction to the assumption that E has $S_{K,p}$-reduction. □

We are ready to construct our desired pairs (E, K). Given a number field K and a prime $p = 5$ or 7, we only need to find $t \in \mathcal{O}_K$ satisfying $Q_p(t) \in U_K$. Here we consider only the case of quadratic fields $K = \mathbb{Q}(\sqrt{m})$, where m is a square-free integer. In this case, the assumption in Theorem 3.2 that $e_{\mathfrak{p}} < p-1$ for the primes $\mathfrak{p}$ of K over p is satisfied for $p = 5$ and 7. Set $t = a + b\sqrt{m} \in \mathcal{O}_K$ with $2a, 2b \in \mathbb{Z}$. Let $0 \neq u = a^2 - mb^2 = \mathrm{Nm}_{K/\mathbb{Q}}(t) \in \mathbb{Z}$ denote the norm of $t \in \mathcal{O}_K$. We consider each of the two cases $p = 5$ and 7 as follows:

4.1 The case $p = 5$

As described above, consider the condition

$$Q_5(t) = t^2 - 11t - 1 \in U_K \Longleftrightarrow \mathrm{Nm}_{K/\mathbb{Q}}(t^2 - 11t - 1) = \pm 1. \tag{10}$$

Since $\mathrm{Nm}_{K/\mathbb{Q}}(t^2 - 11t - 1) = -4a^2 - 22(u-1)a + u^2 + 123u + 1$, the condition (10) is equivalent to the condition

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

with $X = 2a \in \mathbb{Z}$. Furthermore, the equation (11) can be transformed to the Pell equation

$$A^2 - 5B^2 = \pm 4 \tag{12}$$

with

$$\begin{cases} A = 2X + 11(u-1) \in \mathbb{Z}, \\ B = 5(u+1) \in \mathbb{Z}. \end{cases}$$

Let $\varepsilon = \dfrac{1+\sqrt{5}}{2}$ be a fundamental unit of $\mathbb{Q}(\sqrt{5})$. It is well known that the integral solutions of the Pell equation (12) are given by the elements $\pm\varepsilon^n$ for $n = 0, 1, 2, \cdots$. Since $B \in 5\mathbb{Z}$, we note that the solutions of (11) corresponds to the elements $\pm\varepsilon^{5n}$ for $n = 0, 1, 2, \cdots$, namely, we have a correspondence

$$\{t \in \mathcal{O}_K \mid Q_5(t) \in U_K\} \longleftrightarrow \left\{\text{solutions of (12) given by } \pm\varepsilon^{5n}\right\}. \tag{13}$$

Therefore we can construct infinitely many elements $t \in \mathcal{O}_K$ satisfying $Q_5(t) \in U_K$ for $p = 5$. For example, we have that an integral solution $(A, B) = (-11, -5)$ of the Pell equation (12) corresponds the element $-\varepsilon^5 = -\dfrac{11+5\sqrt{5}}{2}$. Then the

solution $(A, B) = (-11, -5)$ further corresponds to a pair $(X, u) = (11, -2)$ satisfying the condition (11).

An easy computation shows that only the pairs

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

satisfy the condition (11) with $|u| < 1000$. For each pair (X, u), we need to compute a solution (a, b, m) and check whether the elliptic curve $E_t^{(5)}, t = a + b\sqrt{m} \in \mathcal{O}_K$ over $K = \mathbb{Q}(\sqrt{m})$ has $S_{K,5}$-reduction as in the following examples:

Example 4.2. Here we give some examples of elliptic curves $E_t^{(5)}$ over $K = \mathbb{Q}(\sqrt{m})$ having both $S_{K,5}$-reduction and a K-rational 5-torsion point.

- For $(X, u) = (10, -1)$, we have a solution $(a, b, m) = (5, 1, 26)$. We see that the elliptic curve $E = E_t^{(5)}, t = a + b\sqrt{m}$ has good reduction everywhere over $K = \mathbb{Q}(\sqrt{26})$ (in fact, this curve appears in Cremona's table [Cre]). Therefore E has $S_{K,5}$-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 $E = E_t^{(5)}, t = a + b\sqrt{m}$ has bad reduction only at the primes of $K = \mathbb{Q}(\sqrt{129})$ over 2. Therefore E has $S_{K,5}$-reduction.
- For $(X, u) = (12, 10)$, we have a solution $(a, b, m) = (6, 1, 26)$. Since the elliptic curve $E = E_t^{(5)}, t = a + b\sqrt{m}$ has bad reduction at the primes of $K = \mathbb{Q}(\sqrt{26})$ over 5, the elliptic curve E does not have $S_{K,5}$-reduction unlike the above two curves.

In Table 2, we list triples (a, b, m) such that the elliptic curve $E_t^{(5)}, t = a + b\sqrt{m} \in \mathcal{O}_K$ over $K = \mathbb{Q}(\sqrt{m})$ has $S_{K,5}$-reduction. Furthermore, for each triple (a, b, m), we also list the class number h_F of $F = K(\zeta_p)$, which can be easily computed by [PARI] (version 2.4.1) (it is a free software library for arithmetic computations). As described in the first paragraph of Section 4, the class number h_F is divisible by p for all the triples (a, b, m) in Table 2.

4.2 The case $p = 7$

As in the case $p = 5$, consider the condition

$$Q_7(t) = t^3 - 8t^2 + 5t + 1 \in U_K \iff \mathrm{Nm}_{K/\mathbb{Q}}(t^3 - 8t^2 + 5t + 1) = \pm 1. \quad (14)$$

Table 2: List of triples (a,b,m) with $|u|<1000$ such that $E_t^{(p)}, t=a+b\sqrt{m}$ over $K=\mathbb{Q}(\sqrt{m})$ has $S_{K,p}$-reduction for $p=5$ and 7 ($u=a^2-mb^2=\mathrm{Nm}_{K/\mathbb{Q}}(t)$ and $F=K(\zeta_p)$)

p	(X,u)	(a,b,m)	h_F
5	$(10,-1)$	$(5,1,26)$*	40
	$(12,-1)$	$(6,1,37)$*	5
	$(11,-2)$	$\left(\frac{11}{2},\frac{1}{2},129\right)$	10
	$(22,-2)$	$(11,1,123)$	160
	$(10,-12)$	$(5,1,37)$*	5
	$(133,-12)$	$\left(\frac{133}{2},\frac{1}{2},17737\right)$	307125
	$(-1342,121)$	$(-671,1,450120)$	320
	$(0,-123)$	$(0,1,123)$	160
	$(1364,-123)$	$(682,1,465247)$	461194240
7	$(6,-1)$	$(3,1,10)$	28
	$(7,-2)$	$\left(\frac{7}{2},\frac{1}{2},57\right)$	56
	$(8,5)$	$(4,1,11)$	28

*These triples define elliptic curves with good reduction everywhere (see Cremona's table [Cre] for list of such elliptic curves)

A easy 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 (14) is equivalent to the condition

$$X^3+(5u-8)X^2+(-8u^2-43u+5)X+(u^3+54u^2+4u+1)=\pm 1 \qquad (15)$$

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 (15) with $|u|<1000$. In Table 2, we also list triples (a,b,m) such that the elliptic curve $E_t^{(7)}, t=a+b\sqrt{m}\in\mathcal{O}_K$ over $K=\mathbb{Q}(\sqrt{m})$ has $S_{K,7}$-reduction. As in the case $p=5$, the class number h_F of $F=K(\zeta_7)$ is divisible by 7 for all the triples (a,b,m).

Remark 4.3. The equation (15) defines a non-singular projective curve C of genus 1. It follows from Siegel's Theorem [Sil86, Section 3] that the set $C(\mathbb{Z})$ of integral solutions is finite. Therefore, unlike in the case $p = 5$, there are only finitely many elements $t \in \mathcal{O}_K$ satisfying $Q_7(t) \in U_K$ for $p = 7$. Furthermore, we note that data of Table 2 are summarized again in Table 3 below in order to show several unramified Kummer extensions over $F = K(\zeta_p)$ for $p = 5, 7$ (we also note that we don't know whether the data of Table 2 can give all the elements of $C(\mathbb{Z})$).

5 Ramification of Kummer extensions

In this section, we study the ramification of the Kummer extension $L = K(E[p])$ over $F = K(\zeta_p)$ for an elliptic curve E over K having a K-rational p-torsion point. The criterion of Néron-Ogg-Shafarevich [Sil86, Theorem 7.1] implies that the ramification of the extension L/F is deeply related with the bad reduction primes of E. Moreover, Kummer generators of L/F help us to study the ramification in more detail. Here we focus on Kummer extensions given by the p-torsion subgroup of $E = E_t^{(p)}$ for $p = 5$ and 7, as defined in Subsection 2.2. We begin to introduce the following main result:

Theorem 5.1 (Theorem 1.1 of [Yas13b]). *For $p = 5$ or 7, set $E = E_t^{(p)}, t \in \mathcal{O}_K$. If the Kummer extension $L = K(E[p])$ over $F = K(\zeta_p)$ has degree p, then the extension L/F is unramified outside the set of primes dividing $Q_p(t) \in \mathcal{O}_K$, where the polynomial $Q_p(X) \in \mathbb{Z}[X]$ is defined in Subsection 2.2.*

Given an elliptic curve $E = E_t^{(p)}, t \in \mathcal{O}_K$ over a number filed K, set $L = K(E[p])$ and $F = K(\zeta_p)$ as in Theorem 5.1. By the criterion of Néron-Ogg-Shafarevich, the extension L/F must be unramified outside the primes dividing p, t and $Q_p(t)$ (resp. p, t, $t-1$ and $Q_p(t)$) in the case $p = 5$ (resp. the case $p = 7$) since the discriminant $\Delta(E)$ of E is equal to $t^5 \cdot Q_5(t)$ (resp. $t^7(t-1)^7 \cdot Q_7(t)$) as described in Section 2.2. In contrast, Theorem 5.1 further tells us that *the extension L/F is unramified outside only the primes dividing $Q_p(t) \in \mathcal{O}_K$* for $p = 5$ and 7.

5.1 Proof of Theorem 5.1

Here we shall give a proof of Theorem 5.1. Given an elliptic curve $E = E_t^{(p)}, t \in \mathcal{O}_K$ for $p = 5$ or 7, our method is to study the ramification of the Kummer

extension $L = K(E[p])$ over $F = K(\zeta_p)$ using Verdure's explicit Kummer generators $a_p(t)$ given in Proposition 2.5. To prove Theorem 5.1, it only suffices to show that the Kummer extension L/F is unramified at the primes $\mathfrak{P}$ of F satisfying $v_{\mathfrak{P}}(Q_p(t)) = 0$; this condition means that the value $Q_p(t)$ is not divisible by $\mathfrak{P}$. Before giving a proof, we give the following well-known result of ramification in Kummer extensions of prime degree.

Lemma 5.2. *Let F be a number field containing the p-th roots of unity, and let $L = F\left(\sqrt[p]{x}\right)$ be a Kummer extension field for some $x \in F$.*

(i) *If $\mathfrak{Q}$ is a prime of F not dividing p, then L/F is unramified at $\mathfrak{Q}$ if and only if $v_{\mathfrak{Q}}(x) \equiv 0 \bmod p$.*

(ii) *Let $\mathfrak{P}$ be a prime of F dividing p with the ramification index $e = e_{\mathfrak{P}}$. Assume $x \in U_{\mathfrak{P}}$. Then L/F is unramified at $\mathfrak{P}$ if and only if the Kummer generator x is congruent to a p-th power modulo $\mathfrak{P}^{ep/(p-1)}$, namely, there exists an element $y \in U_{\mathfrak{P}}$ such that*

$$x \equiv y^p \bmod \mathfrak{P}^{ep/(p-1)} \Longleftrightarrow x \cdot y^{-p} \equiv 1 \bmod \mathfrak{P}^{ep/(p-1)}.$$

Proof. See [CF67, Exercise 2.12] for a proof of (i), and also [Was82, Lemma 9.1 and Exercise 9.3] or [Sai97, Theorem 8.38] for a proof of (ii). □

Then let us prove Theorem 5.1 for each of the two cases $p = 5$ and 7 in the below (the proof is basically taken from [Yas13b, Section 3]):

5.1.1 The case $p = 5$

Let $\mathfrak{Q}$ be a prime of F not dividing 5, and assume $v_{\mathfrak{Q}}(Q_5(t)) = 0$. In this case, we have $v_{\mathfrak{Q}}(a_5(t)) = v_{\mathfrak{Q}}(t - \alpha_5) - v_{\mathfrak{Q}}(t - \beta_5) = 0$ since the prime $\mathfrak{Q}$ divides neither $t - \alpha_5$ nor $t - \beta_5$ due to the assumption $v_{\mathfrak{Q}}(Q_5(t)) = 0$ (we remark that two elements $t - \alpha_5$ and $t - \beta_5$ are in the ring $\mathcal{O}_F$ and we have $v_{\mathfrak{Q}}(t - \alpha_5), v_{\mathfrak{Q}}(t - \beta_5) \geq 0$ due to the assumption $t \in \mathcal{O}_K$). Since the Kummer generator $a_5(t)$ is not divisible by $\mathfrak{Q}$, it follows from Lemma 5.2 (i) that the Kummer extension $L = F\left(\sqrt[5]{a_5(t)}\right)$ over F is unramified at any prime $\mathfrak{Q}$ of F not dividing 5 with $v_{\mathfrak{Q}}(Q_5(t)) = 0$.

Then it only suffices to consider the primes $\mathfrak{P}$ of F dividing 5. As in the above, assume $v_{\mathfrak{P}}(Q_5(t)) = 0$. In this case, the prime $\mathfrak{P}$ is over the prime $\mathfrak{P}_0 = (1-\zeta_5)$ of the cyclotomic field $\mathbb{Q}(\zeta_5) \subset F$, which is the only one prime over 5. The assumption $v_{\mathfrak{P}}(Q_5(t)) = 0$ shows $v_{\mathfrak{P}}(a_5(t)) = 0$ by the same argument as

in the above paragraph, and hence we have $a_5(t) \in U_{\mathfrak{P}}$. To study the ramification of the Kummer extension L/F for the prime $\mathfrak{P}$ over 5, we further need to consider which subgroup $U_{\mathfrak{P}}^{(i)}$ of $U_{\mathfrak{P}}$ contains the Kummer generator $a_5(t)$. For that purpose, we consider

$$a_5(t) - 1 = \frac{\beta_5 - \alpha_5}{t - \beta_5} = \frac{-5(1 + 2\zeta_5 + 2\zeta_5^4)}{t - \beta_5} = \frac{-5(1 - \zeta_5)^2(\zeta_5 + \zeta_5^2)}{t - \beta_5}. \tag{16}$$

From this equation, we clearly have $v_{\mathfrak{P}}(a_5(t) - 1) = e_{\mathfrak{P}} + \frac{e_{\mathfrak{P}}}{2} = \frac{3e_{\mathfrak{P}}}{2}$ since the element $\zeta_5 + \zeta_5^2$ of the field $\mathbb{Q}(\zeta_5)$ is not divisible by $\mathfrak{P}_0 = (1 - \zeta_5)$ and $v_{\mathfrak{P}}(t - \beta_5) = 0$ due to the assumption $v_{\mathfrak{P}}(Q_5(t)) = 0$ (we also note that $v_{\mathfrak{P}}(5) = e_{\mathfrak{P}}$). Hence the Kummer generator $a_5(t)$ is included in the subgroup $U_{\mathfrak{P}}^{(i_0)}$ for $i_0 = \dfrac{3e_{\mathfrak{P}}}{2}$. Since $i_0 > \dfrac{pe_{\mathfrak{P}}}{p-1}$ for $p = 5$, the Kummer extension L/F is unramified at any prime $\mathfrak{P}$ dividing 5 with $v_{\mathfrak{P}}(Q_5(t)) = 0$ by Lemma 5.2 (ii). This completes the proof of Theorem 5.1 in the case $p = 5$. □

5.1.2 The case $p = 7$

By a similar argument in the case $p = 5$, it only suffices to consider the primes $\mathfrak{P}$ dividing 7. Assume $v_{\mathfrak{P}}(Q_7(t)) = 0$. Then the prime $\mathfrak{P}$ is over the prime $\mathfrak{P}_0 = (1 - \zeta_7)$ of the cyclotomic field $\mathbb{Q}(\zeta_7)$, which is the only one prime over 7. The assumption $v_{\mathfrak{P}}(Q_7(t)) = 0$ tells us that we have $v_{\mathfrak{P}}(a_7(t)) = 0$, and hence $a_7(t) \in U_{\mathfrak{P}}$ (the assumption $t \in \mathcal{O}_K$ is necessary for this fact). As in the argument of the case $p = 5$, we need to consider which subgroup $U_{\mathfrak{P}}^{(i)}$ of $U_{\mathfrak{P}}$ contains the Kummer generator $a_7(t)$. By using the software library [PARI], we can easily compute the following:

$$a_7(t) - 1 = \frac{(t - \alpha_7)(t - \beta_7)^2 - (t - \gamma_7)^3}{(t - \gamma_7)^3} = \frac{A(t^2 + Bt + C)}{(t - \gamma_7)^3} \tag{17}$$

where

$$\begin{cases} A = 7(1 + 2\zeta_7^2 + \zeta_7^3 + \zeta_7^4 + 2\zeta_7^5) \text{ with } v_{\mathfrak{P}_0}(A) = 8, \\ B = -5 - 2\zeta_7^2 - 2\zeta_7^5, \\ C = 10 + 8\zeta_7^2 + 4\zeta_7^3 + 4\zeta_7^4 + 8\zeta_7^5. \end{cases}$$

Note that we have $v_{\mathfrak{P}}(t - \gamma_7) = 0$ by the assumption $v_{\mathfrak{P}}(Q_7(t)) = 0$, and $v_{\mathfrak{P}}(t^2 + Bt + C) \geq 0$ since $t^2 + Bt + C \in \mathcal{O}_F$ (it also requires the assumption $t \in \mathcal{O}_K$). From the above consideration, we have

$$v_{\mathfrak{P}}(a_7(t) - 1) \geq v_{\mathfrak{P}}(A) = \frac{8e_{\mathfrak{P}}}{6} = \frac{4e_{\mathfrak{P}}}{3} \tag{18}$$

since $v_{\mathfrak{P}}(\mathfrak{P}_0) = \frac{e_{\mathfrak{P}}}{6}$ due to that the extension degree of $\mathbb{Q}(\zeta_7)$ over $\mathbb{Q}$ is equal to 6. Hence the Kummer generator $a_7(t)$ is included in the subgroup $U_{\mathfrak{P}}^{(i_0)}$ for $i_0 = \frac{4e_{\mathfrak{P}}}{3}$. Since $i_0 > \frac{pe_{\mathfrak{P}}}{p-1}$ for $p = 7$, the Kummer extension $L = F\left(\sqrt[7]{a_7(t)}\right)$ over F is unramified at any prime $\mathfrak{P}$ dividing 7 with $v_{\mathfrak{P}}(Q_7(t)) = 0$ by Lemma 5.2 (ii). This completes the proof of Theorem 5.1 in the case $p = 7$. □

5.2 Unramified Kummer extensions generated from $a_p(t)$

Let $K = \mathbb{Q}(\sqrt{m})$ be a quadratic field, where m is a square-free integer. In his papers [Nak89, Nak91], Nakagoshi gives an explicit condition for when a fundamental unit of quadratic fields gives an unramified Kummer extension over $F = K(\zeta_p)$ of degree p, and he also gives some examples of such unramified Kummer extensions for $p = 3, 5, 7$ and 13 in [Nak89, Table 2 and 3]. In contrast to his examples, we give unramified Kummer extensions over the same field F generated from the Kummer generators $a_p(t)$ given in Proposition 2.5 for $p = 5$ and 7. For that purpose, we need to find elements $t \in \mathcal{O}_K$ with $Q_p(t) \in U_K$ by Theorem 5.1. These elements $t \in \mathcal{O}_K$ have already been found in Section 4 (see also Proposition 4.1). In fact, some pairs (m, t) satisfying our desired condition for $K = \mathbb{Q}(\sqrt{m})$ are shown in Table 2. Hence we can give several unramified Kummer extensions over F generated from the Kummer generators $a_p(t)$ for $p = 5$ and 7, which we summarize in Table 3.

As in Table 2, the class number h_F of F in Table 3 is divisible by p and hence the p-part A_F of the ideal class group of F is not equal to zero (the class numbers h_K and h_F in Table 3 are computed by using [PARI]). Furthermore, since these fields F are constructed by the p-torsion subgroup of elliptic curves, we have $A_F^{\omega^{-1}} \neq 0$ by Proposition 2.3 (cf. only the content in Section 4 cannot show such the result because we cannot determine by Theorem 3.2 whether the Kummer extension generated from $E_t^{(p)}$ is unramified or not). Furthermore, Herbrand's Theorem shows that $A_F^{\omega^{-1}} = 0$ in the case $K = \mathbb{Q}$ for the primes $p \geq 5$ since the Bernoulli number B_2 is equal to $\frac{1}{6}$ (see [Was82, Section 6.3] for details). On the other hand, the data in Table 3 give quadratic fields $K = \mathbb{Q}(\sqrt{m})$ satisfying $A_F^{\omega^{-1}} \neq 0$ for $p = 5$ and 7.

Our method to construct unramified Kummer extensions is quite different from Nakagoshi's one. In fact, he uses fundamental units of quadratic fields

$$\mathbb{Q}(\sqrt{m}) \text{ and } \mathbb{Q}(\sqrt{mp^*}) \text{ with } p^* = (-1)^{(p-1)/2} \cdot p$$

Table 3: List of pairs (m,t) such that the Kummer extension $L = F\left(\sqrt[p]{a_p(t)}\right)$ over $F = K(\zeta_p)$ is unramified for the quadratic field $K = \mathbb{Q}(\sqrt{m})$ and $p = 5$ and 7

p	m	t	h_K	h_F
5	26	$5+\sqrt{26}$	2	40
	$37^\dagger$	$5+\sqrt{37}$ or $6+\sqrt{37}$	1	5
	123	$\sqrt{123}$ or $11+\sqrt{123}$	2	160
	129	$\dfrac{11+\sqrt{129}}{2}$	1	10
	$17737^\dagger$	$\dfrac{133+\sqrt{17737}}{2}$	15	307125
	$450120^\dagger$	$-671+\sqrt{450120}$	4	320
	$465247^\dagger$	$682+\sqrt{465247}$	52	461194240
7	$10^\dagger$	$3+\sqrt{10}$	2	28
	$11^\dagger$	$4+\sqrt{11}$	1	28
	$57^\dagger$	$\dfrac{7+\sqrt{57}}{2}$	1	56

†These quadratic fields $K = \mathbb{Q}(\sqrt{m})$ do not appear in [Nak89, Table 2 and 3].

as Kummer generators for unramified extensions of degree p over $F = K(\zeta_p) = \mathbb{Q}(\zeta_p, \sqrt{m})$ (see [Nak89, Theorem 2 and Proposition 3], or [Nak91, Theorem]). In contrast to his method, we use elements $a_p(t)$ of $K(\zeta_p+\zeta_p^{-1}) \subset F$ as Kummer generators, which are induced by the p-torsion subgroup $E[p]$ of elliptic curves $E = E_t^{(p)}$ over K having a K-rational p-torsion point. Due to such the difference of two methods, many unramified Kummer extensions constructed by the pairs (m,t) in Table 3 do not appear in [Nak89, Table 2 and 3].

Example 5.3. In the following, we describe some typical examples of unramified Kummer extensions constructed by our method:

- For $p = 5$, we take $(m,t) = (37, 6+\sqrt{37})$ from Table 3. Then the element $6+\sqrt{37}$ is the fundamental unit of the quadratic field $K = \mathbb{Q}(\sqrt{37})$, which we denote by ε. Then the Weierstrass equation (4) of the elliptic curve $E = E_t^{(5)}$ for $t = \varepsilon$ is given by (note that we have $\varepsilon^2 = 12\varepsilon + 1$)

$$y^2 + (1-\varepsilon)xy - \varepsilon y = x^3 - \varepsilon x^2,$$

and this curve has good reduction everywhere over $\mathbb{Q}(\sqrt{37})$ since its discriminant is equal to ε^6 (the curve E is isomorphic over $\mathbb{Q}(\sqrt{37})$ to Shimura's curve B_{37} given in [Kag98] since the j-invariant of E is equal to 2^{12}). This curve is also included in Cremona's table [Cre]. Furthermore, the Kummer generator $a_5(t)$ for $t = \varepsilon$ is easily computed as

$$a_5(t) = \varepsilon^{-1}(10\varepsilon\eta - 4\varepsilon + 55\eta + 90)$$

where η denotes the fundamental unit $\dfrac{-1+\sqrt{5}}{2}$ of $\mathbb{Q}(\sqrt{5})$. The element $a_5(t)$ is in the quartic field $\mathbb{Q}(\sqrt{5}, \sqrt{37})$, and it gives a Kummer generator for the unramified Kummer extension $L = K(E[5])$ over $F = K(\zeta_5)$.

- For $p = 7$, we take $(m, t) = (10, 3 + \sqrt{10})$ from Table 3. As in the above example, the element $3 + \sqrt{10}$ is the fundamental unit of the quadratic field $K = \mathbb{Q}(\sqrt{10})$, which we denote by ε. Then the Weierstrass equation (5) of the elliptic curve $E = E_t^{(7)}$ for $t = \varepsilon$ is given by (note that we have $\varepsilon^2 = 6\varepsilon + 1$)

$$y^2 - 5\varepsilon xy - (31\varepsilon + 5)y = x^3 - (31\varepsilon + 5)x^2,$$

and this curve has good reduction over $\mathbb{Q}(\sqrt{10})$ outside the primes over 2 and 3 since its discriminant is equal to $-\varepsilon^9(\varepsilon - 1)^7 = -\varepsilon^9(2 + \sqrt{10})$. Then we can see that the element $a_7(t)$ for $t = \varepsilon$ is included in the field $\mathbb{Q}(\zeta_7 + \zeta_7^{-1}, \sqrt{10})$, and it gives a Kummer generator for the unramified Kummer extension $L = K(E[7])$ over $F = K(\zeta_7)$.

References

[Aga08] A. Agashe, *Rational torsion in elliptic curves and the cuspidal subgroup*, arXiv preprint arXiv:0810.5181 (2008).

[CF67] J.W.S. Cassels and A. Frölich, Algebraic Number Theory, Academic Press, 1967.

[Cre] J. Cremona (compiled), *Elliptic curves with everywhere good reduction over quadratic fields*, available at `http://homepages.warwick.ac.uk/staff/J.E.Cremona//ecegr/ecegrqf.html`.

[Fis00] T. A. Fisher, *On 5 and 7 descents for elliptic curves*, PhD Thesis, The University of Cambridge (2000).

[Fon77] J.-M. Fontaine, *Groupes p-divisible sur les corps locaux*, Astérisque **47–48**, Soc. Math. France, Paris (1977).

[Gre89] C. Greither, *Unramified Kummer extensions of prime power degree*, Manuscripta Math. **64**(3) (1989), 261–290.

[Gro71] 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, Berlin-Heidelberg-New York.

[Kag98] T. Kagawa, *Determination of elliptic curves with everywhere good reduction over* $\mathbb{Q}(\sqrt{37})$, Acta Arith. **89** (1998) 253–269.

[Kam92] S. Kamienny, *Torsion points on elliptic curves and q-coefficients of modular forms*, Invent. Math. **109** (1992), 221–229.

[KM88] M. Kenku and F. Momose, *Torsion points on elliptic curves defined over quadratic fields*, Nagoya Math. J. **109** (1988), 125–149.

[Kub76] D. Kubert, *Universal bounds on the torsion of elliptic curves*, Proc. London Math. Soc. **33** (1976), 193–237.

[Maz77] B. Mazur, *Modular curves and the Eisenstein ideal*, IHES Publ. Math. **47** (1977), 33–186.

[Maz78] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 12–162.

[Nak89] N. Nakagoshi, *On the unramified extensions of the prime cyclotomic number field and its quadratic extensions*, Nagoya Math. J. **15** (1989) 151–164.

[Nak91] N. Nakagoshi, *On the unramified Kummer extensions of quadratic extensions of the prime cyclotomic number field*, Arch. Math. (Basel) **57**(6) (1991) 566–570.

[Kra96] A. Kraus, *Courbes elliptiques semi-stables et corps quadratiques*, Journal of Number Theory **60** (1996), 245-253.

[Ogg75] A. Ogg, *Diophantine equations and modular forms*, Bull. Amer. Math. Soc. **81** (1975), 14–27.

[Par00] P. Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Ann. Inst. Fourier **50** (2000), 723–749.

[Par03] P. Parent, *No 17-torsion on elliptic curves over cubic number fields*, J. Théor. Nombres Bordeaux **15** (2003), 831–838.

[Sai97] S. Saito, Number Theory (in Japanese), Kyoritsu Shuppan Co., Ltd., 1997.

[Sch03] R. Schoof, *Abelian varieties over cyclotomic fields with good reduction everywhere*, Math. Annalen **325** (2003), 413–448.

[Sch05] R. Schoof, *Abelian varieties over $\mathbb{Q}$ with bad reduction in one prime only*, Composito Math. **141** (2005), 847–868.

[Ser72] J. -P. Serre, *Propriétés galoisiennes des points d'ortre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331.

[Ser79] J.-P. Serre, Local fields, Graduate Texts in Math. **67**, Springer-Verlag, Berlin-Heidelberg-New York, 1979.

[Sil86] J. H. Silverman, The Arithmetic of Elliptic Curves, Graduate Texts in Math. **106**, Springer-Verlag, Berlin-Heidelberg-New York, 1986.

[Sil94] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Math. **151**, Springer-Verlag, Berlin-Heidelberg-New York, 1994.

[Sto10] M. Stoll, *Torsion points on elliptic curves over quartic number fields*, (invited) talk at the 9th Algorithmic Number Theory Symposium (ANTS-IX), 2010, available at `http://www.mathe2.uni-bayreuth.de/stoll/talks/ANTS2010-1-EllTorsion.pdf`.

[Tak12] T. Takagi, *The cuspidal class number formula for the modular curves $X_1(2p)$*, Journal of the Mathematical Society of Japan **64**(1) (2012), 23–85 (Its erratum appears also in Journal of the Mathematical Society of Japan **64**(1) (2012), 87–89).

[Tat74] J. Tate, *The arithmetic of elliptic curves*, Invent. Math. **23** (1974), 179–206.

[Tat97] J. Tate, Finite flat group schemes, Modular forms and Fermat's last theorem, Springer-Verlag, Berlin-Heidelberg-New York, 1997, 121–154.

[PARI] The PARI Group, Bordeaux, *PARI/GP*, available from `http://pari.math.u-bordeaux.fr/doc.html`.

[Sage] The Sage Group, *Sage*, available at `http://www.sagemath.org/`.

[Ver06] H. Verdure, *Lagrange resolvents and torsion of elliptic curves*, International Journal of Pure and Applied Mathematics **33**(1) (2006), 75-92.

[Was82] L. C. Washington, Introduction to cyclotomic fields, Graduate Texts in Math. **83**, Springer-Verlag, Berlin-Heidelberg-New York, (1982).

[Yas08] M. Yasuda, *Torsion points of elliptic curves with good reduction*, Kodai Math. J. **31**(3) (2008), 385–403.

[Yas12a] M. Yasuda, *Torsion points of elliptic curves with bad reduction at some primes*, Comment. Math. Univ. St. Pauli **61**(1) (2012), 1–7.

[Yas13a] M. Yasuda, *Torsion points of elliptic curves with bad reduction at some primes II*, Bull. Korean Math. Soc. **50**(1) (2013), 83–96.

[Yas13b] M. Yasuda, *Kummer generators and torsion points of elliptic curves with bad reduction at some primes*, Int. J. Number Theory **09**(07) (2013), 1743–1752.

Masaya Yasuda
Institute of Mathematics for Industry,
Kyushu University
744 Motooka Nishi-ku,
Fukuoka 819-0395, Japan
`yasuda@imi.kyushu-u.ac.jp`