JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Fumio SAIRAIJI et Takuya YAMAUCHI

On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$

Tome 30, nº 3 (2018), p. 893-915.
<http://jtnb.cedram.org/item?id=JTNB_2018__30_3_893_0>

Journal de Théorie des Nombres
de Bordeaux **30** (2018), 893–915

On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$

par Fumio SAIRAIJI et Takuya YAMAUCHI

Dedicated to Professor Hirotada Naito's 60th birthday

Résumé. Soit E une courbe elliptique sur $\mathbb{Q}$ ayant réduction multiplicative en un nombre premier p. Supposons que en tout nombre premier différent de p la courbe E a une réduction multiplicative ou potentiellement bonne. Pour chaque entier positif n on pose $K_n := \mathbb{Q}(E[p^n])$. Le but de cet article est d'étendre nos résultats précédents [13] concernant l'ordre du p-sous-groupe de Sylow du groupe des classes d'idéaux de K_n à un cadre plus général. Nous modifions également la borne inférieure précédente de cet ordre donnée en termes du rang de Mordell–Weil de $E(\mathbb{Q})$ et de la ramification liée à E.

Abstract. Let E be an elliptic curve over $\mathbb{Q}$ which has multiplicative reduction at a fixed prime p. Assume E has multiplicative reduction or potentially good reduction at any prime not equal to p. For each positive integer n we put $K_n := \mathbb{Q}(E[p^n])$. The aim of this paper is to extend the authors' previous results in [13] concerning with the order of the p-Sylow group of the ideal class group of K_n to more general setting. We also modify the previous lower bound of the order given in terms of the Mordell–Weil rank of $E(\mathbb{Q})$ and the ramification related to E.

1. Introduction

This article is a sequel of [13]. Let p be a prime number and E be an elliptic curve over $\mathbb{Q}$. For each positive integer n, we consider the field K_n generated by the coordinates of points on $E[p^n]$ over $\mathbb{Q}$. In [13] the authors studied a lower bound of the p-part of the class number h_{K_n} of K_n in terms of the Mordell–Weil rank of $E(\mathbb{Q})$ when E has prime conductor p. The present article extends this result to a more extensive class of elliptic curves over $\mathbb{Q}$.

For such an elliptic curve, we will carry out a similar estimation done in [13] but at the same time we give an improvement of the method of the estimation. As we have done in [13] the lower bound will be given

Manuscrit reçu le 16 juin 2017, révisé le 8 février 2018, accepté le 5 avril 2018.
2010 *Mathematics Subject Classification.* 11G05, 11G07.
Mots-clefs. elliptic curves, Mordell–Weil rank, class number.
The second author is partially supported by JSPS Grant-in-Aid for Scientific Research KAKENHI (C) No.15K04787.

in terms of the Mordell–Weil rank and the information coming from the ramification related to E. Our formula is reminiscent of Iwasawa's class number formula for $\mathbb{Z}_p$-extension. In fact we have an explicit class number formula in a special case (see Corollary 1.2).

Our study is motivated by the works of Greenberg [6] and Komatsu–Fukuda–Yamagata [5] who have studied a lower bound of Iwasawa invariants for CM fields in terms of the Mordell–Weil group of the corresponding CM abelian varieties. We have pursued an analogue for non-CM elliptic curves since [13].

To state our main theorem we introduce our notation. The Mordell–Weil theorem asserts that $E(\mathbb{Q})$ is a finitely generated abelian group. Thus there exists a free abelian subgroup A of $E(\mathbb{Q})$ of finite rank such that $A + E(\mathbb{Q})_{\mathrm{tors}} = E(\mathbb{Q})$. We denote the rank of A by r. We put $G_n := \mathrm{Gal}(K_n/\mathbb{Q})$ and $L_n := K_n([p^n]_E^{-1}A)$, where $[p^n]_E$ is the multiplication-by-p^n map on E. We denote generators of A by $P_1, \ldots, P_r$. For each j in $\{1, \ldots, r\}$ we take a point T_j of $E(L_n)$ satisfying

$$[p^n]_E(T_j) = P_j.$$

Then we have $L_n = K_n(T_1, \ldots, T_r)$. The Galois action on $\{T_j\}_j$ naturally induces an injective G_n-homomorphism

$$\Phi_n : \mathrm{Gal}(L_n/K_n) \to E[p^n]^r \ : \ \sigma \mapsto ({}^{\sigma}T_j - T_j)_j$$

(cf. [10, p. 116]). In particular, the degree $[L_n : K_n]$ is equal to a power of p.

We denote the maximal unramified abelian extension of K_n by K_n^{ur}. We define the exponent κ_n by

$$[L_n \cap K_n^{\mathrm{ur}} : K_n] = p^{\kappa_n}.$$

Assume that E has multiplicative reduction at p and E has multiplicative reduction or potentially good reduction at any prime $\ell \neq p$.

Then the main theorem of this article is the following theorem.

Theorem 1.1. *Assume that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for each $n \geq 1$ and $p \nmid \mathrm{ord}_p(\Delta)$, where Δ is the minimal discriminant of E. The following inequalities hold:*

(1) *Assume that p is odd. Then for any $n \geq 1$,*

$$\kappa_n \geq 2n(r-1) - 2\sum_{\ell \neq p} \nu_\ell,$$

where we put

$$\nu_\ell := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_\ell(\Delta)), n\} & \text{if } E \text{ has split multiplicative reduction at } \ell \neq p, \\ 0 & \text{otherwise.} \end{cases}$$

(2) *Assume that $p = 2$. Then for any $n \geq 1$,*

$$\kappa_n \geq 2n(r-1) - 2(r_{2,n} - 2) - \delta_2 - 2\sum_{\ell \neq p} \nu_\ell,$$

where $r_{2,n} = 1, 2$ according as $E(\mathbb{Q})/E(\mathbb{Q}) \cap [2^n]_E(E(\mathbb{Q}_p))$ is cyclic or not, and we put

$$\nu_\ell := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_\ell(\Delta)), n\} & \text{if } E \text{ has split multiplicative reduction at } \ell \neq 2, \\ 1 & \text{if } E \text{ has potentially good reduction at } \ell \neq 2 \text{ and } n = 1, \text{ or if } E \text{ has non-split multiplicative reduction at } \ell \neq 2 \text{ and } \mathrm{ord}_\ell(\Delta) \text{ is even,} \\ 0 & \text{otherwise.} \end{cases}$$

and

$$\delta_2 := \begin{cases} 2 & \text{if } n = 1 \text{ and } r_{2,1} = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Corollary 1.2. *Assume that the conductor of E is equal to p. Then*

$$\kappa_n = \begin{cases} 2n(r-1) + 2\nu & (n > \nu) \\ 2nr & (n \leq \nu) \end{cases}$$

for some integer $\nu \geq 0$ (which depends only on P_j).

We explain the conditions imposed on E. Put

$$n_0 := \begin{cases} 1 & \text{if } p > 3 \\ 2 & \text{if } p = 3 \\ 3 & \text{if } p = 2. \end{cases}$$

It is known that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \leq n_0$ implies $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for all $n \geq 1$ (cf. [3, Section 1]). Thus the assumption in Theorem 1.1 can be replaced by $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \leq n_0$. For a given prime number p, there is a criterion for G_n ($n \leq n_0$) to be isomorphic to $\mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ (see [3] for $p = 2$, [4] for $p = 3$, and [14] for $p \geq 5$). The condition $p \nmid \mathrm{ord}_p(\Delta)$ is automatically satisfied when $p > 5$ and E is a semistable elliptic curve (cf. [12, Théorème 1, p. 176]).

While preparing this paper, Hiranouchi [8] generalized Theorem 1.1 (1) to the case where $p > 2$, $E(\mathbb{Q}_p)[p] = \{0\}$, $G_1 \simeq \mathrm{GL}(\mathbb{Z}/p\mathbb{Z})$. He uses the structure theorem of $E(\mathbb{Q}_p)$ and the formal group for E which plays a substitution of Tate curves. He also shows $E(\mathbb{Q}_p)[p] = \{0\}$ for $p > 2$ under the assumption of Theorem 1.1.

The organization of this paper is as follows. In Section 2, we study the extension L_n/K_n. To do this we modify Bashmakov's result [1] from Lang [10] for our elliptic curves. Then we investigate the degree $[L_n : K_n]$ of the extension L_n/K_n. A key point is to show the equality $L_1 \cap K_\infty = K_1$. To do this we separate the situation into the case when p is odd and the case when $p = 2$. The former case will be done in Section 2, but the latter case will be devoted to Section 6 because of the particular treatment in which being $p = 2$ causes. In Section 3 and Section 4, we investigate the degree of the p-adic completion of L_n over the one of K_n, which is used for the estimate of the inertia group in Section 5. We give the proof of Theorem 1.1 in Section 5, and we give numerical examples of κ_n in Section 7.

Acknowledgments. We would like to express our deep appreciation to Professors Matsuno Kazuo and Toshiro Hiranouchi, and Yoshiyasu Ozeki for comments in our previous version. We thank also the referee for helpful suggestions and collections which are useful for improving contents and presentations.

2. The extension L_n over K_n

In this section, we extend some results in [13] which has been done by the arguments essentially based on Bashmakov [1] (cf. [10, Lemma 1, p. 117]).

Let us keep the notation in Section 1 and throughout this paper we assume our elliptic curve E always satisfies the condition in Theorem 1.1. Put $K_\infty := \cup_{n\geq 1} K_n$, $L_\infty := \cup_{n\geq 1} L_n$ and $G_\infty := \mathrm{Gal}(K_\infty/\mathbb{Q})$. For each $n \geq 1$ let us consider the G_n-homomorphism

$$\Phi_n : \mathrm{Gal}(L_n/K_n) \to E[p^n]^r.$$

It follows that the G_∞-homomorphism

$$\Phi_\infty := \varprojlim_n \Phi_n : \mathrm{Gal}(L_\infty/K_\infty) \to T_p(E)^r$$

is injective and the image is a closed subgroup. We are concerned with the order of the image of G_n-homomorphism Φ_n. As we will see below, Φ_1 controls Φ_∞ and then the information for Φ_n comes up from Φ_∞.

To obtain a lower bound of the class number in question, we need to study that the image of Φ_n to guarantee the degree $[L_n : K_n]$ is large enough. We will prove that Φ_n is an isomorphism for any prime p and $n \geq 1$.

Theorem 2.1. *Assume that $G_1 \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$. Then, Φ_1 is an isomorphism for any prime p. In particular, the equality $[L_1 : K_1] = p^{2r}$ holds.*

Proof. The proof given here is almost identical with the proof of Theorem 2.4 in [13]. Therefore we only explain a key point. Since $G_1 \simeq \mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$, the Galois cohomology $H^1(G_1, E[p])$ vanishes by [11]. Then there is an injective homomorphism

$$A/[p]_E A \hookrightarrow \mathrm{Hom}_{G_1}(\mathrm{Gal}(L_1/K_1), E[p])$$

(see [13, p. 283, l. 6]). Therefore we have $\sharp\,\mathrm{Hom}_{G_1}(\mathrm{Gal}(L_1/K_1), E[p]) \geq p^r$, where r is $\mathbb{Z}$-rank of A. On the other hand $\mathrm{Gal}(L_1/K_1) \simeq E[p]^s$ for some $s \leq r$. Then we see that

$$\mathrm{Hom}_{G_1}(\mathrm{Gal}(L_1/K_1), E[p]) \simeq \mathrm{End}_{G_1}(E[p])^s \simeq (\mathbb{Z}/p\mathbb{Z})^s$$

which implies $s \geq r$. Hence $s = r$ and it turns that Φ_1 is an isomorphism. ☐

Theorem 2.1 is different from Theorem 2.4 of [13] at the point where we omit the assumption that N is prime and $p > 2$.

To show that Φ_n is an isomorphism, we have the following lemma.

Lemma 2.2. *Assume that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 1$. Then, the equality $L_1 \cap K_\infty = K_1$ holds for any prime p.*

Proof. In case when p is odd prime the assertion follows from Lemmas 2.1 and 2.2 of [13]. In case when $p = 2$ it follows from Theorem 6.5. ☐

Theorem 2.3. *Assume that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 1$. Then, Φ_n is an isomorphism for $n \geq 1$ and any prime p. In particular, the equality $[L_n : K_n] = p^{2nr}$ holds.*

Proof. By Lemma 2.2, $\mathrm{Gal}(L_1/L_1 \cap K_\infty) = \mathrm{Gal}(L_1/K_1)$. Then we have the following commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xrightarrow{\Phi_\infty} & T_p(E)^r \\ {\scriptstyle \alpha_1}\downarrow & & \downarrow{\scriptstyle \beta_1} \\ \mathrm{Gal}(L_1/K_1) & \xrightarrow{\Phi_1} & E[p]^r, \end{array}$$

where α_1 is the restriction map and β_1 is the reduction modulo p. Clearly these vertical arrows are surjective.

Since Φ_1 is an isomorphism by Theorem 2.1, $\Phi_1 \circ \alpha_1$ is surjective. We see that Φ_∞ is surjective by using Nakayama's Lemma. This gives rise to the commutative diagram

$$\begin{array}{ccc} \mathrm{Gal}(L_\infty/K_\infty) & \xrightarrow[\simeq]{\Phi_\infty} & T_p(E)^r \\ {\scriptstyle \alpha_n}\downarrow & & \downarrow{\scriptstyle \beta_n} \\ \mathrm{Gal}(L_n/L_n \cap K_\infty) & \xrightarrow{\Phi_n} & E[p^n]^r, \end{array}$$

where α_n is the restriction map and β_n is the reduction modulo p^n. Thus it follows that the restriction of Φ_n to $\mathrm{Gal}(L_n/L_n \cap K_\infty)$ is surjective and thus Φ_n is surjective. Since Φ_n is also injective, Φ_n is an isomorphism. Hence $[L_n : K_n] = p^{2nr}$. □

Corollary 2.4. *The equality $L_n \cap K_\infty = K_n$ holds for $n \geq 1$.*

Proof. In the proof of Theorem 2.3, we saw that Φ_n and its restriction to $\mathrm{Gal}(L_n/L_n \cap K_\infty)$ are isomorphisms to $E[p^n]^r$. Thus we have $\mathrm{Gal}(L_n/L_n \cap K_\infty) = \mathrm{Gal}(L_n/K_n)$, and the assertion follows. □

3. The inertia subgroups of $\mathrm{Gal}(L_n/K_n)$ on p

In this section we estimate the order of the inertia subgroups of $\mathrm{Gal}(L_n/K_n)$ on p. We also improve the previous result (cf. [13, Theorem 1.1]).

3.1. The local case. Let us recall the notation in Section 3 of [13]. Fix a natural number n. Put $\mathcal{K}_n := \mathbb{Q}_p(E[p^n])$ and let $\mathfrak{p}$ be the prime ideal of $\mathcal{K}_n$. Put $\mathcal{L}_n := \mathcal{K}_n([p^n]_E^{-1}A)$ and let $\mathfrak{P}$ be the prime ideal of $\mathcal{L}_n$.

We will investigate the order of the inertia subgroup $\mathcal{I}_n$ of $\mathrm{Gal}(\mathcal{L}_n/\mathcal{K}_n)$.

We denote the generators of A by $P_1, \ldots, P_r$, where A is the fixed free subgroup in $E(\mathbb{Q})$. For each j in $\{1, \ldots, r\}$ we take T_j such that $[p^n]_E(T_j) = P_j$. The injectivity of the homomorphism

$$\Phi_n^{\mathrm{loc}} : \mathrm{Gal}(\mathcal{L}_n/\mathcal{K}_n) \to E[p^n]^r \ : \ \sigma \mapsto ({}^\sigma T_j - T_j)_j$$

shows that $[\mathcal{L}_n : \mathcal{K}_n]$ divides p^{2nr}.

A key point is to prove the cyclicity of $\mathcal{I}_n$ and we make use of the Tate curves to confirm it. Since E has multiplicative reduction at p, there exists q in $p\mathbb{Z}_p$ such that E is isomorphic over $\mathcal{M}$ to the Tate curve E_q for some unramified extension $\mathcal{M}$ over $\mathbb{Q}_p$ of degree at most two (cf. [15, Theorem 14.1, p. 357]). We note $E_q(\overline{\mathbb{Q}}_p) \simeq \overline{\mathbb{Q}}_p^*/q^{\mathbb{Z}}$.

We write φ from E to E_q for the isomorphism over $\mathcal{M}$. We define p_j and t_j in $E_q(\overline{\mathbb{Q}}_p)$ by

$$\varphi(P_j) = p_j \quad \text{and} \quad \varphi(T_j) = t_j \quad (1 \leq j \leq r)$$

(see Section 1 for P_j and T_j).

Assume that $p \nmid \mathrm{ord}_p(q)$. We have $\mathcal{M}K_n = \mathcal{M}(\zeta_{p^n}, q^{\frac{1}{p^n}})$. We discuss about generators of $\mathcal{L}_n/\mathcal{K}_n$.

We put

$$H := \begin{cases} \mathbb{Q}_p^* & \text{if } \mathcal{M} = \mathbb{Q}_p \\ \{x \in \mathcal{M}^* \mid N_{\mathcal{M}/\mathbb{Q}_p}(x) \in q^{\mathbb{Z}}\} & \text{if } [\mathcal{M} : \mathbb{Q}_p] = 2. \end{cases}$$

Then we have $q \in H$ and $E(\mathbb{Q}_p) \simeq H/q^{\mathbb{Z}}$ via φ (cf. [15, Theorem 14.1, p. 357]). We have

$$E(\mathbb{Q}_p)/[p^n]_E(E(\mathbb{Q}_p)) \simeq H/\langle H^{p^n}, q\rangle.$$

3.1.1. We consider the case of $\mathcal{M} = \mathbb{Q}_p$. Then $H = \mathbb{Q}_p^*$ and

$$H = \begin{cases} \langle p\rangle \times (\mathbb{Z}/p\mathbb{Z})^* \times (1 + p\mathbb{Z}_p) & \text{if } p \neq 2 \\ \langle 2\rangle \times (\mathbb{Z}/4\mathbb{Z})^* \times (1 + 4\mathbb{Z}_p) & \text{if } p = 2. \end{cases}$$

It follows from $p \nmid \operatorname{ord}_p(q)$ that

$$H/\langle H^{p^n}, q\rangle = \begin{cases} \langle 1 + p\rangle \simeq \mathbb{Z}/p^n\mathbb{Z} & \text{if } p \neq 2 \\ \langle -1\rangle \times \langle 5\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z} & \text{if } p = 2. \end{cases} \tag{3.1}$$

Hence $E(\mathbb{Q}_p)/[p^n]_E(E(\mathbb{Q}_p))$ is an abelian group of type (p^n), $(2^n, 2)$.

We discuss generators of the image of the projection from the subgroup $\langle p_1, \ldots, p_r, q\rangle/q^{\mathbb{Z}}$ to $H/\langle H^{p^n}, q\rangle$.

We first consider the case of $p > 2$. Since $\mathbb{Z}/p^n\mathbb{Z}$ is a local ring, there is a relation of inclusion between every two submodules of $\mathbb{Z}/p^n\mathbb{Z}$. By renumbering, we may assume $\langle p_j\rangle \subset \langle p_1\rangle$ as a subgroup of $H/\langle H^{p^n}, q\rangle$ for each $j \leq r$. In this case $\mathcal{L}_n = \mathcal{K}_n(t_1)$ holds.

Secondly we consider the case of $p = 2$. Since $\mathbb{Z}/2^n\mathbb{Z}$ is a local ring, there is a relation of inclusion between every two submodules of $\mathbb{Z}/2^n\mathbb{Z}$. By renumbering, we may assume $\langle p_j, -1\rangle \subset \langle p_1, -1\rangle$ as a subgroup of $H/\langle H^{2^n}, q\rangle$ for each $j \leq r$. If the rank of $\langle p_1, \ldots, p_r\rangle$ is two, we may assume $p_2 \notin \langle p_1\rangle$. Then we have $p_2 = -p_1^k$. By replacing p_2 by $p_2 p_1^{-k}$, we may assume $p_2 = -1$. In this case $\mathcal{L}_n = \mathcal{K}_n(t_1)$ or $\mathcal{L}_n = \mathcal{K}_n(t_1, \zeta_{2^{n+1}})$ holds.

3.1.2. We consider the case of $[\mathcal{M} : \mathbb{Q}_p] = 2$. Then

$$H := \{x \in \mathcal{M}^* \mid N_{\mathcal{M}/\mathbb{Q}_p}(x) \in q^{\mathbb{Z}}\}$$

and we investigate the structure of H/H^{p^n}.

Since $N_{\mathcal{M}/\mathbb{Q}_p}(q) = q^2$, the image of H via $N_{\mathcal{M}/\mathbb{Q}_p}$ is a subgroup in $q^{\mathbb{Z}}$ of exponent 1 or 2. Thus H contains the group $H_0 = \langle q\rangle \times U_{\mathcal{M},1}$ as a subgroup of exponent 1 or 2, where $U_{\mathcal{M},1}$ is the subgroup of $\mathcal{M}^*$ with norm 1.

We first consider the case of $p > 2$. Since the exponent $[H : H_0]$ is prime to p^n, we have

$$H/H^{p^n} \simeq H_0/H_0^{p^n} \simeq \langle q\rangle \times U_{\mathcal{M},1}/U_{\mathcal{M},1}^{p^n}.$$

We investigate generators of $U_{\mathcal{M},1}/U_{\mathcal{M},1}^{p^n}$. We denote the ring of integers in $\mathcal{M}$ by $\mathcal{O}$.

$$\log \ : \ 1 + p\mathcal{O} \to p\mathcal{O} \ : \ 1 + x \mapsto \log(1 + x)$$

converges and it gives an isomorphism. Since $\log(1+x)$ is a power series with coefficients in $\mathbb{Q}_p$, it commutes with the action of $\operatorname{Gal}(\mathcal{M}/\mathbb{Q}_p)$. Specially each element of $1+p\mathcal{O}$ with norm one corresponds to that of $p\mathcal{O}$ with trace zero.

We put $\mathcal{M} := \mathbb{Q}_p(\sqrt{D})$ for a square-free integer D in $\mathbb{Z}_p$. Then we have

$$p\mathcal{O} \cap \ker Tr_{\mathcal{M}/\mathbb{Q}_p} = p\mathbb{Z}_p\sqrt{D}$$

and

$$(1+p\mathcal{O}) \cap \ker N_{\mathcal{M}/\mathbb{Q}_p} = \exp(p\mathbb{Z}_p\sqrt{D}).$$

Since $\mathcal{O}^* \simeq (\mathcal{O}/p\mathcal{O})^* \times (1+p\mathcal{O})$ and the order of $(\mathcal{O}/p\mathcal{O})^*$ is prime to p,

$$U_{\mathcal{M},1}/U_{\mathcal{M},1}^{p^n} = \langle \exp(p\sqrt{D}) \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

We have

$$H/\langle H^{p^n}, q\rangle \simeq \langle \exp(p\sqrt{D}) \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

By a similar discussion as in the case of $\mathcal{M} = \mathbb{Q}_p$, we may assume $\langle p_j \rangle \subset \langle p_1 \rangle$ as a subgroup of $H/\langle H^{p^n}, q\rangle$ for each $j \le r$.

In this case $\mathcal{M}L_n = \mathcal{M}K_n(t_1)$ holds.

Secondly we consider the case of $p = 2$. We have $N_{\mathcal{M}/\mathbb{Q}_2}\mathcal{M}^* = \langle 2^2 \rangle \times U_{\mathbb{Q}_2}$. It follows from the assumption $2 \nmid \mathrm{ord}_2(\Delta)$ that $2 \nmid \mathrm{ord}_2(q)$. Thus there does not exist y in $\mathcal{M}$ such that $N_{\mathcal{M}/\mathbb{Q}_2}(y) = q$. Thus we have $N_{\mathcal{M}/\mathbb{Q}_2}(x) \in q^{\mathbb{Z}}$ if and only if $N_{\mathcal{M}/\mathbb{Q}_2}(x) \in q^{2\mathbb{Z}}$.

Since $N_{\mathcal{M}/\mathbb{Q}_2}(q) = q^2$, we have

$$H = q^{\mathbb{Z}} \times U_{\mathcal{M},1} \tag{3.2}$$

and

$$H/H^{2^n} \simeq \langle q \rangle \times U_{\mathcal{M},1}/U_{\mathcal{M},1}^{2^n}.$$

We investigate generators of $U_{\mathcal{M},1}/U_{\mathcal{M},1}^{2^n}$.

$$\log\ :\ 1+4\mathcal{O} \to 4\mathcal{O}\ :\ 1+x \mapsto \log(1+x)$$

converges and it gives an isomorphism. We modify discussion in the case of $p > 2$. Since

$$1 \to 1+4\mathcal{O} \to \mathcal{O}^* \to (\mathcal{O}/4\mathcal{O})^* \to 1$$

and

$$(\mathcal{O}/4\mathcal{O})^* = \langle \sqrt{5} \rangle \times \mu_6 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z},$$

we have

$$1 \to (1+4\mathcal{O}) \cap U_{\mathcal{M},1} \to U_{\mathcal{M},1} \to \mu_6 \to 1,$$

where μ_6 is the group of 6-th roots of unity. Thus we have

$$U_{\mathcal{M},1} = \mu_6 \times \langle \exp(4\sqrt{5}) \rangle.$$

Let $U_{\mathcal{M},\pm 1}$ be the subgroup of $\mathcal{M}^*$ with norm ± 1. Then the norm mapping induces the exact sequence

$$1 \to U_{\mathcal{M},1} \to U_{\mathcal{M},\pm 1} \to \langle -1 \rangle \to 1.$$

We note $\varepsilon := (-1+\sqrt{5})/2$ has norm -1. Since $\varepsilon^6 = 1 + 4(-2\varepsilon + 1)$, there exists a unit w such that $\varepsilon^6 = \exp(4w\sqrt{5})$. Since 3 is an unit, we have $\varepsilon^2 = \eta \exp(4w\sqrt{5}/3)$ for some η in μ_3. Thus we have

$$U_{\mathcal{M},1} = \mu_6 \times \langle \varepsilon^2 \rangle. \tag{3.3}$$

We also have

$$H/\langle H^{2^n}, q\rangle = \langle -1\rangle \times \langle \varepsilon^2\rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}. \tag{3.4}$$

By a similar discussion as in the case of $\mathcal{M} = \mathbb{Q}_p$, we may assume $\langle p_j, -1\rangle \subset \langle p_1, -1\rangle$ as a subgroup of $\langle H, q\rangle/\langle H^{2^n}, q\rangle$ for each $j \leq r$. If the rank of $\langle p_1, \ldots, p_r\rangle$ is two, we may assume $p_2 = -1$.

In this case $\mathcal{M}L_n = \mathcal{M}K_n(t_1)$ or $\mathcal{M}L_n = \mathcal{M}K_n(t_1, \zeta_{2^{n+1}})$ holds.

3.1.3. To sum up our discussion, we have the following proposition.

Proposition 3.1. *Assume that $p \nmid \mathrm{ord}_p(q)$. For a suitable change of basis of a maximal free subgroup A of $E(\mathbb{Q})$, the equation $\mathcal{M}L_n = \mathcal{M}K_n(\varphi(T_1))$ or $\mathcal{M}L_n = \mathcal{M}K_n(\varphi(T_1), \zeta_{2^{n+1}})$ holds. The latter case occurs only when $p = 2$, and then we may assume $\varphi(P_2) = -1$, $\varphi(T_2) = \zeta_{2^{n+1}}$.*

3.2. Assume $p > 2$. We investigate the ramified index $\mathcal{M}L_n/\mathcal{M}K_n$. We need the following Lemma.

Lemma 3.2 ([10, p. 118, Theorem 5.1])**.** *Let G be a group and let M be a G-module. Let α be in the center of G. Then $\mathrm{H}^1(G, M)$ is annihilated by the map $x \mapsto \alpha x - x$ on M. In particular, if this map is an automorphism of M, then $\mathrm{H}^1(G, M) = 0$.*

By the inflation-restriction exact sequence, we have

$$0 \to H^1(\mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M}), \mu_{p^n}) \to H^1(G_{\mathcal{M}}, \mu_{p^n}) \\ \to H^1(G_{\mathcal{M}(\zeta_{p^n})}, \mu_{p^n})^{\mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M})}.$$

When $p > 2$, $a-1$ is an unit of $(\mathbb{Z}/p^n\mathbb{Z})^* \simeq \mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M})$ for a primitive root a of $(\mathbb{Z}/p^n\mathbb{Z})^*$. By Lemma 3.2, we have

$$H^1(\mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M}), \mu_{p^n}) = 0.$$

Thus we have

$$0 \to H^1(G_{\mathcal{M}}, \mu_{p^n}) \to H^1(G_{\mathcal{M}(\zeta_{p^n})}, \mu_{p^n})^{\mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M})}.$$

By the Kummer theory we have

$$\mathcal{M}^*/\mathcal{M}^{*p^n} \hookrightarrow (\mathcal{M}(\zeta_{p^n})^*/\mathcal{M}(\zeta_{p^n})^{*p^n})^{\mathrm{Gal}(\mathcal{M}(\zeta_{p^n})/\mathcal{M})} \hookrightarrow \mathcal{M}(\zeta_{p^n})^*/\mathcal{M}(\zeta_{p^n})^{*p^n}.$$

Thus we see that the Galois group of $\mathcal{M}K_n(u^{\frac{1}{p^n}})/\mathcal{M}(\zeta_{p^n})$ is of type (p^n, p^n), where $u = 1+p,\ \exp(p\sqrt{D})$. We have $[\mathcal{M}K_n(u^{\frac{1}{p^n}}) : \mathcal{M}K_n] = p^n$.

We will see that $\mathcal{M}K_n(u^{\frac{1}{p^n}})/\mathcal{M}(\zeta_p)$ is a totally ramified extension.

Suppose that $\mathcal{M}K_n(u^{\frac{1}{p^n}})/\mathcal{M}(\zeta_p)$ is not a totally ramified extension. Since $\mathcal{M}K_n(u^{\frac{1}{p^n}})/\mathcal{M}(\zeta_p)$ is a Galois extension, there exists an intermediate field $\mathcal{N}$ such that $\mathcal{N}/\mathcal{M}(\zeta_p)$ is an unramified extension of degree p.

Since $\mathcal{N}$ is the composite of $\mathcal{M}(\zeta_p)$ and the unramified extension of degree p over $\mathcal{M}$, $\mathcal{N}/\mathcal{M}$ is an abelian extension of degree $p(p-1)$. Since $\mathcal{M}(\zeta_{p^2})$ is the unique intermidiate field between $\mathcal{M}K_n(u^{\frac{1}{p^n}})$ and $\mathcal{M}(\zeta_p)$ which is an abelian extension over $\mathcal{M}$ of degree $p(p-1)$, there does not exist $\mathcal{N}$. This contradicts the assumption.

Hence $\mathcal{M}K_n(u^{\frac{1}{p^n}})/\mathcal{M}(\zeta_p)$ is a totally ramified extension.

When we put

$$p_1 = q^a u^{mp^\nu} w^{p^n} \quad (a \in \mathbb{Z},\ p \nmid m,\ \nu \geq 0,\ w \in \mathcal{M}^*), \tag{3.5}$$

we have

$$t_1 = p_1^{\frac{1}{p^n}} = \zeta_{p^n}^j \times q^{\frac{a}{p^n}} u^{\frac{m}{p^{n-\nu}}} w \quad (j \in (\mathbb{Z}/p^n\mathbb{Z})^*).$$

Since $\zeta_{p^n},\ q^{\frac{1}{p^n}}$ are in $\mathcal{M}K_n$, we have

$$\mathcal{M}L_n = \mathcal{M}K_n(t_1) = \mathcal{M}K_n(u^{\frac{1}{p^{n-\nu}}})$$

and

$$[\mathcal{M}L_n : \mathcal{M}K_n] = \begin{cases} p^{n-\nu} & \text{if } n > \nu \\ 1 & \text{if } n \leq \nu. \end{cases}$$

$\mathcal{M}K_n/\mathcal{K}_n$ is unramified and $\mathcal{M}L_n/\mathcal{M}K_n$ is totally ramified. It follows from $p > 2$ that $[\mathcal{M}K_n : \mathcal{K}_n]$ is coprime to $[\mathcal{L}_n : \mathcal{K}_n]$. Thus $\mathcal{M}L_n/\mathcal{L}_n$ is unramified of degree $[\mathcal{M}K_n : \mathcal{K}_n]$ and $\mathcal{L}_n/\mathcal{K}_n$ is totally ramified of degree $[\mathcal{M}L_n : \mathcal{M}K_n]$ holds.

Let $\mathcal{I}_n$ be the inertia subgroup of $\mathrm{Gal}(\mathcal{L}_n/\mathcal{K}_n)$. Then we have

$$|\mathcal{I}_n| = \begin{cases} p^{n-\nu} & \text{if } n > \nu \\ 1 & \text{if } n \leq \nu. \end{cases}$$

3.3. We consider the case of $p = 2$. We first discuss the case of $\mathcal{M} = \mathbb{Q}_2$. Then $\mathcal{L}_n$ is contained in $\mathcal{K}_n(5^{\frac{1}{2^n}}, \zeta_{2^{n+1}})$. Further $\mathcal{K}_n(\sqrt{5})/\mathcal{K}_n$ is unramified. ζ_{2^n} is in $\mathcal{K}_n$ and $[\mathcal{K}_n(\zeta_{2^{n+1}}) : \mathcal{K}_n] = 2$. Therefore the inertia group of $\mathcal{K}_n(5^{\frac{1}{2^n}}, \zeta_{2^{n+1}})/\mathcal{K}_n$ is of type $(2^m, 2)$ for some $m \leq n-1$. Thus

$$|\mathcal{I}_n| \leq 2^{n-1} \times 2 = 2^n.$$

When $n \geq 2$ and $\mathcal{L}_n = \mathcal{K}_n(t_1)$, we can improve the estimate. Since $\mathcal{L}_n/\mathcal{K}_n$ is cyclic, $\mathcal{I}_n$ is also cyclic. Thus we have

$$|\mathcal{I}_n| \leq 2^{n-1}.$$

When $n = 1$ we can decide $|\mathcal{I}_1|$ directly because $\mathcal{L}_1$ is contained in $\mathcal{K}_1(\sqrt{5}, \zeta_4)$. If $\mathcal{L}_1$ is contained in $\mathcal{K}_1(\sqrt{5})$, then $|\mathcal{I}_1| = 1$. Otherwise, $|\mathcal{I}_1| = 2$.

Secondly we discuss the case of $\mathcal{M} = \mathbb{Q}_2(\sqrt{5})$. Then $\mathcal{M}L_n$ is contained in $\mathcal{M}K_n(\varepsilon^{\frac{1}{2^{n-1}}}, \zeta_{2^{n+1}})$. Further ζ_{2^n} is in $\mathcal{K}_n$ and $[\mathcal{K}_n(\zeta_{2^{n+1}}) : \mathcal{K}_n] = 2$. Therefore the inertia group of $\mathcal{K}_n(\varepsilon^{\frac{1}{2^{n-1}}}, \zeta_{2^{n+1}})/\mathcal{K}_n$ is of type $(2^m, 2)$ for some $m \le n-1$. Thus

$$|\mathcal{I}_n| \le 2^{n-1} \times 2 = 2^n.$$

When $n \ge 2$ and $\mathcal{M}L_n = \mathcal{M}K_n(t_1)$, we can improve the estimate. Since $\mathcal{L}_n/\mathcal{K}_n$ is cyclic, $\mathcal{I}_n$ is also cyclic. Thus we have

$$|\mathcal{I}_n| \le 2^{n-1}.$$

When $n = 1$ we can decide $|\mathcal{I}_1|$ directly because $\mathcal{M}L_1$ is equal to $\mathcal{M}K_1(\zeta_4) = \mathbb{Q}_2(\sqrt{5}, \sqrt{2}, \zeta_4)$. We note $\mathcal{M}K_1 = \mathcal{M}(\sqrt{q}) = \mathcal{M}(\sqrt{\pm 2})$. If $\mathcal{M}L_1$ contains ζ_4 then $|\mathcal{I}_1| = 2$. Otherwise, $|\mathcal{I}_1| = 1$. Specially if $E(\mathbb{Q})/E(\mathbb{Q}) \cap [2]_E(E(\mathbb{Q}_2))$ is not cyclic, then $t_2 = -1$ and thus $|\mathcal{I}_1| = 2$.

3.4. The global case. Let v be any prime above p in K_n and I_v the inertia subgroup of $\mathrm{Gal}(L_n/K_n)$ at v. Put $I_p := \langle I_v \,|\, v|p \rangle$. In this subsection we take a basis of the maximal free subgroup A of $E(\mathbb{Q})$ satisfying the assertion of Proposition 3.1.

We first consider the case of $p > 2$. If $|I_v| = 1$, L_n/K_n is unramified at v. Since both $L_n/\mathbb{Q}$ and $K_n/\mathbb{Q}$ are Galois extensions, L_n/K_n is unramified at any prime above p in K_n. Therefore $I_p = 1$.

We assume that $|I_v| = p^{n-\nu}$.

By Proposition 3.1, we have $\mathcal{M}L_n = \mathcal{M}K_n(\varphi(T_1))$. Thus $L_n/K_n(T_1)$ is unramified at v. Since both $L_n/\mathbb{Q}$ and $K_n(T_n)/\mathbb{Q}$ are Galois extensions, $L_n/K_n(T_1)$ is unramified at any prime above p in $K_n(T_1)$. Thus there exists the injective homomorphism from I_p to $\mathrm{Gal}(K_n(T_1)/K_n)$. Since I_p is generated by elements in I_v and their conjugate, the exponent of I_p is equal to that of I_v. $\mathrm{Gal}(K_n(T_1)/K_n)$ is G_n-isomorphic to $E[p^n]$ and $E[p^{n-\nu}]$ is unique G_n-invariant subgroup of $E[p^n]$ of exponent $p^{n-\nu}$. Since $E[p^{n-\nu}]$ is irreducible with respect to the action of G_n, we have

$$|I_p| = p^{2(n-\nu)}.$$

Secondly we consider the case of $p = 2$. Suppose that $\mathcal{M}L_n = \mathcal{M}K_n(t_1)$ and $n \ge 2$. Then, $|I_v|$ is at most 2^{n-1}. Similarly as above, $L_n/K_n(T_1)$ is unramified at any prime above 2 in $K_n(T_1)$. Since $\mathrm{Gal}(K_n(T_1)/K_n) \simeq E[2^n]$, the inequality

$$|I_2| \le 2^{2(n-1)}$$

holds.

If $n = 1$, $|I_v|$ is at most 2. Since $\mathrm{Gal}(K_1(T_1)/K_1) \simeq E[2]$, the inequality

$$|I_2| \le 2^2$$

holds.

Suppose that $\mathcal{M}L_n = \mathcal{M}K_n(t_1, t_2)$. Then $L_n/K_n(T_1, T_2)$ is unramified at any prime above 2 in $K_n(T_1, T_2)$. Since I_v is of type $(2^m, 2)$ for some $m \leq n-1$ and $\varphi(T_2) = \zeta_{2^{n+1}}$, there exists α in $E[2]$ such that ${}^{\sigma}T_2 = T_2 \oplus_E \alpha$ for σ in I_v and

$$I_v \hookrightarrow E[2^{n-1}] \times E[2]$$

via the isomorphism

$$\mathrm{Gal}(K_n(T_1, T_2)/K_n) \simeq E[2^n] \times E[2^n].$$

Thus the inequality

$$|I_2| \leq 2^{2(n-1)} \times 2^2 = 2^{2n}$$

holds.

If $n = 1$, $|I_v|$ equals 2. Indeed $\mathcal{M}L_1 = \mathbb{Q}_2(\sqrt{5}, \sqrt{2}, \zeta_4)$ and $\mathcal{M}K_1 = \mathcal{M}(\sqrt{\pm 2})$. It follows from $\varphi(T_2) = \zeta_4$ that $K_1(T_2)/K_1$ is ramified. Thus $K_1(T_1, T_2)/K_1(T_2)$ is unramified. Since $\mathrm{Gal}(K_1(T_2)/K_1) \simeq E[2]$, the inequality

$$|I_2| \leq 2^2$$

holds.

Now we have the following theorem.

Theorem 3.3. *Assume $p > 2$ and $p \nmid \mathrm{ord}_p(\Delta)$. Then the equation $|I_p| = p^{2(n-\nu)}$ holds for $n > \nu$ and $|I_p| = 1$ holds for $n \leq \nu$.*

Assume $p = 2$. Then the inequality $|I_p| \leq p^{2(n+r_{2,n}-2)+\delta_2}$ holds for all $n \geq 1$, where $r_{2,n} = 1, 2$ according as $E(\mathbb{Q})/E(\mathbb{Q}) \cap [2^n]_E(E(\mathbb{Q}_2))$ is cyclic or not, and

$$\delta_2 = \begin{cases} 2 & \text{if } n = 1 \text{ and } r_{2,1} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Remark 3.4. *Note that the authors roughly estimated it as $|\Phi_n(I_p)| \leq p^{4n}$ in* [13, Section 4].

When $p = 2$ and $\mathcal{I}_n$ is not cyclic, we may assume $\varphi(T_2) = -1$. Thus ζ_4 is in $\mathcal{L}_1$. We note that $\zeta_4 \notin \mathcal{L}_1$ implies $r_{2,n} = 1$.

4. The inertia subgroups of Gal(L_n/K_n) on $\ell \neq p$

In this section we estimate the order of the inertia subgroups of $\mathrm{Gal}(L_n/K_n)$ on $\ell \neq p$.

4.1. The local case when ℓ is multiplicative. Let $\mathfrak{l}$ be a prime ideal in L_n lying above ℓ. Let $\mathcal{L}_n$ and $\mathcal{K}_n$ be the completion of L_n and K_n respectively. Since E has multiplicative reduction at ℓ, E is isomorphic to the Tate curve E_q for some q in $\ell\mathbb{Z}_\ell$. We denote by φ the isomorphism from E to E_q. The isomorphism φ is defined over an unramified extension $\mathcal{M}$ over $\mathbb{Q}_\ell$ of degree at most two. We have $\mathcal{M}K_n = \mathcal{M}(\zeta_{p^n}, q^{\frac{1}{p^n}})$.

We define p_j in $E_q(\overline{\mathbb{Q}}_\ell)$ by $\varphi(P_j) = p_j$ $(1 \le j \le r)$. We put

$$H := \begin{cases} \mathbb{Q}_\ell^* & \text{if } \mathcal{M} = \mathbb{Q}_\ell \\ \{x \in \mathcal{M}^* \mid N_{\mathcal{M}/\mathbb{Q}_\ell}(x) \in q^{\mathbb{Z}}\} & \text{if } [\mathcal{M} : \mathbb{Q}_\ell] = 2. \end{cases}$$

4.1.1. We consider the case where $\mathcal{M} = \mathbb{Q}_\ell$ and $\ell \neq 2$.

Since

$$\mathbb{Q}_\ell^* = \langle l \rangle \times (\mathbb{Z}/\ell\mathbb{Z})^* \times (1 + \ell\mathbb{Z}_\ell),$$

and the p^n-th power mapping is invertible by $\ell \neq p$, we have

$$H/H^{p^n} = \mathbb{Q}_\ell^*/(\mathbb{Q}_\ell)^{*p^n} = \langle l \rangle \times \langle \zeta_{\ell-1} \rangle \simeq (\mathbb{Z}/p^n\mathbb{Z}) \times (\mathbb{Z}/p^m\mathbb{Z}),$$

where we put $m := \min\{\mathrm{ord}_p(\ell - 1), n\}$. We have

$$H/\langle H^{p^n}, q \rangle = \langle l \rangle \times \langle \zeta_{\ell-1} \rangle \simeq (\mathbb{Z}/p^\nu\mathbb{Z}) \times (\mathbb{Z}/p^m\mathbb{Z}), \tag{4.1}$$

where $\nu := \min\{\mathrm{ord}_p(\mathrm{ord}_\ell(q)), n\}$.

It follows from (4.1) that

$$\mathcal{L}_n \subset \mathcal{K}_n(\zeta_{p^n(\ell-1)}, \ell^{\frac{1}{p^n}})$$

and

$$[\mathcal{K}_n(\zeta_{p^n(\ell-1)}, \ell^{\frac{1}{p^n}}) : \mathcal{K}_n(\zeta_{p^n(\ell-1)})] = p^\nu.$$

We also have

$$\mathbb{Q}_\ell(\zeta_{p^n(\ell-1)}, q^{\frac{1}{p^n}}) = \mathbb{Q}_\ell(\zeta_{p^n(\ell-1)}, \ell^{\frac{1}{p^{n-\nu}}}).$$

Since $\mathcal{L}_n(\zeta_{p^n(\ell-1)})/\mathcal{K}_n(\zeta_{p^n(\ell-1)})$ is cyclic, there exists t_j (say t_1) such that $\mathcal{L}_n(\zeta_{p^n(\ell-1)}) = \mathcal{K}_n(\zeta_{p^n(\ell-1)}, t_1)$.

Since $\mathcal{K}_n(\zeta_{p^n(\ell-1)})/\mathcal{K}_n$ is unramified, the ramification index $\mathcal{L}_n/\mathcal{K}_n$ is equal to that of $\mathcal{L}_n(\zeta_{p^n(\ell-1)})/\mathcal{K}_n(\zeta_{p^n(\ell-1)})$.

On the one hand, $\mathbb{Q}_\ell(\ell^{\frac{1}{p^n}})/\mathbb{Q}_\ell$ is a totally ramified extension of degree p^n. On the other hand, $\mathbb{Q}_\ell(\zeta_{p^n(\ell-1)})/\mathbb{Q}_\ell$ is an unramified extension by $\ell \nmid p^n(\ell - 1)$. Thus the ramified index of the extension $\mathbb{Q}_\ell(\zeta_{p^n(\ell-1)}, \ell^{\frac{1}{p^n}})/\mathbb{Q}_\ell$ is p^n.

We put $\mu := \min\{n,\ \mathrm{ord}_p(\mathrm{ord}_\ell(p_1))\}$. Then we have

$$\mathcal{L}_n(\zeta_{p^n(\ell-1)}) = \mathcal{K}_n(\zeta_{p^n(\ell-1)}, t_1) = \mathbb{Q}_\ell(\zeta_{p^n(\ell-1)}, \ell^{\frac{1}{p^{n-\nu}}}, \ell^{\frac{1}{p^{n-\mu}}}).$$

Hence we have

$$|\mathcal{I}_n| = \begin{cases} p^{\nu-\mu} & \text{if } \mu < \nu \\ 1 & \text{if } \mu \ge \nu. \end{cases}$$

If $\mathrm{ord}_p(\mathrm{ord}_\ell(q)) \le \mu$, we see that $|\mathcal{I}_n| = 1$ for all $n \ge 1$. If $\mathrm{ord}_p(\mathrm{ord}_\ell(q)) > \mu$, we see that $|\mathcal{I}_n|$ does not depend on n for all $n \ge \mathrm{ord}_p(\mathrm{ord}_\ell(q))$.

4.1.2. We consider the case where $[\mathcal{M} : \mathbb{Q}_\ell] = 2$ and $\ell \neq 2$.

Since $N_{\mathcal{M}/\mathbb{Q}_\ell}(q) = q^2$, either $N_{\mathcal{M}/\mathbb{Q}_\ell} H = q^{\mathbb{Z}}$ or $N_{\mathcal{M}/\mathbb{Q}_\ell} H = q^{2\mathbb{Z}}$ holds. We have

$$H = \langle u \rangle \times U_{\mathcal{M},1}$$

for some u in $\mathcal{M}$. We may take u satisfying $N_{\mathcal{M}/\mathbb{Q}_\ell}(u) = q^t$ for $t = 1, 2$. Since $\mathcal{M}$ is unramified over $\mathbb{Q}_\ell$, we have $N_{\mathcal{M}/\mathbb{Q}_\ell}\mathcal{O}^* = \mathbb{Z}_\ell^*$. If $\mathrm{ord}_\ell(q)$ is even, we have $N_{\mathcal{M}/\mathbb{Q}_\ell}(u) = q$. If $\mathrm{ord}_\ell(q)$ is odd, we have $N_{\mathcal{M}/\mathbb{Q}_\ell}(u) = q^2$.

In the case of $t = 2$, u is in $\langle q \rangle \times U_{\mathcal{M},1}$. If either $p > 2$ or $t = 2$ holds, we have

$$H/\langle H^{p^n}, q \rangle = U_{\mathcal{M},1}/U_{\mathcal{M},1}^{p^n}.$$

If $p = 2$ and $t = 1$, we have

$$H/\langle H^{p^n}, q \rangle = \langle u \rangle \times U_{\mathcal{M},1}/U_{\mathcal{M},1}^{p^n}.$$

Since

$$\mathcal{O}^* = (\mathcal{O}/\ell\mathcal{O})^* \times (1 + \ell\mathcal{O}),$$

we have

$$U_{\mathcal{M},1} = \mu_{\ell+1} \times \langle \exp(\ell\sqrt{D}) \rangle.$$

If either $p > 2$ or $t = 2$ holds, we have

$$H/\langle H^{p^n}, q \rangle = \langle \zeta_{\ell+1} \rangle \simeq \mathbb{Z}/p^\mu\mathbb{Z},$$

where we put $\mu := \min\{\mathrm{ord}_p(\ell + 1), n\}$. Then we have

$$\mathcal{M}\mathcal{L}_n \subset \mathcal{M}\mathcal{K}_n(\zeta_{p^n(\ell+1)}).$$

It follows from $\ell \nmid p^n(\ell + 1)$ that $\mathcal{M}\mathcal{K}_n(\zeta_{p^n(\ell+1)})/\mathcal{M}\mathcal{K}_n$ is unramified. Thus $\mathcal{L}_n/\mathcal{K}_n$ is unramified. Hence we have $|\mathcal{I}_n| = 1$.

If both $p = 2$ and $t = 1$ holds, we have

$$H/\langle H^{p^n}, q \rangle = \langle u \rangle \times \langle \zeta_{\ell+1} \rangle \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^\mu\mathbb{Z}.$$

We have

$$\mathcal{M}\mathcal{L}_n \subset \mathcal{M}\mathcal{K}_n(\zeta_{2^n(\ell+1)}, u^{\frac{1}{2^n}}).$$

It follows from $\ell \nmid 2^n(\ell + 1)$ that $\mathcal{M}\mathcal{K}_n(\zeta_{2^n(\ell+1)})/\mathcal{M}\mathcal{K}_n$ is unramified. Thus the ramified index of $\mathcal{L}_n/\mathcal{K}_n$ is less than or equal to two. Hence we have $|\mathcal{I}_n| \leq 2$.

4.1.3. We consider the case of $\ell = 2$ and $\mathcal{M} = \mathbb{Q}_2$.

On the subgroup $\langle -1 \rangle \times (1 + 4\mathbb{Z}_2)$ of

$$\mathbb{Q}_2^* = \langle 2 \rangle \times \langle -1 \rangle \times (1 + 4\mathbb{Z}_2)$$

the p^n-the power homomorphism is invertible by $2 \neq p$. Thus we have

$$H/\langle H^{p^n}, q \rangle = \langle 2 \rangle \simeq \mathbb{Z}/p^\nu\mathbb{Z},$$

where we put $\nu := \min\{n, \mathrm{ord}_p(\mathrm{ord}_2(q))\}$. We have

$$\mathcal{K}_n = \mathbb{Q}_2(\zeta_{p^n}, 2^{\frac{1}{p^{n-\nu}}}).$$

On the one hand, $\mathbb{Q}_2(2^{\frac{1}{p^n}})/\mathbb{Q}_2$ is a totally ramified extension of degree p^n. On the other hand, $\mathbb{Q}_2(\zeta_{p^n})/\mathbb{Q}_2$ is unramified by $2 \nmid p^n$. Thus the ramification index of $\mathbb{Q}_2(\zeta_{p^n}, 2^{\frac{1}{p^n}})/\mathbb{Q}_2$ is p^n.

We put $\mu := \mathrm{ord}_p(\mathrm{ord}_2(p_1))$. Then we have

$$\mathcal{L}_n = \mathcal{K}_n(p_1^{\frac{1}{p^n}}) = \mathbb{Q}_2(\zeta_{p^n}, 2^{\frac{1}{p^{n-\nu}}}, 2^{\frac{1}{p^{n-\mu}}}).$$

Hence we have

$$|\mathcal{I}_n| = \begin{cases} p^{\nu-\mu} & \text{if } \mu < \nu \\ 1 & \text{if } \mu \geq \nu. \end{cases}$$

4.1.4. We consider the case of $\ell = 2$ and $[\mathcal{M} : \mathbb{Q}_2] = 2$. Then $q^{\mathbb{Z}} \times U_{\mathcal{M},1}$ has index at most two in H.

Since $p \neq 2$ and $U_{\mathcal{M},1} = \mu_6 \times \langle \varepsilon^2 \rangle$ by (3.3), we have

$$H/\langle H^{p^n}, q\rangle = \langle \varepsilon^2 \rangle \simeq \mathbb{Z}/p^n\mathbb{Z}$$

for $p \neq 3$ and

$$H/\langle H^{p^n}, q\rangle = \mu_3 \times \langle \varepsilon^2 \rangle \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3^n\mathbb{Z}$$

for $p = 3$.

When $p \neq 3$, we have

$$\mathcal{M}\mathcal{L}_n \subset \mathcal{M}\mathcal{K}_n(\varepsilon^{\frac{2}{p^n}}).$$

Since $p \neq 2$ and ε is unit, $\mathcal{M}\mathcal{L}_n/\mathcal{M}\mathcal{K}_n$ is unramified and thus $\mathcal{L}_n/\mathcal{K}_n$ is unramified.

When $p = 3$, we have

$$\mathcal{M}\mathcal{L}_n \subset \mathcal{M}\mathcal{K}_n(\varepsilon^{\frac{2}{3^n}}, \zeta_{3^{n+1}})$$

Since $\mathbb{Q}_2(\zeta_{3^{n+1}})/\mathbb{Q}_2$ is unramified and ε is unit, we see that $\mathcal{M}L_n/\mathcal{M}K_n$ is unramified. Hence $\mathcal{L}_n/\mathcal{K}_n$ is unramified.

In these cases we have $|\mathcal{I}_n| = 1$.

4.1.5. For a prime ℓ at which E has multiplicative reduction, we define

$$\nu_\ell := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_\ell(\Delta)), n\} & \text{if the reduction is split.} \\ 1 & \text{if } p = 2\text{, the reduction is non-split,} \\ & \text{and } \mathrm{ord}_\ell(\Delta) \text{ is even.} \\ 0 & \text{otherwise.} \end{cases}$$

Then the ramification index of $\mathcal{L}_n/\mathcal{K}_n$ is less than or equal to p^{ν_ℓ} if E has multiplicative reduction at $\ell \neq p$.

Put $I_\ell := \langle I_{\mathfrak{l}} \mid \mathfrak{l}|\ell \rangle$ as before. Since $\mathrm{Gal}(L_n/K_n)$ is of p-th power order, each $I_{\mathfrak{l}}$ factors through tame quotient, hence it is a cyclic group.

If $I_{\mathfrak{l}} = 1$, then $I_\ell = 1$. Suppose that $I_{\mathfrak{l}} \neq 1$. The ramification index $K_n(T_j)/K_n$ at $\mathfrak{l}$ takes the maximal value at some j (say $j = 1$).

If it also takes maximal values at $k \neq 1$, then the ramification index of $K_n(T_1, T_k)/K_n(T_1)$ at $\mathfrak{l}$ is equal to that of $K_n(T_1, T_k)/K_n(T_k)$. Since $I_{\mathfrak{l}}$ is cyclic, both $K_n(T_1, T_k)/K_n(T_1)$ and $K_n(T_1, T_k)/K_n(T_k)$ are unramified at $\mathfrak{l}$.

If the ramification index of $K_n(T_1)/K_n$ at $\mathfrak{l}$ is greater than that of $K_n(T_k)/K_n$, then $K_n(T_1, T_k)/K_n(T_k)$ is ramified at $\mathfrak{l}$. Since $I_{\mathfrak{l}}$ is cyclic, $K_n(T_1, T_k)/K_n(T_1)$ is unramified at $\mathfrak{l}$.

Thus $L_n/K_n(T_1)$ is unramified at $\mathfrak{l}$. Since $K_n(T_1)/\mathbb{Q}$ is a Galois extension, $L_n/K_n(T_1)$ is unramified at $\mathfrak{l}$ are unramified at any prime lying above ℓ.

Therefore we have an upper bound $|I_\ell| \leq p^{2\nu_\ell}$. Now we have proved the following theorem.

Theorem 4.1. *The inequality $|I_\ell| \leq p^{2\nu_\ell}$ holds for a prime $\ell \neq p$ at which E has multiplicative reduction.*

4.2. The local case when ℓ is potentially good. Next we consider the case where E has potentially good reduction at ℓ. For such a prime ℓ we have the following lemma which is a part of Proposition 4.7 of [7] due to Raynaud.

Lemma 4.2. *Let E be an elliptic curve over $\mathbb{Q}$ which has potentially good reduction at ℓ. Put $m_0 = 1$ if $p > 2$, $m_0 = 2$ otherwise. Then the base change E/K_{m_0} has good reduction at any prime in K_{m_0} above ℓ.*

Proof. Put $q = p^{m_0}$. Let $\mathcal{K}_{m_0}$ the completion of K_{m_0} at a prime $\mathfrak{l}$ above ℓ. Let $\rho_{E,p}$ be the p-adic Galois representation from $G_{\mathbb{Q}}$ to $\mathrm{GL}_2(\mathbb{Z}_p)$ associated to the p-adic Tate module $T_p(E)$. It is easy to see that $\rho_{E,p}(G_{K_{m_0}}) = 1 + qM_2(\mathbb{Z}_p)$ is a torsion-free, pro-p group. If the restriction mapping $\rho_{E,p}|_{I_{\mathcal{K}_{m_0}}}$ is non-trivial, the order of $\rho_{E,p}(I_{\mathcal{K}_{m_0}})$ becomes infinite. Since E has potentially good reduction at ℓ, there exists a finite extension $\mathcal{K}'/\mathcal{K}_{m_0}$ such that $E/\mathcal{K}'$ has good reduction. Thus $|\rho_{E,p}(I_{\mathcal{K}_{m_0}})|$ is less than or equal to $[\mathcal{K}' : \mathcal{K}_{m_0}]$. This gives a contradiction. Hence $\rho_{E,p}|_{I_{\mathcal{K}_{m_0}}}$ is trivial and $E/\mathcal{K}_{m_0}$ has good reduction. □

Assume that $(n, p) \neq (1, 2)$. Let $I_{\mathfrak{l}}$ the inertia subgroup of $\mathrm{Gal}(L_n/K_n)$ at a prime $\mathfrak{l}$ of K_n lying above ℓ with $\mathrm{ord}_\ell(N) \geq 2$, where N is the conductor of E. Put $I_\ell := \langle I_{\mathfrak{l}} \mid \mathfrak{l}|\ell \rangle$. Let $\mathcal{K}_n$ the completion of K_n at $\mathfrak{l}$ and R be the ring of integers of $\mathcal{K}_n$.

By Lemma 4.2, E/K_n has good reduction at $\mathfrak{l}$ and then one can take the Néron model $\mathcal{E}$ of E over $\mathcal{K}_n$. By basic properties of Néron models (cf. [2, Definition 1, p. 12 and Corollary 2, p. 16]), we have the reduction map $E(\mathcal{K}_n) = \mathcal{E}(R) \overset{\mathrm{red}}{\to} \widetilde{E}_{\mathfrak{l}}(\mathbb{F}_{\mathfrak{l}})$, where $\widetilde{E}_{\mathfrak{l}}$ is the reduction of E at $\mathfrak{l}$. Then for any σ in $I_{\mathfrak{l}}$ and P in $E(\overline{\mathcal{K}_n})$ we see that $\mathrm{red}({}^\sigma P) = \mathrm{red}(P)$. Thus $\mathrm{red} \circ \Phi_n(I_\ell) = \{0\}$ by the definition of the G_n-isomorphism Φ_n from $\mathrm{Gal}(L_n/K_n)$ to $E[p^n]^r$. It follows from

$$E[p^n]^r \overset{\mathrm{red}}{\overset{\sim}{\to}} \widetilde{E}_{\mathfrak{l}}[p^n]^r,$$

that $\Phi_n(I_{\mathfrak{l}}) = \{0\}$ for any $\mathfrak{l}$ dividing ℓ. Hence we have $|I_\ell| = 1$.

The remaining case is $(n, p) = (1, 2)$. Since the ramification at $\mathfrak{l}$ is tame, $I_{\mathfrak{l}}$ is cyclic. Thus we may assume $L_n/K_n(T_1)$ is unramified at any prime lying above ℓ. Since $\mathrm{Gal}(K_1(T_1))/K_1) \simeq E[2]$, we have $|I_\ell| \le 2^2$.

If l is a potentially good prime, we put $\nu_\ell = 1$ or 0 according as $(n, p) = (1, 2)$ or not. Then $|I_\ell| \le 2^{\nu_\ell}$.

5. Proof of Theorem 1.1

Let us keep our notation in Section 3 and assumptions in Theorem 1.1. Let I be the subgroup of $\mathrm{Gal}(L_n/K_n)$ generated by all I_ℓ satisfying $\ell|N$, where N is the conductor of E. Put

$$s := \sum_{\ell \neq p} \nu_\ell$$

for simplicity.

We first assume that p is odd. We note that $\mathrm{Gal}(L_n/K_n)$ is abelian. By applying the results in Section 3 and Section 4, we have

$$|I| \le \prod_{\ell | N} |I_\ell| = \prod_{\mathrm{ord}_\ell(N)=1} |I_\ell| \le p^{2n+2s}.$$

Thus we have

$$[L_n \cap K_n^{\mathrm{ur}} : K_n] = \frac{[L_n : K_n]}{[L_n : L_n^I]} \ge \frac{p^{2nr}}{p^{2n+2s}} = p^{2n(r-1)-2s}$$

for any $n \ge 1$. Here we use $|I_p| \le p^{2n}$ for simplicity.

Next we assume that $p = 2$. The constant $r_{2,n}$ and δ_2 are due to Theorem 3.3. Then we have

$$|I| \le 2^{2n+2(r_{2,n}-2)+\delta_2+2s}$$

and

$$[L_n \cap K_n^{\mathrm{ur}} : K_n] = \frac{[L_n : K_n]}{[L_n : L_n^I]} \ge \frac{2^{2nr}}{2^{2n+\delta_2+2s}} = 2^{2n(r-1)-2(r_{2,n}-2)-\delta_2-2s}$$

for any $n \ge 1$.

This completes a proof of Theorem 1.1.

We define the integer $\nu \ge 0$ by (3.5). Then $|I_p| = p^{2(n-\nu)}$ holds for $n > \nu$, and $|I_p| = 1$ holds for $n \le \nu$. Thus our main theorem improves as follows:

$$|I| \le p^{2(n-\nu)+2s}, \quad [L_n \cap K_n^{\mathrm{ur}} : K_n] \ge p^{2n(r-1)+2\nu-2s}$$

for $n > \nu$;

$$|I| \le p^{2s}, \quad [L_n \cap K_n^{\mathrm{ur}} : K_n] \ge p^{2nr-2s}$$

for $n \le \nu$.

Next, we give a proof of Corollary 1.2. If the conductor of E is equal to a prime p, we have $p \geq 11$, $\Delta \mid p^5$, and $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$ for $n \geq 1$ (cf. [13]). Thus the assumptions of Theorem 1.1 hold in this case.

Since the conductor is equal to p, we have $|I| = |I_p|$ and $s = 0$. Thus we have

$$\kappa_n = \begin{cases} 2n(r-1) + 2\nu & (n > \nu) \\ 2nr & (n \leq \nu). \end{cases}$$

This completes the proof.

6. $L_1 \cap K_\infty = K_1$ for $p = 2$

Let the notations be the same as in Section 2. Put $N_1 := L_1 \cap K_\infty$. Since N_1/K_1 is a G_1-extension contained in L_1/K_1, the Galois group $\mathrm{Gal}(N_1/K_1)$ is isomorphic to the direct product of some copies of $E[p]$. By our previous paper [13] the equation $N_1 = K_1$ holds for $p > 2$.

In this section, we prove $N_1 = K_1$ in the case of $p = 2$.

Put $H_n := 1 + p^n M_2(\mathbb{Z}_p)$ for any $n \geq 1$. It is isomorphic to $\mathrm{Gal}(K_\infty/K_n)$ since $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/p^n\mathbb{Z})$. Contrary to the case of $p > 2$, we have the issues that the equality $H_1^2 = H_2$ does not hold and $H_1/H_2 \simeq M_2(\mathbb{Z}/2\mathbb{Z})$ contains $E[2]$ as an irreducible G_1-quotient. To obtain $N_1 = K_1$ in the case of $p = 2$ we need more careful analysis.

6.1. Maximal abelian extension of K_1 in K_∞. In this subsection we prove $N_1 \subset K_2$.

Instead of H_1^2 we consider the subgroup $\mathcal{H}$ of H_1 generated by H_1^2. It is easy to see that $\mathcal{H}$ is a normal subgroup of H_1 (and also of $\mathrm{GL}_2(\mathbb{Z}_2)$). Since $H_1/\mathcal{H}$ is of exponent two, $H_1/\mathcal{H}$ is an abelian group.

By the Legendre formula the inequality

$$\mu\left(\begin{bmatrix} \frac{1}{2} \\ j \end{bmatrix} 8^j\right) = -j - \mu(j!) + 3j \geq -j - \frac{j}{2-1} + 3j = j$$

holds for $j \geq 0$. Thus

$$(1 + 8M)^{\frac{1}{2}} = \sum_{j=0}^{\infty} \begin{bmatrix} \frac{1}{2} \\ j \end{bmatrix} (8M)^j = 1 + 4M - 8M^2 + \cdots$$

converges in H_2 for any matrix M in $M_2(\mathbb{Z}_p)$. We have $H_2^2 = H_3$ and

$$H_2 \supset \mathcal{H} \supset H_1^2 \supset H_3.$$

Since $\det h^2 \equiv 1 \bmod 8$ holds for any h in H_1, $\det g \equiv 1 \bmod 8$ holds for any g in $\mathcal{H}$, By direct computation we can check

$$\mathcal{H} = \{g \in H_2 \mid \det g \equiv 1 \bmod 8\}.$$

We have $[H_2 : \mathcal{H}] = 2$ and $[H_1 : \mathcal{H}] = 2^5$. We can also check H_3 is a normal subgroup of $\mathcal{H}$.

Lemma 6.1. *$N_1 \subset K_2$ holds.*

Proof. Since $\mathrm{Gal}(N_1/K_1)$ is of exponent two, we have

$$H_1 \supset \mathrm{Gal}(K_\infty/N_1) \supset \mathcal{H}.$$

It follows from $[H_2 : \mathcal{H}] = 2$ that $\mathrm{Gal}(K_\infty/N_1) \cap H_2$ equals to either H_2 or $\mathcal{H}$.

Suppose that $\mathrm{Gal}(K_\infty/N_1) \cap H_2 = \mathcal{H}$, Then

$$[H_2 : \mathrm{Gal}(K_\infty/N_1) \cap H_2] = [H_2\,\mathrm{Gal}(K_\infty/N_1) : \mathrm{Gal}(K_\infty/N_1)] = 2$$

holds. Since $\mathrm{Gal}(N_1/K_1)$ is isomorphic to the direct product of some copies of $E[2]$, $[H_1 : \mathrm{Gal}(K_\infty/N_1)] = 2^2,\ 2^4$ and thus $[H_1 : \mathrm{Gal}(K_\infty/N_1)H_2] = 2,\ 2^3$. This contradicts that $E[2]$ is irreducible G_1-module.

Therefore $\mathrm{Gal}(K_\infty/N_1) \cap H_2 = H_2$. Now we have $\mathrm{Gal}(K_\infty/N_1) \supset H_2$ and $N_1 \subset K_2$. □

6.2. In this subsection we prove $\mathrm{Gal}(K_2/N_1) = V_2^{(1)},\ V_4$ by using the notations in Lemma 6.2.

We study the $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$-module $M_2(\mathbb{Z}/2\mathbb{Z})$ as below.

Lemma 6.2. *There are exactly four non-trivial* $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$*-submodules of* $V_4 := M_2(\mathbb{Z}/2\mathbb{Z})$ *and they are given by*

$$V_1 = \left\langle \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle,\ V_2^{(1)} = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle,\ V_2^{(2)} = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \right\rangle,$$

and $V_3 = M_2(\mathbb{Z}/2\mathbb{Z})^{\mathrm{tr}=0}$. *The relations* $V_4 = V_2^{(1)} \oplus V_2^{(2)}$ *and* $V_2^{(2)} \subset V_3$, $V_1 \subset V_2^{(1)}$ *holds. Further only isotypic G_1-quotient modules of $M_2(\mathbb{Z}/2\mathbb{Z})$ are* $V_4/V_3 \simeq \mathbb{Z}/2\mathbb{Z}$, $V_2^{(1)}/V_1 \simeq \mathbb{Z}/2\mathbb{Z}$ *and* $V_2^{(2)} \simeq (\mathbb{Z}/2\mathbb{Z})^{\oplus 2}$.

Proof. Since $\mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z})$ is generated by $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, we have only to compute the orbit decomposition of $M_2(\mathbb{Z}/2\mathbb{Z})$ under the actions of these two elements. □

As in the proof of Lemma 2.2 of [13], the G_1-module $\mathrm{Gal}(N_1/K_1)$ is isomorphic to a copy of the irreducible G_1-module $E[2]$. By Lemma 6.2 we have $\mathrm{Gal}(K_2/N_1) = V_2^{(1)},\ V_4$. In particular, we have $\mathrm{Gal}(N_1/K_1) \simeq \{0\},\ E[2]$.

6.3. The proof of $N_1 = K_1$. In this subsection we decide the inertia group of a prime ideal lying above 2 in K_2 over $\mathbb{Q}$ and we give a proof of $N_1 = K_1$.

Put $\mathcal{K}_1 = \mathbb{Q}_2(E[2])$ and $\mathcal{K}_2 = \mathbb{Q}_2(E[4])$. Since E has multiplicative reduction, there exists some q in $2\mathbb{Z}_2$ such that E is isomorphic to the Tate curve E_q over the unramified extension $\mathcal{M}$ of $\mathbb{Q}_2$ for $\mathcal{M} = \mathbb{Q}_2,\ \mathbb{Q}_2(\sqrt{-3})$. It follows from

$$\Delta = q \prod_{n\geq 1}(1-q^n)^{24}$$

(cf. [15, p. 356]) that

$$\mathbb{Q}_2(E_q[2]) = \mathbb{Q}_2(\sqrt{q}) = \mathbb{Q}_2(\sqrt{\Delta}),\ \ \mathbb{Q}_2(E_q[4]) = \mathbb{Q}_2(\sqrt[4]{q},\zeta_4) = \mathbb{Q}_2(\sqrt[4]{\Delta},\zeta_4).$$

Since $\mathrm{ord}_2(q)$ is odd, $\mathbb{Q}_2(\sqrt{q})/\mathbb{Q}_2$ is a totally ramified extension of degree two. $\mathbb{Q}_2(\sqrt[4]{q},\zeta_4)/\mathbb{Q}_2$ is a totally ramified extension of degree eight.

Suppose $\mathcal{M} = \mathbb{Q}_2(\sqrt{-3})$. Put φ is an isomorphism from E to E_q. Then ${}^{\sigma}\varphi = \varphi \circ [-1]_E$ for the generator σ of $\mathrm{Gal}(\mathcal{M}/\mathbb{Q}_2)$. Since $\mathbb{Q}_2(\sqrt[4]{q},\zeta_4)/\mathbb{Q}_2$ is totally ramified and $\mathcal{M}/\mathbb{Q}_2$ is unramified, $\mathbb{Q}_2(\sqrt[4]{q},\zeta_4)\cap\mathcal{M} = \mathbb{Q}_2$. Thus we can prolong σ from $\mathrm{Gal}(\mathcal{M}/\mathbb{Q}_2)$ to $\mathrm{Gal}(\mathcal{M}(E[4])/\mathbb{Q}_2)$ such that σ is the identity on $\mathbb{Q}_2(\sqrt[4]{q},\zeta_4)$. For P in $E[4]$ we have

$$\varphi(P) = {}^{\sigma}\varphi(P) = \varphi\circ[-1]_E({}^{\sigma}P).$$

Thus we have ${}^{\sigma}P = [-1]_E(P)$. Therefore

$$\mathbb{Q}_2(E[2]) = \mathbb{Q}_2(E_q[2]), \quad \mathbb{Q}_2(E[4]) = \mathcal{M}(E_q[4]).$$

Now we have the following lemma.

Lemma 6.3. *Assume that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ for $n = 1, 2$. Then we have*

$$\mathcal{K}_1 = \mathbb{Q}_2(\sqrt{q}), \quad \mathcal{K}_2 = \mathcal{M}(\sqrt[4]{q},\zeta_4).$$

The inertia group in $\mathcal{K}_2/\mathcal{K}_1$ is equal to $\mathrm{Gal}(\mathcal{M}(\sqrt[4]{q},\zeta_4)/\mathcal{M}(\sqrt{q}))$. It is generated by two elements:

$$\sqrt[4]{q} \mapsto \sqrt[4]{q}, \quad \zeta_4 \mapsto -\zeta_4$$

and

$$\sqrt[4]{q} \mapsto -\sqrt[4]{q}, \quad \zeta_4 \mapsto \zeta_4.$$

Their matrix representation with respect to $E[4]$ is equal to those with respect to $E_q[4] = \langle \sqrt[4]{q}, \zeta_4\rangle$ and they are

$$1 + 2\begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}, \quad 1 + 2\begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix},$$

respectively. By using

$$\left\langle \begin{bmatrix}0 & 0\\ 0 & 1\end{bmatrix}, \begin{bmatrix}0 & 0\\ 1 & 0\end{bmatrix}\right\rangle \cap V_2^{(1)} = \{0\},$$

we have the following lemma.

Lemma 6.4. *Assume that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ for $n = 1, 2$. The fixed field of $V_2^{(1)}$ in K_2/K_1 is a totally ramified extension over K_1 of degree four.*

We put $\mathbb{Q}_2 N_1 = \mathcal{N}_1$. By (3.1) and (3.4) we have

$$\mathcal{N}_1 \subset \mathcal{L}_1 \subset \mathcal{M}(\sqrt{q}, \zeta_4).$$

Thus the ramification index of $\mathcal{N}_1/\mathcal{K}_1$ is at most two. By Lemma 6.4 we see that $\mathrm{Gal}(K_2/N_1) = V_2^{(1)}$ does not occur.

Now we have $\mathrm{Gal}(K_2/N_1) = V_4$ and $N_1 = K_1$.

Theorem 6.5. *The equality $N_1 = K_1$ holds for $p = 2$.*

7. Examples

In this section we will give elliptic curves which satisfy the condition in Theorem 1.1. The computation is done by using Mathematica, version 10, and databases Sage [16] for elliptic curves over $\mathbb{Q}$ and [9] for local fields.

7.1. $p = 2$. Let E be the elliptic curve defined by $y^2 + xy + y = x^3 - 141x + 624$. This elliptic curve has the conductor $N = 2 \cdot 71^2 = 10082$, the minimal discriminant $\Delta = 2^3 \cdot 71^3$, and j-invariant $2^{-3} \cdot 5^3 \cdot 19^3$. By the criterion of [3] one can check that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ for any $n \geq 1$ since $4t^3(t+1) + j = 0$ does not have a rational solution in t. By [16] we see that $E(\mathbb{Q}) \simeq \mathbb{Z}^2$ and it is generated by $P_1 = (-6, 38)$ and $P_2 = (6, -1)$.

We apply Theorem 1.1 to E for $p = 2$. Since E has non-split multiplicative reduction at 2, we have $\nu_{71} = 1$. $r_{2,n} = 1, 2$ holds. Thus $\kappa_1 \geq 2 \cdot 1 \cdot (2-1) - 2(r_{2,n} - 2) - \delta_2 - 2 \cdot 1 = 0$. (It becomes a trivial inequality.) We also have $\kappa_n \geq 2n(2-1) - 2(r_{2,n} - 2) - 2 \cdot 1 \geq 2n - 4$ for $n \geq 2$. Hence the class number $h_{\mathbb{Q}(E[2^n])}$ satisfies

$$2^{2(n-2)} \mid h_{\mathbb{Q}(E[2^n])}$$

for any $n \geq 2$. In this case we can check $\zeta_4 = \sqrt{-1} \in \mathcal{L}_1$.

7.2. $p = 2$ and $r_{2,n} = 1$. Let E be the elliptic curve defined by

$$h(x, y) := -(y^2 + xy + y) + x^3 + x^2 - 55238x + 4974531 = 0.$$

This elliptic curve has the conductor $N = 2 \cdot 5^2 \cdot 313 = 15650$, the minimal discriminant $\Delta = -2^{19} \cdot 5^6 \cdot 313$, and j-invariant $-2^{-19} \cdot 313^{-1} \cdot 7^3 \cdot 103^3 \cdot 139^3$. Further it has split (resp. non-split) multiplicative reduction at $p = 2$ (resp. 313) and potentially good reduction at 5.

Similarly one can check that $G_n \simeq \mathrm{GL}_2(\mathbb{Z}/2^n\mathbb{Z})$ for any $n \geq 1$. By [16] we see that $E(\mathbb{Q}) \simeq \mathbb{Z}^2$ and it is generated by $P_1 = (\frac{37305}{64}, -\frac{6849551}{512})$ and $P_2 = (-75, 2987)$.

A direct computation shows that L_1 is obtained by adding the roots of the following two equations to K_1:

$$f(x) = 64x^4 - 149220x^3 + 6883875x^2 3 + 5695579750x - 548615793125,$$

$$g(x) = x^4 + 300x^3 + 110850x^2 - 56367500x + 4518668125.$$

These polynomials are obtained as follows. Firstly we compute

$$2P = (f_1(x,y), g_1(x,y)),\ f_1, g_1 \in \mathbb{Q}(x,y)$$

for $P = (x,y)$. For P_1, we have the system of algebraic equations

$$f_1(x,y) = \frac{37305}{64},\ g_1(x,y) = -\frac{6849551}{512},\ h(x,y) = 0.$$

By deleting y we obtain $f(x)$ as a unique common factor. Similarly we obtain $g(x)$ from P_2.

Since E has split multiplicative reduction at $p = 2$, we have $\mathcal{M} = \mathbb{Q}_2$. By using [9] we see that

$$\mathcal{K}_1 = \mathbb{Q}_2(\sqrt{-2}),\ \mathcal{L}_1 = \mathbb{Q}_2(\sqrt{-2}, \sqrt{-3}, \sqrt{-10}) = \mathcal{K}_1(\sqrt{-3}).$$

Therefore $\zeta_4 = \sqrt{-1} \notin \mathcal{L}_1$ and hence $r_{2,n} = 1$.

We now apply Theorem 1.1 to E for $p = 2$. Since E has potentially good reduction at 5, $\nu_5 = 1, 0$ according as $n = 1$ or $n \geq 2$. Since E has non-split reduction at 313 and $\mathrm{ord}_{313}(\Delta)$ is odd, $\nu_{313} = 0$. Then we have $\kappa_1 \geq 2 \cdot 1 \cdot (2-1) - 2(1-2) - 2 - 2 \cdot (1+0) = 0$ and $\kappa_n \geq 2n \cdot (2-1) - 2(1-2) - 0 - 2 \cdot (0+0) = 2n+2$ for $n \geq 2$. Hence the class number $h_{\mathbb{Q}(E[2^n])}$ satisfies

$$2^{2n+2} \mid h_{\mathbb{Q}(E[2^n])}\ (n \geq 2).$$

7.3. $p = 3$. Let E be the elliptic curve defined by $y^2 + xy = x^3 + 543x + 10026$. This elliptic curve has the conductor $N = 3 \cdot 67^2 = 13467$, the minimal discriminant $\Delta = -3^{11} \cdot 67^3$, and j-invariant $3^{-11} \cdot 389^3$. By [16] we see that $G_1 \simeq \mathrm{Gal}(\mathbb{Z}/3\mathbb{Z})$ and $E(\mathbb{Q}) \simeq \mathbb{Z}^2$ whose generators are given by $P_1 = (-13, 35)$ and $P_2 = (39, 282)$. Then we can apply the criterion of [4] (see also the j-invariant in [3, p. 961]) for G_2 to obtain $G_2 \simeq \mathrm{GL}_2(\mathbb{Z}/3^2\mathbb{Z})$. Therefore the conditions in Theorem 1.1 for E is fulfilled. It follows from $r = 2$, $\nu_{67} = 0$ that $\kappa_n \geq 2n(2-1) = 2n$. Hence the class number $h_{\mathbb{Q}(E[3^n])}$ satisfies

$$3^{2n} \mid h_{\mathbb{Q}(E[3^n])}$$

for each $n \geq 1$.

References

[1] M. I. Bashmakov, "The cohomology of abelian varieties over a number field", *Usp. Mat. Nauk* **27** (1972), no. 6, p. 25-66, translation in *Russ. Math. Surv.* **17** (1972), no. 1, p. 25-70.

[2] S. Bosch, W. Lütkebohmert & M. Raynaud, *Néron models*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 21, Springer, 1990.

[3] T. Dokchitser & V. Dokchitser, "Surjectivity of mod 2^n representations of elliptic curves", *Math. Z.* **272** (2012), no. 3-4, p. 961-964.

[4] N. Elkies, "Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9", preprint, 2006.

[5] T. Fukuda, K. Komatsu & S. Yamagata, "Iwasawa λ-invariants and Mordell–Weil ranks of abelian varieties with complex multiplication", *Acta Arith.* **127** (2007), no. 4, p. 305-307.

[6] R. Greenberg, "Iwasawa theory past and present", in *Class field theory its centenary and prospect (Tokyo, 1998)*, Advanced Studies in Pure Mathematics, vol. 30, Mathematical Society of Japan, 2001, p. 335-385.

[7] A. Grothendieck, "Modèles de Néron et monodromie", in *Seminaire de géométrie algébrique Du Bois-Marie 1967-1969 (SGA 7)*, Lecture Notes in Mathematics, vol. 288, Springer, 1972, p. 313-523.

[8] T. Hiranouchi, "Class numbers associated to elliptic curves over $\mathbb{Q}$ with good reduction at p", preprint, 2016.

[9] J. W. Jones & D. P. Roberts, "Database of Local Fields", available at `https://math.la.asu.edu/~jj/localfields/`.

[10] S. Lang, *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften, vol. 231, Springer, 1978.

[11] T. Lawson & C. Wuthrich, "Vanishing of some Galois cohomology groups for elliptic curves", in *Elliptic curves, modular forms and Iwasawa theory*, Springer Proceedings in Mathematics & Statistics, vol. 188, Springer, 2016, p. 373-399.

[12] J.-F. Mestre & J. Oesterlé, "Courbes de Weil semi-stables de discriminant une puissance m-iéme", *J. Reine Angew. Math.* **400** (1989), p. 173-184.

[13] F. Sairaiji & T. Yamauchi, "On the class numbers of the fields of the p^n-torsion points of certain elliptic curves over $\mathbb{Q}$", *J. Number Theory* **156** (2015), p. 277-289.

[14] J.-P. Serre, "Proprietes galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15** (1972), no. 4, p. 259-331.

[15] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 106, Springer, 1986.

[16] The LMFDB Collaboration, "Elliptic Curves over Number Fields", `http://www.lmfdb.org/EllipticCurve/`.

Fumio Sairaiji
Faculty of Nursing,
Hiroshima International University,
Hiro, Hiroshima
737-0112, Japan
E-mail: `sairaiji@hirokoku-u.ac.jp`

Takuya Yamauchi
Mathematical Institute,
Tohoku University
6-3, Aoba, Aramaki, Aoba-Ku, Sendai
980-8578, Japan
E-mail: `yamauchi@math.tohoku.ac.jp`