HIROSHIMA MATH. J.
49 (2019), 117–127

Local torsion primes and the class numbers associated to an elliptic curve over $\mathbb{Q}$

Toshiro HIRANOUCHI

(Received November 8, 2017)
(Revised October 13, 2018)

ABSTRACT. Using the rank of the Mordell-Weil group $E(\mathbb{Q})$ of an elliptic curve E over $\mathbb{Q}$, we give a lower bound of the class number of the number field $\mathbb{Q}(E[p^n])$ generated by p^n-division points of E when the curve E does not possess a p-adic point of order p: $E(\mathbb{Q}_p)[p] = 0$.

1. Introduction

Let E be an elliptic curve over $\mathbb{Q}$ with complex multiplication (abbreviated as CM in the following) satisfying $\mathrm{End}_{\mathbb{C}}(E) = \mathcal{O}_F$ the ring of integers of an imaginary quadratic field F. When E has good ordinary reduction at $p > 2$, the prime p splits completely in F as $p = \pi\bar{\pi}$ where $\pi \in \mathcal{O}_F$ and $\bar{\pi}$ is the complex conjugation of π. Let $F_n := F(E[\pi^n])$ be the field generated by π^n-torsion points of E over F. The extension $F_\infty := \bigcup_n F_n$ of F_1 is a $\mathbb{Z}_p$-extension so that there exist $\lambda, \mu \in \mathbb{Z}_{\geq 0}$ and $\nu \in \mathbb{Z}$ which are all independent of n such that we have

$$\#\mathrm{Cl}_p(F_n) = p^{\lambda n + \mu p^n + \nu}, \qquad \text{for } n \gg 0,$$

where $\mathrm{Cl}_p(F_n)$ is the p-Sylow subgroup of the ideal class group of F_n. It is known that the invariant λ of the $\mathbb{Z}_p$-extension has a lower bound

$$\lambda \geq r - 1,$$

where r is the ($\mathbb{Z}$-)rank of the group of $\mathbb{Q}$-rational points $E(\mathbb{Q})$ ([4], Sect. 5).

For an elliptic curve E over $\mathbb{Q}$ which may not have CM and a prime number $p > 3$, in recent papers [7] and [8], Sairaiji and Yamauchi give a lower bound of the class number $\#\mathrm{Cl}_p(K_n)$ in terms of the rank of $E(\mathbb{Q})$ associated to

This work was supported by KAKENHI 17K05174.
2010 *Mathematics Subject Classification*. Primary 11R29; Secondary 11G05
Key words and phrases. Elliptic curves, and Class number.

the field $K_n := \mathbb{Q}(E[p^n])$ generated by p^n-torsion points $E[p^n] := E(\overline{\mathbb{Q}})[p^n]$ under the following conditions[1]:

(**Red**$_l$) E has multiplicative reduction or potentailly good reduction at any prime $l \neq p$,

(**Red**$_p$) E has multiplicative reduction at p,

(**Disc**) $p \nmid \mathrm{ord}_p(\Delta)$, where Δ is the minimal discriminant of E, and

(**Full**) $\mathrm{Gal}(K_1/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p\mathbb{Z})$.

When $p > 5$ and E is semistable, (**Disc**) is automatically satisfied (*cf.* [8], Sect. 1). The objective of this note is to propose a condition

(**Tor**) $E(\mathbb{Q}_p)[p] = 0$

instead of using (**Red**$_p$) and (**Disc**) above, and give the same form of a lower bound of $\#\mathrm{Cl}_p(K_n)$ as in [8]. The main theorem is the following:

THEOREM 1. *Let E be an elliptic curve over $\mathbb{Q}$ with minimal discriminant Δ and let p be a prime number > 2. Put $K_n := \mathbb{Q}(E[p^n])$. Assume the conditions* (**Tor**) *and* (**Full**) *noted above. Then, for all $n \in \mathbb{Z}_{\geq 1}$, we have the following inequality:*

$$\mathrm{ord}_p(\#\mathrm{Cl}_p(K_n)) \geq 2n(r-1) - 2\sum_{l \neq p,\, l \mid \Delta} v_l,$$

where r is the rank of $E(\mathbb{Q})$ and

$$v_l := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_l(\Delta)), n\}, & \text{if } E \text{ has split multiplicative reduction at } l, \\ n, & \text{if } p = 3,\ E \text{ has additive reduction at } l, \text{ and } c_l = 3, \\ 0, & \text{otherwise}, \end{cases}$$

where c_l is the Tamagawa number at l (cf. (2) *in Section* 2*) and* ord_p *(resp.* ord_l*) is the p-adic (resp. l-adic) valuation on $\mathbb{Q}$.*

REMARK 1. (i) *The condition* (**Full**) *means that the Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(E[p]) \simeq GL_2(\mathbb{Z}/p\mathbb{Z})$ is full (i.e., surjective). This can be checked by some criterions* [9], *Sect.* 2.8 *(see also* [8], *Sect.* 1*).*

(ii) *In* [1], *for an elliptic curve E over $\mathbb{Q}$, a prime number p which does not satisfy* (**Tor**), *that is, $E(\mathbb{Q}_p)[p] \neq 0$, is called a* ***local torsion prime*** *for E. It is expected that when E does not have CM, there are only finitely many local torsion primes (*[1], *Conj.* 1.1*).*

A proof of Theorem 1 is given in Section 3. In Section 2, we give some sufficient conditions for (**Tor**). In fact, the conditions (**Red**$_p$) and (**Disc**) imply

[1] In [7], the cases $p = 2$ and 3 have been studied under the additional condition: $\mathrm{Gal}(K_n/\mathbb{Q}) \simeq GL_2(\mathbb{Z}/p^n\mathbb{Z})$ for all $n \geq 1$. In fact, for $p > 3$, (**Full**) implies this condition (*cf.* [8], Sect. 1).

the condition (**Tor**) (Lem. 3). Not only the theorem above can be applied to an elliptic curve and a prime p of a wider class than [8], but the proof is simplified.

Closing this section, let us consider the elliptic curve E over $\mathbb{Q}$ defined by

$$y^2 + y = x^3 + x^2 - 2x$$

(the Cremona label 389a1) which has the smallest conductor among those of $r = 2$. This E does not have CM and $\Delta = 389$ (E has multiplicative reduction at 389). By using SAGE [2], one can confirm that the condition (**Full**) holds for all primes p and (**Tor**) holds for any odd prime $< 10^6$. Thus, our main theorem says that, for all odd primes $p < 10^6$ (which may be $p = 389$), we have

$$\mathrm{ord}_p(\#\mathrm{Cl}_p(K_n)) \geq 2n.$$

Acknowledgement

The author would like to thank Professor Fumio Sairaiji and Professor Takuya Yamauchi who taught the author their results in [7] and [8]. Not only they generously sent the author their preprint [8], but also gave suggestions and comments which are improved the main theorem in this note. The arguments in the latter part of Lemma 5 are due to them. The author would like to thank Professor Kazuo Matsuno for pointing out an error of the proof of Lemma 3 in an early draft of this note. The author would like to thank also the referee for some comments which amend this note.

2. Local torsion primes

Throughout this note, we use the following notation:

- p: a prime number > 2,
- E: an elliptic curve over $\mathbb{Q}$,
- Δ: the minimal discriminant of E ([10], Chap. VIII, Sect. 8),
- $[p^n] : E \to E$: the isogeny multiplication by p^n ([10], Chap. III, Sect. 4), and
- $E[p^n] := E(\overline{\mathbb{Q}})[p^n]$: the p^n-torsion subgroup of $E(\overline{\mathbb{Q}})$.

Structure theorem on $E(\mathbb{Q}_l)$. For a second prime number l (which may be p), we denote also by E the base change $E \otimes_{\mathbb{Q}} \mathbb{Q}_l$ of the elliptic curve E to $\mathbb{Q}_l$. Define

- $\pi : E(\mathbb{Q}_l) \to \bar{E}(\mathbb{F}_l)$: the reduction map modulo l ([10], Chap. VII, Sect. 2),

- $\bar{E}_{\mathrm{ns}}(\mathbb{F}_l)$: the set of non-singular points in the reduction $\bar{E}(\mathbb{F}_l)$ (*cf.* [10], Chap. III, Prop. 2.5), and
- $E_0(\mathbb{Q}_l) := \pi^{-1}(\bar{E}_{\mathrm{ns}}(\mathbb{F}_l))$.

The reduction map $\pi : E(\mathbb{Q}_l) \to \bar{E}(\mathbb{F}_l)$ modulo l induces a short exact sequence (of abelian groups)

$$0 \to E_1(\mathbb{Q}_l) \to E_0(\mathbb{Q}_l) \xrightarrow{\pi} \bar{E}_{\mathrm{ns}}(\mathbb{F}_l) \to 0, \tag{1}$$

where $E_1(\mathbb{Q}_l)$ is defined by the exactness (*cf.* [10], Chap. VII, Prop. 2.1).

LEMMA 1. (i) $E_1(\mathbb{Q}_l)[p] = 0$.

(ii) (a) *If E has multiplicative reduction at l, then $\bar{E}_{\mathrm{ns}}(\mathbb{F}_l) \subset \bar{E}_{\mathrm{ns}}(\mathbb{F}_{l^2}) \simeq (\mathbb{F}_{l^2})^{\times}$.*

(b) *If E has additive reduction at l, then $\bar{E}_{\mathrm{ns}}(\mathbb{F}_l) \simeq \mathbb{F}_l$ as additive groups.*

(iii) (a) *If E has split multiplicative reduction at l, then $E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l) \simeq \mathbb{Z}/\mathrm{ord}_l(\Delta)\mathbb{Z}$.*

(b) *If E has non-split multiplicative reduction at l, then $E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l)$ is a finite group of order at most 2.*

(c) *In all other cases, namely, E has good reduction or additive reduction at l, the quotient $E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l)$ is a finite group of order at most 4.*

(iv) *We have an isomorphism*

$$E(\mathbb{Q}_l) \simeq \mathbb{Z}_l \oplus E(\mathbb{Q}_l)_{\mathrm{tor}}$$

as abelian groups, where $E(\mathbb{Q}_l)_{\mathrm{tor}}$ is the torsion subgroup of $E(\mathbb{Q}_l)$ which is finite.

PROOF. (i) We have $E_1(\mathbb{Q}_l) \simeq \hat{E}(l\mathbb{Z}_l)$, where $\hat{E}(l\mathbb{Z}_l)$ is the group associated to the formal group $\hat{E}$ of E ([10], Chap. VII, Prop. 2.2). Since every torsion element of the group $\hat{E}(l\mathbb{Z}_l)$ has order a power of l ([10], Chap. IV, Prop. 3.2 (b)), we obtain $\hat{E}(l\mathbb{Z}_l)[p] = 0$ if $l \neq p$. For the remaining case $l = p > 2$, the assertion follows from $E_1(\mathbb{Q}_p) \simeq \hat{E}(p\mathbb{Z}_p) \simeq p\mathbb{Z}_p \simeq \mathbb{Z}_p$ ([10], Chap. IV, Thm. 6.4 (b)).

(ii) [10], Chapter III, Exercise 3.5.

(iii) [10], Chapter VII, Theorem 6.1 (for the cases (a) and (c)) and [11], Chapter IV, Remark 9.6 (for the case (b)).

(iv) The quotients $E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l), E_0(\mathbb{Q}_l)/E_1(\mathbb{Q}_l) \simeq \bar{E}_{\mathrm{ns}}(\mathbb{F}_l)$ are finite by (ii) and (iii). From the exact sequence (1), it is enough to show

$$E_1(\mathbb{Q}_l) \simeq \mathbb{Z}_l \oplus E_1(\mathbb{Q}_l)_{\mathrm{tor}},$$

where $E_1(\mathbb{Q}_l)_{\mathrm{tor}}$ is the torsion subgroup of $E_1(\mathbb{Q}_l)$ which is finite. In fact, as in the proof of (i), we have $E_1(\mathbb{Q}_l) \simeq \hat{E}(l\mathbb{Z}_l)$. For the case $l > 2$, the formal

logarithm induces $\hat{E}(l\mathbb{Z}_l) \simeq l\mathbb{Z}_l \simeq \mathbb{Z}_l$. On the other hand, for the case $l = 2$, we have $\hat{E}(2^2\mathbb{Z}_2) \simeq 2^2\mathbb{Z}_2 \simeq \mathbb{Z}_2$ and the quotient $\hat{E}(2\mathbb{Z}_2)/\hat{E}(2^2\mathbb{Z}_2) \simeq 2\mathbb{Z}_2/2^2\mathbb{Z}_2$ is finite ([10], Chap. IV, Prop. 3.2 (a)). The assertion follows from these structure of $\hat{E}(l\mathbb{Z}_l)$. □

Recall that the **Tamagawa number** c_l at a prime l for E is defined by

$$c_l := (E(\mathbb{Q}_l) : E_0(\mathbb{Q}_l)). \tag{2}$$

LEMMA 2. *Suppose that E has additive reduction at a prime $l \neq p$. We further assume the following conditions:*

(a) $p > 3$, *or*

(b) $c_l \neq 3$, *where c_l is the Tamagawa number at l (cf. (2)).*

Then, $E(\mathbb{Q}_l)[p] = 0$.

PROOF. As E has additive reduction at l, we have $\bar{E}_{\mathrm{ns}}(\mathbb{F}_l)[p] = 0$ (Lem. 1 (ii-b)). On the other hand, $E_1(\mathbb{Q}_l)[p] = 0$ (Lem. 1 (i)) so that $E_0(\mathbb{Q}_l)[p] = 0$ by (1). As $c_l = \#E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l) \leq 4$ (Lem. 1 (iii)), the quotient $E(\mathbb{Q}_l)/E_0(\mathbb{Q}_l)$ does not possess elements of order p under the additional assumption (a) or (b). We obtain $E(\mathbb{Q}_l)[p] = 0$. □

Multiplicative reduction at p.

LEMMA 3. *Suppose the condition* (**Red**$_p$) *in Introduction, that is, E has multiplicative reduction at p. We further assume one of the following conditions:*

(**Disc**) $p \nmid \mathrm{ord}_p(\Delta)$, *or*

(a) *E has non-split multiplicative reduction at p.*

Then, the condition (**Tor**)*: $E(\mathbb{Q}_p)[p] = 0$ holds.*

PROOF. As E has multiplicative reduction at p, $\bar{E}_{\mathrm{ns}}(\mathbb{F}_p) \subset \bar{E}_{\mathrm{ns}}(\mathbb{F}_{p^2}) \simeq (\mathbb{F}_{p^2})^\times$ (Lem. 1 (ii-a)). In particular, $\bar{E}_{\mathrm{ns}}(\mathbb{F}_p)[p] = 0$. On the other hand, $E_1(\mathbb{Q}_p)[p] = 0$ (Lem. 1 (i)) and hence $E_0(\mathbb{Q}_p)[p] = 0$ by (1).

Case (a): First, we suppose that E has non-split multiplicative reduction. In this case, the quotient group $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ is a finite group of order at most 2 (Lem. 1 (iii)) so that we obtain $E(\mathbb{Q}_p)[p] = 0$.

Case (Disc): Next, we assume $p \nmid \mathrm{ord}_p(\Delta)$. From Case (a) above, we may assume that E has split multiplicative reduction at p. The assertion follows from $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p) \simeq \mathbb{Z}/\mathrm{ord}_p(\Delta)\mathbb{Z}$ (Lem. 1 (iii)). □

REMARK 2. *When the elliptic curve E over $\mathbb{Q}$ has multiplicative reduction at 2, by considering the isomorphism $E(\mathcal{K}) \simeq \mathcal{K}^\times/q^{\mathbb{Z}}$ for some unramified extension $\mathcal{K}/\mathbb{Q}_2$ locally, $-1 \in \mathcal{K}^\times$ gives a 2-torsion element in $E(\mathbb{Q}_2)$. Thus the condition* (**Tor**) *at 2 does not hold: $E(\mathbb{Q}_2)[2] \neq 0$.*

Good reduction at p.

LEMMA 4. *Suppose that E has good reduction at p.*

(i) *We further assume one of the following conditions:*
   (a) $\bar{E}(\mathbb{F}_p)[p] = 0$, *or*
   (b) $E(\mathbb{Q})_{\mathrm{tor}} \neq 0, p \geq 11$.
   Then, the condition (**Tor**) *holds.*

(ii) *Assume that E has CM, and $p \geq 7$. Then,* (**Tor**) *holds if and only if* $\bar{E}(\mathbb{F}_p)[p] = 0$.

The lemma above essentially follows from [1], Proposition 2.1. For the sake of completeness, we give a proof.

PROOF (of Lem. 4). (i) **Case (a):** We have $E_1(\mathbb{Q}_p)[p] = 0$ (Lem. 1 (i)). The condition can be checked by using the exact sequence

$$0 \to E(\mathbb{Q}_p)[p] \xrightarrow{\pi} \bar{E}(\mathbb{F}_p)[p] \xrightarrow{\delta} \hat{E}(p\mathbb{Z}_p)/p\hat{E}(p\mathbb{Z}_p),$$

where δ is the connecting homomorphism. The assumption $\bar{E}(\mathbb{F}_p)[p] = 0$ implies the condition (**Tor**).

Case (b): Assume $E(\mathbb{Q}_p)[p] \neq 0$. By [1], Proposition 2.1 (1), we have $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}/p\mathbb{Z}$. From the assumption $p \geq 11$, this contradicts with Mazur's theorem on $E(\mathbb{Q})_{\mathrm{tor}}$ ([10], Chap. VIII, Thm. 7.5).

(ii) From (i) (the case (a)), it is enough to show that if $\bar{E}(\mathbb{F}_p)[p] \neq 0$, then $E(\mathbb{Q}_p)[p] \neq 0$. From Hasse's theorem ([10], Chap. V, Thm. 1.1) and $p \geq 7$, $\#\bar{E}(\mathbb{F}_p) = p$. We have $a_p(E) := p + 1 - \#\bar{E}(\mathbb{F}_p) = 1$. This implies $E(\mathbb{Q}_p)[p] \neq 0$ by [1], Proposition 2.1 (3) under the assumption that E has CM. □

When E has CM, Lemma 4 (ii) gives a criterion for the condition (**Tor**). On the other hand, Lemma 4 (i) says that, for $p \geq 11$, (**Tor**) does not hold only if

(a′) $\bar{E}(\mathbb{F}_p)[p] \neq 0$, and
(b′) $E(\mathbb{Q})_{\mathrm{tor}} = 0$.

For our purpose, we further impose

(c′) E does not have CM, and
(d′) the rank $r > 1$ (to exclude cases where our main theorem (Thm. 1) becomes trivial).

The following calculations are given by using SAGE [2]. There are 1733 elliptic curves with conductor $N < 10^4$ satisfying (b′)–(d′) above. Among them, only 50 curves have a local torsion prime p in the range $11 \leq p < 10^6$, *i.e.*, $E(\mathbb{Q}_p)[p] \neq 0$ listed below:

	curve	p		curve	p		curve	p		curve	p
1	1639b1	2833	14	4976a1	11	27	7497c1	13	40	9082a1	13
2	1957a1	163	15	5171a1	23	28	7520e1	11	41	9149c1	23
3	2299b1	31	16	5736f1	11	29	7826d1	19	42	9395a1	37
4	2343c1	17	17	5763d1	23	30	8025d1	43	43	9467a1	19
5	2541c1	197	18	5982h1	197	31	8025d2	43	44	9510c1	103
6	2728d1	443	19	6334b1	11	32	8048f1	2593	45	9535a1	31
7	3220a1	41	20	6405c1	113	33	8384j1	157	46	9706b1	367
8	3333b1	19	21	6792a1	97	34	8495a1	43	47	9783b1	11
9	3997a1	167	22	6848p1	23	35	8551a1	293	48	9789f1	541
10	4024b1	47	23	6896e1	29	36	8768h1	17	49	9797b1	19
11	4279c1	13	24	7152a1	79	37	8950m1	271	50	9865b1	11
12	4504b1	19	25	7233a1	11	38	8974c1	1063			
13	4768a1	109	26	7366g1	11	39	8988d1	37			

Table 1. Local torsion primes

3. Elliptic curve over $\mathbb{Q}$

We keep the notation of the last section. We further define

- $K_n := \mathbb{Q}(E[p^n])$ (*cf.* [10], Chap. VIII, Prop. 1.2 (d)),
- $r :=$ the rank of $E(\mathbb{Q})$ (which is finite by the Mordell-Weil theorem [10], Chap. VIII),
- $P_1, \ldots, P_r \in E(\mathbb{Q})$: generators of the free part of $E(\mathbb{Q})$, and
- $L_n := K_n([p^n]^{-1}P_1, \ldots, [p^n]^{-1}P_r)$.

Following [5], Chapter V, Section 5, for each $1 \leq i \leq r$, define

$$\Phi^{(i)} : \mathrm{Gal}(L_n/K_n) \to E[p^n]; \sigma \mapsto \sigma(Q_i) - Q_i, \tag{3}$$

where $Q_i \in E(\overline{\mathbb{Q}})$ with $[p^n]Q_i = P_i$. Since $E[p^n] \subset E(K_n)$, the map $\Phi^{(i)}$ does not depend on the choice of Q_i. These homomorphisms $(\Phi^{(i)})_{1 \leq i \leq r}$ induce an injective homomorphism

$$\Phi : \mathrm{Gal}(L_n/K_n) \to E[p^n]^{\oplus r}; \sigma \mapsto (\Phi^{(i)}(\sigma))_i. \tag{4}$$

From $E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^{\oplus 2}$ ([10], Chap. III, Cor. 6.4) the extension L_n/K_n is an abelian extension with $[L_n : K_n] \leq p^{2nr}$.

Inertia subgroups. For any prime number l and a prime ideal $\mathfrak{l}$ in (the ring of integers of) K_n above l (we write $\mathfrak{l}|l$ in the following), we denote by

- $I_{\mathfrak{l}}$: the inertia subgroup of $\mathrm{Gal}(L_n/K_n)$ at $\mathfrak{l}$ (for L_n/K_n is abelian, the inertia subgroup $I_{\mathfrak{l}}$ is independent of a choice of a prime ideal in L_n above $\mathfrak{l}$), and
- $I_l := \langle I_{\mathfrak{l}};$ prime ideal $\mathfrak{l}|l$ in $K_n \rangle$: the subgroup of $\mathrm{Gal}(L_n/K_n)$ generated by $I_{\mathfrak{l}}$ for all $\mathfrak{l}|l$.

For any prime $\mathfrak{l}|l$ of K_n, and a prime $\mathfrak{L}$ of L_n above $\mathfrak{l}$ (we write $\mathfrak{L}|\mathfrak{l}$), we denote by

- $(K_n)_{\mathfrak{l}}$: the completion of K_n at $\mathfrak{l}$, and
- $(L_n)_{\mathfrak{L}}$: the completion of L_n at $\mathfrak{L}$.

LEMMA 5. *We assume the condition* (**Tor**). *Then, we have* $\#I_p \leq p^{2n}$.

PROOF. By the structure theorem on $E(\mathbb{Q}_p)$ (Lem. 1 (iv)),

$$E(\mathbb{Q}_p) \simeq \mathbb{Z}_p \oplus E(\mathbb{Q}_p)_{\mathrm{tor}}.$$

From the condition (**Tor**), we have $E(\mathbb{Q}_p)_{\mathrm{tor}}/[p^n]E(\mathbb{Q}_p)_{\mathrm{tor}} = 0$ and hence

$$E(\mathbb{Q}_p)/[p^n]E(\mathbb{Q}_p) \simeq \mathbb{Z}/p^n\mathbb{Z}.$$

Let $\overline{P} \in E(\mathbb{Q}_p)/[p^n]E(\mathbb{Q}_p)$ (the residue class represented by a point $P \in E(\mathbb{Q}_p)$) be a generator of the cyclic group $E(\mathbb{Q}_p)/[p^n]E(\mathbb{Q}_p)$ and, for each index $1 \leq i \leq r$, write

$$\overline{P_i} = \overline{a_i} \cdot \overline{P} \qquad \text{in } E(\mathbb{Q}_p)/[p^n]E(\mathbb{Q}_p)$$

for some $\overline{a_i} \in \mathbb{Z}/p^n\mathbb{Z}$ $(a_i \in \mathbb{Z})$. Take $1 \leq i \leq r$ such that

$$\mathrm{ord}_p(a_i) \leq \mathrm{ord}_p(a_j)$$

for all $1 \leq j \leq r$. For any prime $\mathfrak{P}|p$ of L_n, we denote by $\mathfrak{p}$ the prime in K_n below $\mathfrak{P}$. Using the chosen index i, we obtain

$$(L_n)_{\mathfrak{P}} = (K_n)_{\mathfrak{p}}([p^n]^{-1}P_i). \tag{5}$$

Put $K_n' := K_n([p^n]^{-1}P_i) \subset L_n$. From the equality (5), the extension L_n/K_n' is unramified (at all primes in K_n') above $\mathfrak{p}$. As the extension $K_n/\mathbb{Q}$ is Galois, this extension L_n/K_n' is unramified above p. Since $I_p \cap \mathrm{Gal}(L_n/K_n') = \{1\}$, the restriction $\Phi^{(i)}|_{I_p} : I_p \to E[p^n]$ of $\Phi^{(i)}$ defined in (3) is injective and hence $\#I_p \leq p^{2n}$. □

LEMMA 6. *Let l be a prime number with $l \neq p$.*

(i) *We have $\#I_l \leq p^{2n}$.*

(ii) *Suppose that E has multiplicative reduction at l. We have $\#I_l \leq p^{2v_l}$, where*

$$v_l := \begin{cases} \min\{\mathrm{ord}_p(\mathrm{ord}_l(\Delta)), n\}, & \text{if } E \text{ has split multiplicative reduction at } l, \\ 0, & \text{if } E \text{ has non-split multiplicative reduction at } l. \end{cases}$$

(iii) *Suppose that E has additive reduction at l. We further assume the following conditions:*

(a) $p > 3$, *or*
(b) $c_l \neq 3$, *where* c_l *is the Tamagawa number at* l *(cf.* (2)*).*
Then, we have $\#I_l = 1$.

PROOF. (i) Take any $\mathfrak{l}|l$ in K_n. For a prime $\mathfrak{L}|\mathfrak{l}$ in L_n, let $(T_n)_{\mathfrak{L}} := ((L_n)_{\mathfrak{L}})^{I_{\mathfrak{l}}}$ be the inertia field of $\mathfrak{L}$ over $(K_n)_{\mathfrak{l}}$ which is the fixed field of $I_{\mathfrak{l}}$ (*cf.* [6], Chap. II, Def. 9.10). Since $l \neq p$, the extension L_n/K_n is tamely ramified at any prime $\mathfrak{L}|\mathfrak{l}$ in L_n. The inertia subgroup $I_{\mathfrak{l}} = \mathrm{Gal}((L_n)_{\mathfrak{L}}/(T_n)_{\mathfrak{L}})$ is cyclic (*cf.* [6], Chap. II, Sect. 9). There exists $1 \leq i \leq r$ such that

$$(T_n)_{\mathfrak{L}}([p^n]^{-1}P_j) \subset (T_n)_{\mathfrak{L}}([p^n]^{-1}P_i)$$

for any $1 \leq j \leq r$. Since $I_{\mathfrak{l}}$ does not depend on the choice of $\mathfrak{L}|\mathfrak{l}$ in L_n, the index i above can be chosen independent of $\mathfrak{L}|\mathfrak{l}$. We obtain

$$(L_n)_{\mathfrak{L}} = (T_n)_{\mathfrak{L}}([p^n]^{-1}P_i) \tag{6}$$

for any prime $\mathfrak{L}|\mathfrak{l}$.

Put $K_n' := K_n([p^n]^{-1}P_i) \subset L_n$. The extension $(T_n)_{\mathfrak{L}}/(K_n)_{\mathfrak{l}}$ of local fields is unramified from the definition of $(T_n)_{\mathfrak{L}}$ for any prime $\mathfrak{L}|\mathfrak{l}$ in L_n. Using the equality (6) the extension

$$(L_n)_{\mathfrak{L}} = (T_n)_{\mathfrak{L}}([p^n]^{-1}P_i) \qquad \text{over } (K_n)_{\mathfrak{l}}([p^n]^{-1}P_i)$$

is also unramified ([6], Chap. II, Prop. 7.2). This implies that L_n/K_n' is unramified at all primes $\mathfrak{L}|\mathfrak{l}$ in L_n. As the extension $K_n/\mathbb{Q}$ is Galois, this extension L_n/K_n' is unramified above l. Since $I_l \cap \mathrm{Gal}(L_n/K_n') = \{1\}$, the restriction $\Phi^{(i)}|_{I_l} : I_l \to E[p^n]$ of $\Phi^{(i)}$ defined in (3) is injective and hence $\#I_l \leq p^{2n}$.

(ii) This assertion is [8], Theorem 4.1.

(iii) By Lemma 1 (iv), we have

$$E(\mathbb{Q}_l) \simeq \mathbb{Z}_l \oplus E(\mathbb{Q}_l)_{\mathrm{tor}}.$$

From $E(\mathbb{Q}_l)[p] = 0$ (Lem. 2), we have

$$E(\mathbb{Q}_l)/[p^n]E(\mathbb{Q}_l) = 0.$$

Hence, $P_i \in [p^n]E(\mathbb{Q}_l)$ for each i. This implies that, for any prime $\mathfrak{l}|l$ in K_n, $(K_n)_{\mathfrak{l}}([p^n]^{-1}P_i) = (K_n)_{\mathfrak{l}}$ and hence

$$(L_n)_{\mathfrak{L}} = (K_n)_{\mathfrak{l}}$$

for any $\mathfrak{L}|\mathfrak{l}$ in L_n. In particular, L_n/K_n is unramified at all primes $\mathfrak{L}|\mathfrak{l}$ in L_n. As the extension $K_n/\mathbb{Q}$ is Galois, this extension L_n/K_n is unramified above l. Hence $I_l = \{1\}$.

Proof of Theorem 1. In the rest of this section, we show Theorem 1. As in the beginning of this section, first we choose

- $P_1, \dots, P_r \in E(\mathbb{Q})$: generators of the free part of $E(\mathbb{Q})$, and put
- $L_n := K_n([p^n]^{-1}P_1, \dots, [p^n]^{-1}P_r)$.

Next, we define

- $\tilde{K}_n$: the Hilbert p-class field, that is, the maximal unramified abelian p-extension of K_n, and
- $I := \langle I_l; l = p \text{ or } l|\Delta \rangle \subset \mathrm{Gal}(L_n/K_n)$: the subgroup generated by the inertia subgroups I_p and I_l for all prime number $l|\Delta$.

By class field theory (*cf.* [6], Chap. VI, Prop. 6.9), we have

$$\#\mathrm{Cl}_p(K_n) = [\tilde{K}_n : K_n] \geq [L_n \cap \tilde{K}_n : K_n] = \frac{[L_n : K_n]}{[L_n : L_n \cap \tilde{K}_n]}. \tag{7}$$

From the condition (**Full**) and $p > 2$, $\Phi : \mathrm{Gal}(L_n/K_n) \to E[p^n]^{\oplus r}$ defined in (4) is bijective ([7], Thm. 2.4[2], see also [5], Chap. V, Lem. 1) and hence

$$[L_n : K_n] = p^{2nr}. \tag{8}$$

Since the extension L_n/K_n is unramified outside $\{p, \infty\} \cup \{l|\Delta\}$ ([10], Chap. VIII, Prop. 1.5 (b)), we have

$$[L_n : L_n \cap \tilde{K}_n] = [L_n : L_n^I] = \#I. \tag{9}$$

Using the upper bound of $\#I_l$ given in Lemma 5 (for $l = p$ under the condition (**Tor**)) and Lemma 6 (for $l \neq p$), we have

$$\#I \leq \#I_p \cdot \prod_{l \neq p,\, l|\Delta} \#I_l \leq p^{2n} \cdot p^{2\sum_{l \neq p,\, l|\Delta} v_l}. \tag{10}$$

Finally, Theorem 1 follows from the following inequalities:

$$\begin{aligned} \#\mathrm{Cl}_p(K_n) &\geq \frac{[L_n : K_n]}{[L_n : L_n \cap \tilde{K}_n]} \qquad \text{(by (7))} \\ &= \frac{p^{2nr}}{\#I} \qquad \text{(by (8) and (9))} \\ &\geq p^{2n(r-1)-2\sum_{l \neq p,\, l|\Delta} v_l} \qquad \text{(by (10))}. \end{aligned}$$

□

[2] In [7], it is considered the case where $p \geq 11$. However, the arguments of Theorem 2.4 in [7] works for $p > 2$.

References

[1] C. David and T. Weston, Local torsion on elliptic curves and the deformation theory of Galois representations, Math. Res. Lett. **15** (2008), no. 3, 599–611.
[2] The Sage Developers, Sagemath, the Sage Mathematics Software System (Version 7.4), 2016, http://www.sagemath.org.
[3] N. D. Elkies, Elliptic curves with 3-adic Galois representation surjective mod 3 but not mod 9, arXiv:0612734 [math.NT].
[4] R. Greenberg, Iwasawa theory—past and present, Class field theory—its centenary and prospect (Tokyo, 1998), Adv. Stud. Pure Math., vol. 30, Math. Soc. Japan, Tokyo, 2001, pp. 335–385.
[5] S. Lang, Elliptic curves: Diophantine analysis, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 231, Springer-Verlag, Berlin-New York, 1978.
[6] J. Neukirch, Algebraic number theory, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.
[7] F. Sairaiji and 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), 277–289.
[8] F. Sairaiji and T. Yamauchi, On the class numbers of the fields of the p^n-torsion points of elliptic curves over $\mathbb{Q}$, arXiv:1603.01296v3 [math.NT].
[9] J.-P. Serre, Propriétés galoisiennes des points d'ordre fini des courbes elliptiques, Invent. Math. **15** (1972), no. 4, 259–331.
[10] J. H. Silverman, The arithmetic of elliptic curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[11] J. H. Silverman, Advanced topic in the arithmetic of elliptic curves, Graduate Texts in Mathematics, vol. 151, Springer, Dordrecht, 2013.

Toshiro Hiranouchi
Department of Basic Sciences
Graduate School of Engineering
Kyushu Institute of Technology
1-1 *Sensui-cho, Tobata-ku, Kitakyushu-shi*
Fukuoka 804-8550, *Japan*
E-mail: hira@mns.kyutech.ac.jp