COMMENTARII MATHEMATICI
UNIVERSITATIS SANCTI PAULI
Vol. 50, No. 2 2001

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

Calculation of Selmer Groups of Elliptic Curves with Rational 2-Torsions and θ-Congruent Number Problem

by

Takeshi GOTO

(Received January 10, 2001)
(Revised March 15, 2001)

1. Introduction

A natural number n is called a *congruent number* if it is the area of a right triangle with rational sides. It is well known that n is congruent if and only if the Mordell-Weil rank of the following elliptic curve E_n is positive ([5]):

$$E_n : y^2 = x(x+n)(x-n)\,.$$

Tunnell's theorem ([9]) gives a criterion to tell whether a given n is congruent or not. This criterion is complete if the weak form of the Birch and Swinnerton-Dyer conjecture is true.

Fujiwara [3] defined the generalized concept, a *θ-congruent number* by considering triangles with rational sides and an angle θ. For such a triangle, $\cos\theta$ is necessarily rational, thus we write $\cos\theta = s/r$ with $\gcd(r, s) = 1$ and $r > 0$. Then $\sin\theta = \sqrt{r^2 - s^2}/r$.

DEFINITION. A natural number n is *θ-congruent* if $n\sqrt{r^2 - s^2}$ is the area of a triangle with rational sides and an angle θ.

For $\theta = \pi/2$, we have $r = 1$ and $s = 0$. Hence $\pi/2$-congruent numbers are nothing but the classical congruent numbers. Since n is θ-congruent if and only if c^2n is θ-congruent for some integer c, we may assume without loss of generality that n is a squarefree natural number. The θ-congruent numbers are also connected with the following elliptic curves:

$$E_{n,\theta} : y^2 = x(x + (r+s)n)(x - (r-s)n)\,. \tag{1.1}$$

THEOREM 1.1 (Fujiwara, [3]). *Let n be any squarefree natural number. Then*

(1) *n is θ-congruent if and only if $E_{n,\theta}$ has a rational point of order greater than* 2.

(2) *For $n \neq 1, 2, 3, 6$, n is θ-congruent if and only if $E_{n,\theta}(\mathbf{Q})$ has a positive rank.*

The *θ-congruent number problem* is to find a simple criterion to determine whether a given integer is a θ-congruent number or not. In view of Fujiwara's theorem, this problem is equivalent to determining whether the $\mathbf{Q}$-rank of $E_{n,\theta}$ is positive or not. Clearly $E_{n,\theta}$ has rational 2-torsions. Conversely, it can be shown that an elliptic curve with rational

2-torsions is isomorphic to some $E_{n,\theta}$ over $\mathbf{Q}$. In this paper, we study the Selmer group of the following elliptic curve:

$$E_{\alpha,\beta} : y^2 = x(x-\alpha)(x-\beta) \quad (\alpha, \beta \in \mathbf{Q},\ \alpha \neq \beta,\ \alpha \neq 0,\ \beta \neq 0)\,.$$

The Selmer group gives a bound of the rank. We recall the definition and some basic facts of the Selmer group in §2. Our main result in vague form is as follows.

MAIN THEOREM. We have the complete formula for the Selmer group of $E_{\alpha,\beta}$ associated to 2-isogeny. The order of the group is also explicitly given.

The precise statements of this theorem are given in Theorem 4.2 and Theorem 4.4.

Aoki [1] calculated the Selmer groups of the elliptic curves connected with the classical congruent number problem. Most ideas in this paper owe those origin to Aoki [1]. One of the methods is to study how local points at bad primes appear. The results of the investigations and some examples are described in §3. The proofs are in §6. We derive the formula for the dimension of Selmer group in §4. It is applied to a part of the θ-congruent number problem in §5, where the following corollary is proved.

COROLLARY 1.2. *Let p be a prime. Then*

(1) $p \equiv 7$ *or* $13 \pmod{24} \Rightarrow 2p$ *is NOT* $\pi/3$*-congruent.*

(2) $p \equiv 5, 11, 17$ *or* $19 \pmod{24} \Rightarrow 3p$ *is NOT* $\pi/3$*-congruent.*

(3) $p \equiv 13$ *or* $19 \pmod{24} \Rightarrow 2p$ *is NOT* $2\pi/3$*-congruent.*

(4) $p \equiv 17 \pmod{24} \Rightarrow 3p$ *is NOT* $2\pi/3$*-congruent.*

The main result applied, we can obtain analogous facts with the other angles θ or the other numbers n. This corollary is an analogy of the following theorem in [3].

THEOREM 1.3. *Let p be a prime. Then*

(1) $p \equiv 5, 7$ *or* $19 \pmod{24} \Rightarrow p$ *is NOT* $\pi/3$*-congruent.*

(2) $p \equiv 7$ *or* $11 \pmod{24} \Rightarrow p$ *is NOT* $2\pi/3$*-congruent.*

Fujiwara [3] also says

$$p \equiv 13 \pmod{24} \Rightarrow p \textit{ is NOT } 2\pi/3\textit{-congruent}.$$

But the computation of Selmer group is not enough to deduce this fact. The proof is in Kan [4].

2. Preliminaries

In this section, we recall some basic facts on the Selmer groups of elliptic curves with at least one 2-torsion rational point. For details, we refer [7, Chapter 3] and [6, Chapter 10]. There are isogenies $\varphi : E \to E'$ and $\varphi' : E' \to E$ of degree 2, dual to each other, between the following two elliptic curves:

$$E : y^2 = x^3 + Ax^2 + Bx \quad (A, B \in \mathbf{Q})\,,$$
$$E' : y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x = x^3 + A'x^2 + B'x\,.$$

These maps are given by the following formulae:

$$\varphi(P)=\begin{cases}\left(\dfrac{y^2}{x^2},\ \dfrac{y(x^2-B)}{x^2}\right), & \text{if } P=(x,y)\neq(0,0),\mathcal{O},\\ \mathcal{O}, & \text{if } P=(0,0),\mathcal{O},\end{cases}$$

$$\varphi'(P)=\begin{cases}\left(\dfrac{y^2}{4x^2},\ \dfrac{y(x^2-B')}{8x^2}\right), & \text{if } P=(x,y)\neq(0,0),\mathcal{O},\\ \mathcal{O}, & \text{if } P=(0,0),\mathcal{O},\end{cases}$$

where we denote by $\mathcal{O}$ the origin (the point at infinity) of each elliptic curve. We note that $\varphi\circ\varphi'$ and $\varphi'\circ\varphi$ are the duplication maps. Let k be a field containing $\mathbf{Q}$, and consider the following exact sequence of $\mathrm{Gal}(\bar{k}/k)$-modules

$$0\longrightarrow E[\varphi]\longrightarrow E\xrightarrow{\varphi}E'\longrightarrow 0,$$

where $E[\varphi]:=\mathrm{Ker}(\varphi)=\{(0,0),\mathcal{O}\}$. Taking Galois cohomology, we obtain an exact sequence

$$0\longrightarrow E'(k)/\varphi(E(k))\xrightarrow{\delta_k}H^1(k,E[\varphi])\longrightarrow H^1(k,E)[\varphi]\longrightarrow 0.$$

The map δ_k is called the *connecting homomorphism*. When $k=\mathbf{Q}$ (resp. $k=\mathbf{Q}_p$, $k=\mathbf{R}$), we simply write δ (resp. δ_p,δ_∞) for δ_k. Interchanging the role of E and E', we obtain another exact sequence

$$0\longrightarrow E(k)/\varphi'(E'(k))\xrightarrow{\delta'_k}H^1(k,E'[\varphi'])\longrightarrow H^1(k,E')[\varphi']\longrightarrow 0.$$

Since we have the formula (cf. [7, Chapter 3])

$$\operatorname{rank}E(\mathbf{Q})=\log_2|E(\mathbf{Q})/\varphi'(E'(\mathbf{Q}))|+\log_2|E'(\mathbf{Q})/\varphi(E(\mathbf{Q}))|-2,\tag{2.1}$$

our goal is to calculate the order of $|E(\mathbf{Q})/\varphi'(E'(\mathbf{Q}))|$ and $|E'(\mathbf{Q})/\varphi(E(\mathbf{Q}))|$. This amounts to calculating the images $\mathrm{Im}(\delta)$ and $\mathrm{Im}(\delta')$ because of the injectivity of δ and δ'. Since $H^1(k,E[\varphi])$ is isomorphic to $k^\times/k^{\times2}$, we can regard δ as a map $E'(\mathbf{Q})\to\mathbf{Q}^\times/\mathbf{Q}^{\times2}$. Similarly δ' is a map $E(\mathbf{Q})\to\mathbf{Q}^\times/\mathbf{Q}^{\times2}$. Then δ and δ' can be described explicitly as follows:

$$\delta(P)=\begin{cases}x, & \text{if } P=(x,y)\neq(0,0),\mathcal{O},\\ B', & \text{if } P=(0,0),\\ 1, & \text{if } P=\mathcal{O}.\end{cases}$$

$$\delta'(P)=\begin{cases}x, & \text{if } P=(x,y)\neq(0,0),\mathcal{O},\\ B, & \text{if } P=(0,0),\\ 1, & \text{if } P=\mathcal{O}.\end{cases}$$

Therefore, in order to determine $\mathrm{Im}(\delta)$ (resp. $\mathrm{Im}(\delta')$), we must check what numbers (modulo square) appear in the x-coordinates of the rational points on E' (resp. E). The coordinates of a rational point of order greater then 2 on E are written as

$$x=\frac{dM^2}{e^2},\quad y=\frac{dMN}{e^3},$$

where $MNe \neq 0$, $(M, e) = (N, e) = 1$ and d is a divisor of B. These numbers must satisfy the equation (coming from the equation of E)

$$N^2 = dM^4 + AM^2e^2 + \left(\frac{B}{d}\right)e^4 . \tag{2.2}$$

Hence d ($\neq 1, B$) is in $\mathrm{Im}(\delta')$ if and only if (2.2) has a non-trivial integral solution. But in general, to determine whether or not (2.2) has such a solution is an unsolved problem. So we call d the element of the *Selmer group* $S^{(\varphi')}(E'/\mathbf{Q})$ when (2.2) has a solution in $\mathbf{R}$ and in $\mathbf{Q}_p$ for every prime p. In this paper, we write $Sel(\varphi')$ for $S^{(\varphi')}(E'/\mathbf{Q})$. In other words,

$$Sel(\varphi') := \bigcap_{p \in M_{\mathbf{Q}}} \mathrm{Im}(\delta'_p) , \quad Sel(\varphi) := \bigcap_{p \in M_{\mathbf{Q}}} \mathrm{Im}(\delta_p) ,$$

where $M_{\mathbf{Q}} = \{\text{primes}\} \cup \{\infty\}$, and the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ are regarded as subgroups of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. So $Sel(\varphi')$ and $Sel(\varphi)$ are subgroups of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. Clearly $Sel(\varphi') \supset \mathrm{Im}(\delta')$, $Sel(\varphi) \supset \mathrm{Im}(\delta)$. In general, $Sel(\varphi')$ and $Sel(\varphi)$ are finite groups, and thus can be regarded as finite-dimensional vector spaces over $\mathbf{F}_2$. We write $\dim Sel(\varphi')$ and $\dim Sel(\varphi)$ for their dimensions over $\mathbf{F}_2$. Namely $\dim Sel(\varphi') = \log_2 |Sel(\varphi')|$, $\dim Sel(\varphi) = \log_2 |Sel(\varphi)|$. By (2.1), we have

$$\operatorname{rank} E(\mathbf{Q}) \leq \dim Sel(\varphi') + \dim Sel(\varphi) - 2 . \tag{2.3}$$

Let us define the *Tate-Shafarevich groups* by

$$Ш[\varphi'] := Sel(\varphi')/(E(\mathbf{Q})/\varphi'(E'(\mathbf{Q}))) , \quad Ш[\varphi] := Sel(\varphi)/(E'(\mathbf{Q})/\varphi(E(\mathbf{Q}))) .$$

Then we obtain the following exact sequences of finite groups

$$0 \longrightarrow E(\mathbf{Q})/\varphi'(E'(\mathbf{Q})) \xrightarrow{\delta'} Sel(\varphi') \longrightarrow Ш[\varphi'] \longrightarrow 0 ,$$

$$0 \longrightarrow E'(\mathbf{Q})/\varphi(E(\mathbf{Q})) \xrightarrow{\delta} Sel(\varphi) \longrightarrow Ш[\varphi] \longrightarrow 0 .$$

Therefore by (2.1), we have

$$\operatorname{rank} E(\mathbf{Q}) = \dim Sel(\varphi') + \dim Sel(\varphi) - \dim Ш[\varphi'] - \dim Ш[\varphi] - 2 , \tag{2.4}$$

where $\dim Ш[\varphi'] = \log_2 |Ш[\varphi']|$, $\dim Ш[\varphi] = \log_2 |Ш[\varphi]|$.

In the next section, in order to calculate $Sel(\varphi')$ and $Sel(\varphi)$ for $E_{\alpha,\beta}$, we study $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$. In view of the following theorem, if one of the groups $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ is given, the other group is automatically determined (see for example [2]).

THEOREM 2.1. *Let $p \in M_{\mathbf{Q}}$ and let $(\ , \ )_p$ be the Hilbert symbol. For a subgroup $V \subset \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$, we define $V^\perp = \{x \in \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} \mid (x, y)_p = 1 \text{ for all } y \in V\}$. Then*

$$\mathrm{Im}(\delta_p) = \mathrm{Im}(\delta'_p)^\perp .$$

3. Images of the connecting homomorphisms

In this paper, we study the following elliptic curves:

$$E = E_{\alpha,\beta} : y^2 = x^3 - (\alpha + \beta)x^2 + \alpha\beta x = x^3 + Ax^2 + Bx\,,$$
$$E' = E'_{\alpha,\beta} : y^2 = x^3 + 2(\alpha + \beta)x^2 + (\alpha - \beta)^2 x = x^3 + A'x^2 + B'x\,.$$

Without loss of generality, we can assume that α, β are integers and $\gcd(\alpha, \beta)$ is squarefree. In this section, we give the formulae for the images of the connecting homomorphisms δ'_p, δ_p. We give the proofs in §6. At first, a statement in the case that $p = \infty$ is given.

PROPOSITION 3.1. *The images of* δ'_∞ *and* δ_∞ *are given as follows.*

(1) *If* $\alpha > 0$ *and* $\beta > 0$, *then* $\mathrm{Im}(\delta'_\infty) = \{1\}$, $\mathrm{Im}(\delta_\infty) = \{\pm 1\}$.

(2) *If* $\alpha < 0$ *or* $\beta < 0$, *then* $\mathrm{Im}(\delta'_\infty) = \{\pm 1\}$, $\mathrm{Im}(\delta_\infty) = \{1\}$.

Next, we have the case that p is an odd and good prime. In general, if p is an odd prime, $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2} = \{1, u, p, pu\}$, where $u \in \mathbf{Z}_p^\times$ is non-square element modulo p. In this paper, u represents such an element.

PROPOSITION 3.2. *Let p be a prime not dividing* 2Δ, *then* $\mathrm{Im}(\delta'_p) = \{1, u\}$, $\mathrm{Im}(\delta_p) = \{1, u\}$.

The most important case is when p is a bad prime. The discriminant of $E_{\alpha,\beta}$ is

$$\Delta = 16\alpha^2\beta^2(\alpha - \beta)^2\,.$$

So bad primes are classified into

- odd primes which divide both α and β,
- odd primes which divide either α or β,
- odd primes which divide not α but $\alpha - \beta$,
- even prime 2.

Note that the prime 2 may be a good prime, since the above discriminant may not necessarily be minimal at 2. But it is not a serious matter.

First, we have the statement for odd primes which divide both α and β. For $c_1, \cdots, c_n \in \mathbf{Q}$, we denote by $\langle c_1, \cdots, c_n \rangle$ the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ or $\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$ for some $p \in M_\mathbf{Q}$ generated by $c_1, \cdots, c_n$.

PROPOSITION 3.3. *Let p be an odd prime, and suppose that* $\mathrm{ord}_p(\alpha) \geq 1$, $\mathrm{ord}_p(\beta) = 1$. *Then*

$$\mathrm{Im}(\delta'_p) = \langle \alpha, \beta \rangle\,.$$

The other group $\mathrm{Im}(\delta_p)$ can be obtained by Theorem 2.1.

Secondly, we describe the proposition for odd primes which divide either α or β. We denote by $(\;/\;)$ the Legendre symbol.

PROPOSITION 3.4. *Let p be an odd prime, and suppose that* $\mathrm{ord}_p(\alpha) = a \geq 1$, $\mathrm{ord}_p(\beta) = 0$. *Then the following holds.*

(1) *If a is even and* $(-\beta/p) = -1$, *then* $\mathrm{Im}(\delta'_p) = \{1, u\}$, $\mathrm{Im}(\delta_p) = \{1, u\}$.

(2) *In the other case*, $\mathrm{Im}(\delta'_p) = \{1, u, p, pu\}$, $\mathrm{Im}(\delta_p) = \{1\}$.

Thirdly, in the case of odd primes which divide not α but $\alpha - \beta$, we have the following proposition.

PROPOSITION 3.5. *Let p be an odd prime, and suppose that* $\mathrm{ord}_p(\alpha) = 0$, $\mathrm{ord}_p(\alpha - \beta) = a \geq 1$. *Then the following holds.*

(1) *If* $(\alpha/p) = 1$, *then* $\mathrm{Im}(\delta'_p) = \{1\}$, $\mathrm{Im}(\delta_p) = \{1, u, p, pu\}$.
(2) *If* $(\alpha/p) = -1$, *then* $\mathrm{Im}(\delta'_p) = \{1, u\}$, $\mathrm{Im}(\delta_p) = \{1, u\}$.

Lastly, we consider the case that $p = 2$. In this case, $\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2} = \{\pm 1, \pm 5, \pm 2, \pm 10\}$. For a while, in order to simplify the problem, we assume that α and β satisfy one of the following conditions.

(A) $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 0$,
(B) $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 1$.

Even in the case that α and β satisfy neither condition, some translation of the curve will give $E_{\alpha,\beta}$ satisfying either condition. But we note that the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ may change by a translation.

PROPOSITION 3.6. *Suppose that* $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 0$. *Then* $\mathrm{Im}(\delta'_2) = \langle \alpha, \beta \rangle$ *except the following three cases.*

(1) *If* $\mathrm{ord}_2(\alpha - \beta) = 2$ *and* $\alpha + \beta \equiv 14 \pmod{16}$, *then* $\mathrm{Im}(\delta'_2) = \langle -1, 5 \rangle$.
(2) *If* $\mathrm{ord}_2(\alpha - \beta) = 3$ *and* $\alpha \equiv 3 \pmod 4$, *then* $\mathrm{Im}(\delta'_2) = \langle -1, 5 \rangle$.
(3) *If* $\mathrm{ord}_2(\alpha - \beta) = 4$ *and* $\alpha \equiv 1 \pmod 8$, *then* $\mathrm{Im}(\delta'_2) = \langle 5 \rangle$.

PROPOSITION 3.7. *Suppose that* $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 1$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(\alpha - \beta) = 2$, *then* $\mathrm{Im}(\delta'_2) = \mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$.
(2) *If* $\mathrm{ord}_2(\alpha - \beta) = 3$, *then* $\mathrm{Im}(\delta'_2) = \langle \alpha, 5 \rangle$.
(3) *If* $\mathrm{ord}_2(\alpha - \beta) \geq 4$, *then* $\mathrm{Im}(\delta'_2) = \langle \alpha \rangle$.

We have prepared to calculate Selmer groups $Sel(\varphi')$ and $Sel(\varphi)$.

EXAMPLE 3.8. Consider the elliptic curve

$$E : y^2 = x(x + 483)(x - 483).$$

If the $\mathbf{Q}$-rank of E were positive, 483 would be $\pi/2$-congruent. By the propositions in this section, the images of δ'_p, δ_p for the bad primes $p = 2, 3, 7$ and 23, are determined as in the following table:

Table 1.

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
7	$\mathbf{Q}_7^\times/\mathbf{Q}_7^{\times 2}$	$\{1\}$
23	$\mathbf{Q}_{23}^\times/\mathbf{Q}_{23}^{\times 2}$	$\{1\}$

Recall that Selmer group $Sel(\varphi')$ is an intersection of all $\mathrm{Im}(\delta'_p)$ considered subgroups of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$. Therefore by the above table it is clear that $Sel(\varphi') = \langle -1, 3, 7, 23 \rangle$ and $Sel(\varphi) = \{1\}$. This gives $\mathrm{rank}\, E(\mathbf{Q}) \leq 2$ (cf. (2.3)). See Example 3.12 for further discussion of this example.

The following propositions are useful when one computes directly the images $\mathrm{Im}(\delta_2')$ and $\mathrm{Im}(\delta_2)$ for an elliptic curve not satisfying either conditions (A) or (B).

PROPOSITION 3.9. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2$, $\mathrm{ord}_2(\beta) = 1$. *Then the following holds.*

(1) *If* $\alpha + \beta \equiv 2 \pmod 8$, *then* $\mathrm{Im}(\delta_2') = \langle \alpha, \beta, -5 \rangle$.

(2) *If* $\alpha + \beta \equiv 6 \pmod 8$, *then* $\mathrm{Im}(\delta_2') = \langle \alpha, \beta, -1 \rangle$.

PROPOSITION 3.10. *Suppose that* $\mathrm{ord}_2(\alpha) = 1$, $\mathrm{ord}_2(\beta) = 0$. *Then*

$$\mathrm{Im}(\delta_2') = \langle \alpha, \beta, 5 \rangle .$$

PROPOSITION 3.11. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2$, $\mathrm{ord}_2(\beta) = 0$ *and put* $\alpha = 2^a\alpha'$ $(\alpha' \in \mathbf{Z}_2^\times)$. *Then images* $\mathrm{Im}(\delta_2')$ *and* $\mathrm{Im}(\delta_2)$ *are determined as the following table*:

Table 2.

$\beta \bmod 8$	$\mathrm{ord}_2(\alpha)$	$\alpha' \bmod 4$	$\mathrm{Im}(\delta_2')$	$\mathrm{Im}(\delta_2)$
1	2	1	$\langle 5 \rangle$	$\langle -1, 5 \rangle$
		-1	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
	3	1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
		-1	$\langle -2, 5 \rangle$	$\langle -5 \rangle$
	≥ 4	1	$\langle 2, 5 \rangle$	$\langle -1 \rangle$
		-1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
-1	2	1	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
		-1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
	3	—	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
	4	—	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
	≥ 5	—	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
5	2	1	$\langle 5 \rangle$	$\langle -1, 5 \rangle$
		-1	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
	3	1	$\langle 2, 5 \rangle$	$\langle -1 \rangle$
		-1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
	even ≥ 4	1	$\langle -2, 5 \rangle$	$\langle -5 \rangle$
		-1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
	odd ≥ 5	1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
		-1	$\langle -2, 5 \rangle$	$\langle -5 \rangle$
-5	2	1	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
		-1	$\langle -1, 5 \rangle$	$\langle 5 \rangle$
	odd ≥ 3	—	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
	even ≥ 4	—	$\langle -1, 5 \rangle$	$\langle 5 \rangle$

EXAMPLE 3.12. Consider the curve $E : y^2 = x(x+483)(x-483)$ in Example 3.8 once more. By some translation, we have the curve

$$F : y^2 = x(x-483)(x-966)\,.$$

Note that rank $E(\mathbf{Q}) =$ rank $F(\mathbf{Q})$. By the above propositions, the images of the connecting homomorphisms are clear.

Table 3.

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{1\}$	$\{\pm 1\}$
2	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
7	$\langle -7\rangle$	$\langle 7\rangle$
23	$\langle -23\rangle$	$\langle 23\rangle$

By this table, it is clear that $Sel(\varphi') \subset \langle 2, 3, 7, 23\rangle$ and $Sel(\varphi) \subset \langle -1, 7, 23\rangle$. In fact, $Sel(\varphi') = \langle 2, 483\rangle$ and $Sel(\varphi) = \{1\}$. The detail is described in Examples 4.3, 4.5. This gives rank $F(\mathbf{Q}) = 0$, so 483 is not $\pi/2$-congruent.

REMARK 3.13. The curve E in Example 3.8 and the curve F in Example 3.12 are essentially the same. But 2-isogenies given in §2 are different. As we have seen, the bound of the rank can change by a change of the 2-isogenies. So we can take the smallest bound of the three.

4. Formula for the Selmer group

In this section, the formula for the dimensions of $Sel(\varphi')$ and $Sel(\varphi)$ is given. Recall that α and β are integers such that $\gcd(\alpha, \beta)$ is squarefree.

DEFINITION. For fixed α and β as above, we introduce the following notations.

(1) $$S_{1,1} := \left\{ p : \text{odd primes} \;\middle|\; \begin{array}{c} \mathrm{ord}_p(\alpha) \geq 1,\ \mathrm{ord}_p(\beta) \geq 1, \\ \alpha \not\equiv 1 \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2}),\ \beta \not\equiv 1 \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2}), \\ \alpha \not\equiv \beta \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2}) \end{array} \right\}.$$

(2) $$S_{1,2} := \left\{ p : \text{odd primes} \;\middle|\; \begin{array}{l} \mathrm{ord}_p(\alpha) = 0,\ \mathrm{ord}_p(\beta) \geq 1, \\ \mathrm{ord}_p(\beta) \text{ is odd or } (-\alpha/p) = 1 \end{array} \right\}.$$

(3) $$S_{1,3} := \left\{ p : \text{odd primes} \;\middle|\; \begin{array}{l} \mathrm{ord}_p(\alpha) \geq 1,\ \mathrm{ord}_p(\beta) = 0, \\ \mathrm{ord}_p(\alpha) \text{ is odd or } (-\beta/p) = 1 \end{array} \right\}.$$

(4) $S_1 := S_{1,1} \cup S_{1,2} \cup S_{1,3}$.

(5) $S_2 := \{p : \text{odd primes} \mid \mathrm{ord}_p(\alpha) = 0,\ \mathrm{ord}_p(\alpha - \beta) \geq 1,\ (\alpha/p) = 1\}$.

(6) $S_3 := \{p : \text{odd primes} \mid \mathrm{ord}_p(\alpha) \geq 1,\ \mathrm{ord}_p(\beta) \geq 1,\ \alpha \equiv \beta \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2})\}$.

(7) $S_{(\alpha)} := \{p : \text{odd primes} \mid \mathrm{ord}_p(\alpha) = 1,\ \mathrm{ord}_p(\beta) \geq 2,\ \beta \equiv 1 \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2})\}$.

(8) $S_{(\beta)} := \{p : \text{odd primes} \mid \mathrm{ord}_p(\alpha) \geq 2,\ \mathrm{ord}_p(\beta) = 1,\ \alpha \equiv 1 \ (\mathrm{mod}\, \mathbf{Q}_p^{\times 2})\}$.

PROPOSITION 4.1. *Let p be an odd prime. Then the following holds.*

(1) $p \in S_1 \Leftrightarrow \mathrm{Im}(\delta'_p) = \{1, u, p, pu\}$, $\mathrm{Im}(\delta_p) = \{1\}$.

(2) $p \in S_2 \Leftrightarrow \mathrm{Im}(\delta'_p) = \{1\}$, $\mathrm{Im}(\delta_p) = \{1, u, p, pu\}$.

(3) $p \in S_3 \Rightarrow \mathrm{Im}(\delta'_p) = \{1, \alpha\} = \{1, \beta\}$, $\mathrm{Im}(\delta_p) = \{1, -\alpha\}$.

(4) $p \in S_{(\alpha)} \Rightarrow \mathrm{Im}(\delta'_p) = \{1, \alpha\} \neq \{1, \beta\}$, $\mathrm{Im}(\delta_p) = \{1, -\alpha\}$.

(5) $p \in S_{(\beta)} \Rightarrow \mathrm{Im}(\delta'_p) = \{1, \beta\} \neq \{1, \alpha\}$, $\mathrm{Im}(\delta_p) = \{1, -\beta\}$.

(6) *the other cases* $\Rightarrow \mathrm{Im}(\delta'_p) = \{1, u\}$, $\mathrm{Im}(\delta_p) = \{1, u\}$.

In (3), (4), *and* (5), *the groups* $\mathrm{Im}(\delta'_p)$ *and* $\mathrm{Im}(\delta_p)$ *are either* $\langle p \rangle$ *or* $\langle pu \rangle$.

Proof. This is an immediate consequence of Propositions 3.2~3.5 and Theorem 2.1. □

DEFINITION. Let S, T be the following sets.

$$S = S_1 \cup S_3 \cup S_{(\alpha)} \cup S_{(\beta)} \cup A_S\,,$$
$$T = S_2 \cup S_3 \cup S_{(\alpha)} \cup S_{(\beta)} \cup A_T\,,$$

where $A_S, A_T \subset \{-1, 2\}$ are determined as follows:

- -1 is in either A_S or A_T. If $\alpha > 0$ and $\beta > 0$, then $-1 \in A_T$, otherwise $-1 \in A_S$.
- If $\mathrm{Im}(\delta'_2) \subset \{\pm 1, \pm 5\}$, then $2 \notin A_S$, otherwise $2 \in A_S$. If $\mathrm{Im}(\delta_2) \subset \{\pm 1, \pm 5\}$, then $2 \notin A_T$, otherwise $2 \in A_T$.

Let V_X be the subgroup of $\mathbf{Q}^\times/\mathbf{Q}^{\times 2}$ generated by the elements of the set X. By Propositions 4.1 and 3.1,

$$Sel(\varphi') \subset V_S\,, \quad Sel(\varphi) \subset V_T\,.$$

Let $(\;,\;)_p$ be the Hilbert symbol. For $x \in V_S$,

$$x \in Sel(\varphi') \iff x \in \mathrm{Im}(\delta'_p) \quad \text{for } \forall p \in M$$
$$\underset{\text{(Prop. 4.1)}}{\iff} \begin{cases} (x, p)_p = 1 & \text{for } \forall p \in S_2\,, \\ (x, -\alpha)_p = 1 & \text{for } \forall p \in S_3 \cup S_{(\alpha)}\,, \\ (x, -\beta)_p = 1 & \text{for } \forall p \in S_{(\beta)}\,, \\ x \in \mathrm{Im}(\delta'_2)\,. \end{cases}$$

Similarly for $x \in V_T$,

$$x \in Sel(\varphi) \iff x \in \mathrm{Im}(\delta_p) \quad \text{for } \forall p \in M$$
$$\underset{\text{(Prop. 4.1)}}{\iff} \begin{cases} (x, p)_p = 1 & \text{for } \forall p \in S_1\,, \\ (x, \alpha)_p = 1 & \text{for } \forall p \in S_3 \cup S_{(\alpha)}\,, \\ (x, \beta)_p = 1 & \text{for } \forall p \in S_{(\beta)}\,, \\ x \in \mathrm{Im}(\delta_2)\,. \end{cases}$$

This prompts the following definition.

DEFINITION. Let $(a, b)_p$ be the Hilbert symbol, and we let

$$\{a, b\}_p := \begin{cases} 0, & \text{if } (a, b)_p = 1\,, \\ 1, & \text{if } (a, b)_p = -1\,. \end{cases}$$

Next, we define the map $\lambda' : V_S \to (\mathbf{Z}/2\mathbf{Z})^{m'}$ and $\lambda : V_T \to (\mathbf{Z}/2\mathbf{Z})^{m}$ (m' and m are natural numbers which depend on α, β) as follows:

$$\begin{aligned}\lambda'(x) &:= (*,\ \{x,p\}_p\ (p \in S_2),\ \{x,-\alpha\}_p\ (p \in S_3 \cup S_{(\alpha)}),\ \{x,-\beta\}_p\ (p \in S_{(\beta)}))\,,\\ \lambda(x) &:= (**,\ \{x,p\}_p\ (p \in S_1),\ \{x,\alpha\}_p\ (p \in S_3 \cup S_{(\alpha)}),\ \{x,\beta\}_p\ (p \in S_{(\beta)}))\,,\end{aligned} \tag{4.1}$$

where for example $\{x,p\}_p$ $(p \in S_2)$ represents the numbers $\{x,p\}_p$ for all $p \in S_2$ arranged horizontally. And $*$, $**$ represent the numbers described in the following table.

Table 4.

$\mathrm{Im}(\delta_2')$	$\mathrm{Im}(\delta_2)$	$*$	$**$
$\{1\}$	$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{x,-1\}_2, \{x,2\}_2$	
$\langle -1\rangle$	$\langle 2,5\rangle$	$\{x,2\}_2$	$\{x,-1\}_2$
$\langle 5\rangle$	$\langle -1,5\rangle$	$\{x,-1\}_2$	
$\langle -5\rangle$	$\langle -2,5\rangle$	$\{x,-2\}_2$	$\{x,-5\}_2$
$\langle 2\rangle$	$\langle -1,2\rangle$	$\{x,-1\}_2, \{x,2\}_2$	$\{x,2\}_2$
$\langle -2\rangle$	$\langle 2,-5\rangle$	$\{x,2\}_2, \{x,-5\}_2$	$\{x,-2\}_2$
$\langle 10\rangle$	$\langle -1,10\rangle$	$\{x,-1\}_2, \{x,10\}_2$	$\{x,10\}_2$
$\langle -10\rangle$	$\langle -2,-5\rangle$	$\{x,-2\}_2, \{x,-5\}_2$	$\{x,-10\}_2$
$\langle -1,5\rangle$	$\langle 5\rangle$		$\{x,-1\}_2$
$\langle -1,2\rangle$	$\langle 2\rangle$	$\{x,2\}_2$	$\{x,-1\}_2, \{x,2\}_2$
$\langle -1,10\rangle$	$\langle 10\rangle$	$\{x,10\}_2$	$\{x,-1\}_2, \{x,10\}_2$
$\langle 2,5\rangle$	$\langle -1\rangle$	$\{x,-1\}_2$	$\{x,2\}_2$
$\langle -2,5\rangle$	$\langle -5\rangle$	$\{x,-5\}_2$	$\{x,-2\}_2$
$\langle 2,-5\rangle$	$\langle -2\rangle$	$\{x,-2\}_2$	$\{x,2\}_2, \{x,-5\}_2$
$\langle -2,-5\rangle$	$\langle -10\rangle$	$\{x,-10\}_2$	$\{x,-2\}_2, \{x,-5\}_2$
$\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$	$\{1\}$		$\{x,-1\}_2, \{x,2\}_2$

THEOREM 4.2. *The Selmer groups $Sel(\varphi')$ and $Sel(\varphi)$ are given by the following formulae*:

$$Sel(\varphi') = \mathrm{Ker}\,\lambda'\,, \qquad Sel(\varphi) = \mathrm{Ker}\,\lambda\,.$$

Proof. We see only $Sel(\varphi')$, since $Sel(\varphi)$ is computed similarly. Let $x \in \mathrm{Ker}\,\lambda'$. Then x satisfies

$$\begin{cases} (x,p)_p = 1 & \text{for } \forall p \in S_2\,,\\ (x,-\alpha)_p = 1 & \text{for } \forall p \in S_3 \cup S_{(\alpha)}\,,\\ (x,-\beta)_p = 1 & \text{for } \forall p \in S_{(\beta)}\,.\end{cases}$$

Moreover $x \in \mathrm{Im}(\delta_2')$. Indeed, $x \in \mathrm{Im}(\delta_2')$ if and only if the values $*$ in Table 4 are all 0. Conversely, if $x \in Sel(\varphi')$, then clearly $x \in \mathrm{Ker}\,\lambda'$. This proves the theorem. □

EXAMPLE 4.3. For the curve $y^2 = x(x-483)(x-966)$ in Example 3.12,

$$S_1 = \{3\}, \quad S_2 = \phi, \quad S_3 = \{7, 23\}, \quad S_{(\alpha)} = \phi, \quad S_{(\beta)} = \phi.$$

And $S = \{2, 3, 7, 23\}$, $T = \{-1, 7, 23\}$. Then

$$\begin{aligned}
\lambda'(2) &= (\{2,7\}_7, \{2,23\}_{23}) = (0,0),\\
\lambda'(3) &= (\{3,7\}_7, \{3,23\}_{23}) = (1,0),\\
\lambda'(7) &= (\{7,7\}_7, \{7,23\}_{23}) = (1,1),\\
\lambda'(23) &= (\{23,7\}_7, \{23,23\}_{23}) = (0,1).
\end{aligned}$$

By Theorem 4.2, we have $2 \in Sel(\varphi')$, $3, 7, 23 \notin Sel(\varphi')$. Since λ' is additive, $\lambda'(483) = \lambda'(3) + \lambda'(7) + \lambda'(23) = (0,0)$, so $483 \in Sel(\varphi')$. But it is trivial because $\delta'((483, 0)) = 483$. Since $\delta'((966, 0)) = 2$, it is also trivial that $2 \in Sel(\varphi')$. In this example, there is not a non-trivial element in either $Sel(\varphi')$ or $Sel(\varphi)$, so the rank is 0.

DEFINITION. Let us define the matrices Λ', Λ as follows:

$$\Lambda' := (\lambda'(p)) \ (p \in S), \qquad \Lambda := (\lambda(p)) \ (p \in T),$$

where $\lambda'(p)$ and $\lambda(p)$ are row vectors defined in (4.1).

THEOREM 4.4. *The dimensions of the Selmer groups $Sel(\varphi')$ and $Sel(\varphi)$ are given by the following formulae*:

$$\dim Sel(\varphi') = |S| - \operatorname{rank} \Lambda', \qquad \dim Sel(\varphi) = |T| - \operatorname{rank} \Lambda.$$

Proof. This is an immediate consequence of Theorem 4.2. □

Theorem 4.2 and Theorem 4.4 are extensions of the theorems stated in [1] for the elliptic curves connected with a classical congruent number problem. But Aoki [1] calculated not only the Selmer groups associated to 2-isogeny but also the 2-Selmer groups.

EXAMPLE 4.5. Let us see what Theorem 4.4 means by considering the curve in Example 4.3 again. For this curve

$$\Lambda' = \begin{array}{c} \\ 2 \\ 3 \\ 7 \\ 23 \end{array} \begin{array}{c} \begin{array}{cc} 7 & 23 \end{array} \\ \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 1 \end{pmatrix} \end{array}.$$

The meaning of the numbers outside the matrix is an obvious one. For example, that (1, 1)-entry is 0 means $2 \in \mathrm{Im}(\delta'_7)$, and that (2, 1)-entry is 1 means $3 \notin \mathrm{Im}(\delta'_7)$ (however Λ', Λ were defined by the Hilbert symbol, one can also compute the entries by checking whether or not $2 \in \mathrm{Im}(\delta'_7)$ and so on). Therefore that the entries in the first row are all 0 means $2 \in Sel(\varphi')$.

Let us do the elementary transformation in order to compute the rank of the matrix. First, add the second row to the third row. Then we have

$$\begin{array}{cc} & \begin{array}{cc} 7 & 23 \end{array} \\ \begin{array}{c} 2 \\ 3 \\ 3\cdot 7 \\ 23 \end{array} & \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 1 \end{pmatrix} \end{array}.$$

Note that the meaning of the third row has changed. Next, add the third row to the fourth row. Then we have

$$\begin{array}{cc} & \begin{array}{cc} 7 & 23 \end{array} \\ \begin{array}{c} 2 \\ 3 \\ 21 \\ 483 \end{array} & \begin{pmatrix} 0 & 0 \\ 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{pmatrix} \end{array}.$$

Hence we have rank $\Lambda' = 2$ and $Sel(\varphi') = \langle 2, 483\rangle$.

EXAMPLE 4.6. Consider the curve $E : y^2 = x(x-8)(x-14)$. The bad primes are 2, 3 and 7. But the bad prime 3 behaves like a good prime by Proposition 3.5. We have

$$\Lambda' = \begin{pmatrix} \{2,2\}_2 \\ \{7,2\}_2 \end{pmatrix} = \begin{array}{cc} & 2 \\ \begin{array}{c} 2 \\ 7 \end{array} & \begin{pmatrix} 0 \\ 0 \end{pmatrix} \end{array},$$

$$\Lambda = \begin{pmatrix} \{-1,-1\}_2 & \{-1,2\}_2 \\ \{2,-1\}_2 & \{2,2\}_2 \end{pmatrix} = \begin{array}{cc} & \begin{array}{cc} 2 & 2' \end{array} \\ \begin{array}{c} -1 \\ 2 \end{array} & \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{array}.$$

In this Λ, there are two steps in order to determine whether -1 and 2 belong to $\mathrm{Im}(\delta_2)$ since $\mathrm{Im}(\delta_2) = \langle 2\rangle$ (see Table 4). We have $Sel(\varphi') = \langle 2, 7\rangle$, $Sel(\varphi) = \langle 2\rangle$ and rank $E(\mathbf{Q}) \leq 1$. A well-known conjecture says that the parity of the bound of rank obtained by the Selmer groups equals the parity of the true rank, so it is expected that rank $E(\mathbf{Q}) = 1$. The non-trivial element of the Selmer groups is essentially only 2. Hence rank $E(\mathbf{Q}) = 1$ if and only if $2 \in \mathrm{Im}(\delta)$, which amounts to that the equation

$$N^2 = 2M^4 + 44M^2e^2 + 18e^4$$

has an integer solution with $MNe \neq 0$ (see (2.2) in §2). In fact, the equation has a solution $(M, N, e) = (1, 8, 1)$, so rank $E(\mathbf{Q}) = 1$.

5. Application to the $\pi/3$-congruent problem

In this section, we apply the result in §4 to the $\pi/3$-congruent number problem, and describe corollaries which contain Corollary 1.2 and Theorem 1.3.

Recall that $E_{n,\theta}$ represents the curve defined by (1.1). When $\theta = \pi/3$ or $\theta = 2\pi/3$, we must consider the elliptic curves

$$E_{n,\frac{\pi}{3}} : y^2 = x(x+3n)(x-n)\,,$$
$$E_{n,\frac{2\pi}{3}} : y^2 = x(x+n)(x-3n)\,.$$

Suppose that p is a prime greater than 3, and $n = p, 2p$, or $3p$. The following corollaries give the Selmer groups of our elliptic curves and contain Corollary 1.2 and Theorem 1.3.

COROLLARY 5.1. *For* $E = E_{p,\frac{\pi}{3}}$ $(n = p, \theta = \pi/3)$,
$p \equiv 1 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \langle p\rangle$,
$p \equiv 5, 7, 19 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 11, 17, 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 13 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \langle p\rangle$.
Therefore, by (2.4) *in* §2

$$\operatorname{rank} E(\mathbf{Q}) + \dim Ш[\varphi'] + \dim Ш[\varphi] = \begin{cases} 2, & \text{if } p \equiv 1 \pmod{24}, \\ 1, & \text{if } p \equiv 11, 13, 17, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 5, 7, 19 \pmod{24}. \end{cases}$$

COROLLARY 5.2. *For* $E = E_{2p,\frac{\pi}{3}}$ $(n = 2p, \theta = \pi/3)$,
$p \equiv 1 \pmod{24} \Rightarrow Sel(\varphi') = \langle 2, -3, p\rangle,\ Sel(\varphi) = \langle p\rangle$,
$p \equiv 5, 17 \pmod{24} \Rightarrow Sel(\varphi') = \langle 2, -3, p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 7, 13 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, 2p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 11, 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle -2, -3, -p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 19 \pmod{24} \Rightarrow Sel(\varphi') = \langle -2, -3, -p\rangle,\ Sel(\varphi) = \langle p\rangle$.
Therefore

$$\operatorname{rank} E(\mathbf{Q}) + \dim Ш[\varphi'] + \dim Ш[\varphi] = \begin{cases} 2, & \text{if } p \equiv 1, 19 \pmod{24}, \\ 1, & \text{if } p \equiv 5, 11, 17, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 7, 13 \ (\ \text{mod } 24). \end{cases}$$

COROLLARY 5.3. *For* $E = E_{3p,\frac{\pi}{3}}$ $(n = 3p, \theta = \pi/3)$,
$p \equiv 1, 13 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \langle p\rangle$,
$p \equiv 5, 11, 17, 19 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 7 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -p\rangle,\ Sel(\varphi) = \langle p\rangle$,
$p \equiv 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -p\rangle,\ Sel(\varphi) = \langle 3\rangle$.
Therefore

$$\operatorname{rank} E(\mathbf{Q}) + \dim Ш[\varphi'] + \dim Ш[\varphi] = \begin{cases} 2, & \text{if } p \equiv 1, 13 \pmod{24}, \\ 1, & \text{if } p \equiv 7, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 5, 11, 17, 19 \pmod{24}. \end{cases}$$

COROLLARY 5.4. *For* $E = E_{p,\frac{2\pi}{3}}$ $(n = p, \theta = 2\pi/3)$,
$p \equiv 1, 13 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \langle p\rangle$,
$p \equiv 5, 17, 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 7, 11 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -p\rangle,\ Sel(\varphi) = \{1\}$,
$p \equiv 19 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -p\rangle,\ Sel(\varphi) = \langle p\rangle$.
Therefore

$$\operatorname{rank} E(\mathbf{Q}) + \dim \text{Ш}[\varphi'] + \dim \text{Ш}[\varphi] = \begin{cases} 2, & \textit{if } p \equiv 1, 13 \pmod{24}, \\ 1, & \textit{if } p \equiv 5, 17, 19, 23 \pmod{24}, \\ 0, & \textit{if } p \equiv 7, 11 \pmod{24}. \end{cases}$$

Note. Kan [4] has showed that the Tate-Shafarevich groups are non-trivial in the case that $p \equiv 13 \pmod{24}$.

COROLLARY 5.5. *For* $E = E_{2p,\frac{2\pi}{3}}$ $(n = 2p, \theta = 2\pi/3)$,
$p \equiv 1 \pmod{24} \Rightarrow Sel(\varphi') = \langle -2, -3, p\rangle,\ Sel(\varphi) = \langle p\rangle,$
$p \equiv 5, 17 \pmod{24} \Rightarrow Sel(\varphi') = \langle -2, -3, p\rangle,\ Sel(\varphi) = \{1\},$
$p \equiv 7 \pmod{24} \Rightarrow Sel(\varphi') = \langle 2, -3, -p\rangle,\ Sel(\varphi) = \langle p\rangle,$
$p \equiv 11, 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle 2, -3, -p\rangle,\ Sel(\varphi) = \{1\},$
$p \equiv 13, 19 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, -2p\rangle,\ Sel(\varphi) = \{1\}.$
Therefore

$$\operatorname{rank} E(\mathbf{Q}) + \dim \text{Ш}[\varphi'] + \dim \text{Ш}[\varphi] = \begin{cases} 2, & \textit{if } p \equiv 1, 7 \pmod{24}, \\ 1, & \textit{if } p \equiv 5, 11, 17, 23 \pmod{24}, \\ 0, & \textit{if } p \equiv 13, 19 \pmod{24}. \end{cases}$$

COROLLARY 5.6. *For* $E = E_{3p,\frac{2\pi}{3}}$ $(n = 3p, \theta = 2\pi/3)$,
$p \equiv 1 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \langle 3, p\rangle,$
$p \equiv 5, 11, 23 \pmod{24} \Rightarrow Sel(\varphi') = \langle -1, 3, p\rangle,\ Sel(\varphi) = \{1\},$
$p \equiv 7, 19 \ (\mathrm{mod}24) \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \langle 3p\rangle,$
$p \equiv 13 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \langle p\rangle,$
$p \equiv 17 \pmod{24} \Rightarrow Sel(\varphi') = \langle -3, p\rangle,\ Sel(\varphi) = \{1\}.$
Therefore

$$\operatorname{rank} E(\mathbf{Q}) + \dim \text{Ш}[\varphi'] + \dim \text{Ш}[\varphi] = \begin{cases} 2, & \textit{if } p \equiv 1 \pmod{24}, \\ 1, & \textit{if } p \equiv 5, 7, 11, 13, 19, 23 \pmod{24}, \\ 0, & \textit{if } p \equiv 17 \pmod{24}. \end{cases}$$

These corollaries follow immediately from Theorem 4.2. The following lemmas are useful to calculate the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$.

LEMMA 5.7. *For* $E_{n,\frac{\pi}{3}}$, *the images of the connecting homomorphisms* δ'_p *are given as follows.*

(1) *Let* p $(\neq 2, 3)$ *be a prime which divides* n, *then*

$$\mathrm{Im}(\delta'_p) = \begin{cases} \langle n\rangle, & \textit{if } p \equiv 1 \pmod{3}, \\ \mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}, & \textit{if } p \equiv -1 \pmod{3}. \end{cases}$$

(2) $$\mathrm{Im}(\delta'_3) = \begin{cases} \langle -3\rangle, & \textit{if } n \equiv 6 \pmod{9}, \\ \mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}, & \textit{if } n \not\equiv 6 \pmod{9}. \end{cases}$$

(3) $$\mathrm{Im}(\delta'_2) = \begin{cases} \langle 5\rangle, & \textit{if } n \equiv 5 \pmod{8}, \\ \langle -1, 5\rangle, & \textit{if } n \equiv \pm 1, -5 \pmod{8}, \\ \langle 2, 5\rangle, & \textit{if } n \equiv 2 \pmod{8}, \\ \langle -2, 5\rangle, & \textit{if } n \equiv -2 \pmod{8}. \end{cases}$$

Proof. This is an immediate consequence of Propositions 3.3, 3.4, 3.6 and 3.7. □

LEMMA 5.8. *For $E_{n,\frac{\pi}{3}}$, the images of the connecting homomorphisms δ_p are given as follows.*

(1) *Let p $(\neq 2, 3)$ be a prime which divides n, then*

$$\mathrm{Im}(\delta_p) = \begin{cases} \langle -n \rangle, & \text{if } p \equiv 1 \pmod 3, \\ \{1\}, & \text{if } p \equiv -1 \pmod 3. \end{cases}$$

(2) $\mathrm{Im}(\delta_3) = \begin{cases} \langle 3 \rangle, & \text{if } n \equiv 6 \pmod 9, \\ \{1\}, & \text{if } n \not\equiv 6 \pmod 9. \end{cases}$

(3) $\mathrm{Im}(\delta_2) = \begin{cases} \langle -1, 5 \rangle, & \text{if } n \equiv 5 \pmod 8, \\ \langle 5 \rangle, & \text{if } n \equiv \pm 1, -5 \pmod 8, \\ \langle -1 \rangle, & \text{if } n \equiv 2 \pmod 8, \\ \langle -5 \rangle, & \text{if } n \equiv -2 \pmod 8. \end{cases}$

Proof. This is an immediate consequence of Lemma 5.7 and Theorem 2.1. □

Using the notations stated in §4, we have

$$\begin{aligned} S_1 &= \{\text{odd primes which divide } n \text{ and congruent to } -1 \text{ modulo } 3\} \\ &\quad (\cup\{3\} \text{ if } n \not\equiv 6 \pmod 9)\,, \\ S_2 &= \phi\,, \\ S_3 &= \{\text{odd primes which divide } n \text{ and congruent to } 1 \text{ modulo } 3\}\,, \\ S_{(n)} &= \phi \ \ (\cup\{3\} \text{ if } n \equiv 6 \pmod 9)\,, \\ S_{(-3n)} &= \phi\,, \\ S &= \{\text{primes which divide } n\} \cup \{-1, 3\}\,, \\ T &= \{\text{odd primes which divide } n \text{ and congruent to } 1 \text{ modulo } 3\} \\ &\quad (\cup\{3\} \text{ if } n \equiv 6 \pmod 9)\,. \end{aligned}$$

REMARK 5.9. We have two remarks. First, since $E_{-n,\frac{\pi}{3}} = E_{n,\frac{2\pi}{3}}$ (in general, $E_{-n,\theta} = E_{n,\pi-\theta}$), we can regard the $\pi/3$ and $2\pi/3$-congruent number problems as the same, admitting n to be negative. Lemmas 5.8 and 5.9 are also valid for negative n. Secondly, for $E_{n,\frac{\pi}{3}}$, the row of -1 is equal to the row of 3 in Λ' since $-3 \in Sel(\varphi')$.

Since Corollary 5.1 is contained in [3], we prove only Corollary 5.2.

Proof of Corollary 5.2.

In the case that $p \equiv 1 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle 2, 5 \rangle$	$\langle -1 \rangle$
3	$\mathbb{Q}_3^\times/\mathbb{Q}_3^{\times 2}$	$\{1\}$
p	$\langle 2p \rangle$	$\langle -2p \rangle$

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \begin{array}{c} \begin{array}{cc} 2 & p \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \\ 1 & 0 \\ 0 & 0 \end{pmatrix} \end{array}, \quad \Lambda = \begin{array}{cccc} & 2 & 3 & p \\ p & (0 & 0 & 0) \end{array}.$$

Therefore $Sel(\varphi') = \langle 2, -3, p \rangle$, $Sel(\varphi) = \langle p \rangle$.

In the case that $p \equiv 5, 17 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle 2, 5\rangle$	$\langle -1\rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
p	$\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$	$\{1\}$

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \!\!\begin{array}{c} 2 \\ \left(\begin{array}{c} 1 \\ 0 \\ 1 \\ 0 \end{array}\right) \end{array}, \quad \Lambda = \text{empty}.$$

Therefore $Sel(\varphi') = \langle 2, -3, p\rangle$, $Sel(\varphi) = \{1\}$.

In the case that $p \equiv 7 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle -2, 5\rangle$	$\langle -5\rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
p	$\langle 2p\rangle$	$\langle -2p\rangle$

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \!\!\begin{array}{c} \begin{array}{cc} 2 & p \end{array} \\ \left(\begin{array}{cc} 1 & 1 \\ 1 & 0 \\ 1 & 1 \\ 1 & 0 \end{array}\right) \end{array}, \quad \Lambda = \begin{array}{c} \\ p \end{array} \!\!\begin{array}{c} \begin{array}{ccc} 2 & 3 & p \end{array} \\ \left(\begin{array}{ccc} 1 & 0 & 1 \end{array}\right) \end{array}.$$

Therefore $Sel(\varphi') = \langle -3, 2p\rangle$, $Sel(\varphi) = \{1\}$.

In the case that $p \equiv 13 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle 2, 5\rangle$	$\langle -1\rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
p	$\langle 2p\rangle$	$\langle -2p\rangle$

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \!\!\begin{array}{c} \begin{array}{cc} 2 & p \end{array} \\ \left(\begin{array}{cc} 1 & 0 \\ 0 & 1 \\ 1 & 0 \\ 0 & 1 \end{array}\right) \end{array}, \quad \Lambda = \begin{array}{c} \\ p \end{array} \!\!\begin{array}{c} \begin{array}{ccc} 2 & 3 & p \end{array} \\ \left(\begin{array}{ccc} 1 & 0 & 1 \end{array}\right) \end{array}.$$

Therefore $Sel(\varphi') = \langle -3, 2p\rangle$, $Sel(\varphi) = \{1\}$.

In the case that $p \equiv 19 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle -2, 5\rangle$	$\langle -5\rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
p	$\langle 2p\rangle$	$\langle -2p\rangle$

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \!\!\begin{array}{c} \begin{array}{cc} 2 & p \end{array} \\ \left(\begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{array}\right) \end{array}, \quad \Lambda = \begin{array}{c} \\ p \end{array} \!\!\begin{array}{c} \begin{array}{ccc} 2 & 3 & p \end{array} \\ \left(\begin{array}{ccc} 0 & 0 & 0 \end{array}\right) \end{array}.$$

Therefore $Sel(\varphi') = \langle -2, -3, -p\rangle$, $Sel(\varphi) = \langle p\rangle$.

In the case that $p \equiv 11, 23 \pmod{24}$,

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{\pm 1\}$	$\{1\}$
2	$\langle -2, 5\rangle$	$\langle -5\rangle$
3	$\mathbf{Q}_3^\times/\mathbf{Q}_3^{\times 2}$	$\{1\}$
p	$\mathbf{Q}_p^\times/\mathbf{Q}_p^{\times 2}$	$\{1\}$

$$\Lambda' = \begin{array}{cc} & 2 \\ \begin{array}{c}-1\\2\\3\\p\end{array} & \begin{pmatrix}1\\1\\1\\1\end{pmatrix}\end{array}, \quad \Lambda = \text{empty}.$$

Therefore $Sel(\varphi') = \langle -2, -3, -p\rangle$, $Sel(\varphi) = \{1\}$. □

6. Proofs of the propositions

In this section, we prove the propositions in §3. Recall that our elliptic curve is

$$E = E_{\alpha,\beta} : y^2 = x(x-\alpha)(x-\beta) = x^3 + Ax^2 + Bx\,,$$

where α, β are non-zero different integers, and $\gcd(\alpha, \beta)$ is squarefree. We write E for $E_{\alpha,\beta}$ when there is no fear of confusion.

Proof of Proposition 3.1. The statement for $\mathrm{Im}(\delta'_\infty)$ is clear from the locus $E(\mathbf{R})$. By Theorem 2.1, $\mathrm{Im}(\delta_\infty)$ is also clear. □

Proof of Proposition 3.2. We give a simple proof using Theorem 2.1. Let $(x, y) \in E(\mathbf{Q}_p)$, and $x = p^e w$ with $e \in \mathbf{Z}$, $w \in \mathbf{Z}_p^\times$. Then

$$\begin{aligned} y^2 &= p^{3e}w^3 + p^{2e}Aw^2 + p^e Bw \\ &= p^{3e}w^3(1 + p^{-e}Aw^{-1} + p^{-2e}Bw^{-2}) \qquad (6.1)\\ &= p^e w(p^{2e}w^2 + p^e Aw + B)\,. \qquad (6.2) \end{aligned}$$

If $e < 0$, then e must be even and $w \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}$ by (6.1), so $x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}$. Recall that p does not divide B since p is a good prime. If $e > 0$, then e must be even and $w \equiv B \pmod{\mathbf{Q}_p^{\times 2}}$ by (6.2), so $x \equiv B \pmod{\mathbf{Q}_p^{\times 2}}$. We have shown $\mathrm{Im}(\delta'_p) \subset \{1, u\}$, and similarly $\mathrm{Im}(\delta_p) \subset \{1, u\}$ (note that p does not divide B'). Hence the proposition holds by Theorem 2.1. □

In this proof, we have shown that $x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}$, if $\mathrm{ord}_p(x) < 0$. The generalized fact is useful, so we have the following lemma.

LEMMA 6.1. *Let p be an odd prime and consider the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ with $\mathrm{ord}_p(A) = a$, $\mathrm{ord}_p(B) = b$. Suppose that (x, y) is a $\mathbf{Q}_p$-point on the curve and $x = p^e w$ with $e = \mathrm{ord}_p(x)$, $w \in \mathbf{Z}_p^\times$. Then*

$$e \le \min\left\{a - 1, \frac{b-1}{2}\right\} \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}\,.$$

Proof. Put $A = p^a A'$, $B = p^b B'$, then

$$y^2 = p^{3e}w^3 + p^{2e+a}A'w^2 + p^{e+b}B'w = p^{3e}w^3(1 + p^{-e+a}A'w^{-1} + p^{-2e+b}B'w^{-2})\,.$$

If $-e+a \geq 1$ and $-2e+b \geq 1$, then e must be even and $w \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}$, so we have $x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}$. □

For our elliptic curve $E_{\alpha,\beta}$, since α, β are integers, we have

$$\mathrm{ord}_p(x) \leq -2 \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}.$$

Moreover if $a \geq 1$, $b \geq 1$, then

$$\mathrm{ord}_p(x) = 0 \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_p^{\times 2}}.$$

We have one more lemma.

LEMMA 6.2. *Let (x, y) be a point on $E(\mathbf{Q}) \backslash E[2]$. Then the following formulae hold.*

(1) $(x, y) + (0, 0) = \left(\dfrac{\alpha\beta}{x}, -\dfrac{\alpha\beta y}{x^2}\right)$.

(2) $(x, y) + (\alpha, 0) = \left(\dfrac{\alpha(x-\beta)}{x-\alpha}, -\dfrac{\alpha(\alpha-\beta)y}{(x-\alpha)^2}\right)$.

(3) $(x, y) + (\beta, 0) = \left(\dfrac{\beta(x-\alpha)}{x-\beta}, -\dfrac{\beta(\beta-\alpha)y}{(x-\beta)^2}\right)$.

Proof. This follows immediately from the addition formula. □

We define subsets of $E(\mathbf{Q}_p)$ as follows ([8]):

$$E_\nu(\mathbf{Q}_p) := \{(x, y) \in E(\mathbf{Q}_p) \mid \mathrm{ord}_p(x) \leq -2\nu\} \cup \{\mathcal{O}\} \quad (\nu = 1, 2, \cdots),$$
$$E_0(\mathbf{Q}_p) := \{(x, y) \in E(\mathbf{Q}_p) \mid (\tilde{x}, \tilde{y}) \in \tilde{E}_{\mathrm{ns}}(\mathbf{F}_p)\} \cup \{\mathcal{O}\}.$$

The following is a key lemma of Proposition 3.3.

LEMMA 6.3. *Let p be an odd prime, and suppose that* $\mathrm{ord}_p(\alpha) = a \geq 1$, $\mathrm{ord}_p(\beta) = 1$. *And let $(x, y) \in E(\mathbf{Q}_p)$. If $a = 1$, the following holds.*

(1) *If* $\mathrm{ord}_p(x) \geq 2$, *then* $P \equiv (0, 0) \pmod{E_0(\mathbf{Q}_p)}$.

(2) *If* $\mathrm{ord}_p(x) = 1$, *then* $P \equiv (\alpha, 0)$ *or* $(\beta, 0) \pmod{E_0(\mathbf{Q}_p)}$.

If $a \geq 2$, the following holds.

(1) *If* $\mathrm{ord}_p(x) \geq a+1$, *then* $P \equiv (0, 0) \pmod{E_0(\mathbf{Q}_p)}$.

(2) *If* $\mathrm{ord}_p(x) = a$, *then* $P \equiv (\alpha, 0) \pmod{E_0(\mathbf{Q}_p)}$.

(3) *There does not exist a point with* $2 \leq \mathrm{ord}_p(x) \leq a-1$.

(4) *If* $\mathrm{ord}_p(x) = 1$, *then* $P \equiv (\beta, 0) \pmod{E_0(\mathbf{Q}_p)}$.

In both cases, we have $E(\mathbf{Q}_p)/E_0(\mathbf{Q}_p) \cong E[2]$.

Proof. In this case, the equation of $\tilde{E}$ is $y^2 = x^3$. Since the singular point of this curve is $(0, 0)$, we have

$$E_0(\mathbf{Q}_p) = \{(x, y) \in E(\mathbf{Q}_p) \mid \mathrm{ord}_p(x) \leq 0\} \cup \{\mathcal{O}\}.$$

The formulae in Lemma 6.2 are used many times. The y-coordinates are not important, so they are represented by □. First, we see the case that $a = 1$.

(1) Put $P' := P + (0,0) = \left(\frac{\alpha\beta}{x}, \square\right)$. Since $\mathrm{ord}_p(\alpha\beta) = 2$ and $\mathrm{ord}_p(x) \geq 2$, we have $P' \in E_0(\mathbf{Q}_p)$. Hence $P \equiv (0,0) \pmod{E_0(\mathbf{Q}_p)}$.

(2) Since $\mathrm{ord}_p(x) = 1$, we have $\mathrm{ord}_p(x-\alpha) \neq \mathrm{ord}_p(x-\beta)$. Indeed, if $\mathrm{ord}_p(x-\alpha) = \mathrm{ord}_p(x-\beta)$, then $\mathrm{ord}_p(x(x-\alpha)(x-\beta))$ is odd, a contradiction. For example, if $\mathrm{ord}_p(x-\alpha) > \mathrm{ord}_p(x-\alpha)$, then

$$P + (\alpha, 0) = \left(\frac{\alpha(x-\beta)}{x-\alpha}, \square\right) \in E_0(\mathbf{Q}_p).$$

Hence $P \equiv (\alpha, 0) \pmod{E_0(\mathbf{Q}_p)}$. Similarly, if $\mathrm{ord}_p(x-\alpha) < \mathrm{ord}_p(x-\alpha)$, then we have $P \equiv (\beta, 0) \pmod{E_0(\mathbf{Q}_p)}$.

Next, we see the case that $a \geq 2$.

(1) Put $P' := P+(0,0) = \left(\frac{\alpha\beta}{x}, \square\right)$. Since $\mathrm{ord}_p(\alpha\beta) = a+1$ and $\mathrm{ord}_p(x) \geq a+1$, we have $P' \in E_0(\mathbf{Q}_p)$. Hence $P \equiv (0,0) \pmod{E_0(\mathbf{Q}_p)}$.

(2) Since $\mathrm{ord}_p(x) = a$, we have $\mathrm{ord}_p(x-\beta) = 1$, $\mathrm{ord}_p(x-\alpha) \geq a$. But since $\mathrm{ord}_p(x(x-\alpha)(x-\beta))$ is even, we have $\mathrm{ord}_p(x-\alpha) \geq a+1$. Then

$$P + (\alpha, 0) = \left(\frac{\alpha(x-\beta)}{x-\alpha}, \square\right) \in E_0(\mathbf{Q}_p)\,.$$

Hence $P \equiv (\alpha, 0) \pmod{E_0(\mathbf{Q}_p)}$.

(3) Assume that $\mathrm{ord}_p(x) = b$ with $1 \leq b \leq a-1$. Then $\mathrm{ord}_p(x-\alpha) = b$ and $\mathrm{ord}_p(x-\beta) = 1$, so $\mathrm{ord}_p(x(x-\alpha)(x-\beta))$ is odd, a contradiction.

(4) Since $\mathrm{ord}_p(x) = 1$, we have $\mathrm{ord}_p(x-\alpha) = 1$, $\mathrm{ord}_p(x-\beta) \geq 1$. But since $\mathrm{ord}_p(x(x-\alpha)(x-\beta))$ is even, we have $\mathrm{ord}_p(x-\beta) \geq 2$. Then

$$P + (\beta, 0) = \left(\frac{\beta(x-\alpha)}{x-\beta}, \square\right) \in E_0(\mathbf{Q}_p)\,.$$

Hence $P \equiv (\beta, 0) \pmod{E_0(\mathbf{Q}_p)}$. □

Proof of Proposition 3.3. By Lemma 6.1, $\delta'_p(E_0(\mathbf{Q}_p)) = \{1\}$. So the proposition holds by Lemma 6.3. □

Lemma 6.3 says that in the case that p divides both α and β, representatives of E/E_0 can be selected as these are only trivial points (we call the points of order 2 trivial). So this case is easy, but the other cases are more difficult. The following lemma describes this situation.

LEMMA 6.4. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax^2 + Bx$ with $A, B \in \mathbf{Z}$. Suppose that p is an odd prime and* $\mathrm{ord}_p(A) = 0$, $\mathrm{ord}_p(B) = a \geq 1$, $P = (x, y) \in E(\mathbf{Q}_p)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_p(x) \leq 0$, *then* $P \equiv \mathcal{O} \pmod{E_0(\mathbf{Q}_p)}$.

(2) *If* $\mathrm{ord}_p(x) \geq a$, *then* $P \equiv (0,0) \pmod{E_0(\mathbf{Q}_p)}$.

(3) *If $(A/p) = -1$, then there does not exist a point with* $1 \leq \mathrm{ord}_p(x) \leq a-1$. *If $(A/p) = 1$, then there exist points with* $\mathrm{ord}_p(x) = 1, 2, \cdots, a-1$, *and any elements of $\mathbf{Z}_p^\times$ appear in p-free part of x.*

Proof. (1) In this case, the equation of $\tilde{E}$ is $y^2 = x^3 + Ax^2 = x^2(x + A)$. Since the singular point of this curve is $(0, 0)$, we have

$$E_0(\mathbf{Q}_p) = \{(x, y) \in E(\mathbf{Q}_p) \mid \mathrm{ord}_p(x) \le 0\} \cup \{\mathcal{O}\}.$$

So the statement is clear.

(2) By Lemma 6.2,

$$P' := P + (0, 0) = \left(\frac{B}{x}, \square\right).$$

Since $\mathrm{ord}_p(B) = a$ and $\mathrm{ord}_p(x) \ge a$, we have $P' \in E_0(\mathbf{Q}_p)$. Hence $P \equiv (0, 0)$ $(\mathrm{mod}\, E_0(\mathbf{Q}_p))$.

(3) Let $x = p^e w$ with $1 \le e \le a - 1$, $w \in \mathbf{Z}_p^\times$ and suppose that $B = p^a B'$, then

$$\begin{aligned} y^2 &= p^{3e}w^3 + Ap^{2e}w^2 + Bp^e w \\ &= p^{2e}w^2(p^e w + A + p^{a-e}B'w^{-1}). \end{aligned}$$

Note that $e \ge 1$, $a - e \ge 1$. The number $y \in \mathbf{Q}_p$ exists if and only if A is square modulo p. Conversely if A is square, then e and w may be arbitrary. □

The following lemma is used in the proof of Proposition 3.4.

LEMMA 6.5. *Let p be an odd prime. Suppose that* $\mathrm{ord}_p(\alpha) = a \ge 1$ *and* $\mathrm{ord}_p(\beta) = 0$. *Then*

$$u \in \delta'_p(E_0(\mathbf{Q}_p) \backslash E_1(\mathbf{Q}_p)).$$

(Recall that u represents a non-square element modulo p.)

Proof. Suppose that $(x, y) \in E_0(\mathbf{Q}_p) \backslash E_1(\mathbf{Q}_p)$, namely $\mathrm{ord}_p(x) = 0$. Since $x(x - \alpha) \equiv x^2 \pmod{p}$, $x - \beta$ is square modulo p. Assume that such x must be square modulo p. Then β must be square modulo p since $(\beta, 0) \in E$ and $\mathrm{ord}_p(\beta) = 0$. Next, consider that $x = 2\beta$, then $x - \beta$ is square modulo p, so 2β must be also square modulo p. Repeating this step, we have squares

$$\beta, 2\beta, \cdots, (p-1)\beta.$$

Since $\beta \in (\mathbf{Z}/p\mathbf{Z})^\times$, this is a rearrangement of $1, 2, \cdots, p - 1$. It is a contradiction that $1, 2, \cdots, p - 1$ are all squares modulo p. □

Proof of Proposition 3.4. In view of Theorem 2.1, we may consider only $\mathrm{Im}(\delta'_p)$. By Lemma 6.5, $\mathrm{Im}(\delta'_p) \supset \{1, u\}$. First, suppose that a is odd. Since $\delta'_p((0, 0)) = \alpha\beta$, p or pu is in $\mathrm{Im}(\delta'_p)$, consequently $\mathrm{Im}(\delta'_p) = \{1, u, p, pu\}$. Next, suppose that a is even and $(-\beta/p) = 1$. Since there exists a point of order 1 by Lemma 6.4, we have $\mathrm{Im}(\delta'_p) = \{1, u, p, pu\}$.

Lastly, suppose that a is even and $(-\beta/p) = -1$. Let $P = (x, y) \in E(\mathbf{Q}_p)$. By Lemma 6.1, if $\mathrm{ord}_p(x) < 0$, then $x \equiv 1$ $(\mathrm{mod}\, \mathbf{Q}^{\times 2})$. If $\mathrm{ord}_p(x) = 0$, then $x \equiv 1$ or u $(\mathrm{mod}\, \mathbf{Q}^{\times 2})$. By Lemma 6.4, there does not exist a point of order which is from 1 to $a - 1$. If $\mathrm{ord}_p(x) \ge a$, then $P \equiv (0, 0)$ $(\mathrm{mod}\, E_0(\mathrm{Q}_p))$, so $x \equiv 1$ or u $(\mathrm{mod}\, \mathbf{Q}^{\times 2})$. We have found that p and pu do not appear, hence $\mathrm{Im}(\delta'_p) = \{1, u\}$. □

In the proof of Proposition 3.5, we calculate $\mathrm{Im}(\delta_p)$, since the method is similar to that of Proposition 3.4. The following lemma is used in the proof of Proposition 3.5.

LEMMA 6.6. *Let p be an odd prime. Suppose that* $\mathrm{ord}_p(\alpha) = 0$ *and* $\mathrm{ord}_p(\alpha - \beta) \geq 1$. *Then*

$$u \in \delta_p(E'_0(\mathbf{Q}_p)\backslash E'_1(\mathbf{Q}_p)) .$$

Proof. The equation of E' is

$$y^2 = x^3 + 2(\alpha + \beta)x^2 + (\alpha - \beta)^2 x = x^2(x + 2(\alpha + \beta)) + (\alpha - \beta)^2 x .$$

We shall show that there exists $x \in \mathbf{Z}_p^\times$ such that $x \equiv -2(\alpha + \beta) \pmod p$ and the right hand side is in $\mathbf{Q}_p^{\times 2}$ (this fact is not trivial). Let $x = p^e z - 2(\alpha + \beta)$ with $e \in \mathbf{N}$, $z \in \mathbf{Z}_p^\times$ and $\alpha - \beta = p^b \gamma$ with $b \in \mathbf{N}$, $\gamma \in \mathbf{Z}_p^\times$, then

$$y^2 = x^2(p^e z) + p^{2b}\gamma^2 x = p^e x^2(z + p^{2b-e}\gamma^2 x^{-1}) . \tag{6.3}$$

If there exists an even number e such that $1 \leq e < 2b$, the right hand side can be in $\mathbf{Q}_p^{\times 2}$, hence there exists x satisfying the conditions. There is not such number e if and only if $b = 1$, so suppose that $b = 1$. Moreover if $e = 2$, then

$$\text{the right hand side of (6.3)} = p^2 x^2 z + p^2 \gamma^2 x = p^2 x^2 (z + \gamma^2 x^{-1}) .$$

Since $z + \gamma^2 x^{-1}$ can be square modulo p, there exists x satisfying the conditions.

Let us come back to the proof of the proposition. If $-2(\alpha + \beta)$ is non-square modulo p, the proposition holds by the above fact. Suppose that it is square. Putting $x = -4(\alpha+\beta)$ the right side hand is square, so the proposition holds if $-4(\alpha + \beta)$ is non-square modulo p. If we always have square elements in repeating this step, then we have squares

$$-2(\alpha + \beta), -4(\alpha + \beta), \cdots , -2(p - 1)(\alpha + \beta) ,$$

a contradiction. □

Proof of Proposition 3.5. By Lemma 6.6, we have $\mathrm{Im}(\delta_p) \supset \{1, u\}$.

$$\left(\frac{A'}{p}\right) = \left(\frac{2(\alpha + \beta)}{p}\right) = \left(\frac{4\alpha}{p}\right) = \left(\frac{\alpha}{p}\right) ,$$

so the proposition holds by Lemma 6.4. □

Now, we shall prove the propositions for $\mathrm{Im}(\delta'_2)$. The following lemma is an alanogy of Lemma 6.1.

LEMMA 6.7. *Consider the elliptic curve* $y^2 = x^3 + Ax^2 + Bx$ *with* $\mathrm{ord}_2(A) = a$, $\mathrm{ord}_2(B) = b$ *over* $\mathbf{Q}_2$. *Let* $(x, y) \in E(\mathbf{Q}_2)$ *and* $x = 2^e w$ *with* $e = \mathrm{ord}_2(x)$, $w \in \mathbf{Z}_2^\times$. *Then*

$$e \leq \min\left\{a - 3, \frac{b - 3}{2}\right\} \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_2^{\times 2}} .$$

Proof. The proof is similar to that of Lemma 6.1. □

For our elliptic curve $E_{\alpha,\beta}$, since α, β are integers,

$$\mathrm{ord}_2(x) \leq -4 \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_2^{\times 2}} .$$

Moreover if $a \geq 1$, then

$$\mathrm{ord}_2(x) = -2 \Rightarrow x \equiv 1 \pmod{\mathbf{Q}_2^{\times 2}}.$$

REMARK 6.8. The following equation appears in the proof of Lemma 6.7 (see the proof of Lemma 6.1):

$$y^2 = 2^{3e}w^3(1 + 2^{-e+a}A'w^{-1} + 2^{-2e+b}B'w^{-2}).$$

Put $X := 2^{-e+a}A'w^{-1} + 2^{-2e+b}B'w^{-2}$, then

$$y^2 = 2^{3e}w^3(1 + X).$$

Therefore if $\mathrm{ord}_2(X) \geq 3$, then $x \equiv 1 \pmod{\mathbf{Q}_2^{\times 2}}$. It is sufficient that $-e + a \geq 3$, $-2e + b \geq 3$, then we got Lemma 6.7. Note that it is also sufficient that $-e + a = -2e + b = 2$. We have one more important remark. If $\mathrm{ord}_2(X) = 2$, then $x \equiv 5 \pmod{\mathbf{Q}_2^{\times 2}}$.

We have lemmas in order to prove Proposition 3.6.

LEMMA 6.9. *Suppose that* $\mathrm{ord}_2(\alpha) = 0$, $\mathrm{ord}_2(\beta) = 0$, $\mathrm{ord}_2(\alpha - \beta) = 1$. *And let* $(x, y) \in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x) \geq 1$, *then* $P \equiv (0, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(2) *If* $\mathrm{ord}_2(x) = 0$, *then* $P \equiv (\alpha, 0)$ *or* $(\beta, 0) \pmod{E_1(\mathbf{Q}_2)}$.

Therefore $E(\mathbf{Q}_2)/E_1(\mathbf{Q}_2) \cong E[2]$.

Proof. (1) By Lemma 6.2, $P + (0, 0) = \left(\frac{\alpha\beta}{x}, \square\right) \in E_1(\mathbf{Q}_2)$. Hence $P \equiv (0, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(2) In this case, $\mathrm{ord}_2(x - \alpha) \neq \mathrm{ord}_2(x - \beta)$. Indeed, if $2^a \,||\, x - \alpha,\ x - \beta$ with $a \geq 1$, then $2^{a+1} \mid \alpha - \beta$. This is contradictory to the hypothesis $\mathrm{ord}_2(\alpha - \beta) = 1$. For example, if $\mathrm{ord}_2(x - \alpha) > \mathrm{ord}_2(x - \beta)$, then

$$P + (\alpha, 0) = \left(\frac{\alpha(x - \beta)}{x - \alpha}, \square\right) \in E_1(\mathbf{Q}_2).$$

Hence $P \equiv (\alpha, 0) \pmod{E_1(\mathbf{Q}_2)}$. Similarly, if $\mathrm{ord}_2(x - \alpha) < \mathrm{ord}_2(x - \beta)$, then $P \equiv (\beta, 0) \pmod{E_1(\mathbf{Q}_2)}$. □

Lemma 6.9 says that in the case that $\mathrm{ord}_2(\alpha - \beta) = 1$, representatives of E/E_1 can be selected as these are only trivial points. But in the case that $\mathrm{ord}_2(\alpha - \beta) \geq 2$, the other situation can occur. In fact, the point which is not equivalent to any trivial point modulo $E_1(\mathbf{Q}_2)$ is in $E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)$. So we need the following lemma.

LEMMA 6.10. *Suppose that* $\mathrm{ord}_2(\alpha) = 0$, $\mathrm{ord}_2(\beta) = 0$, $\mathrm{ord}_2(\alpha - \beta) \geq 2$. *Then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) \subset \langle \alpha, \beta \rangle$ *except the following three cases.*

(1) *If* $\mathrm{ord}_2(\alpha - \beta) = 2$ *and* $\alpha + \beta \equiv 14 \pmod{16}$, *then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) = \{\pm 1, \pm 5\}$.

(2) *If* $\mathrm{ord}_2(\alpha - \beta) = 3$ *and* $\alpha \equiv 3 \pmod 4$, *then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) = \{-1, \pm 5\}$.

(3) *If* $\mathrm{ord}_2(\alpha - \beta) = 4$ *and* $\alpha \equiv 1 \pmod 8$, *then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) = \{1, 5\}$.

Proof. Let $(x, y) \in E(\mathbf{Q}_2)$ and put $x = 2^e z + \alpha$ with $e \geq 1$, $z \in \mathbf{Z}_2^\times$. We investigate how x appears for each number e. If $e \geq 3$, then $x \equiv \alpha \pmod{\mathbf{Q}_2^{\times 2}}$. In fact, there is such a point $(\alpha, 0)$, so we must investigate only the points of $e = 1, 2$.

First, let $e = 1$ and $x = 2z + \alpha$, then

$$\begin{aligned} y^2 &= (2z + \alpha) \cdot 2z(2z + \alpha - \beta)\,, \\ \left(\frac{y}{2}\right)^2 &= z(2z + \alpha)\left(z + \frac{\alpha - \beta}{2}\right) \\ &\equiv 2\alpha - \beta + \frac{\alpha(\alpha - \beta) + 4}{2} z \pmod 8\,. \end{aligned} \tag{6.4}$$

The last expression must be congruent to 1 modulo 8.

Secondly, consider the points of $e = 2$. Suppose that $\mathrm{ord}_2(\alpha - \beta) = 2$. If $e = 2$, then $x \equiv \beta \pmod{\mathbf{Q}_2^{\times 2}}$. In fact, there is such a point $(\beta, 0)$, so we do not have to investigate the points of $e = 2$. Next, suppose that $\mathrm{ord}_2(\alpha - \beta) \geq 3$. Put $x = 4z + \alpha$, then

$$\begin{aligned} y^2 &= (4z + \alpha) \cdot 4z(4z + \alpha - \beta)\,, \\ \left(\frac{y}{4}\right)^2 &= z(4z + \alpha)\left(z + \frac{\alpha - \beta}{4}\right) \\ &\equiv 2\alpha - \beta + \frac{\alpha(\alpha - \beta) + 16}{4} z \pmod 8\,. \end{aligned} \tag{6.5}$$

The last expression must be congruent to 1 modulo 8.

In the case that $\mathrm{ord}_2(\alpha - \beta) = 2$, we must investigate only the points of $e = 1$. The expression (6.4) is congruent to α modulo 4, so it must hold that $\alpha \equiv 1 \pmod 4$. For example, suppose that $\alpha \equiv 1 \pmod{16}$. Then the expression (6.4) is congruent to 1 modulo 8 if and only if $\beta \equiv 13 \pmod{16}$. Consequently we have the following conditions.

- $\alpha \equiv 1 \pmod{16}$, $\beta \equiv 13 \pmod{16}$,
- $\alpha \equiv 5 \pmod{16}$, $\beta \equiv 9 \pmod{16}$,
- $\alpha \equiv 9 \pmod{16}$, $\beta \equiv 5 \pmod{16}$,
- $\alpha \equiv 13 \pmod{16}$, $\beta \equiv 1 \pmod{16}$.

These conditions are equivalent to $\alpha + \beta \equiv 14 \pmod{16}$. Conversely if this condition holds, we have $\delta_2'(E_0(\mathbf{Q}_2) \backslash E_1(\mathbf{Q}_2)) = \{\pm 1, \pm 5\}$.

In the case that $\mathrm{ord}_2(\alpha - \beta) = 3$, we must consider the points of $e = 1, 2$. First, consider the points of $e = 1$. Since $\alpha(\alpha - \beta) + 4 \equiv 8 + 4 \equiv 12 \pmod{16}$, the expression (6.4) is congruent to $\alpha + 6z$ modulo 8. So this is congruent to 1 modulo 8 if and only if one of the following two conditions holds.

- $\alpha \equiv 3 \pmod 8$, $z \equiv 1 \pmod 4$,
- $\alpha \equiv 7 \pmod 8$, $z \equiv 3 \pmod 4$.

In both cases, $x = 2z + \alpha \equiv 5 \pmod 8$. Next, consider the points of $e = 2$. In order to the expression (6.5) is congruent to 1 modulo 8, it is necessary that $\alpha \equiv 3 \pmod 4$. In this case, we have $x = \alpha + 4z \equiv \alpha + 4 \pmod 8$. We have shown that $\delta_2'(E_0(\mathbf{Q}_2) \backslash E_1(\mathbf{Q}_2)) = \{-1, \pm 5\}$ if $\alpha \equiv 3 \pmod 4$.

Next, we see the case that $\mathrm{ord}_2(\alpha-\beta)=4$. First, consider the points of $e=1$. Since the expression (6.4) is congruent to $\alpha+2z$ modulo 8, this is congruent to 1 modulo 8 if and only if one of the following conditions holds.

- $\alpha \equiv 3 \pmod 8$, $z \equiv 3 \pmod 4$,
- $\alpha \equiv 7 \pmod 8$, $z \equiv 1 \pmod 4$.

In both cases, we have $x=2z+\alpha \equiv 1 \pmod 8$. Next, consider the points of $e=2$. Since the expression (6.5) is congruent to α modulo 8, this is congruent to 1 modulo 8 if and only if $\alpha \equiv 1 \pmod 8$. In this case, we have $x=4z+\alpha \equiv 5 \pmod 8$. We have shown that $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2))=\{1,5\}$ if $\alpha \equiv 1 \pmod 8$.

In the case that $\mathrm{ord}_2(\alpha-\beta)\geq 5$, most situations are the same as the last case. Since the expression (6.5) is congruent to $\alpha+4$ modulo 8, this is congruent to 1 modulo 8 if and only if $\alpha \equiv 5 \pmod 8$. In this case, we have $x=4z+\alpha \equiv 1 \pmod 8$. □

Proof of Proposition 3.6. By Lemma 6.7, $\delta'_2(E_1(\mathbf{Q}_2))=\{1\}$. When $\mathrm{ord}_2(\alpha-\beta)=1$, the proposition holds by Lemma 6.9. When $\mathrm{ord}_2(\alpha-\beta)\geq 2$, it holds that

$$\mathrm{ord}_2(x)\geq 1 \Rightarrow P\equiv(0,0) \pmod{E_1(\mathbf{Q}_2)}$$

(see the proof of Lemma 6.9). So $\mathrm{Im}(\delta'_2)$ is generated by $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2))$ and $\delta'_2(E[2])$. Hence the proposition holds by Lemma 6.10. □

Next, we prove Proposition 3.7.

LEMMA 6.11. *Suppose that* $\mathrm{ord}_2(\alpha)=1$, $\mathrm{ord}_2(\beta)=1$. *And let* $(x,y)\in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x)\geq 2$, *then* $P\equiv(0,0) \pmod{E_0(\mathbf{Q}_2)}$.

(2) *If* $\mathrm{ord}_2(x)=1$, *then* $P\equiv(\alpha,0)$ *or* $(\beta,0) \pmod{E_0(Q_2)}$.

Therefore $E(\mathbf{Q}_2)/E_0(\mathbf{Q}_2)\cong E[2]$.

Proof. The proof is similar to that of Lemma 6.3. □

Proof of Proposition 3.7. First, suppose that $\mathrm{ord}_2(\alpha-\beta)=2$, then $\mathrm{ord}_2(\alpha+\beta)\geq 2$. By Remark 6.8, we have $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2))=\{5\}$. Hence $\mathrm{Im}(\delta'_2)=\langle\alpha,\beta,5\rangle=\mathbf{Q}_2^\times/\mathbf{Q}_2^{\times 2}$ by Lemma 6.11.

Next, suppose that $\mathrm{ord}_2(\alpha-\beta)\geq 3$, then $\mathrm{ord}_2(\alpha+\beta)=2$. By Remark 6.8, we have $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2))=\{1\}$. Hence $\mathrm{Im}(\delta'_2)=\langle\alpha,\beta\rangle$ by Lemma 6.11. Moreover when $\mathrm{ord}_2(\alpha-\beta)=3$, we have $\mathrm{Im}(\delta'_2)=\langle\alpha,5\rangle$. When $\mathrm{ord}_2(\alpha-\beta)\geq 4$, we have $\mathrm{Im}(\delta'_2)=\langle\alpha\rangle$. □

We have lemmas to prove Proposition 3.9.

LEMMA 6.12. *Suppose that* $\mathrm{ord}_2(\alpha)=a\geq 2$, $\mathrm{ord}_2(\beta)=1$. *And let* $(x,y)\in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x)\geq a+1$, *then* $P\equiv(0,0) \pmod{E_0(\mathbf{Q}_2)}$.

(2) *If* $\mathrm{ord}_2(x)=a$, *then* $P\equiv(\alpha,0) \pmod{E_0(\mathbf{Q}_2)}$.

(3) *There does not exist a point with* $2\leq \mathrm{ord}_2(x)\leq a-1$.

(4) *If* $\mathrm{ord}_2(x)=1$, *then* $P\equiv(\beta,0) \pmod{E_0(Q_2)}$.

Therefore, $E(\mathbf{Q}_2)/E_0(\mathbf{Q}_2)\cong E[2]$.

Proof. The proof is similar to that of Lemma 6.3. □

LEMMA 6.13. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2$, $\mathrm{ord}_2(\beta) = 1$. *And let* $(x, y) \in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\alpha + \beta \equiv 2 \pmod 8$, *then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) = \{-5\}$.

(2) *If* $\alpha + \beta \equiv 6 \pmod 8$, *then* $\delta'_2(E_0(\mathbf{Q}_2)\backslash E_1(\mathbf{Q}_2)) = \{-1\}$.

Proof. When $\mathrm{ord}_2(x) = 0$, we have

$$y^2 = x^3 - (\alpha + \beta)x^2 + \alpha\beta x = x^2(x - (\alpha + \beta)) + \alpha\beta x \equiv x - (\alpha + \beta) \pmod 8 .$$

Hence the lemma holds. □

Proof of Proposition 3.9. By Lemma 6.7, we have $\delta'_2(E_1(\mathbf{Q}_2)) = \{1\}$. So the proposition follows immediately from Lemmas 6.12 and 6.13. □

Next, we proof the Proposition 3.10.

LEMMA 6.14. *Suppose that* $\mathrm{ord}_2(\alpha) = 1$, $\mathrm{ord}_2(\beta) = 0$. *And let* $(x, y) \in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x) \geq 2$, *then* $P \equiv (0, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(2) *If* $\mathrm{ord}_2(x) = 1$, *then* $P \equiv (\alpha, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(3) *If* $\mathrm{ord}_2(x) = 0$, *then* $P \equiv (\beta, 0) \pmod{E_1(\mathbf{Q}_2)}$.

Therefore $E(\mathbf{Q}_2)/E_1(\mathbf{Q}_2) \cong E[2]$.

Proof. The proof is similar to that of Lemma 6.3. □

Proof of Proposition 3.10. By Lemma 6.7, we have $\delta'_2(E_2(\mathbf{Q}_2)) = \{1\}$. By Remark 6.8, we have $\delta'_2(E_1(\mathbf{Q}_2)\backslash E_2(\mathbf{Q}_2)) = \{5\}$. Hence the proposition holds by Lemma 6.14. □

Lastly, the proof of Proposition 3.11 is given.

LEMMA 6.15. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2$, $\mathrm{ord}_2(\beta) = 0$. *And let* $(x, y) \in E(\mathbf{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x) \geq a + 1$, *then* $P \equiv (0, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(2) *If* $\mathrm{ord}_2(x) = a$, *then* $P \equiv (\alpha, 0) \pmod{E_1(\mathbf{Q}_2)}$.

(3) *If* $\mathrm{ord}_2(x) = 0$, *then* $P \equiv (\beta, 0) \pmod{E_1(\mathbf{Q}_2)}$.

Proof. The proof is similar to that of Lemma 6.3. □

Lemma 6.15 does not mention the points with $1 \leq \mathrm{ord}_2(x) \leq a - 1$. Actually, this part is most complicated and the cause of the big table in Proposition 3.11.

Proof of Proposition 3.11. By Remark 6.8, we have $\delta'_2(E_1(\mathbf{Q}_2)\backslash E_2(\mathbf{Q}_2)) = \{5\}$ and $\langle \alpha, \beta, 5 \rangle \subset \mathrm{Im}(\delta'_2)$. For this subgroup, we have

$$\langle \alpha, \beta, 5 \rangle = \begin{cases} \langle \alpha, 5 \rangle, & \text{if } \beta \equiv 1 \pmod 4, \\ \langle \alpha, -1, 5 \rangle, & \text{if } \beta \equiv -1 \pmod 4. \end{cases}$$

By Lemma 6.7, $\delta'_2(E_2(\mathbf{Q}_2)) = \{1\}$. In view of Lemma 6.15, we must investigate the points of $1 \leq \mathrm{ord}_2(x) \leq a - 1$.

In the equation of E,

$$y^2 = x(x-\alpha)(x-\beta) = x^3 + Ax^2 + Bx\,,$$

where A is odd and $\mathrm{ord}_2(B) = a$. Put $B = 2^a B'$, then $B' = \alpha'\beta$ is odd. Put $x = 2^e w$ and $B = 2^a B'$, then

$$y^2 = 2^{3e}w^3 + A\cdot 2^{2e}w^2 + 2^a B'\cdot 2^e w = 2^{2e}w^2(2^e w + A + 2^{-e+a}B'w^{-1})\,.$$

Suppose that $1 \le e \le a-1$, then $e \ge 1$, $-e+a \ge 1$. Put $X = 2^e w + 2^{-e+a}B'w^{-1}$, then $\mathrm{ord}_2(X) \ge 1$ and we have

$$y^2 = 2^{2e}w^2(X+A)\,.$$

For example, when $A \equiv 1 \pmod 8$, there are points such that $X \equiv 0 \pmod 8$. Investigating the condition of α, β to exist a point of $e \ge 1$, $-e+a \ge 1$, and the contribution of such points to $\mathrm{Im}(\delta_2')$, we can see that the table in Proposition 3.11 holds. □

Acknowledgements

I would like to thank Professor M. Kaneko and Professor Y. Sueyoshi for their many advices and encouragement.

References

[1] N. Aoki, *On the* 2*-Selmer groups of elliptic curves arising from the congruent number problem*, Comm. Math. Univ. Sancti Pauli, **48** (1999), 77–101.

[2] N. Aoki, *Selmer groups and ideal class groups*, Comm. Math. Univ. Sancti Pauli, **42** (1993), 209–229.

[3] M. Fujiwara, *θ-congruent numbers*, Number Theory (ed. by K. Győry et al.), Walter de Gruyter, 1998, 235–241.

[4] M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith., **XCIV.2** (2000), 153–160.

[5] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics 97, Springer, 1984.

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer, 1986.

[7] J. H. Silverman and J. Tate, *Rational Points on Elliptic curves*, Springer, 1992.

[8] J. Tate, *Algorithm for determining the type of singular fiber in elliptic pencil*, in *Modular Functions of One Variable IV*, Lect. Notes in Math. 476, Springer-Verlag, 1975.

[9] Tunnell, *A classical Diophantine problem and modular forms of weight* 3/2, Invent. Math. **72** (1983), 323–334.

Graduate School of Mathematics
Kyushu University 33
Fukuoka 812–8581, Japan

e-mail address: tgoto@math.kyushu-u.ac.jp