KYUSHU UNIVERSITY
DOCTORAL THESIS (2002)

A STUDY ON THE SELMER GROUPS OF ELLIPTIC CURVES WITH A RATIONAL 2-TORSION

TAKESHI GOTO

Abstract. A natural number is called a *congruent number* if it is the area of a right triangle with rational sides. M. Fujiwara introduced the generalized concept, *θ-congruent numbers* by considering triangles with rational sides and an angle θ. The *θ-congruent number problem* is to find a criterion to determine whether a given integer is a θ-congruent number or not. From Fujiwara's theorem, this problem is connected to the $\mathbb{Q}$-rank of an elliptic curve with three rational 2-torsions. The main result of this article is an explicit formula of the Selmer group of an elliptic curve with at least *one* rational 2-torsion (see (4.2) and Section 7.1). Since the Selmer group gives an upper bound of the rank, we obtain some results about the θ-congruent number problem.

Contents

2000 *Mathematics Subject Classification.* Primary 11G05, Secondary 14H52.
Key words and phrases. elliptic curve, Selmer group, congruent number.

1. Introduction

1.1. **Mordell-Weil rank and Selmer rank.** Suppose that E is an elliptic curve defined by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where a_i are in a number field K. Then $E(K)$ is finitely generated abelian group from the Mordell-Weil theorem. Hence the Mordell-Weil group $E(K)$ has the form

$$E(K) \cong E_{\mathrm{tors}}(K) \times \mathbb{Z}^r,$$

where the torsion subgroup $E_{\mathrm{tors}}(K)$ is finite and the *(Mordell-Weil) rank* r of $E(K)$ is a non-negative integer. From the generalized Nagell-Lutz theorem the torsion subgroup is computable, but there is no known procedure which is guaranteed to yield the rank.

However computing the rank is difficult, it is known that the *Selmer rank* is computable. In this article, the Selmer rank means the upper bound of the rank given by the *Selmer group*. We recall the definition of the Selmer group in Section 2. The main result of this article, the explicit formula for the Selmer rank of the elliptic curve over $\mathbb{Q}$ with a rational 2-torsion (see (4.2)). Such an elliptic curve has the equation

$$y^2 = x^3 + Ax^2 + Bx,$$

where $A, B \in \mathbb{Q}$. The essential parts of the main result are the formulae of images of the *connecting homomorphisms*. These formulae are stated in Section 7 (see also Section 10). In Sections 4 and 5, we treat the special cases

$$y^2 = x^3 + Dx, \quad \text{and} \quad y^2 = x(x-\alpha)(x-\beta),$$

where $D, \alpha, \beta \in \mathbb{Q}$.

1.2. **The θ-congruent numbers.** The *congruent number problem* is one of the motivation to study the rank of the elliptic curve. A natural number n is called a *congruent number* if it is the area of a right triangle with rational sides. The congruent number problem is to find a simple criterion to determine whether a given integer is a congruent number or not. 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 (see Koblitz [18, chap.1] or Knapp [17, pp.52,53,88]):

$$E_n : y^2 = x(x+n)(x-n). \tag{1.1}$$

Tunnell's theorem ([27]) gives a (possibly invalid) criterion to tell whether a given n is congruent or not. This criterion is verified if the weak form of the Birch and Swinnerton-Dyer conjecture is true.

Fujiwara [9] 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 called *θ-congruent number* 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:

$$E_{n,\theta} : y^2 = x(x + (r + s)n)(x - (r - s)n). \tag{1.2}$$

Theorem 1.1 (Fujiwara [9])**.** *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 $E_{n,\theta}(\mathbb{Q})$ 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 $\mathbb{Q}$-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 $\mathbb{Q}$. In Section 5, we study such an elliptic curve, then the result is applied to the θ-congruent number problem in Section 6.

2. Preliminaries

2.1. **Selmer group.** In this part, we recall some basic facts on the Selmer groups of elliptic curves with at least one 2-torsion rational point. For details, we refer Silverman and Tate [24, chap.3] and Silverman [23, chap.10].

Let E, E' be elliptic curves defined over $\mathbb{Q}$, and we assume that there exists an isogeny $\varphi : E \to E'$ over $\mathbb{Q}$. Let k be a field containing $\mathbb{Q}$. Then there is the exact sequence of $\mathrm{Gal}(\bar{k}/k)$-modules

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

where $E[\,\varphi\,] = \mathrm{Ker}(\varphi)$. Taking Galois cohomology, we obtain the exact sequence

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

where $H^1(k, E)[\,\varphi\,]$ denotes the kernel of the map $H^1(k, E) \xrightarrow{\varphi} H^1(k, E')$. The map δ_k is called the *connecting homomorphism*. When $k = \mathbb{Q}$ (resp. $k = \mathbb{Q}_p$, $k = \mathbb{R}$), we simply write δ (resp. δ_p, δ_∞) for δ_k. Consider the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \to & E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) & \xrightarrow{\delta} & H^1(\mathbb{Q}, E[\,\varphi\,]) & \to & H^1(\mathbb{Q}, E)[\,\varphi\,] & \to & 0 \\
 & & \downarrow & & \downarrow \prod \mathrm{res}_p & & \downarrow & & \\
0 & \to & \prod E'(\mathbb{Q}_p)/\varphi(E(\mathbb{Q}_p)) & \xrightarrow{\prod \delta_p} & \prod H^1(\mathbb{Q}_p, E[\,\varphi\,]) & \to & \prod H^1(\mathbb{Q}_p, E)[\,\varphi\,] & \to & 0,
\end{array}$$

where the symbol $\prod$ means the direct product over $M_\mathbb{Q} = \{\text{primes}\} \cup \{\infty\}$. Then we define the *$\varphi$-Selmer group* $S^{(\varphi)}(E/\mathbb{Q})$ by

$$S^{(\varphi)}(E/\mathbb{Q}) = \mathrm{Ker}\left\{H^1(\mathbb{Q}, E[\,\varphi\,]) \to \prod H^1(\mathbb{Q}_p, E)[\,\varphi\,]\right\}$$

and the *Shafarevich-Tate group* $Ш(E/\mathbb{Q})$ by

$$Ш(E/\mathbb{Q}) = \mathrm{Ker}\left\{H^1(\mathbb{Q}, E) \to \prod H^1(\mathbb{Q}_p, E)\right\}.$$

From the commutative diagram above and the definition of the Selmer and Shafarevich-Tate groups, we immediately obtain the exact sequence

$$0 \to E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \to S^{(\varphi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\,\varphi\,] \to 0. \tag{2.1}$$

Let $\varphi' : E' \to E$ be the dual isogeny of φ. Interchanging the role of E and E', we obtain another exact sequence

$$0 \to E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) \to S^{(\varphi')}(E'/\mathbb{Q}) \to Ш(E'/\mathbb{Q})[\varphi'] \to 0. \tag{2.2}$$

And there is the exact sequence

$$0 \to \frac{E'(\mathbb{Q})[\varphi']}{\varphi(E(\mathbb{Q})[m])} \to \frac{E'(\mathbb{Q})}{\varphi(E(\mathbb{Q}))} \xrightarrow{\varphi'} \frac{E(\mathbb{Q})}{m(E(\mathbb{Q}))} \to \frac{E(\mathbb{Q})}{\varphi'(E'(\mathbb{Q}))} \to 0, \tag{2.3}$$

where $m = \deg \varphi$. Note that these groups are all finite from the weak Mordell-Weil theorem. Moreover the Selmer group is finite by a general theory.

From now on, we let E, E' be the elliptic curves defined by the equations

$$\begin{aligned} E &: y^2 = x^3 + Ax^2 + Bx, \\ E' &: y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x, \end{aligned}$$

where $A, B \in \mathbb{Q}$. There is the isogeny of degree 2 between these curves given by the formula

$$\varphi : E \to E' \quad ((x, y) \mapsto (y^2/x^2,\, y(B - x^2)/x^2).$$

Note that $E[\varphi] = \{\mathcal{O},\, (0, 0)\}$ (we denote by $\mathcal{O}$ the point at infinity on the elliptic curve). From (2.3), we obtain

$$\begin{aligned} \dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) = &\dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) + \dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) \\ &- \dim_{\mathbb{F}_2} E'(\mathbb{Q})[\varphi']/\varphi(E(\mathbb{Q})[2]) \end{aligned}$$

and it holds that

$$\begin{aligned} &\dim_{\mathbb{F}_2} E'(\mathbb{Q})[\varphi']/\varphi(E(\mathbb{Q})[2]) = \begin{cases} 0, & \text{if } A^2 - 4B \text{ is a square,} \\ 1, & \text{otherwise,} \end{cases} \\ &\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) + \begin{cases} 2, & \text{if } A^2 - 4B \text{ is a square,} \\ 1, & \text{otherwise.} \end{cases} \end{aligned} \tag{2.4}$$

Consequently, the rank of the elliptic curve is given by the following formula:

$$\operatorname{rank} E(\mathbb{Q}) = \dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) + \dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) - 2. \tag{2.5}$$

From (2.1) and (2.2), we have

$$\begin{aligned} \dim_{\mathbb{F}_2} E(\mathbb{Q})/\varphi'(E'(\mathbb{Q})) &= \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\varphi'], \\ \dim_{\mathbb{F}_2} E'(\mathbb{Q})/\varphi(E(\mathbb{Q})) &= \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi]. \end{aligned}$$

Then using (2.5), we have

$$\begin{aligned} \operatorname{rank} E(\mathbb{Q}) = &\dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) \\ &- \dim_{\mathbb{F}_2} Ш(E/\mathbb{Q})[\varphi] - \dim_{\mathbb{F}_2} Ш(E'/\mathbb{Q})[\varphi'] - 2. \end{aligned}$$

In particular, it holds that

$$\operatorname{rank} E(\mathbb{Q}) \le \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - 2. \tag{2.6}$$

The value of the right hand side is called the *Selmer rank*.

We now give the method of calculating the Selmer group. From the commutative diagram and the definition of the Selmer group, we have the equivalent definition

$$\begin{aligned} S^{(\varphi)}(E/\mathbb{Q}) =& \{x \in H^1(\mathbb{Q}, E[\,\varphi\,]) \mid \mathrm{res}_p(x) \in \mathrm{Im}(\delta_p) \text{ for } \forall p \in M_{\mathbb{Q}}\} \\ =& \bigcap_{p \in M_{\mathbb{Q}}} \mathrm{Im}(\delta_p), \end{aligned} \tag{2.7}$$

where the groups $\mathrm{Im}(\delta_p)$ are regarded as the subgroups of the group $H^1(\mathbb{Q}, E[\,\varphi\,])$. Roughly speaking, *the Selmer group is the intersection of all images of the connecting homomorphisms*. Then the problem is how to calculate the images of the connecting homomorphisms. Since $H(k, E[\,\varphi\,]) \cong H(k, \{\pm 1\}) \cong k^\times/k^{\times 2}$, the connecting homomorphism δ_k can be regarded as the map to $k^\times/k^{\times 2}$. Then we verify the formula

$$\delta_k(P) = \begin{cases} x, & \text{if } P = (x, y) \neq (0,0), \mathcal{O}, \\ B', & \text{if } P = (0,0), \\ 1, & \text{if } P = \mathcal{O} \end{cases} \tag{2.8}$$

from the definition of the connecting homomorphism. Therefore in order to obtain $\mathrm{Im}(\delta_k)$, we must check what numbers (modulo square) appear in the x-coordinates of the k-rational points on the elliptic curve E'. Similarly, we must check the x-coordinates of the k-rational points of the elliptic curve E to obtain the image of connecting homomorphism $\delta'_k : E(k)/\varphi'(E'(k)) \to k^\times/k^{\times 2}$. 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 given (see for example Aoki [2]).

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

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

We can describe the Selmer group in other words. The coordinates of a rational point of order greater then 2 on E are written as

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

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)

$$N^2 = dM^4 + AM^2e^2 + \left(\frac{B}{d}\right)e^4. \tag{2.9}$$

Hence $d\,(\neq 1, B)$ is in $\mathrm{Im}(\delta')$ if and only if (2.9) has a non-trivial integral solution. But in general, to determine whether or not (2.9) has such a solution is the unsolved problem. So we call d the element of the Selmer group $S^{(\varphi')}(E'/\mathbb{Q})$ when (2.9) has a solution in $\mathbb{R}$ and in $\mathbb{Q}_p$ for every prime p. Note that the Selmer groups $S^{(\varphi')}(E'/\mathbb{Q})$ and $S^{(\varphi)}(E/\mathbb{Q})$ can be regarded as subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ since the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ are regarded as subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Clearly $S^{(\varphi')}(E'/\mathbb{Q}) \supset \mathrm{Im}(\delta')$ and $S^{(\varphi)}(E/\mathbb{Q}) \supset \mathrm{Im}(\delta)$. Hence the Selmer groups give the upper bound of the rank.

Finally, we see about the 2-Selmer group. Let $E = E'$, $\varphi = [\,2\,]$ on (2.1), then we have

$$\dim_{\mathbb{F}_2} E(\mathbb{Q})/2E(\mathbb{Q}) = \dim_{\mathbb{F}_2} S^{(2)}(E/\mathbb{Q}) - \dim_{\mathbb{F}_2} Ш\,(E/\mathbb{Q})[\,2\,].$$

Suppose that A^2-4B is a square, i.e. the elliptic curve has three rational 2-torsions. Then it holds that

$$\operatorname{rank} E(\mathbb{Q}) \leq \dim_{\mathbb{F}_2} S^{(2)}(E/\mathbb{Q}) - 2$$

by (2.4). The value of the right hand side is called the *2-Selmer rank*. Since there is the exact sequence

$$0 \to S^{(\varphi)}(E/\mathbb{Q}) \to S^{(2)}(E/\mathbb{Q}) \xrightarrow{\varphi} S^{(\varphi')}(E/\mathbb{Q}),$$

the 2-Selmer rank is smaller (or same) than the (φ-)Selmer rank. In Section 8, we study the 2-Selmer rank of the elliptic curve connected with the $\pi/2$ or $\pi/3$-congruent number problem.

2.2. **Hensel's lemma.** When we calculate the Selmer group, Hensel's lemma is a very useful tool. This lemma is often used later. The following version of Hensel's lemma is the most powerful (see Birch and Swinnerton-Dyer [4]).

Lemma 2.2 ([4])**.** *Let $l \in \mathbb{N}$, $x_0 \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[X]$. Suppose that $n = \operatorname{ord}_p(f(x_0))$ and $k = \operatorname{ord}_p(f'(x_0))$. For an odd prime p, consider the question: "Does the equation $y^2 = f(x)$ have an solution $x \in \mathbb{Z}_p$ with $x \equiv x_0 \pmod{p^l}$?" The answer is "yes" if*

- *$f(x_0)$ is a p-adic square, or*
- *$k < l$ and $n \geq k + l$.*

The answer is "no" if

- *$k < l$ and $n < k + l$, or*
- *$k \geq l$ and $n < 2l$.*

The above lemma does not mention the case that $k \geq l$ and $n \geq 2l$. In this case, we can obtain the answer by considering the congruence with a higher power, that is $x \equiv x_0 + p^m x_1 \pmod{p^{l+m}}$ with $m \geq 1$ and $0 \leq x_1 < p$. The similar statement with $p = 2$ is slightly complicated.

Lemma 2.3 ([4])**.** *Let $l \in \mathbb{N}$, $x_0 \in \mathbb{Z}$ and $f(x) \in \mathbb{Z}[X]$. Suppose that $n = \operatorname{ord}_2(f(x_0))$ and $k = \operatorname{ord}_2(f'(x_0))$. Consider the question: "Does the equation $y^2 = f(x)$ have an solution $x \in \mathbb{Z}_2$ with $x \equiv x_0 \pmod{2^l}$?" The answer is "yes" if*

- *$f(x_0)$ is a 2-adic square,*
- *$k < l$ and $n \geq k + l$,*
- *$k < l$ and $n = k + l - 1$ is even, or*
- *$k < l$ and $n = k + l - 2$ is even and the 2-free part of $f(x_0)$ is congruent to 5 modulo 8.*

The answer is "yes" or "no" if

- *$k \geq l$ and $n \geq 2l$, or*
- *$k \geq l$, $n = 2l - 2$ and the 2-free part of $f(x_0)$ is congruent to 5 modulo 8.*

In the other case, the answer is "no".

The following lemma is the special case of Lemmas 2.2 and 2.3 (see Silverman [23, p.322] or Serre [22, p.14]). The statement is simple, but useful.

Lemma 2.4 ([23],[22])**.** *Let p be prime and $f(x) \in \mathbb{Z}[X]$. Suppose that*

$$\operatorname{ord}_p(f(x_0)) > 2 \operatorname{ord}_p(f'(x_0))$$

for some $x_0 \in \mathbb{Z}$. Then the equation $f(x) = 0$ has a solution in $\mathbb{Z}_p$.

3. Overview of the θ-congruent number problem

For the old history about the congruent numbers, see Dickson ([8, pp.459–472]) and Guy ([12, D27]). For example, Genocchi (1855) and/or Bastien (1915) showed that an integer n which has one of the following forms (in which p and q are prime) is not congruent.

(1) $n = p$ with $p \equiv 3 \pmod 8$.
(2) $n = 2p$ with $p \equiv 5 \pmod 8$.
(3) $n = pq$ with $p \equiv q \equiv 3 \pmod 8$.
(4) $n = 2pq$ with $p \equiv q \equiv 5 \pmod 8$.
(5) $n = 2p$ with $p \equiv 9 \pmod{16}$.

In the cases (1),(2),(3),(4), the Selmer rank of the elliptic curve E_n is 0 (cf. Theorems 4.7 and 4.8). Hence we can show the non-congruence of n easily. But in the case (5), calculating the Selmer rank is not sufficient to show it. In fact, the 2-torsion part of the Shafarevich-Tate group is non-trivial in this case.

Serf [21] listed more sequences of non-congruent numbers, calculating the 2-Selmer rank (though he does not mention the Selmer group). But his method is slightly complicated and not enough to calculate the 2-Selmer rank in some cases.

Aoki [1] and Monsky (appendix in Heath-Brown [16]) give each formula for the 2-Selmer rank of the curve E_n defined by (1.1) in different methods. For example, Monsky's formula is

$$2^s = 2k - \operatorname{rank} M,$$

where s is 2-Selmer rank of E_n, k is the number of distinct primes dividing n, and $M \in M_{2k}(\mathbb{F}_2)$ is some matrix defined by Legendre symbols. The author could not apply Monsky's method to the θ-congruent number problem with $\theta \neq \pi/2$, but we shall give an algorithm for the 2-Selmer rank of the elliptic curve connected with $\pi/2$ and $\pi/3$-congruent number problem in Section 8. Roughly speaking, our method is to calculate the images of the connecting homomorphisms. Using this method, we can find more non-congruent numbers containing Serf's results (see Section 9).

While calculating the Selmer groups gives non-congruent numbers, many mathematicians tried to list congruent numbers. In 1986, G. Kramarz listed all congruent numbers up to 2000, calculating the critical values of Hasse-Weil L-function of E_n (see [18, chap.2]). This list was extended by P. Serf (1991, [21]) to 3000, by K. Noda and H. Wada (1993) to 10000 and by F. R. Nemenzo (1998, [20]) to 40000. They used the Coates-Wiles theorem and the Gross-Zagier theorem. These theorems are parts of the Birch and Swinnerton-Dyer conjecture. This conjecture says: "The rank is equal to the *analytic rank*, namely the order of Hasse-Weil L-function at $s = 1$." It is also believed that the parity of the rank is equal to that of the Selmer rank. This conjecture is called the Selmer conjecture. These two conjectures lead a new conjecture: "The parity of the analytic rank is equal to that of the Selmer rank." The parity of the analytic rank can be identified with the *root number*, namely the sign at the functional equation of Hasse-Weil L-function. Part of the last conjecture is proved by Monsky [19]. Consequently, this conjecture is valid about the curve connected with θ-congruent number problem. It is known that the analytic rank of E_n is odd if and only if $n \equiv 5, 6$ or $7 \pmod 8$. Hence the

Selmer rank is also odd in this case. If the Birch and Swinnerton-Dyer conjecture is true, the rank is also odd, hence such n is congruent.

Let us go to the θ-congruent number problem. M. Fujiwara, M, Kan and M. Negiki showed the following theorem.

Theorem 3.1 ([9]). *Let p be a prime. Then*

(1) $p \equiv 5, 7$ *or* $19 \pmod{24} \Rightarrow$ *p is NOT $\pi/3$-congruent.*
(2) $p \equiv 7, 11$ *or* $13 \pmod{24} \Rightarrow$ *p is NOT $2\pi/3$-congruent.*

Most of this theorem can be proved by the Selmer rank. But only the calculation of the Selmer rank is not sufficient to prove the statement

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

In this case, the 2-torsion part of the Shafarevich-Tate group is non-trivial. The proof of this statement is in Kan [15]. Using our method, namely calculating the images of the connecting homomorphisms, we can prove the analogue statements (see Theorem 6.7).

In the cases not mentioned in Theorem 3.1, the Selmer rank is 1 or 2. If the Selmer rank is 1, it is conjectured that the rank is also 1 from the Selmer conjecture. About this topic, Hibino and Kan [13] proved the following theorem, using the theory of the Heegner points.

Theorem 3.2 ([13]). *Let p be a prime congruent to* 23 *modulo* 24. *Then p is $\pi/3$-congruent and $2\pi/3$-congruent.*

Yoshida [30] showed the following theorem at the same time.

Theorem 3.3 ([30]). *Let p be a prime congruent to* 23 *modulo* 24. *Then $p, 2p$ and $3p$ are $2\pi/3$-congruent.*

In the case that the analytic rank is odd, the rank is also odd if the Birch and Swinnerton-Dyer conjecture is true. Hence it is expected that the following conjecture is true.

Conjecture 3.4. *Let n be a positive squarefree integer.*

(1) *If $n \equiv 6, 10, 11, 13, 17, 18, 21, 22$ or $23 \pmod{24}$, then n is $\pi/3$-congruent.*
(2) *If $n \equiv 5, 9, 10, 15, 17, 19, 21, 22$ or $23 \pmod{24}$, then n is $2\pi/3$-congruent.*

In the above cases, the Selmer ranks of the correspondence elliptic curves are odd by Monsky's theorem.

Yoshida [31] also established the analogous result of Tunnel's theorem with $\theta = 2\pi/3$, using the theory of modular forms of half-integral weight and Waldspuger's theorem.

4. The curve $y^2 = x^3 + Dx$

However the main object of this article is the curve $y^2 = x^3 + Ax^2 + Bx$, we study the special curve in this section and the next section. You may skip Sections 4.2, 5 and 6 (in Section 4.1, we define some notations and deduce an useful formula for the Selmer rank). The contents in this section are also in the author's paper [11].

Let D be a non-zero integer. The curve

$$E_D : y^2 = x^3 + Dx$$

is studied by many mathematicians. For example, Birch and Swinnerton-Dyer [4],[5] give the table containing the Selmer rank of E_D with small D. Birch and Stephens [3] give the formula for the parity of the Selmer rank of E_D, and showed the parity is equal to that of the analytic rank. For the curve E_p with a prime p, it is well-known that

$$\text{Selmer rank } = \begin{cases} 2, & \text{if } p \equiv 1 \pmod 8, \\ 1, & \text{if } p \equiv 3, 5, 13, 15 \pmod{16}, \\ 0, & \text{if } p \equiv 7, 11 \pmod{16}. \end{cases} \tag{4.1}$$

Bremner and Cassels [6] studied the curve E_p with $p \equiv 5 \pmod 8$. Yoshida [30] studied the case of D is a product of distinct two primes. Note that the elliptic curve concerned with the congruent number problem (see the equation (1.1)) is also this type with $D = -n^2$. We can suppose without loss of generality that D is a fourth-power free integer and not divided by 4 (if necessary, we must consider the dual curve E_{-4D}, whose $\mathbb{Q}$-rank is equal to that of E_D).

4.1. **Calculating the Selmer group.** In order to calculate the Selmer group, we give formulae for the images of the connecting homomorphisms. For a good prime, namely odd prime not dividing the discriminant of the elliptic curve, we have

$$\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}, \ \mathrm{Im}(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$$

from the local Tate duality. For our curve, this fact can be easily obtained by Theorem 2.1.

In the case that $p = \infty$, it clearly holds that

$$D > 0 \Rightarrow \ \mathrm{Im}(\delta'_\infty) = \{1\}, \mathrm{Im}(\delta_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2},$$
$$D < 0 \Rightarrow \ \mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}, \mathrm{Im}(\delta_\infty) = \{1\}$$

from locus $E_D(\mathbb{R})$. The following propositions give the images of the connecting homomorphisms δ'_p and δ_p for the bad primes of E_D. In this article, we denote by $\langle c_1, \cdots, c_n \rangle$ the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ or $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ for some $p \in M_\mathbb{Q}$ generated by $c_1, \cdots, c_n \in \mathbb{Q}$, and u represents a non-square element modulo p. Note that $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} = \{1, u, p, pu\}$ for odd prime p, and $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} = \{\pm 1, \pm 5, \pm 2, \pm 10\}$.

Proposition 4.1. *Let p be an odd prime dividing D, and $\mathrm{ord}_p(D) = a$, $D = p^a D'$. Then the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$ are obtained as follows:*

1. *If $a = 1$ or 3, then $\mathrm{Im}(\delta'_p) = \langle D \rangle$, $\mathrm{Im}(\delta_p) = \langle -D \rangle$.*
2. *Suppose that $a = 2$ and $p \equiv 1 \pmod 4$.*
   - (a) *If D is a p-adic square, then*
     - (i) $(-D')^{(p-1)/4} \equiv 1 \pmod p \Rightarrow \ \mathrm{Im}(\delta'_p) = \langle p \rangle$, $\mathrm{Im}(\delta_p) = \langle p \rangle$,
     - (ii) $(-D')^{(p-1)/4} \equiv -1 \pmod p \Rightarrow \ \mathrm{Im}(\delta'_p) = \langle pu \rangle$, $\mathrm{Im}(\delta_p) = \langle pu \rangle$.
   - (b) *If D is a p-adic non-square, then $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, $\mathrm{Im}(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.*
3. *Suppose that $a = 2$ and $p \equiv 3 \pmod 4$.*
   - (a) *If D is a p-adic square, then $\mathrm{Im}(\delta'_p) = \{1\}$, $\mathrm{Im}(\delta_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.*
   - (b) *If D is a p-adic non-square, then $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, $\mathrm{Im}(\delta_p) = \{1\}$.*

Note that $(-D')^{(p-1)/4} \equiv 1 \pmod p$ if and only if $-D'$ is a quartic residue modulo p.

Proposition 4.2. *The images $\mathrm{Im}(\delta'_2)$ and $\mathrm{Im}(\delta_2)$ are obtained as follows:*

(1) *If* $D \equiv 1 \pmod 8$, *then* $\mathrm{Im}(\delta_2') = \{1\}$, $\mathrm{Im}(\delta_2) = \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$.
(2) *If* $D \equiv 5 \pmod 8$, *then* $\mathrm{Im}(\delta_2') = \langle 5\rangle$, $\mathrm{Im}(\delta_2) = \mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
(3) *If* $D \equiv 3 \pmod{16}$, *then* $\mathrm{Im}(\delta_2') = \langle -5\rangle$, $\mathrm{Im}(\delta_2) = \langle -2, 5\rangle$.
(4) *If* $D \equiv 7, 11 \pmod{16}$, *then* $\mathrm{Im}(\delta_2') = \mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$, $\mathrm{Im}(\delta_2) = \langle 5\rangle$.
(5) *If* $D \equiv 15 \pmod{16}$, *then* $\mathrm{Im}(\delta_2') = \langle -1\rangle$, $\mathrm{Im}(\delta_2) = \langle 2, 5\rangle$.
(6) *If* D *is even, then* $\mathrm{Im}(\delta_2) = \langle -D\rangle$ *and* $\mathrm{Im}(\delta_2')$ *is given by Theorem 2.1.*

Propositions 4.1 and 4.2 are the special cases of the propositions in Section 7, but we prove these propositions in the next part as a prototype.

Now, We have prepared to calculate Selmer groups $S^{(\varphi')}(E'/\mathbb{Q})$ and $S^{(\varphi)}(E/\mathbb{Q})$.

Example 4.3. Let p be a prime congruent to 1 modulo 8, and consider the curve E_p. From Propositions 4.1 and 4.2, we can obtain the images of the connecting homomorphisms as the following table:

l	$\mathrm{Im}(\delta_l')$	$\mathrm{Im}(\delta_l)$
∞	$\{1\}$	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$
2	$\{1\}$	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
p	$\langle p\rangle$	$\langle p\rangle$

From the definition of the Selmer group (see (2.7)), it is clear that

$$S^{(\varphi')}(E_p'/\mathbb{Q}) = \langle p\rangle,\ S^{(\varphi)}(E_p/\mathbb{Q}) = \langle -1, 2, p\rangle.$$

Hence the Selmer rank is 2 (see (2.6)). In this way, we can show the fact (4.1).

Example 4.4. Let $D = 775 = 5^2 \cdot 31$ and consider the curve E_D. Note that 31 is a quartic residue modulo 5. By Propositions 4.1 and 4.2, the images of the connecting homomorphisms are obtained as follows:

p	$\mathrm{Im}(\delta_p')$	$\mathrm{Im}(\delta_p)$
∞	$\{1\}$	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$
2	$\mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$	$\langle 5\rangle$
5	$\langle 10\rangle$	$\langle 10\rangle$
31	$\langle 31\rangle$	$\langle -31\rangle$

From this table, it is clear that $\langle 5, 31\rangle \subset S^{(\varphi')}(E_D'/\mathbb{Q})$, $\langle -1, 5, 31\rangle \subset S^{(\varphi)}(E_D/\mathbb{Q})$. For a convenience, we define a few notations:

$$S = \{p : \text{bad prime} \mid \mathrm{Im}(\delta_p') - \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \neq \phi\} \cup S_\infty,$$
$$T = \{p : \text{bad prime} \mid \mathrm{Im}(\delta_p) - \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \neq \phi\} \cup T_\infty,$$

where S_∞, T_∞ are the sets defined by

$$\begin{cases} -1 \in \mathrm{Im}(\delta_p) & \Rightarrow \quad S_\infty = \phi,\ T_\infty = \{-1\}, \\ -1 \in \mathrm{Im}(\delta_p') & \Rightarrow \quad S_\infty = \{-1\},\ T_\infty = \phi. \end{cases}$$

For the set X, we denote by V_X the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ generated by all elements of X. In the case of the curve E_D with $D = 775$,

$$S = \{5, 31\},\ T = \{-1, 5, 31\},\ V_S = \langle 5, 31\rangle,\ V_T = \langle -1, 5, 31\rangle.$$

It is clear that $V_S \subset S^{(\varphi')}(E_D/\mathbb{Q})$ and $V_T \subset S^{(\varphi)}(E_D/\mathbb{Q})$. Then we give the matrices Λ', Λ over $\mathbb{F}_2$:

$$\Lambda' = \begin{array}{c} \\ 5 \\ 31 \end{array} \begin{array}{c} \begin{array}{cc} 5 & 31 \end{array} \\ \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \end{array}, \quad \Lambda = \begin{array}{c} \\ -1 \\ 5 \\ 31 \end{array} \begin{array}{c} \begin{array}{ccc} 2 & 5 & 31 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array},$$

where the numbers outside the matrix are the elements of S or T. We shall give the exact definition of the matrices later. Roughly speaking, the meanings of the matrices are as follows. For example, that $(1,1)$-entry of Λ' is 1 means $5 \notin \mathrm{Im}(\delta'_5)$, and that $(1,2)$-entry is 0 means $5 \in \mathrm{Im}(\delta'_{31})$. Therefore that the entries in the second row are all 0 means $31 \in S^{(\varphi')}(E'_D/\mathbb{Q})$. It is clear that $-1, 5, 31 \notin S^{(\varphi)}(E_D/\mathbb{Q})$. But it follows that $-31 \in S^{(\varphi)}(E_D/\mathbb{Q})$ since $V_T/(\mathrm{Im}(\delta_p) \cap V_T)$ are groups of order 2 for $p = 2, 5, 31$. Note that this does not always hold for $p = 2$, and hence the definitions of Λ' and Λ are rather complicated (see the table in p.12) Consequently, $S^{(\varphi')}(E/\mathbb{Q}) = \langle 31 \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle -31 \rangle$, and the Selmer rank of E_{775} is 0.

In general, we have the useful formula

$$\text{Selmer rank } = |S| + |T| - \operatorname{rank}\Lambda' - \operatorname{rank}\Lambda - 2. \tag{4.2}$$

From now on, we use this formula to calculate the Selmer rank. In order to see the validness of the equation (4.2), let us do the elementary transformation and compute the rank of the matrix Λ. Add the first row to the third row, then we have

$$\begin{array}{c} \\ -1 \\ 5 \\ -31 \end{array} \begin{array}{c} \begin{array}{ccc} 2 & 5 & 31 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \end{array}.$$

Note that the meaning of the third row has changed. This expression means the rank of Λ is 2, and the dimension of $S^{(\varphi)}(E_D/\mathbb{Q})$ is $1\,(= |T| - \operatorname{rank}\Lambda)$.

Example 4.5. Let $D = 1975 = 5^2 \cdot 79$. Note that the *type* of 1975 and 775 are almost the same, but 79 is a quartic non-residue modulo 5. In the case that $D = 1975$, the images of the connecting homomorphisms are obtained as follows:

p	$\mathrm{Im}(\delta'_p)$	$\mathrm{Im}(\delta_p)$
∞	$\{1\}$	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$
2	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$	$\langle 5 \rangle$
5	$\langle 5 \rangle$	$\langle 5 \rangle$
79	$\langle 79 \rangle$	$\langle -79 \rangle$

$$\Lambda' = \begin{array}{c} \\ 5 \\ 79 \end{array} \begin{array}{c} \begin{array}{cc} 5 & 79 \end{array} \\ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \end{array}, \quad \Lambda = \begin{array}{c} \\ -1 \\ 5 \\ 79 \end{array} \begin{array}{c} \begin{array}{ccc} 2 & 5 & 79 \end{array} \\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 1 \end{pmatrix} \end{array}.$$

Therefore $S^{(\varphi')}(E'_D) = \langle 5, 79 \rangle$, $S^{(\varphi)}(E_D) = \langle 5, -79 \rangle$ and the Selmer rank is 2 by (4.2). It is fortunate that we can obtain the true rank in this case. Since $\delta'((0,0)) = 79$, $\delta((0,0)) = -79$, the non-trivial elements of the Selmer groups are

essentially only $5 \in S^{(\varphi')}(E'_D/\mathbb{Q})$ and $5 \in S^{(\varphi)}(E_D/\mathbb{Q})$. The element 5 is in $\mathrm{Im}(\delta')$ if and only if

$$N^2 = 5M^4 + 5 \cdot 79e^4$$

has an integer solution with $MNe \neq 0$ (see (2.9)). In fact, the equation has a solution $(M, e, N) = (1, 1, 20)$. Similarly we can see $5 \in \mathrm{Im}(\delta)$, hence the rank is 2.

Definition. We give the exact definition of the matrices Λ', Λ to keep the equation (4.2) valid. First, we define some sets:

$$\begin{aligned}
A_1 &= \{p : \text{odd bad primes} \mid \mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}\},\\
A_2 &= \{p : \text{odd bad primes} \mid \mathrm{Im}(\delta'_p) = \{1\}\},\\
A_3 &= \{p : \text{odd bad primes} \mid \mathrm{Im}(\delta'_p) = \langle p\rangle\},\\
A_4 &= \{p : \text{odd bad primes} \mid \mathrm{Im}(\delta'_p) = \langle pu\rangle\}.
\end{aligned}$$

Then we have $S = A_1 \cup A_3 \cup A_4 \cup A_S$, $T = A_2 \cup A_3 \cup A_4 \cup A_T$, where $A_S, A_T \subset \{-1, 2\}$. Let $(a, b)_p$ be the Hilbert symbol, and 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 $\lambda' : V_S \to (\mathbb{F}_2)^{m'}$ and $\lambda : V_T \to (\mathbb{F}_2)^m$ (m' and m are natural numbers which depend on the curve) as follows:

$$\begin{aligned}
\lambda'(x) &= (*, \quad \{x, -p\}_p \ (p \in A_2 \cup A_3), \quad \{x, -pu\}_p \ (p \in A_4)),\\
\lambda(x) &= (**, \quad \{x, p\}_p \ (p \in A_1 \cup A_3), \quad \{x, pu\}_p \ (p \in A_4)),
\end{aligned}$$

where for example $\{x, pu\}_p$ $(p \in A_4)$ represents the numbers $\{x, pu\}_p$ for all $p \in A_4$ arranged horizontally. And $*, **$ represent the numbers described in the following table.

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

For example, $x \in \mathrm{Im}(\delta_2')$ if and only if the values $*$ in the table above are all 0. Then we have

$$S^{(\varphi')}(E/\mathbb{Q}) = \mathrm{Ker}\,\lambda',\ S^{(\varphi)}(E/\mathbb{Q}) = \mathrm{Ker}\,\lambda.$$

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

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

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

Example 4.6. Let $D = 2pq^2$ with $p \equiv 1$, $q \equiv 3 \pmod 8$, $(q/p) = -1$, and consider the curve E_D. Then we have

l	$\mathrm{Im}(\delta_l')$	$\mathrm{Im}(\delta_l)$
∞	$\{1\}$	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$
2	$\langle 2, -5\rangle$	$\langle -2\rangle$
p	$\langle p\rangle$	$\langle p\rangle$
q	$\{1\}$	$\mathbb{Q}_q^\times/\mathbb{Q}_q^{\times 2}$

$$\Lambda' = \begin{array}{c} \\ 2 \\ p \end{array} \begin{array}{c} \begin{array}{ccc} 2 & p & q \end{array} \\ \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix} \end{array}, \quad \Lambda = \begin{array}{c} \\ -1 \\ 2 \\ p \\ q \end{array} \begin{array}{c} \begin{array}{ccc} 2 & 2' & p \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \end{array}.$$

Since $\mathrm{Im}(\delta_2) = \langle -2\rangle$, the group $V_T/(\mathrm{Im}(\delta_2) \cap V_T)$ is Klein's four group. Therefore the definition of the matrix Λ is slightly complicated. For example, that $(1,1)$-entry of Λ is 0 means $-1 \in \{\pm 1, \pm 2\} \subset \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, and that $(1,2)$-entry is 1 means $-1 \notin \{1, 5, -2, -10\} \subset \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$. From the formula (4.2), the Selmer rank of E_D is 1.

Recall that the curve E_D with $D = -n^2$ is connected with the congruent number problem. Aoki [1] gives the formula of the Selmer rank of this curve. Propositions 4.1 and 4.2 are the extensions of the corresponding facts in [1].

Iskra [14] showed the following theorem.

Theorem 4.7 ([14])**.** *Let primes $p_1, \cdots, p_r$ satisfy the following two conditions:*

- $p_i \equiv 3 \pmod 8$.
- $(p_i/p_j) = 1$ *for* $i < j$, *where* $(\ /\ )$ *is the Legendre Symbol.*

And let $D = -p_1^2 \cdots p_r^2$. Then the rank of the curve E_D is 0.

In this case, the Selmer rank is $2 \cdot [(r-1)/2]$ ([ ] is the Gauss symbol), but the 2-Selmer rank is 0. Iskra proved this theorem by a direct calculation, but this is also deduced by Monsky's formula. We can obtain the analogous facts using the Propositions 4.1, 4.2 and the formula (4.2).

Theorem 4.8. *When D has one of the following forms, the rank of the curve E_D is* 0.

(1) $D = 2p_1 \cdots p_r$ *with* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = 1$ *for* $\forall i \neq j$.
(2) $D = 2p_1 \cdots p_r$ *with r is even,* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = -1$ *for* $\forall i \neq j$.
(3) $D = p_1^2 \cdots p_r^2$ *with* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = 1$ *for* $\forall i \neq j$.
(4) $D = p_1^2 \cdots p_r^2$ *with r is even,* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = -1$ *for* $\forall i \neq j$.

(5) $D = 2p_1^2 \cdots p_r^2$ *with* $p_i \equiv 5 \pmod 8$.
(6) $D = 2p_1^3 \cdots p_r^3$ *with* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = 1$ *for* $\forall i \neq j$.
(7) $D = 2p_1^3 \cdots p_r^3$ *with* r *is even,* $p_i \equiv 5 \pmod 8$ *and* $(p_j/p_i) = -1$ *for* $\forall i \neq j$.

Remark that the cases (3),(4) are connected with the congruent number problem.

Proof. We give only the short proof of (1). In the case that r is even,

l	$\mathrm{Im}(\delta'_l)$	$\mathrm{Im}(\delta_l)$
∞	$\{1\}$	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$
2	$\langle 2, -5\rangle$	$\langle -2\rangle$
p_1	$\langle 2p_1\rangle$	$\langle 2p_1\rangle$
$\vdots$	$\vdots$	$\vdots$
p_r	$\langle 2p_r\rangle$	$\langle 2p_r\rangle$

$$\Lambda' = \begin{array}{c} \\ 2 \\ p_1 \\ \vdots \\ p_r \end{array} \begin{array}{c} \begin{array}{cccc} 2 & p_1 & \cdots & p_r \end{array} \\ \begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & I_r & \\ 1 & & & \end{pmatrix} \end{array}, \qquad \Lambda = \begin{array}{c} \\ -1 \\ 2 \\ p_1 \\ \vdots \\ p_r \end{array} \begin{array}{c} \begin{array}{ccccc} 2 & 2' & p_1 & \cdots & p_r \end{array} \\ \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & & & \\ \vdots & \vdots & & I_r & \\ 1 & 0 & & & \end{pmatrix} \end{array},$$

where I_r is the identity matrix of degree r. Hence we have

$$\text{Selmer rank } = (r+1) + (r+2) - r - (r+1) - 2 = 0,$$

and $\operatorname{rank} E_D(\mathbb{Q}) = 0$. In the case that r is odd, the proof is similar. □

4.2. **Proofs of the propositions.** In this part, we give proofs of Propositions 4.1 and 4.2. In view of Theorem 2.1, it is sufficient that we calculate one of the images $\mathrm{Im}(\delta'_p)$ and $\mathrm{Im}(\delta_p)$.

Proof of Proposition 4.1. Let p be an odd prime dividing D, and $\mathrm{ord}_p(D) = a$, $D = p^a D'$. For $(x, y) \in E(\mathbb{Q}_p)$, we let $\mathrm{ord}_p(x) = e$, $x = p^e w$ $(w \in \mathbb{Z}_p^\times)$, then

$$y^2 = p^{3e}w^3 + p^{e+a}D'w$$
$$= p^{3e}w^3(1 + p^{-2e+a}D'w^{-2}) \tag{4.3}$$
$$= p^{e+a}w(p^{2e-a}w^2 + D') \tag{4.4}$$

from the equation of E_D. If $e \leq (a-1)/2$, then e must be even and $w \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$ by (4.3), hence $x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$. Similarly, if $e \geq (a+1)/2$, then $x \equiv D \pmod{\mathbb{Q}_p^{\times 2}}$ by (4.4).

In the case that $\underline{a = 1 \text{ or } 3}$, the other points do not exist, hence we have proved (1).

From now on, we assume that $\underline{a = 2}$, then we must investigate the set

$$H = \{(x, y) \in E_D(\mathbb{Q}_p) \mid \mathrm{ord}_p(x) = 1\}.$$

We set $a = 2, e = 1$, then

$$y^2 = p^3 w(w^2 + D') \tag{4.5}$$

from (4.4). Therefore when $\underline{(-D'/p) = -1}$, $H = \phi$ and hence $\mathrm{Im}(\delta'_p) = \langle D\rangle$. Now we have proved (2),(b) and (3),(a).

Assume that $\underline{(-D'/p) = 1}$. Let $-D = p^2c^2$ $(c \in \mathbb{Z}_p^\times)$, then

$$y = p^3w(w+c)(w-c)$$

from (4.5). Hence w must be congruent to c or $-c$ modulo p. For example, if $w - c = p^{2n-3}z$ $(n \geq 2,\ z \in \mathbb{Z}_p^\times)$, then

$$y^2 = p^{2n}z(p^{2n-3}z + c)(p^{2n-3}z + 2c).$$

From this representation, $y \in \mathbb{Q}_p$ exists if and only if $z \equiv 2 \pmod{\mathbb{Q}_p^{\times 2}}$. In this case, $x = pw = p(p^{2n-3}z + c) \equiv pc \pmod{\mathbb{Q}_p^{\times 2}}$. When $w + c = p^{2n-3}z$, we have $x \equiv -pc \pmod{\mathbb{Q}_p^{\times 2}}$. Hence we have $\delta_p'(H) = \{\pm pc\}$. Therefore $\mathrm{Im}(\delta_p') = \{1, D, pc, -pc\} = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ in the case that $\underline{p \equiv 3 \pmod 4}$. We have proved (3),(b). When $\underline{p \equiv 1 \pmod 4}$, it follows that $\mathrm{Im}(\delta_p') = \{1, pc\} = \langle p\rangle$ or $\langle pu\rangle$ according as c is a quadratic residue modulo p or not, i.e. $-D'$ is a quartic residue modulo p or not. □

Proof of Proposition 4.2. Firstly, we assume that $\underline{D \text{ is odd}}$. Let $(x, y) \in E_D(\mathbb{Q}_2)$, then

$$\begin{array}{lll} \mathrm{ord}_2(x) > 1 & \Rightarrow & x \equiv D \pmod{\mathbb{Q}_2^{\times 2}}, \\ \mathrm{ord}_2(x) < -1 & \Rightarrow & x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}. \end{array}$$

We must consider the points of $\mathrm{ord}_2(x) = 0$, so we let

$$H_n = \{(x, y) \in E_D(\mathbb{Q}_2) \mid \mathrm{ord}_2(x) = 0,\ \mathrm{ord}_2(y) = n\} \quad (n \geq 1).$$

If $\underline{D \equiv 1 \pmod 4}$, then $\cup H_n = \phi$ since $\mathrm{ord}_2(x^3 + Dx) = 1$. Hence $\mathrm{Im}(\delta_2') = \langle D\rangle$, and we have proved (1) and (2).

Secondly, if $\underline{D \equiv 3 \pmod 8}$, then $\cup_{n=2}^\infty H_n = \phi$ since $\mathrm{ord}_2(x^3 + Dx) = 2$. We must investigate the set H_1. For example, when $D \equiv 3 \pmod{32}$,

$$x^3 + Dx \in \mathbb{Q}_2^{\times 2} \iff x^3 + Dx \equiv 4 \pmod{32} \iff x \equiv 1, 3 \pmod{16}.$$

Therefore it follows that $\delta_2'(H_1) = \{1, -5\}$, and $\mathrm{Im}(\delta_2') = \langle -5\rangle$. In the other case, a similar discussion shows that $\mathrm{Im}(\delta_2') = \langle -5\rangle$ or $\langle -1, 5\rangle$ according as $D \equiv 3$ or $11 \pmod{16}$.

Thirdly, if $\underline{D \equiv 7 \pmod 8}$, then $H_1 = \phi$ since $\mathrm{ord}_2(x^3 + Dx) \geq 3$. We must investigate the set H_n $(n \geq 2)$. We let $-D = c^2$ $(c \in \mathbb{Z}_2^\times)$, then

$$y^2 = x(x + c)(x - c)$$

from the equation of E_D. Hence x must be congruent to c or $-c$ modulo 8. For example, if $x - c = 2^{2n-1}w$ $(w \in \mathbb{Q}_2^\times)$, then

$$y^2 = 2^{2n}w(w^{2n-1}w + c)(2^{2n-2}w + c).$$

From this representation, $y \in \mathbb{Q}_p$ exists if and only if $w \equiv 5 \pmod 8$ for $n = 2$, and $w \equiv 1 \pmod 8$ for $n \geq 3$. In both cases, $x = 2^{2n-1}w + c \equiv c \pmod{\mathbb{Q}_2^{\times 2}}$. Hence we have $\delta_2'(\cup H_n) = \{\pm c\}$. Moreover when $D \equiv 7 \pmod{16}$, it holds that $c \equiv \pm 5 \pmod 8$ and $\mathrm{Im}(\delta_2') = \mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$. When $D \equiv 15 \pmod{16}$, it holds that $c \equiv \pm 1 \pmod 8$ and $\mathrm{Im}(\delta_2') = \langle -1\rangle$.

Lastly, we assume that $\underline{D = 2D' \text{ is even}}$. We study $\mathrm{Im}(\delta_2)$ rather than $\mathrm{Im}(\delta_2')$ since the structure of E_{-4D} is simpler than that of E_D. We let $x = 2^e w$ ($w \in \mathbb{Z}_2^\times$), then

$$\begin{aligned} y^2 &= 2^{3e}w^3 - 2^{e+3}D'w \\ &= 2^{e+3}w(w^{2e-3}w^2 - D') \qquad (4.6) \\ &= 2^{3e}w^3(1 - 2^{-2e+3}D'w^{-2}) \qquad (4.7) \end{aligned}$$

from the equation of E_{-4D}. If $e \leq 0$, then $x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$ by (4.6). If $e \geq 3$, then $x \equiv -D \pmod{\mathbb{Q}_2^{\times 2}}$ by (4.7). Moreover, we find that the points of $e = 1, 2$ do not exist. Therefore we have $\mathrm{Im}(\delta_2) = \langle -D \rangle \pmod{\mathbb{Q}_2^{\times 2}}$. □

5. The curve $y^2 = x(x-\alpha)(x-\beta)$

In this section, we give formulae for the images of the connecting homomorphisms of the curve $y^2 = x(x-\alpha)(x-\beta)$, where α, β are non-zero distinct rational numbers. The contents in this section and the next section are also in the author's paper [10]. Without loss of generality, we can assume that α, β are integers and $\gcd(\alpha, \beta)$ is squarefree. From the locus $E(\mathbb{R})$ the images of δ_∞' and δ_∞ are clearly given as follows.

(1) If $\alpha > 0$ and $\beta > 0$, then $\mathrm{Im}(\delta_\infty') = \{1\}$, $\mathrm{Im}(\delta_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$.
(2) If $\alpha < 0$ or $\beta < 0$, then $\mathrm{Im}(\delta_\infty') = \mathbb{R}^\times/\mathbb{R}^{\times 2}$, $\mathrm{Im}(\delta_\infty) = \{1\}$.

The discriminant of the curve 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.

5.1. **Formulae for the images of the connecting homomorphisms.** Firstly, we give the statement for odd primes which divide both α and β.

Proposition 5.1. *Let p be an odd prime. If $\mathrm{ord}_p(\alpha) \geq 1$, $\mathrm{ord}_p(\beta) = 1$, 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 5.2. *Let p be an odd prime. Suppose that $\mathrm{ord}_p(\alpha) = a \geq 1$ and $p \nmid \beta$. Then the following holds.*

(1) *If a is even and $(-\beta/p) = -1$, then $\mathrm{Im}(\delta_p') = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$, $\mathrm{Im}(\delta_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.*
(2) *In the other case, $\mathrm{Im}(\delta_p') = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, $\mathrm{Im}(\delta_p) = \{1\}$.*

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

Proposition 5.3. *Let p be an odd prime. Suppose that $\mathrm{ord}_p(\alpha-\beta)\geq 1$ and $p\nmid\alpha$. Then the following holds.*

(1) *If $(\alpha/p)=1$, then $\mathrm{Im}(\delta'_p)=\{1\},\ \mathrm{Im}(\delta_p)=\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.*
(2) *If $(\alpha/p)=-1$, then $\mathrm{Im}(\delta'_p)=\mathbb{Z}_p^\times\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2},\ \mathrm{Im}(\delta_p)=\mathbb{Z}_p^\times\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.*

Lastly, we consider the case that $p=2$.

Proposition 5.4. *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 $\mathrm{Im}(\delta'_2)=\mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.*
(2) *If $\mathrm{ord}_2(\alpha-\beta)=3$ and $\alpha\equiv 3\pmod 4$, then $\mathrm{Im}(\delta'_2)=\mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.*
(3) *If $\mathrm{ord}_2(\alpha-\beta)=4$ and $\alpha\equiv 1\pmod 8$, then $\mathrm{Im}(\delta'_2)=\langle 5\rangle$.*

Proposition 5.5. *If $\mathrm{ord}_2(\alpha)=1$, $\mathrm{ord}_2(\beta)=0$, then*

$$\mathrm{Im}(\delta'_2)=\langle\alpha,\beta,5\rangle.$$

Proposition 5.6. *Suppose that $\mathrm{ord}_2(\alpha)=\mathrm{ord}_2(\beta)=1$. Then the following holds.*

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

Proposition 5.7. *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 5.8. *Suppose that $\mathrm{ord}_2(\alpha)=a\geq 2$, $\mathrm{ord}_2(\beta)=0$ and put $\alpha=2^a\alpha'$ ($\alpha'\in\mathbb{Z}_2^\times$). Then images $\mathrm{Im}(\delta'_2)$ and $\mathrm{Im}(\delta_2)$ are obtained as the following table:*

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

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

Example 5.9. Consider the elliptic curve

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

If the $\mathbb{Q}$-rank of E were positive, 483 would be 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 obtained as the following table:

p	$\mathrm{Im}(\delta_p')$	$\mathrm{Im}(\delta_p)$
∞	$\mathbb{R}^\times/\mathbb{R}^{\times 2}$	$\{1\}$
2	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$	$\langle 5\rangle$
3	$\mathbb{Q}_3^\times/\mathbb{Q}_3^{\times 2}$	$\{1\}$
7	$\mathbb{Q}_7^\times/\mathbb{Q}_7^{\times 2}$	$\{1\}$
23	$\mathbb{Q}_{23}^\times/\mathbb{Q}_{23}^{\times 2}$	$\{1\}$

Recall that Selmer group $S^{(\varphi')}(E'/\mathbb{Q})$ is the intersection of all $\mathrm{Im}(\delta_p')$ regarded as subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Therefore by the above table it is clear that $S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, 7, 23\rangle$ and $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$. It follows that $\mathrm{rank}\, E(\mathbb{Q}) \leq 2$ by (2.6).

By some translation, the curve E will be

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

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

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

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

From this matrices we have $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, 483\rangle$, $S^{(\varphi)}(E'/\mathbb{Q}) = \{1\}$. Hence it follows that $\operatorname{rank} F(\mathbb{Q}) = 0$ and 483 is not congruent.

The curves E and F are essentially the same. But 2-isogenies given in Section 2 are different. As we have seen, the Selmer rank can change by a change of the 2-isogenies. So we can take the smallest bound of the three. But the 2-Selmer rank is smaller (or same) than these Selmer ranks.

5.2. **Proofs of the propositions.** Recall that our elliptic curve and the dual curve are given by the equations

$$E \,:\, y^2 = x(x-\alpha)(x-\beta) = x^3 - (\alpha+\beta)x^2 + \alpha\beta x,$$
$$E' \,:\, y^2 = x^3 - 2(\alpha+\beta)x^2 + (\alpha-\beta)^2 x,$$

where α, β are non-zero distinct integers and $\gcd(\alpha, \beta)$ is squarefree. We define subsets of $E(\mathbb{Q}_p)$ as follows ([26]):

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

where the tilde means the reduction modulo p and $\tilde{E}_{\mathrm{ns}}$ is the set of non-singular points of $\tilde{E}$. If $(0,0) \in \tilde{E}$ is singular, then

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

If $(0,0) \in \tilde{E}$ is non-singular, then

$$E_0(\mathbb{Q}_p) \subset \{(x,y) \in E(\mathbb{Q}_p) \mid \operatorname{ord}_p(x) \ne 0\} \cup \{\mathcal{O}\}.$$

The order of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ can be obtained by Tate's algorithm (see Tate [26] or Cremona [7, pp.64–68], but this algorithm is not used in this article). If the representatives of $E(\mathbb{Q}_p)/E_0(\mathbb{Q}_p)$ and $\delta'_p(E_0(\mathbb{Q}_p))$ are given, we can obtain the image $\operatorname{Im}(\delta'_p)$. This method owes its origin to Aoki [1]. The following lemma describes the cases that the order of the x-coordinate is enough small or large.

Lemma 5.10. *Let p be an odd prime and consider the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ with $\operatorname{ord}_p(A) = a$, $\operatorname{ord}_p(B) = b$. Suppose that (x,y) is a $\mathbb{Q}_p$-point on the curve and $x = p^e w$ with $e = \operatorname{ord}_p(x)$, $w \in \mathbb{Z}_p^\times$. Then*

$$e \le \min\left\{a-1, \frac{b-1}{2}\right\} \;\Rightarrow\; x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}},$$
$$e \ge \max\left\{-a+b+1, \frac{b+1}{2}\right\} \;\Rightarrow\; x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}.$$

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

$$y^2 = p^{3e}w^3 + p^{2e+a}A'w^2 + p^{e+b}B'w$$
$$= p^{3e}w^3(1 + p^{-e+a}A'w^{-1} + p^{-2e+b}B'w^{-2}) \tag{5.1}$$
$$= p^{e+b}w(p^{2e-b}w^2 + p^{e+a-b}A'w + B'). \tag{5.2}$$

If $-e+a \geq 1$ and $-2e+b \geq 1$, then e must be even and $w \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$ by (5.1). Hence we have $x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$. If $2e-b \geq 1$ and $e+a-b \geq 1$, then $e+b$ must be even and $w \equiv B' \pmod{\mathbb{Q}_p^{\times 2}}$ by (5.2). Hence we have $x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$. □

For our elliptic curve, we have

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

since α, β are integers. In particular, if $a \geq 1$, $b \geq 1$, then

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

When $p = 2$, the different situation occurs.

Lemma 5.11. *Consider the elliptic curve $y^2 = x^3 + Ax^2 + Bx$ with $\mathrm{ord}_2(A) = a$, $\mathrm{ord}_2(B) = b$. Suppose that (x, y) is a $\mathbb{Q}_2$-point on the curve and $x = 2^e w$ with $e = \mathrm{ord}_2(x)$, $w \in \mathbb{Z}_2^{\times}$. Then*

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

$$e \geq \max\left\{-a+b+3, \ \frac{b+3}{2}\right\} \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}.$$

Proof. The proof is similar to that of the previous lemma. □

For our elliptic curve $E_{\alpha,\beta}$,

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

since α, β are integers. In particular, if $a \geq 1$, then

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

Remark. The following equation appears in the proof of Lemma 5.11 (see the proof of Lemma 5.10):

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

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 $x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$. It is sufficient that $-e+a \geq 3$, $-2e+b \geq 3$, then we obtained Lemma 5.11. 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 $x \equiv 5 \pmod{\mathbb{Q}_2^{\times 2}}$.

We prepare one more lemma.

Lemma 5.12. *Let (x, y) be a point on $E(\mathbb{Q}) \backslash E[2]$. 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. □

The following lemma is a key of Proposition 5.1.

Lemma 5.13. *Let p be an odd prime. Suppose that $\mathrm{ord}_p(\alpha) = a \geq 1$, $\mathrm{ord}_p(\beta) = 1$. Consider a point $(x, y) \in E(\mathbb{Q}_p)$. If $a = 1$, then the following holds.*

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

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

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

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

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

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

The formulae in Lemma 5.12 are used many times. The y-coordinates are not important, so they are represented by $\square$. First, we see the case that $a = 1$.

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

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

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

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

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

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

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

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

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

Proof of Proposition 5.1. By Lemma 5.10, $\delta'_p(E_0(\mathbb{Q}_p)) = \{1\}$. Hence the proposition holds by Lemma 5.13. □

Lemma 5.13 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 5.14. *Let E be an elliptic curve defined by $y^2 = x^3 + Ax^2 + Bx$ with $A, B \in \mathbb{Z}$. Suppose that p is an odd prime and $\mathrm{ord}_p(A) = 0$, $\mathrm{ord}_p(B) = b \geq 1$, $P = (x, y) \in E(\mathbb{Q}_p)$. Then the following holds.*

(1) *If $\mathrm{ord}_p(x) \leq 0$, then $P \equiv \mathcal{O} \pmod{E_0(\mathbb{Q}_p)}$.*
(2) *If $\mathrm{ord}_p(x) \geq b$, then $P \equiv (0,0) \pmod{E_0(\mathbb{Q}_p)}$.*
(3) *If $(A/p) = -1$, then there does not exist a point with $1 \leq \mathrm{ord}_p(x) \leq b-1$. If $(A/p) = 1$, then there exist points with $\mathrm{ord}_p(x) = 1, 2, \cdots, b-1$, and any elements of $\mathbb{Z}_p^\times$ appear in the 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 point $(0, 0)$ at this curve is singular, we have

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

So the statement is clear.
(2) By Lemma 5.12,

$$P + (0, 0) = \left(\frac{B}{x}, \square\right) \in E_0(\mathbb{Q}_p).$$

Hence $P \equiv (0, 0) \pmod{E_0(\mathbb{Q}_p)}$.
(3) Let $x = p^e w$ with $1 \leq e \leq b-1$, $w \in \mathbb{Z}_p^\times$ and suppose that $B = p^b B'$, then

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

Note that $e \geq 1$, $-e + b \geq 1$. The number $y \in \mathbb{Q}_p$ exists if and only if A is a square modulo p. In this case, e and w may be arbitrary. □

The following lemma is also used in the proof of Proposition 5.2.

Lemma 5.15. *Let p be an odd prime. Suppose that $\mathrm{ord}_p(\alpha) = a \geq 1$ and $p \nmid \beta$. Then we have*

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

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

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

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

Since $\beta \in (\mathbb{Z}/p\mathbb{Z})^\times$, 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 5.2. In view of Theorem 2.1, we must consider only $\mathrm{Im}(\delta'_p)$. By Lemma 5.15, $\mathrm{Im}(\delta'_p) \supset \{1, u\}$. 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 5.14, we have $\mathrm{Im}(\delta'_p) = \{1, u, p, pu\}$.

Lastly, suppose that a is even and $(-\beta/p) = -1$. Let $P = (x, y) \in E(\mathbb{Q}_p)$. By Lemma 5.10, if $\mathrm{ord}_p(x) < 0$, then $x \equiv 1 \pmod{\mathbb{Q}^{\times 2}}$. If $\mathrm{ord}_p(x) = 0$, then $x \equiv 1$ or $u \pmod{\mathbb{Q}^{\times 2}}$. By Lemma 5.14, there does not exist a point of order which is from 1 to $a-1$. If $\mathrm{ord}_p(x) \geq a$, then $P \equiv (0,0) \pmod{E_0(\mathbb{Q}_p)}$, so $x \equiv 1$ or $u \pmod{\mathbb{Q}^{\times 2}}$. We have found that p and pu do not appear, hence $\mathrm{Im}(\delta'_p) = \{1, u\}$. □

Next, we prove Proposition 5.3 by calculating the image $\mathrm{Im}(\delta_p)$. The following lemma is used in the proof.

Lemma 5.16. *Let p be an odd prime. Suppose that $\mathrm{ord}_p(\alpha - \beta) \geq 1$ and $p \nmid \alpha$. Then we have*

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

Proof. The equation of E' is

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

Hence the point $(0,0)$ at E' is singular, and

$$E'_0(\mathbb{Q}_p) = \{(x, y) \in E'(\mathbb{Q}_p) \mid \mathrm{ord}_p(x) \leq 0\}.$$

We shall show that there exists $x \in \mathbb{Z}_p^\times$ such that $x \equiv -2(\alpha+\beta) \pmod{p}$ and the right hand side is in $\mathbb{Q}_p^{\times 2}$. This fact can be shown by Hensel's lemma, but we prove it more elementarily. Let $x = p^e z - 2(\alpha+\beta)$ with $e \in \mathbb{N}$, $z \in \mathbb{Z}_p^\times$ and $\alpha - \beta = p^b \gamma$ with $b \in \mathbb{N}$, $\gamma \in \mathbb{Z}_p^\times$, then

$$y^2 = x^2(p^e z) + p^{2b}\gamma^2 x = p^e x^2 (z + p^{2b-e}\gamma^2 x^{-1}). \tag{5.3}$$

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

$$\text{the right hand side of (5.3)} \quad = p^2 x^2 z + p^2 \gamma^2 x = p^2 x^2 (z + \gamma^2 x^{-1}).$$

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

Let us come back to the proof of the lemma. If $-2(\alpha+\beta)$ is a non-square modulo p, the proposition holds by the above fact. Suppose that it is a square. Putting $x = -4(\alpha+\beta)$ the right side hand is a square, so the proposition holds if $-4(\alpha+\beta)$ is a 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 5.3. By Lemma 5.16, 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 5.14. □

We prepare lemmas in order to prove Proposition 5.4.

Lemma 5.17. *Suppose that* $\mathrm{ord}_2(\alpha)=0$, $\mathrm{ord}_2(\beta)=0$, $\mathrm{ord}_2(\alpha-\beta)=1$. *Consider a point* $(x,y)\in E(\mathbb{Q}_2)$. *Then the following holds.*

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

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

Proof. (1) By Lemma 5.12, $P+(0,0)=\left(\dfrac{\alpha\beta}{x},\square\right)\in E_1(\mathbb{Q}_2)$. Hence $P\equiv(0,0) \pmod{E_1(\mathbb{Q}_2)}$.
(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 $2^{a+1}\,|\,\alpha-\beta$. This is contradictory to the assumption $\mathrm{ord}_2(\alpha-\beta)=1$. For example, if $\mathrm{ord}_2(x-\alpha)>\mathrm{ord}_2(x-\beta)$, then

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

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

Lemma 5.17 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. The point which is not equivalent to any trivial point modulo $E_1(\mathbb{Q}_2)$ must be in $E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)$. So we need the following lemma.

Lemma 5.18. *Suppose that* $\mathrm{ord}_2(\alpha)=0$, $\mathrm{ord}_2(\beta)=0$, $\mathrm{ord}_2(\alpha-\beta)\geq 2$. *Then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2))\subset\langle\alpha,\beta\rangle$ *except the following three cases.*

(1) *If* $\mathrm{ord}_2(\alpha-\beta)=2$ *and* $\alpha+\beta\equiv 14 \pmod{16}$, *then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2))=\{\pm1,\pm5\}$.
(2) *If* $\mathrm{ord}_2(\alpha-\beta)=3$ *and* $\alpha\equiv 3 \pmod 4$, *then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2))=\{-1,\pm5\}$.
(3) *If* $\mathrm{ord}_2(\alpha-\beta)=4$ *and* $\alpha\equiv 1 \pmod 8$, *then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2))=\{1,5\}$.

Proof. Consider a point $(x,y)\in E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)$. Let $x=2^e z+\alpha$ with $e\geq 1$, $z\in\mathbb{Z}_2^\times$. We investigate how x appears for each number e. If $e\geq 3$, then $x\equiv\alpha \pmod{\mathbb{Q}_2^{\times 2}}$. In fact, there is such a point $(\alpha,0)$, so we must consider only the points of $e=1,2$.

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

$$\begin{aligned}\left(\frac{y}{2}\right)^2&=z(2z+\alpha)\left(z+\frac{\alpha-\beta}{2}\right)\\ &\equiv 2\alpha-\beta+\frac{\alpha(\alpha-\beta)+4}{2}z \pmod 8. \qquad (5.4)\end{aligned}$$

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

$$\begin{aligned}\left(\frac{y}{4}\right)^2&=z(4z+\alpha)\left(z+\frac{\alpha-\beta}{4}\right)\\ &\equiv 2\alpha-\beta+\frac{\alpha(\alpha-\beta)+16}{4}z \pmod 8. \qquad (5.5)\end{aligned}$$

The last expression must be congruent to 1 modulo 8.

In the case that $\mathrm{ord}_2(\alpha-\beta)=2$, we must consider only the points of $e=1$. The expression (5.4) 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 (5.4) is congruent to 1 modulo 8 if and only if $\beta \equiv 13 \pmod{16}$. In this way, 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 $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{\pm 1, \pm 5\}$.

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 (5.4) 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 (5.5) 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 $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{-1, \pm 5\}$ 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 (5.4) 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 (5.5) 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 $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{1, 5\}$ 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 (5.5) 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 5.4. By Lemma 5.11, $\delta_2'(E_1(\mathbb{Q}_2)) = \{1\}$. When $\mathrm{ord}_2(\alpha-\beta) = 1$, the proposition holds by Lemma 5.17. When $\mathrm{ord}_2(\alpha-\beta) \geq 2$, it holds that

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

(see the proof of Lemma 5.17). So $\mathrm{Im}(\delta_2')$ is generated by $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2))$ and $\delta_2'(E[2])$. Hence the proposition holds by Lemma 5.18. □

We proof the Proposition 5.5.

Lemma 5.19. *Suppose that* $\mathrm{ord}_2(\alpha)=1$, $\mathrm{ord}_2(\beta)=0$. *Consider a point* $(x,y) \in E(\mathbb{Q}_2)$. *Then the following holds.*

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

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

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

Proof. The proof is similar to that of Lemma 5.13. □

Proof of Proposition 5.5. By Lemma 5.11, we have $\delta_2'(E_2(\mathbb{Q}_2)) = \{1\}$. By the remark below Lemma 5.11, we have $\delta_2'(E_1(\mathbb{Q}_2)\backslash E_2(\mathbb{Q}_2)) = \{5\}$. Hence the proposition holds by Lemma 5.19. □

We prove Proposition 5.6.

Lemma 5.20. *Suppose that* $\mathrm{ord}_2(\alpha) = \mathrm{ord}_2(\beta) = 1$. *Consider a point* $(x, y) \in E(\mathbb{Q}_2)$. *Then the following holds.*

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

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

Proof. The proof is similar to that of Lemma 5.13. □

Proof of Proposition 5.6. First, suppose that $\mathrm{ord}_2(\alpha-\beta) = 2$, then $\mathrm{ord}_2(\alpha+\beta) \geq 3$. By the remark below Lemma 5.11, we have $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{5\}$. Hence $\mathrm{Im}(\delta_2') = \langle \alpha, \beta, 5\rangle = \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ by Lemma 5.20.

Next, suppose that $\mathrm{ord}_2(\alpha - \beta) \geq 3$, then $\mathrm{ord}_2(\alpha + \beta) = 2$. By the remark below Lemma 5.11, we have $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{1\}$. Hence $\mathrm{Im}(\delta_2') = \langle \alpha, \beta\rangle$ by Lemma 5.20. In particular, 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 prepare the lemmas to prove Proposition 5.7.

Lemma 5.21. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2, \mathrm{ord}_2(\beta) = 1$. *Consider a point* $(x, y) \in E(\mathbb{Q}_2)$. *Then the following holds.*

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

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

Proof. The proof is similar to that of Lemma 5.13. □

Lemma 5.22. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2, \mathrm{ord}_2(\beta) = 1$. *Consider a point* $(x, y) \in E(\mathbb{Q}_2)$. *Then the following holds.*

(1) *If* $\alpha + \beta \equiv 2 \pmod 8$, *then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{-5\}$.
(2) *If* $\alpha + \beta \equiv 6 \pmod 8$, *then* $\delta_2'(E_0(\mathbb{Q}_2)\backslash E_1(\mathbb{Q}_2)) = \{-1\}$.

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 5.7. By Lemma 5.11, we have $\delta_2'(E_1(\mathbb{Q}_2)) = \{1\}$. So the proposition follows immediately from Lemmas 5.21 and 5.22. □

Lastly, we prove Proposition 5.8.

Lemma 5.23. *Suppose that* $\mathrm{ord}_2(\alpha) = a \geq 2, \mathrm{ord}_2(\beta) = 0$. *Consider a point* $(x, y) \in E(\mathbb{Q}_2)$. *Then the following holds.*

(1) *If* $\mathrm{ord}_2(x) \geq a+1$, *then* $P \equiv (0,0) \pmod{E_1(\mathbb{Q}_2)}$.
(2) *If* $\mathrm{ord}_2(x) = a$, *then* $P \equiv (\alpha, 0) \pmod{E_1(\mathbb{Q}_2)}$.
(3) *If* $\mathrm{ord}_2(x) = 0$, *then* $P \equiv (\beta, 0) \pmod{E_1(\mathbb{Q}_2)}$.

Proof. The proof is similar to that of Lemma 5.13. □

Lemma 5.23 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 5.8.

Proof of Proposition 5.8. From the remark below Lemma 5.11, it follows that $\delta_2'(E_1(\mathbb{Q}_2)\backslash E_2(\mathbb{Q}_2)) = \{5\}$ 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 5.11, $\delta_2'(E_2(\mathbb{Q}_2)) = \{1\}$. In view of Lemma 5.23, we must consider the points of $1 \leq \mathrm{ord}_2(x) \leq a-1$.

The equation of E is

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

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

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

Suppose that $1 \leq e \leq a-1$, then $e \geq 1$, $-e+a \geq 1$. Put $X = 2^e w + 2^{-e+a} B' w^{-1}$, then $\mathrm{ord}_2(X) \geq 1$ 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 $e \geq 1$, $-e+a \geq 1$, and the contribution of such points to $\mathrm{Im}(\delta_2')$, we have the table in the proposition. □

6. Application to the θ-congruent number problem

In this section, we apply the result in Section 5 to the θ-congruent number problem. Recall that the θ-congruent number problem is connected with the elliptic curve $E_{n,\theta}$ defined by (1.2).

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 $3p$, then we have the following theorems which give the Selmer groups of our elliptic curves.

Theorem 6.1. *For* $E = E_{p,\frac{\pi}{3}}$ $(n = p, \theta = \pi/3)$, *we have the following.*

(1) $p \equiv 1 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p\rangle$,
(2) $p \equiv 5, 7, 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 11, 17, 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(4) $p \equiv 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p\rangle$.

Therefore, the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1 \pmod{24}, \\ 1, & \text{if } p \equiv 11, 13, 17, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 5, 7, 19 \pmod{24}. \end{cases}$

Theorem 6.2. *For* $E = E_{2p, \frac{\pi}{3}}$ $(n = 2p, \theta = \pi/3)$*, we have the following.*

(1) $p \equiv 1 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(2) $p \equiv 5, 17 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 7, 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, 2p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(4) $p \equiv 11, 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(5) $p \equiv 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$.

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1, 19 \pmod{24}, \\ 1, & \text{if } p \equiv 5, 11, 17, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 7, 13 \pmod{24}. \end{cases}$

Theorem 6.3. *For* $E = E_{3p, \frac{\pi}{3}}$ $(n = 3p, \theta = \pi/3)$*, we have the following.*

(1) $p \equiv 1, 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(2) $p \equiv 5, 11, 17, 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 7 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(4) $p \equiv 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -p \rangle$, $S^{(\varphi)} = \langle 3 \rangle$.

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1, 13 \pmod{24}, \\ 1, & \text{if } p \equiv 7, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 5, 11, 17, 19 \pmod{24}. \end{cases}$

Theorem 6.4. *For* $E = E_{p, \frac{2\pi}{3}}$ $(n = p, \theta = 2\pi/3)$*, we have the following.*

(1) $p \equiv 1, 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(2) $p \equiv 5, 17, 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 7, 11 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(4) $p \equiv 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$.

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1, 13 \pmod{24}, \\ 1, & \text{if } p \equiv 5, 17, 19, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 7, 11 \pmod{24}. \end{cases}$

Theorem 6.5. *For* $E = E_{2p, \frac{2\pi}{3}}$ $(n = 2p, \theta = 2\pi/3)$*, we have the following.*

(1) $p \equiv 1 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(2) $p \equiv 5, 17 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 7 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,
(4) $p \equiv 11, 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, -p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(5) $p \equiv 13, 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, -2p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1, 7 \pmod{24}, \\ 1, & \text{if } p \equiv 5, 11, 17, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 13, 19 \pmod{24}. \end{cases}$

Theorem 6.6. *For* $E = E_{3p, \frac{2\pi}{3}}$ $(n = 3p, \theta = 2\pi/3)$*, we have the following.*

(1) $p \equiv 1 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 3, p \rangle$,
(2) $p \equiv 5, 11, 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$,
(3) $p \equiv 7, 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 3p \rangle$,
(4) $p \equiv 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p \rangle$,

(5) $p \equiv 17 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1 \pmod{24}, \\ 1, & \text{if } p \equiv 5, 7, 11, 13, 19, 23 \pmod{24}, \\ 0, & \text{if } p \equiv 17 \pmod{24}. \end{cases}$

From these theorems, we obtain the following result.

Theorem 6.7. *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* $13 \pmod{24} \Rightarrow$ *$2p$ is NOT $\pi/3$-congruent.*
(3) $p \equiv 5, 11, 17$ *or* $19 \pmod{24} \Rightarrow$ *$3p$ is NOT $\pi/3$-congruent.*
(4) $p \equiv 7$ *or* $11 \pmod{24} \Rightarrow$ *p is NOT $2\pi/3$-congruent.*
(5) $p \equiv 13$ *or* $19 \pmod{24} \Rightarrow$ *$2p$ is NOT $2\pi/3$-congruent.*
(6) $p \equiv 17 \pmod{24} \Rightarrow$ *$3p$ is NOT $2\pi/3$-congruent.*

Some of these results have already been proved by Fujiwara [9] (see Theorem 3.1), and Yoshida [30] also proved all of them by a direct calculation. But the method in this article makes the calculation easier for arbitrary θ and n. The tables in Section 9 contain the curves with another n and $\theta = \pi/3$. The following lemmas are useful to calculate the Selmer groups for $E_{n,\frac{\pi}{3}}$.

Lemma 6.8. *For $E_{n,\frac{\pi}{3}}$, the images of the connecting homomorphisms δ'_p are given as follows.*

(1) *Let p (≥ 5) be a prime which divides n, then*

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

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

(3) $\mathrm{Im}(\delta'_2) = \begin{cases} \langle 5\rangle, & \text{if } n \equiv 5 \pmod{8}, \\ \mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}, & \text{if } n \equiv \pm 1, -5 \pmod{8}, \\ \langle 2, 5\rangle, & \text{if } n \equiv 2 \pmod{8}, \\ \langle -2, 5\rangle, & \text{if } n \equiv -2 \pmod{8}. \end{cases}$

Proof. This is the immediate consequence of Propositions 5.1, 5.2, 5.4 and 5.6. □

Lemma 6.9. *For $E_{n,\frac{\pi}{3}}$, the images of the connecting homomorphisms δ_p are given as follows.*

(1) *Let p (≥ 5) 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) $\mathrm{Im}(\delta_2) = \begin{cases} \mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}, & \text{if } n \equiv 5 \pmod{8}, \\ \langle 5\rangle, & \text{if } n \equiv \pm 1, -5 \pmod{8}, \\ \langle -1\rangle, & \text{if } n \equiv 2 \pmod{8}, \\ \langle -5\rangle, & \text{if } n \equiv -2 \pmod{8}. \end{cases}$

Proof. This is the immediate consequence of Lemma 6.8 and Theorem 2.1. □

Using the notations stated in Section 4, we have

$$S = \{\text{primes which divide } n\} \cup \{-1, 3\},$$
$$T = \{\text{odd primes which divide } n \text{ and congruent to 1 modulo 3}\}$$
$$(\cup \{3\} \text{ if } n \equiv 6 \pmod 9).$$

Remark that $E_{-n,\frac{\pi}{3}} = E_{n,\frac{2\pi}{3}}$ (in general, $E_{-n,\theta} = E_{n,\pi-\theta}$). Hence we can regard the $\pi/3$ and $2\pi/3$-congruent number problems as the same, admitting n to be negative.

Since Theorem 6.1 is contained in [9], we prove only Theorem 6.2. The others can be proved similarly.

Proof of Theorem 6.2. In the case that $p \equiv 1 \pmod{24}$,

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

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

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle p\rangle$.
In the case that $p \equiv 5, 17 \pmod{24}$,

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

$$\Lambda' = \begin{array}{c} \\ -1 \\ 2 \\ 3 \\ p \end{array} \begin{array}{c} \begin{array}{c} 2 \end{array} \\ \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \end{pmatrix} \end{array}, \quad \Lambda = \text{empty}.$$

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, -3, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.
In the case that $p \equiv 7 \pmod{24}$,

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

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

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, 2p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.
In the case that $p \equiv 13 \pmod{24}$,

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

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

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle -3, 2p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.

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

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

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

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, -p\rangle$, $Se^{(\varphi)}(E/\mathbb{Q}) = \langle p\rangle$.

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

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

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

Therefore $S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -3, -p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$. □

Remark. From our method, we can see that the Selmer rank of the elliptic curve $E_{n,\frac{\pi}{3}}$ depends on only the *type* of the factorization of the integer n, namely the primes modulo 24 and the Legendre symbols of one another (cf. the tables in Section 9).

The result in Section 5 can be applied to the other integers n or the other angles θ. For example, let θ be the angle with $\cos\theta = 1/3$. Then we have the following.

Theorem 6.10. *Let p be a prime and θ the angle with $\cos\theta = 1/3$. Then for the curve $E = E_{p,\theta}$, the following holds.*

(1) $p \equiv 1 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 2, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 2, p\rangle$.
(2) $p \equiv 5, 7, 19 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.
(3) $p \equiv 11 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 3p\rangle$.
(4) $p \equiv 13 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, 2, p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \{1\}$.
(5) $p \equiv 17 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 2, p\rangle$.
(6) $p \equiv 23 \pmod{24} \Rightarrow S^{(\varphi')}(E'/\mathbb{Q}) = \langle -2, -p\rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle 6\rangle$.

Therefore the Selmer rank $= \begin{cases} 3, & \text{if } p \equiv 1 \pmod{24}, \\ 2, & \text{if } p \equiv 17 \pmod{24}. \\ 1, & \text{if } p \equiv 11, 13, 23 \pmod{24}. \\ 0, & \text{if } p \equiv 5, 7, 19 \pmod{24}. \end{cases}$

In particular, a prime p is not θ-congruent number if $p \equiv 5, 7$ or $19 \pmod{24}$.

Proof. The equation of the elliptic curve $E_{p,\theta}$ is

$$y^2 = x(x + 4p)(x - 2p).$$

The bad primes of the curve are $2, 3$ and p. Using Propositions 5.1, 5.3 and 5.7, the following holds.

$$\mathrm{Im}(\delta'_2) = \begin{cases} \langle -p, 2p, -1\rangle, & \text{if } p \equiv 1 \pmod 4, \\ \langle -p, 2p, -5\rangle, & \text{if } p \equiv -1 \pmod 4. \end{cases}$$

$$\mathrm{Im}(\delta'_3) = \begin{cases} \mathbb{Z}_3^\times \mathbb{Q}_3^\times / \mathbb{Q}_3^{\times 2}, & \text{if } p \equiv 1 \pmod 3, \\ \mathbb{Q}_3^{\times 2} / \mathbb{Q}_3^{\times 2}, & \text{if } p \equiv -1 \pmod 3. \end{cases}$$

$$\mathrm{Im}(\delta'_p) = \begin{cases} \langle -p\rangle, & \text{if } p \equiv 1, 3 \pmod 8, \\ \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}, & \text{if } p \equiv 5, 7 \pmod 8. \end{cases}$$

Then we can prove the theorem similarly to Theorem 6.2. □

Next, we fix $n = 1$ and vary the angle θ.

Theorem 6.11. *Let p be Sophie Germain's prime, i.e. $q = 2p - 1$ is also prime, and θ be the angle with $\cos\theta = (p-1)/p$. Then for the curve $E = E_{1,\theta}$, the following holds.*

(1) $p \equiv 1 \pmod 4 \ \Rightarrow\ S^{(\varphi')}(E'/\mathbb{Q}) = \langle -1, q\rangle,\ S^{(\varphi)}(E/\mathbb{Q}) = \langle 2, p\rangle.$
(2) $p \equiv 3 \pmod 4 \ \Rightarrow\ S^{(\varphi')}(E'/\mathbb{Q}) = \langle -q\rangle,\ S^{(\varphi)}(E/\mathbb{Q}) = \langle 2p\rangle.$

Therefore the Selmer rank $= \begin{cases} 2, & \text{if } p \equiv 1 \pmod 4, \\ 0, & \text{if } p \equiv 3 \pmod 4. \end{cases}$
In particular, 1 is not θ-congruent for arbitrary small angle θ if Sophie Germain's primes p with $p \equiv 3 \pmod 4$ exist infinitely.

Proof. The equation of the elliptic curve $E_{1,\theta}$ is

$$y^2 = x(x + q)(x - 1).$$

The bad primes of the curve are $2, p$ and q. Using Proposition 5.2, 5.3 and 5.4, we can prove the theorem similarly to Theorem 6.2. □

7. The curve $y^2 = x^3 + Ax^2 + Bx$

In this section, we study our main object, namely the elliptic curve with a rational 2-torsion. In this section, we let $f(x) = x^3 + Ax^2 + Bx$. Without loss of generality, we can assume that either A is squarefree or B is fourth-power-free.

From the locus $E(\mathbb{R})$, the images of δ'_∞ and δ_∞ are clearly given as follows.

(1) If $B > 0$ and ($A < 0$ or $A^2 - 4B < 0$), then $\mathrm{Im}(\delta'_\infty) = \{1\}$, $\mathrm{Im}(\delta_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$.
(2) In the other case, $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$, $\mathrm{Im}(\delta_\infty) = \{1\}$.

The discriminant of the curve is

$$\Delta = 16B^2(A^2 - 4B).$$

So bad primes are classified into

- odd primes which divide both A and B,
- odd primes which divide not A but B,
- odd primes which divide not B but $A^2 - 4B$,
- 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.

7.1. **Formulae for the images of the connecting homomorphisms.** First, we give the statements for odd primes which divide the discriminant Δ.

Proposition 7.1. *Let p be an odd prime dividing both A and B. Put $\mathrm{ord}_p(A) = a$, $\mathrm{ord}_p(B) = b$ and $A = p^a A'$, $B = p^b B'$. Then the images of homomorphisms are obtained as follows.*

(1) *If $b = 1$, or $b = 3$ and $a \geq 2$, then $\mathrm{Im}(\delta'_p) = \langle B \rangle$.*
(2) *If $b \geq 3$ and $a = 1$, then $\mathrm{Im}(\delta'_p) = \langle -A, B \rangle$.*
(3) *Suppose that $b = 2$ and $a \geq 2$.*
  (a) *If $-B$ is a p-adic non-square, then $\mathrm{Im}(\delta'_p) = \langle B \rangle$.*
  (b) *Suppose that $-B$ is a p-adic square.*
    (i) *If $p \equiv 3 \pmod 4$, then $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.*
    (ii) *If $p \equiv 1 \pmod 4$, then*
      (A) $(-B')^{(p-1)/4} \equiv 1 \pmod p \Rightarrow \mathrm{Im}(\delta'_p) = \langle p \rangle$,
      (B) $(-B')^{(p-1)/4} \equiv -1 \pmod p \Rightarrow \mathrm{Im}(\delta'_p) = \langle pu \rangle$.
(4) *Suppose that $b = 2$ and $a = 1$.*
  (a) *If $(A'^2 - 4B'/p) = 0$, then $\mathrm{Im}(\delta_p) = \langle 2A, A^2 - 4B \rangle$.*
  (b) *If $(A'^2 - 4B'/p) = -1$, then $\mathrm{Im}(\delta'_p) = \langle B \rangle$.*
  (c) *Suppose that $(A'^2 - 4B'/p) = 1$.*
    (i) *If B is not a p-adic square, then $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.*
    (ii) *If B is a p-adic square, then the congruence $x^2 \equiv B' \pmod p$ has solutions. Let $\sqrt{B'}$ be one of the solutions, then*
      (A) $(A' + 2\sqrt{B'}/p) = 1 \Rightarrow \mathrm{Im}(\delta_p) = \langle p \rangle$.
      (B) $(A' + 2\sqrt{B'}/p) = -1 \Rightarrow \mathrm{Im}(\delta_p) = \langle pu \rangle$.

Proposition 7.2. *Let p be an odd prime dividing not A but B. Put $\mathrm{ord}_p(B) = b$ and $B = p^b B'$. Then the images of the connecting homomorphisms are obtained as follows.*

(1) *If b is even and $(A/p) = -1$, then $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2} / \mathbb{Q}_p^{\times 2}$.*
(2) *In the other case, $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.*

Proposition 7.3. *Let p be an odd prime dividing not B but $A^2 - 4B$. Put $a = \mathrm{ord}_p(A^2 - 4B)$. Then the images of the connecting homomorphisms are obtained as follows.*

(1) *If a is even and $(-2A/p) = -1$, then $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2} / \mathbb{Q}_p^{\times 2}$.*
(2) *In the other case, $\mathrm{Im}(\delta'_p) = \{1\}$.*

Next, we give the statements for $\mathrm{Im}(\delta'_2)$ and $\mathrm{Im}(\delta_2)$. One of the propositions below can be applied to either the original curve or the dual curve (for details, see Section 10).

Proposition 7.4. *Suppose that $\mathrm{ord}_2(A) = \mathrm{ord}_2(B) = 0$. Then the following holds.*

(1) *If $B \equiv 3 \pmod 4$ or $A \equiv B + 2 \pmod 8$, then $\mathrm{Im}(\delta'_2) = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2} / \mathbb{Q}_2^{\times 2}$.*
(2) *In the other case, $\mathrm{Im}(\delta'_2) = \langle 5 \rangle$.*

Proposition 7.5. *Suppose that $\mathrm{ord}_2(A) = 0$, $\mathrm{ord}_2(B) = b \geq 1$. Then the image $\mathrm{Im}(\delta'_2)$ is obtained as the following table.*

$A \bmod 8$	b	$\mathrm{Im}(\delta_2')$
1	1	$\langle 5, B\rangle$
	2, 3	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	4	$\mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$
	≥ 5	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
3	1	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	2	$\langle 5, B\rangle$
	3	$\langle 2, 5, B\rangle$
	≥ 4	$\langle -2, 5, B\rangle$

$A \bmod 8$	b	$\mathrm{Im}(\delta_2')$
5	1	$\langle 5, B\rangle$
	2	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 3 : *odd*	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 4 : *even*	$\mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$
7	1	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	2	$\langle 5, B\rangle$
	3	$\langle -2, 5, B\rangle$
	≥ 4	$\langle 2, 5, B\rangle$

Proposition 7.6. *If* $\mathrm{ord}_2(A) \geq 1$, $\mathrm{ord}_2(B) = 1$ *or* $\mathrm{ord}_2(A) = 1$, $\mathrm{ord}_2(B) = 2$, *then* $\mathrm{Im}(\delta_2') = \langle B, (B+1)(-A+1)\rangle$.

Proposition 7.7. *Suppose that* $\mathrm{ord}_2(A) = 1$, $\mathrm{ord}_2(B) \geq 3$. *Then the image* $\mathrm{Im}(\delta_2')$ *is obtained as the following table.*

$A \mod 16$	$B \mod 32$	$\mathrm{Im}(\delta_p')$
2	0	$\langle -1, 2, B\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle -1, 10, B\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
6	0	$\langle -2, -5, B\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle 2, -5, B\rangle$
	24	$\langle 2, -5\rangle$

$A \mod 16$	$B \mod 32$	$\mathrm{Im}(\delta_2')$
10	0	$\langle -1, 10, B\rangle$
	8	$\langle -1, 2\rangle$
	16	$\langle -1, 2, B\rangle$
	24	$\langle -1, 10\rangle$
14	0	$\langle 2, -5, B\rangle$
	8	$\langle 2, -5\rangle$
	16	$\langle -2, -5, B\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

Proposition 7.8. *If* $\mathrm{ord}_2(A) \geq 2$, $\mathrm{ord}_2(B) = 0$, *then the following holds.*

(1) *If* $B \equiv 3 \pmod 4$ *and* $A+B \equiv 7$ *or* $11 \pmod{16}$, *then* $\mathrm{Im}(\delta_2') = \mathbb{Z}_2^\times\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
(2) *In the other case,* $\mathrm{Im}(\delta_2') = \langle B\rangle$.

Proposition 7.9. *If* $\mathrm{ord}_2(A) = 2$, $\mathrm{ord}_2(B) = 3$, *then* $\mathrm{Im}(\delta_2') = \langle 5, B\rangle$.

Proposition 7.10. *If* $\mathrm{ord}_2(A) \geq 3$, $\mathrm{ord}_2(B) = 3$, *then* $\mathrm{Im}(\delta_2') = \langle B\rangle$.

Now, we have prepared to calculate the Selmer group. For example, Stroeker and Top [25] showed the following theorem.

Theorem 7.11 ([25])**.** *Let* p *be prime and* E *be the elliptic curve defined by the equation* $y^2 = (x+p)(x^2+p^2)$. *Then*

$$\textit{the Selmer rank of } E = \begin{cases} 3, & \textit{if } p \equiv 1 \pmod 8 \textit{ and } ((1+\sqrt{-1})/p) = 1, \\ 1, & \textit{if } p \equiv 1 \pmod 8 \textit{ and } ((1+\sqrt{-1})/p) = -1, \\ & \textit{or } p \equiv 7 \pmod 8, \\ 0, & \textit{if } p \equiv \pm 5 \pmod 8 \textit{ or } p = 2. \end{cases}$$

We give another proof using the propositions in this section.

Proof. By some translation, E will be the curve whose equation is

$$y^2 = x^3 - 2px^2 + 2p^2x.$$

From the locus of this curve, we have $\mathrm{Im}(\delta'_\infty) = \{1\}$. If p is odd, then

$$\mathrm{Im}(\delta'_p) = \begin{cases} \langle p \rangle, & \text{if } p \equiv 1 \pmod 8 \text{ and } ((1+\sqrt{2})/p) = 1, \\ \langle pu \rangle, & \text{if } p \equiv 1 \pmod 8 \text{ and } ((1+\sqrt{2})/p) = -1, \\ \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}, & \text{if } p \equiv 3 \pmod 8, \\ \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}, & \text{if } p \equiv 5 \pmod 8, \\ \{1\}, & \text{if } p \equiv 7 \pmod 8 \end{cases}$$

from Proposition 7.1. Note that $((1+\sqrt{2})/p) = ((1+\sqrt{-1})/p)$ since $(1+\sqrt{2})(1+\sqrt{-1}) = (1+\zeta_8)^2$, where ζ_8 is a primitive 8-th root of unity ($\zeta_8 \in \mathbb{Q}_p$ since $p \equiv 1 \pmod 8$). By Propositions 7.6 and 7.9, we have

$$\mathrm{Im}(\delta'_2) = \begin{cases} \langle 2 \rangle, & \text{if } p \equiv 1 \pmod 4, \\ \langle 2, 5 \rangle, & \text{if } p \equiv 3 \pmod 4 \text{ or } p = 2. \end{cases}$$

Considering the matrices Λ', Λ (see the proof of Theorem 6.2), we have the following.

- If $p \equiv 1 \pmod 8$ and $((1+\sqrt{-1})/p) = 1$, then $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2, p \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle -1, 2, p \rangle$,
- If $p \equiv 1 \pmod 8$ and $((1+\sqrt{-1})/p) = -1$, then $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2 \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle -1, 2 \rangle$,
- If $p \equiv \pm 5 \pmod 8$ or $p = 2$, then $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2 \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle -1 \rangle$,
- If $p \equiv 7 \pmod 8$, then $S^{(\varphi')}(E'/\mathbb{Q}) = \langle 2 \rangle$, $S^{(\varphi)}(E/\mathbb{Q}) = \langle -1, p \rangle$.

Hence the proof is complete. □

7.2. **Proofs of the propositions.** Suppose that p is an odd prime which divides both A and B, and let $\mathrm{ord}_p(A) = a$, $\mathrm{ord}_p(B) = b$, $A = p^a A'$, $B = p^b B'$.

Proof of Proposition 7.1. (1) Let $(x, y) \in E(\mathbb{Q}_p)$. In the case that $b = 1$,

- $\mathrm{ord}_p(x) \le 0 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \ge 1 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$,

by Lemma 5.10. Hence $\mathrm{Im}(\delta'_p) = \langle B \rangle$. In the case that $b = 3$ and $a \ge 2$,

- $\mathrm{ord}_p(x) \le 1 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \ge 2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$.

Hence $\mathrm{Im}(\delta'_p) = \langle B \rangle$.

(2) Let $b \ge 3$ and $a = 1$. By Lemma 5.10,

- $\mathrm{ord}_p(x) \le 0 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \ge b \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$.

Let $x = p^e w$ with $w \in \mathbb{Z}_p^\times$. From the equation of the elliptic curve,

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

The right hand side is not a p-adic square if $2 \le e \le b-2$. Hence we must consider only a point with $e = 1$ (if $\mathrm{ord}_p(x) = b-1$, then the order of the x-coordinate of $(x, y) + (0, 0)$ is 1). If $e = 1$, then the equation will be

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

so it is necessary that $w \equiv -A' \pmod{p}$, that is $x \equiv -A \pmod{\mathbb{Q}_p^{\times 2}}$. We show that such a point exists using Hensel's lemma (see Section 2.2). Let k be an integer, then $f(-A+p^2k) \equiv p^4(kA' - A'B') \pmod{p^5}$. When $k \equiv A'^{-1}B' \pmod{p}$, we have $\mathrm{ord}_p(f(-A+p^2k)) \geq 5$ and $f'(-A+p^2k) \equiv A^2 \pmod{p^2}$. By Hensel's lemma, a point with $x \equiv -A + p^2k \pmod{p^3}$ does exist. Hence $-A \in \mathrm{Im}(\delta'_p)$.

(3) Let $b = 2$ and $a \geq 2$. By Lemma 5.10,

- $\mathrm{ord}_p(x) \leq 0 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \geq 2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$.

Hence we must consider only a point with $\mathrm{ord}_p(x) = 1$. Let $x = pw$ with $w \in \mathbb{Z}_p^{\times}$, then the equation of the curve will be

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

so it is necessary that $-B$ is a p-adic square. We have proved (a). Assume that $-B$ is a p-adic square. Let w be an integer satisfying $w^2 \equiv -B' \pmod{p}$. We show that a point with $x \equiv pw \pmod{p^2}$ exists using Hensel's lemma. Since $-B' \equiv w^2 \pmod{p}$, there exists a integer l satisfying $B = -p^2w^2 + p^3l$. Let k be an integer, then $f(pw + p^2k) \equiv p^4(2kw^2 + p^{a-2}A'w^2 + lw) \pmod{p^5}$. Hence $\mathrm{ord}_p(f(pw+p^2k)) \geq 5$ for a suitable k. And we have $f'(pw+p^2k) \equiv 2p^2w^2 \pmod{p^3}$. By Hensel's lemma, a point with $x \equiv pw \pmod{p^2}$ does exist.

If $p \equiv 3 \pmod 4$, then $\mathrm{Im}(\delta'_p) = \{1, pw, -pw, B\} = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$. If $p \equiv 1 \pmod 4$, then $\mathrm{Im}(\delta'_p) = \{1, pw\} = \langle p \rangle$ or $\langle pu \rangle$ according as w is a quadratic residue modulo p or not, i.e. $-B'$ is a quartic residue modulo p or not.

(4) Let $b = 2$ and $a = 1$. By Lemma 5.10,

- $\mathrm{ord}_p(x) \leq 0 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \geq 2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$.

Hence we must consider only a point with $\mathrm{ord}_p(x) = 1$. Let $x = pw$ with $w \in \mathbb{Z}_p^{\times}$, then the equation of the curve will be

$$y^2 = p^3 w(w^2 + A'w + B'),$$

so it is necessary that that $A'^2 - 4B'$ is a square modulo p. We have proved (b). If $A'^2 - 4B' \equiv 0 \pmod{p}$, then $\mathrm{ord}_p(A^2 - 4B) \geq 3$. About the dual curve

$$y^2 = x^3 - 2Ax^2 + (A^2 - 4B)x,$$

we have $\mathrm{ord}_p(-2A) = 1$, $\mathrm{ord}_p(A^2 - 4B) \geq 3$, and hence $\mathrm{Im}(\delta_p) = \langle 2A, A^2 - 4B \rangle$ from the statement (2). We have proved (a).

Suppose that $A'^2 - 4B'$ is a non-zero square modulo p. Let w be an integer satisfying $w^2 + A'w + B' \equiv 0 \pmod{p^2}$. We show that a point with $x \equiv pw \pmod{p^2}$ exists using Hensel's lemma. By a direct calculation, we have $f(pw) \equiv 0 \pmod{p^5}$ and $f'(pw) \equiv p^2(3w^2 + 2A'w + B') \pmod{p^3}$. Since w is not a double root of the congruence $w^3 + A'w^2 + B'w \equiv 0 \pmod{p}$, we have $\mathrm{ord}_p(f'(pw)) = 2$. By Hensel's lemma, a point with $x \equiv pw \pmod{p^2}$ does exist.

If B is a p-adic non-square, then $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$. Suppose that B is a p-adic square, then $\mathrm{Im}(\delta'_p) = \langle p \rangle$ or $\langle pu \rangle$ according as w is a quadratic residue or not. We give another algorithm. Now the equation of the dual curve is

$$y^2 = x(x - (A + 2\sqrt{B}))(x - (A - 2\sqrt{B})).$$

By Proposition 5.1 (note that this proposition also holds when $\alpha, \beta \in \mathbb{Q}_p$ from the proof of it), we have $\mathrm{Im}(\delta_p) = \{1, A+2\sqrt{B}, A-2\sqrt{B}, A^2-4B\}$. Since A^2-4B is a p-adic square, $\mathrm{Im}(\delta_p) = \langle p(A'+2\sqrt{B'})\rangle$. Hence the proof is complete. □

Proof of Proposition 7.2. Let $(x,y) \in E(\mathbb{Q}_p)$. From Lemma 5.10, the following holds.

- $\mathrm{ord}_p(x) \leq -2 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_p^{\times 2}}$,
- $\mathrm{ord}_p(x) \geq b+2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_p^{\times 2}}$.

There does not exist a point with $\mathrm{ord}_p(x) = -1$ or $b+1$. Lemma 5.14 (3) describes the points with $1 \leq \mathrm{ord}_p(x) \leq b-1$.

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

Hence we must investigate points with $\mathrm{ord}_p(x) = 0$.

Claim. $u \in \delta_p'(E_0(\mathbb{Q}_p)\backslash E_1(\mathbb{Q}_p))$.

First, assume that $(-A/p) = 1$. Suppose that $(x,y) \in E_0(\mathbb{Q}_p)\backslash E_1(\mathbb{Q}_p)$, i.e. $\mathrm{ord}_p(x) = 0$. Since $x^3 + Ax^2 + Bx \equiv x^2(x+A) \pmod p$, $x+A$ is a square modulo p. Conversely, if $x+A$ is a square modulo p, then $x \in x(E_0(\mathbb{Q}_p)\backslash E_1(\mathbb{Q}_p))$. Assume that such x must be a square modulo p. Then we have squares $-A, -2A, \cdots, -(p-1)A$. Since $A \in (\mathbb{Z}/p\mathbb{Z})^{\times}$, 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.

Next, assume that $(-A/p) = -1$. Since $A^2 - 4B$ is a square modulo p, the quadratic equation $x^2 + Ax + B = 0$ has solutions $\alpha, \beta \in \mathbb{Q}_p$. Then we obtain the points $(\alpha, 0), (\beta, 0) \in E(\mathbb{Q}_p)$. Since one of α, β is congruent to $-A$ modulo p, the claim holds.

Let us come back to the proof of the proposition. If b is odd, then $B \equiv p$ or $pu \pmod{\mathbb{Q}_p^{\times 2}}$, and hence $\mathrm{Im}(\delta_p') = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$. Suppose that b is even. If $(A/p) = 1$, then the point (x,y) with $1 \leq \mathrm{ord}_p(x) \leq b-1$ and $x \equiv p \pmod{\mathbb{Q}_p^{\times 2}}$ does exist, and hence $\mathrm{Im}(\delta_p') = \mathbb{Q}_p^{\times}/\mathbb{Q}_p^{\times 2}$. If $(A/p) = -1$, then p and pu do not appear, and hence $\mathrm{Im}(\delta_p') = \mathbb{Z}_p^{\times}\mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$. □

Proof of Proposition 7.3. This is the immediate consequence of Proposition 7.2 and Theorem 2.1. □

Proof of Proposition 7.4. Let $(x,y) \in E(\mathbb{Q}_2)$. From Lemma 5.11 and the remark below the lemma, the following holds.

- $\mathrm{ord}_2(x) \leq -4 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = -2 \ \Rightarrow \ x \equiv 5 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = 2 \ \Rightarrow \ x \equiv 5B \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq 3 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

Hence we have $\mathrm{Im}(\delta_2') = \mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ when $B \equiv 3 \pmod 4$. Assume that $B \equiv 1 \pmod 4$. We must consider the point with $\mathrm{ord}_2(x) = 0$. The equation $y^2 = f(x)$ has a solution with $x \equiv 3 \pmod 4$ if and only if

$$f(3) = 27 + 9A + 3B \equiv 1 \pmod 8.$$

Therefore $\mathrm{Im}(\delta_2') = \mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ or $\langle 5 \rangle$ according as $A \equiv B+2 \pmod 8$ or not. □

Proof of Proposition 7.5. Let $(x, y) \in E(\mathbb{Q}_2)$. From Lemma 5.11 and the remark below the lemma, the following holds.

- $\mathrm{ord}_2(x) \leq -4 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = -2 \ \Rightarrow \ x \equiv 5 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = b+2 \ \Rightarrow \ x \equiv 5B \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq b+4 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

If $b \geq 6$, then the following holds. This fact is similar to Lemma 5.14 (3).

- If $A \equiv 1 \pmod 8$, then there exist points with $3 \leq \mathrm{ord}_2(x) \leq b-3$, and any elements of $\mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ appear in the 2-free part of x.
- In the other case, there does not exist a point with $3 \leq \mathrm{ord}_2(x) \leq b-3$.

Then we must consider points with $\mathrm{ord}_2(x) = 0, 1$ or 2. Note that we need not consider points with $\mathrm{ord}_2(x) = b, b-1$ or $b-2$ since

$$(x, y) + (0, 0) = \left(\frac{B}{x}, -\frac{By}{x^2} \right). \tag{7.1}$$

Suppose that $\underline{\mathrm{ord}_2(x) = 0}$. The equation $y^2 = f(x)$ has a solution with $x \equiv 3 \pmod 4$ if and only if

$$f(3) = 27 + 9A + 3B \equiv 0 \pmod 4$$

from Hensel's lemma. Hence $\mathrm{Im}(\delta_2') \supset \mathbb{Z}_2^{\times}\mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$ if $A + B \equiv 1 \pmod 4$. Suppose that $\underline{\mathrm{ord}_2(x) = 1}$. From (7.1), we may assume that $b \geq 2$. In this case, we have $\mathrm{ord}_2(\overline{f(x)}) = 2$. Hence the following holds.

- $f(2)/4 = 2 + A + B/2 \equiv 1 \pmod 8 \ \Rightarrow \ 2, 10 \in \mathrm{Im}(\delta_2')$.
- $f(-2)/4 = -2 + A - B/2 \equiv 1 \pmod 8 \ \Rightarrow \ -2, -10 \in \mathrm{Im}(\delta_2')$.

Suppose that $\underline{\mathrm{ord}_2(x) = 2}$. From (7.1), we may assume that $b \geq 3$. In this case, we have $\mathrm{ord}_2(\overline{f(x)}) = 4$. Hence $-1, -5 \in \mathrm{Im}(\delta_2')$ if

$$f(-4)/16 = -4 + A - B/4 \equiv 1 \pmod 8.$$

From the facts above, we have the table in the proposition. □

Proof of Proposition 7.6. When $\mathrm{ord}_2(A) \geq 1$ and $\mathrm{ord}_2(B) = 1$, the following holds.

- $\mathrm{ord}_2(x) \leq -2 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq 3 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

When $\mathrm{ord}_2(A) = 1$ and $\mathrm{ord}_2(B) = 2$, the following holds.

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

Let $\mathrm{ord}_2(x) = 0$, then

$$y^2 = x^3 + Ax^2 + Bx \equiv (B+1)x + A \equiv 1 \pmod 8,$$

and hence $x \equiv (B+1)(-A+1) \pmod 8$. The proof is complete. □

Proof of Proposition 7.7. Let $(x, y) \in E(\mathbb{Q}_2)$, then the following holds.

- $\mathrm{ord}_2(x) \leq -2 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq b+2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

Let $\mathrm{ord}_2(x) = 0$, then

$$y^2 = x^3 + Ax^2 + Bx \equiv x + A \equiv 1 \pmod 8,$$

and hence $x \equiv -A + 1 \pmod{\mathbb{Q}_2^{\times 2}}$.

Since points with $2 \leq \mathrm{ord}_2(x) \leq b - 2$ do not exist, we must consider points with $\mathrm{ord}_2(x) = 1$. In this case, $\mathrm{ord}_2(f(x)) \geq 4$ and $\mathrm{ord}_2(f'(x)) = 2$. From Hensel's lemma, $2 \in \mathrm{Im}(\delta_2')$ if

$$f(2) \equiv 0 \text{ or } 16 \pmod{64}.$$

This is equivalent to that $2A + B \equiv 4$ or $28 \pmod{32}$. Similarly, the following holds.

- $-2 \in \mathrm{Im}(\delta_2')$ if $2A - B \equiv 4$ or $12 \pmod{32}$.
- $10 \in \mathrm{Im}(\delta_2')$ if $2A + B \equiv 12$ or $20 \pmod{32}$.
- $-10 \in \mathrm{Im}(\delta_2')$ if $2A - B \equiv 20$ or $28 \pmod{32}$.

From these facts, we have the table in the proposition. □

Proof of Proposition 7.8. Let $(x, y) \in E(\mathbb{Q}_2)$, then the following holds.

- $\mathrm{ord}_2(x) \leq -2 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq 2 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

Let $\mathrm{ord}_2(x) = 0$, then

$$x^3 + Ax^2 + Bx \equiv (B + 1)x \equiv 0 \pmod 4,$$

and hence it must follow that $B \equiv 3 \pmod 4$. The equation $y^2 = f(x)$ has a solution with $x \equiv 5 \pmod 8$ if and only if

$$f(5) \equiv 0 \text{ or } 4 \pmod{16}$$

from Hensel's lemma. This is equivalent to that $A + B \equiv 7$ or $11 \pmod{16}$. □

Proof of Proposition 7.9. Let $(x, y) \in E(\mathbb{Q}_2)$, then the following holds.

- $\mathrm{ord}_2(x) \leq -2 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = 0 \ \Rightarrow \ x \equiv 5 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) = 3 \ \Rightarrow \ x \equiv 5B \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq 5 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

Since points with $\mathrm{ord}_2(x) = 1$ or 2 do not exist, the proposition holds. □

Proof of Proposition 7.10. Let $(x, y) \in E(\mathbb{Q}_2)$, then the following holds.

- $\mathrm{ord}_2(x) \leq 0 \ \Rightarrow \ x \equiv 1 \pmod{\mathbb{Q}_2^{\times 2}}$,
- $\mathrm{ord}_2(x) \geq 3 \ \Rightarrow \ x \equiv B \pmod{\mathbb{Q}_2^{\times 2}}$.

Since points with $\mathrm{ord}_2(x) = 1$ or 2 do not exist, the proposition holds. □

8. Complete 2-descent

In this section, we calculate the 2-Selmer rank of the elliptic curve connected with the $\pi/2$ or $\pi/3$-congruent number problem. Recall that the 2-Selmer group is defined by

$$S^{(2)}(E/\mathbb{Q}) = \bigcap_{p \in M_{\mathbb{Q}}} \mathrm{Im}(\bar{\delta_p}),$$

where $\bar{\delta_p}$ is the connecting homomorphism:

$$\bar{\delta_p} \ : \ E(\mathbb{Q}_p)/2E(\mathbb{Q}_p) \to H^1(\mathbb{Q}_p, E[\,2\,]).$$

From now on, we consider an elliptic curve E whose equation is

$$y^2 = x(x-\alpha)(x-\beta),$$

where $\alpha, \beta \in \mathbb{Q}$. About this curve, $E[\,2\,] = \{\mathcal{O},\ (0,0),\ (\alpha,0),\ (\beta,0)\} \cong \mathbb{F}_2 \oplus \mathbb{F}_2$, and hence $H^1(\mathbb{Q}_p, E[\,2\,]) \cong \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \oplus \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \cong K$, where

$$K = \{(a,b,c) \mid a,b,c \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2},\ abc \in \mathbb{Q}_p^{\times 2}\}.$$

So the connecting homomorphism $\bar{\delta}_p$ can be regarded as the map to K. Then we verify the formula

$$\bar{\delta}(P) = \begin{cases} (x, x-\alpha, x-\beta), & \text{if } P \notin E[\,2\,], \\ (\alpha, \alpha(\alpha-\beta), \alpha-\beta), & \text{if } P = (\alpha,0), \\ (\beta, \beta-\alpha, \beta(\beta-\alpha)), & \text{if } P = (\beta,0), \\ (\alpha\beta, -\alpha, -\beta), & \text{if } P = (0,0), \\ (1,1,1), & \text{if } P = \mathcal{O}. \end{cases} \tag{8.1}$$

from the definition of the connecting homomorphism. Remark that the order of the elements is not essential, and the third element can be omitted.

We can describe the connecting homomorphism $\bar{\delta}_p$ as follows. Let F and G be the curves defined by

$$F\ :\ y^2 = x(x+\alpha)(x+\alpha-\beta),$$
$$G\ :\ y^2 = x(x+\beta)(x-\alpha+\beta).$$

Note that the curves F and G can be given by translations of E. Let $\delta_{E,k}$ denote the connecting homomorphism for the curve E defined by (2.8). Then the map $\bar{\delta}_p$ is described by $\bar{\delta}_p(\mathcal{O}) = (1,1,1)$ and

$$\bar{\delta}_p(x,y) = (\delta'_{E,p}(x,y),\ \delta'_{F,p}(x-\alpha,y),\ \delta'_{G,p}(x-\beta,y)).$$

Consider the elliptic curve connected with the $\pi/2$-congruent number problem, namely

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

Set $\alpha = -n$ and $\beta = n$ at the equation (8.1). Then the following proposition holds.

Proposition 8.1. *The images of the connecting homomorphisms for $E_{n,\frac{\pi}{2}}$ are obtained as follows.*

(1) $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1,1), (-1,1,-1)\}$.

(2) *For an odd prime p dividing n,*

$$\mathrm{Im}(\bar{\delta}_p) = \{(1,1,1),\ (n,2n,2),\ (-n,2,-2n),\ (-1,n,-n)\}.$$

(3) *If n is odd, then*

$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (1,5,5),\ (n,2n,2),\ (n,10n,10), \\ (-n,2,-2n),\ (-n,10,-10n),\ (-1,n,-n),\ (-1,5n,-5n) \end{array} \right\}.$$

(4) *If $n \equiv 2 \pmod 8$, then*

$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (5,-1,-5),\ (n,2n,2),\ (-n,2,-2n), \\ (5n,-2n,-10),\ (-5n,-2,10n),\ (-5,-n,5n),\ (-1,n,-n) \end{array} \right\}.$$

(5) *If $n \equiv 6 \pmod 8$, then*

$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (5,-5,-1),\ (n,2n,2),\ (-n,2,-2n), \\ (5n,-10n,-2),\ (-5n,-10,2n),\ (-5,-5n,n),\ (-1,n,-n) \end{array} \right\}.$$

Proof. Let E, F, G be the curves defined by

$$E : y^2 = x(x+n)(x-n),$$
$$F : y^2 = x(x-n)(x-2n),$$
$$G : y^2 = x(x+n)(x+2n).$$

(1) This statement is clear from the loci $E(\mathbb{R}), F(\mathbb{R})$ and $G(\mathbb{R})$.
(2) Let $(x,y) \in E(\mathbb{Q}_p)$. From Proposition 5.1 and the proof of it, the following holds.

- If $\mathrm{ord}_p(x) \leq 0$, then $\delta'_{E,p}(x,y) = 1$.
- If $\mathrm{ord}_p(x) = 1$, then $\delta'_{E,p}(x,y) = n$ or $-n$.
- If $\mathrm{ord}_p(x) \geq 2$, then $\delta'_{E,p}(x,y) = -1$.

Let $(x,y) \in F(\mathbb{Q}_p)$, then the following holds.

- If $\mathrm{ord}_p(x) \leq 0$, then $\delta'_{F,p}(x,y) = 1$.
- If $\mathrm{ord}_p(x) = 1$, then $\delta'_{F,p}(x,y) = n$ or $2n$.
- If $\mathrm{ord}_p(x) \geq 2$, then $\delta'_{F,p}(x,y) = 2$.

Let $(x,y) \in G(\mathbb{Q}_p)$, then the following holds.

- If $\mathrm{ord}_p(x) \leq 0$, then $\delta'_{G,p}(x,y) = 1$.
- If $\mathrm{ord}_p(x) = 1$, then $\delta'_{G,p}(x,y) = -n$ or $-2n$.
- If $\mathrm{ord}_p(x) \geq 2$, then $\delta'_{G,p}(x,y) = 2$.

From now on, suppose that $(x,y) \in E(\mathbb{Q}_p)$. If $\mathrm{ord}_p(x) \leq 0$, then $\mathrm{ord}_p(x+n) \leq 0$ and $\mathrm{ord}_p(x-n) \leq 0$, and hence $\bar{\delta}_p(x,y) = (1,1,1)$.

Next, suppose that $\mathrm{ord}_p(x) = 1$. If $\mathrm{ord}_p(x+n) = 1$, then $\mathrm{ord}_p(x-n) \geq 2$ from the equation of E. Hence $\bar{\delta}_p(x,y) = (n, 2n, 2)$ (note that the product of the three must be a square in $\mathbb{Q}_p^\times$). If $\mathrm{ord}_p(x-n) = 1$, then $\mathrm{ord}_p(x+n) \geq 2$, and hence $\bar{\delta}_p(x,y) = (-n, 2, -2n)$.

Lastly, suppose that $\mathrm{ord}_p(x) \geq 2$. Then $\mathrm{ord}_p(x+n) = \mathrm{ord}_p(x-n) = 1$, and hence $\bar{\delta}_p(x,y) = (-1, n, -n)$ or $(-1, 2n, -2n)$. But it must be $(-1, n, -n)$ by the group low of $\mathrm{Im}(\bar{\delta}_p)$. We have proved (2).

The proof of the statements (3),(4) and (5) are similar to that of (2), but slightly complicated. We only give the proof of (3).

Let $(x,y) \in E(\mathbb{Q}_2)$. From Proposition 5.4 and the proof of it, the following holds.

- If $\mathrm{ord}_2(x) \leq -2$, then $\delta'_{E,2}(x,y) = 1$.
- If $\mathrm{ord}_2(x) = 0$, then $\delta'_{E,2}(x,y) = n$ or $-n$.
- If $\mathrm{ord}_2(x) \geq 2$, then $\delta'_{E,2}(x,y) = -1$.

Let $(x,y) \in F(\mathbb{Q}_2)$. From Proposition 5.5 and the proof of it, the following holds.

- If $\mathrm{ord}_2(x) \leq -4$, then $\delta'_{F,2}(x,y) = 1$.
- If $\mathrm{ord}_2(x) = -2$, then $\delta'_{F,2}(x,y) = 5$.
- If $\mathrm{ord}_2(x) = 0$, then $\delta'_{F,2}(x,y) = n$ or $5n$.
- If $\mathrm{ord}_2(x) = 1$, then $\delta'_{F,2}(x,y) = 2n$ or $10n$.
- If $\mathrm{ord}_2(x) = 3$, then $\delta'_{F,2}(x,y) = 10$.
- If $\mathrm{ord}_2(x) \geq 5$, then $\delta'_{F,2}(x,y) = 2$.

Let $(x,y) \in G(\mathbb{Q}_2)$. From Proposition 5.5 and the proof of it, the following holds.

- If $\mathrm{ord}_2(x) \leq -4$, then $\delta'_{G,2}(x,y) = 1$.
- If $\mathrm{ord}_2(x) = -2$, then $\delta'_{G,2}(x,y) = 5$.
- If $\mathrm{ord}_2(x) = 0$, then $\delta'_{G,2}(x,y) = -n$ or $-5n$.

- If $\mathrm{ord}_2(x) = 1$, then $\delta'_{G,2}(x, y) = -2n$ or $-10n$.
- If $\mathrm{ord}_2(x) = 3$, then $\delta'_{G,2}(x, y) = 10$.
- If $\mathrm{ord}_2(x) \geq 5$, then $\delta'_{G,2}(x, y) = 2$.

From now on, suppose that $(x, y) \in E(\mathbb{Q}_2)$. If $\mathrm{ord}_2(x) \leq -4$, then $\mathrm{ord}_2(x+n) \leq -4$ and $\mathrm{ord}_2(x - n) \leq -4$, and hence $\bar{\delta_2}(x, y) = (1, 1, 1)$. If $\mathrm{ord}_2(x) = -2$, then $\mathrm{ord}_2(x + n) = -2$ and $\mathrm{ord}_2(x - n) = -2$, and hence $\bar{\delta_2}(x, y) = (1, 5, 5)$.

The trivial elements $\bar{\delta_2}(0, 0) = (-1, n, -n)$, $\bar{\delta_2}(n, 0) = (n, 2n, 2)$, $\bar{\delta_2}(-n, 0) = (-n, 2, -2n)$ are in $\mathrm{Im}(\bar{\delta_2})$. Therefore $(-1, 5n, -5n)$, $(n, 10n, 10)$, $(-n, 10, -10n)$ are also in $\mathrm{Im}(\bar{\delta_2})$ by its group low. No other elements are in this group from the facts above. □

Example 8.2. Let $n = 570 = 2 \cdot 3 \cdot 5 \cdot 19$. Then the Selmer rank of the curve $E = E_{570,\frac{\pi}{2}}$ is 2, but the 2-Selmer rank is 0, hence 570 is not $\pi/2$-congruent.

From Proposition 8.1, the images of the connecting homomorphisms are given as follows.

p	$\mathrm{Im}(\bar{\delta_p})$
-1	$\{(1,1,1), (-1,1,-1)\}$
2	$(1,1,1), (5,-1,-5), (10,5,2), (-10,2,-5),$ $(2,-5,-10), (-2,-2,1), (-5,-10,2), (-1,10,-10)$
3	$\{(1,1,1), (3,-3,-1), (-3,-1,3), (-1,3,-3)\}$
5	$\{(1,1,1), (5,10,2), (5,2,10), (1,5,5)\}$
19	$\{(1,1,1), (19,-19,-1), (-19,-1,19), (-1,19,-19)\}$

The Selmer group $S^{(2)}(E/\mathbb{Q})$ is the subgroup of the group generated by

$$(1,2,2), (1,3,3), (1,5,5), (1,19,19),$$
$$(-1,1,-1), (2,1,2), (3,1,3), (5,1,5), (19,1,19).$$

For example, $(1,2,2) \notin S^{(2)}(E/\mathbb{Q})$ since $(1,2,2) \notin \mathrm{Im}(\bar{\delta_2})$. Checking the 2^9 elements in this way, we have

$$S^{(2)}(E/\mathbb{Q}) = \{(1,1,1), (-1,570,-570), (570,1140,2), (-570,2,-1140)\}$$
$$(= \bar{\delta}(E[\,2\,])\,).$$

Therefore the 2-Selmer rank is 0.

Remark. We can also formulate the 2-Selmer rank similarly to (4.2), but this formulation is rather complicated. From this formulation, we can see that the 2-Selmer rank of the elliptic curve $E_{n,\frac{\pi}{2}}$ depends on only the *type* of the factorization of the integer n similarly to the case of Selmer rank. For details, see the tables in Section 9.

Next, consider the elliptic curve connected with the $\pi/3$-congruent number problem, namely

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

Set $\alpha = -3n$ and $\beta = n$ at the equation (8.1). Then the following propositions hold. The proof is similar to that of Proposition 8.1.

Proposition 8.3. *The image of the connecting homomorphism $\bar{\delta}_\infty$ for $E_{n,\frac{\pi}{3}}$ is obtained as follows.*

(1) *If $n > 0$, then* $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1,1),(-1,1,-1)\}$.
(2) *If $n < 0$, then* $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1,1),(-1,-1,1)\}$.

Proposition 8.4. *Let p be an odd prime which divides n and is greater than 3. For the curve $E_{n,\frac{\pi}{3}}$,*

$$\mathrm{Im}(\bar{\delta}_p) = \{(1,1,1),\ (n,n,1),\ (-3n,3,-n),\ (-3,3n,-n)\}.$$

Proposition 8.5. *The image of the connecting homomorphism $\bar{\delta}_3$ for $E_{n,\frac{\pi}{3}}$ is obtained as follows.*

(1) *If $n \equiv 1 \pmod 3$, then*
$$\mathrm{Im}(\bar{\delta}_3) = \{(1,1,1),(-1,-1,1),(3,-3,-1),(-3,3,-1)\}$$
(2) *If $n \equiv 2 \pmod 3$, then*
$$\mathrm{Im}(\bar{\delta}_3) = \{(1,1,1),(-1,-1,1),(3,3,1),(-3,-3,1)\}$$
(3) *If $3 \mid n$, then*
$$\mathrm{Im}(\bar{\delta}_3) = \{(1,1,1),(n,n,1),(-3n,3,-n),(-3,3n,-n)\}$$

Proposition 8.6. *The image of the connecting homomorphism $\mathrm{Im}(\bar{\delta}_2)$ for $E_{n,\frac{\pi}{3}}$ is obtained as follows.*

(1) *If $n \equiv 1 \pmod 8$, then*
$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (1,5,5),\ (-1,2,-2),\ (-1,10,-10), \\ (-5,-10,2),\ (-5,-2,10),\ (5,-5,-1),\ (5,-1,-5) \end{array} \right\}.$$
(2) *If $n \equiv -1, \pm 5 \pmod 8$, then*
$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (1,5,5),\ (n,5n,5),\ (n,n,1), \\ (5n,-1,-5n),\ (5n,-5,-n),\ (5,-5n,-n),\ (5,-n,-5n) \end{array} \right\}.$$
(3) *If $n \equiv 2 \pmod 8$, then*
$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (1,-1,-1),\ (n,n,1),\ (n,-n,-1), \\ (5n,5,n),\ (5n,-5,-n),\ (5,5n,n),\ (5,-5n,-n) \end{array} \right\}.$$
(4) *If $n \equiv -2 \pmod 8$, then*
$$\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1,1),\ (1,-5,-5),\ (n,-5n,-5),\ (n,n,1), \\ (5n,-5,-n),\ (5n,1,5n),\ (5,n,5n),\ (5,-5n,-n) \end{array} \right\}.$$

Remark. We can also see that the 2-Selmer rank of the elliptic curve $E_{n,\frac{\pi}{3}}$ depends on only the *type* of the factorization of the integer n similarly to the case of Selmer rank. For details, see the tables in Section 9.

9. Tables

In the table below, we let p denote a prime, and $s_1(D)$ the Selmer rank of the curve $y^2 = x^3 + Dx$.

Table 1.

(The Selmer rank of the curve $y^2 = x^3 + Dx$, where D has one odd prime factor)

type of D	$s_1(D)$	$s_1(-D)$	$s_1(2D)$	$s_1(-2D)$
$(p \equiv 1 \pmod{16})$				
$D = p$	2	2	2	3
$D = p^2$	2	2	†	††
$D = p^3$	2	2	2	3
$(p \equiv 3 \pmod{16})$				
$D = p$	1	0	0	1
$D = p^2$	1	0	1	0
$D = p^3$	0	0	0	1
$(p \equiv 5 \pmod{16})$				
$D = p$	1	1	0	1
$D = p^2$	0	1	0	1
$D = p^3$	1	0	0	1
$(p \equiv 7 \pmod{16})$				
$D = p$	0	1	2	1
$D = p^2$	1	1	1	2
$D = p^3$	0	1	2	1
$(p \equiv 9 \pmod{16})$				
$D = p$	2	1	2	3
$D = p^2$	2	2	†	††
$D = p^3$	2	1	2	3
$(p \equiv 11 \pmod{16})$				
$D = p$	0	0	0	1
$D = p^2$	1	0	1	0
$D = p^3$	1	0	0	1
$(p \equiv 13 \pmod{16})$				
$D = p$	1	0	0	1
$D = p^2$	0	1	0	1
$D = p^3$	1	1	0	1
$(p \equiv 15 \pmod{16})$				
$D = p$	1	1	2	1
$D = p^2$	1	1	1	2
$D = p^3$	1	1	2	1

† the Selmer rank is 2 or 0 according as 2 is a quartic residue modulo p or not.

†† the Selmer rank is 3 or 1 according as 2 is a quartic residue modulo p or not.

In the table below, we let $s_2(n)$ be the 2-Selmer rank of the curve E_n defined by (1.1). The meanings of the other columns are as follows:

- type : the type of the factorization of n (for example, 2×1 means that $n = 2p$ with $p \equiv 1 \pmod 8$).
- Legendre : the value of the Legendre symbol of the two odd prime factors.
- ex. : the smallest example.

TABLE 2.

(The 2-Selmer rank of E_n, where n has one or two odd prime factors)

type	Legendre	ex.	$s_2(n)$	type	Legendre	ex.	$s_2(n)$
1		17	2	5×5		65	2
3		3	0	5×7	1	155	2
5		5	1		-1	35	0
7		7	1	7×7		161	2
2×1		34	2	$2\times1\times1$	1	3026	4
2×3		6	1		-1	1394	2
2×5		10	0	$2\times1\times3$	1	438	3
2×7		14	1		-1	102	1
1×1	1	1513	4	$2\times1\times5$	1	410	2
	-1	697	2		-1	170	0
1×3	1	219	2	$2\times1\times7$	1	1582	3
	-1	51	0		-1	238	1
1×5	1	205	3	$2\times3\times3$		66	0
	-1	85	1	$2\times3\times5$		30	1
1×7	1	791	3	$2\times3\times7$	1	138	2
	-1	119	1		-1	42	0
3×3		33	0	$2\times5\times5$		130	0
3×5		15	1	$2\times5\times7$		70	1
3×7		21	1	$2\times7\times7$		322	2

Note that Wada [28] showed the rank of E_{1513} is 2.

In the following table, $1\times1\times3$, $(+,-,-)$ means that $n=pqr$ with $p\equiv q\equiv1$, $r\equiv3 \pmod 8$ and $(p/q)=1$, $(p/r)=(q/r)=-1$.

TABLE 3.

(*All* types of $n=pqr$ and $2pqr$ with $s_2(n)=0$)

type	Legendre	ex.	type	Legendre	ex.
$1\times1\times3$	$(+,-,-)$	4539	$2\times1\times1\times5$	$(+,-,-)$	23290
	$(-,+,-)$	3723		$(-,+,-)$	6970
	$(-,-,-)$	2091		$(-,-,-)$	12410
$1\times3\times3$	$(+,-,+)$	969	$2\times1\times3\times3$	$(+,-,+)$	1938
	$(+,-,-)$	2937		$(+,-,-)$	5874
$1\times5\times7$	$(+,-,-)$	1435	$2\times1\times3\times7$	$(+,-,-)$	3066
	$(-,+,-)$	3955		$(-,+,-)$	4746
	$(-,-,+)$	2635		$(-,-,+)$	2346
	$(-,-,-)$	595		$(-,-,-)$	714
$3\times3\times3$	$(+,+,+)$	1947	$2\times1\times5\times5$	$(+,-,+)$	11890
$3\times5\times5$	$(+,-,-)$	195		$(+,-,-)$	2210
	$(-,-,+)$	435	$2\times3\times3\times5$	$(+,+,+)$	2090
	$(-,-,-)$	795		$(+,+,-)$	570
$3\times5\times7$	$(+,+,-)$	385		$(+,-,-)$	1290
	$(+,-,-)$	273	$2\times3\times5\times7$	$(+,+,-)$	770
	$(-,+,-)$	345		$(+,-,+)$	1554
	$(-,-,-)$	105		$(-,+,-)$	690
$3\times7\times7$	$(+,-,+)$	483		$(-,-,+)$	930
			$2\times5\times5\times5$	$(+,+,+)$	31610
				$(+,+,-)$	3770
			$2\times5\times7\times7$	$(+,-,+)$	4186

The following table is the cases that $s_2(n) = 1$. It is conjectured that such n are congruent.

TABLE 4.

(*All* types of $n = pqr$ and $2pqr$ with $s_2(n) = 1$)

type	Legendre	ex.	type	Legendre	ex.
$1\times5\times5$	$(+,-,-)$	11645	$2\times1\times1\times3$	$(+,-,-)$	9078
	$(-,+,-)$	3485		$(-,+,-)$	7446
	$(-,-,-)$	6205		$(-,-,-)$	4182
$1\times1\times7$	$(+,-,-)$	10591	$2\times1\times1\times7$	$(+,-,-)$	21182
	$(-,+,-)$	13447		$(-,+,-)$	26894
	$(-,-,-)$	4879		$(-,-,-)$	9758
$1\times3\times5$	$(+,-,+)$	1615	$2\times1\times3\times5$	$(+,-,+)$	3230
	$(+,-,-)$	1095		$(+,-,-)$	2190
	$(-,+,+)$	663		$(-,+,+)$	1326
	$(-,+,-)$	615		$(-,+,-)$	1230
	$(-,-,+)$	935		$(-,-,+)$	1870
	$(-,-,-)$	255		$(-,-,-)$	510
$1\times3\times7$	$(+,-,+)$	2373	$2\times1\times5\times7$	$(+,-,+)$	10166
	$(+,-,-)$	1533		$(+,-,-)$	2870
	$(-,-,+)$	357		$(-,+,+)$	24518
$3\times3\times5$		165		$(-,+,-)$	7910
$3\times3\times7$		231		$(-,-,+)$	5270
$5\times5\times5$	$(+,-,-)$	3445		$(-,-,-)$	1190
	$(-,-,-)$	2405	$2\times3\times3\times3$	$(+,+,+)$	3894
$5\times5\times7$	$(+,+,-)$	1015	$2\times3\times3\times7$		462
	$(+,-,-)$	2135	$2\times3\times5\times5$		390
	$(-,+,-)$	1295	$2\times3\times7\times7$	$(+,-,+)$	966
	$(-,-,-)$	455		$(+,-,-)$	1974
$5\times7\times7$	$(+,-,+)$	2093		$(-,-,+)$	1302
	$(+,-,-)$	1085	$2\times5\times5\times7$		910
	$(-,-,+)$	805	$2\times7\times7\times7$	$(+,-,+)$	9982
$7\times7\times7$	$(+,-,+)$	4991			

Note that some of types in TABLES 3 and 4 are in Serf [21].

From now on, we consider the $\pi/3$-congruent number problem. Let $s_3(n)$ be the 2-Selmer rank of the elliptic curve

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

In the TABLES 5,6,7,8 and 9, the meanings of the types of n is different from the previous one. For example, 3×1 means that $n = 3p$ with $p \equiv 1 \pmod{24}$.

TABLE 5.

(The 2-Selmer rank of $E_{n,\frac{\pi}{3}}$, where n has one odd prime factor)

type	ex.	$s_3(n)$	$s_3(-n)$	type	ex.	$s_3(n)$	$s_3(-n)$
1	73	2	2	3×1	219	2	2
5	5	0	1	3×5	15	0	1
7	7	0	0	3×7	21	1	1
11	11	1	0	3×11	33	0	1
13	13	1	2	3×13	39	2	1
17	17	1	1	3×17	51	0	0
19	19	0	1	3×19	57	0	1
23	23	1	1	3×23	69	1	1
2×1	146	2	2	6×1	438	3	2
2×5	10	1	1	6×5	30	1	0
2×7	14	0	2	6×7	42	1	0
2×11	22	1	1	6×11	66	1	2
2×13	26	0	0	6×13	78	1	0
2×17	34	1	1	6×17	102	1	0
2×19	38	2	0	6×19	114	1	2
2×23	46	1	1	6×23	138	1	2

TABLE 6.

(*All* types of $n = pq, 2pq, 3pq$ and $6pq$ with $s_3(n) = 0$)

type	Legendre	ex.	type	Legendre	ex.
1×5	-1	365	$2\times 11\times 23$	-1	506
1×7	-1	511	$2\times 13\times 13$		962
1×19	-1	1843	$2\times 13\times 19$	-1	494
5×5		145	$2\times 17\times 23$	-1	782
5×11	-1	319	$3\times 1\times 5$	-1	1095
5×23	-1	115	$3\times 1\times 11$	-1	2409
7×7		217	$3\times 1\times 17$	-1	3723
7×11	-1	77	$3\times 1\times 19$	-1	5529
7×13	-1	91	$3\times 5\times 5$		435
11×11		649	$3\times 5\times 7$	1	465
11×17	-1	187	$3\times 5\times 13$	-1	195
13×17	-1	533	$3\times 5\times 17$		255
13×19	-1	247	$3\times 5\times 23$	-1	345
17×23	-1	391	$3\times 7\times 11$	-1	231
19×19		817	$3\times 7\times 17$	-1	273
19×23	-1	437	$3\times 7\times 23$	-1	483
$2\times 1\times 7$	-1	1022	$3\times 11\times 17$	1	2937
$2\times 1\times 13$	-1	1898	$3\times 11\times 19$	1	627
$2\times 5\times 5$		290	$3\times 13\times 17$	-1	1599
$2\times 5\times 11$	-1	110	$3\times 13\times 23$	-1	1833
$2\times 5\times 17$	-1	170	$3\times 17\times 17$		2091
$2\times 7\times 13$		182	$3\times 17\times 19$	1	969
$2\times 7\times 19$	-1	602	$3\times 19\times 23$		1311

TABLE 7.

(*All* types of $n = pq, 2pq, 3pq$ and $6pq$ with $s_3(-n) = 0$)

type	Legendre	ex.	type	Legendre	ex.
1×7	-1	511	$3 \times 11 \times 19$	1	627
1×11	-1	803	$3 \times 17 \times 17$		2091
5×7	-1	35	$6 \times 1 \times 5$	-1	2190
5×11	1	55	$6 \times 1 \times 7$	-1	3066
13×19	-1	247	$6 \times 1 \times 13$	-1	5694
13×23	-1	611	$6 \times 1 \times 17$	-1	7446
17×19	-1	779	$6 \times 5 \times 7$		210
17×23	-1	391	$6 \times 5 \times 11$	1	330
$2 \times 1 \times 13$	-1	1898	$6 \times 5 \times 13$	1	1830
$2 \times 1 \times 19$	-1	3686	$6 \times 5 \times 17$	1	1230
$2 \times 5 \times 5$		290	$6 \times 7 \times 11$	-1	462
$2 \times 5 \times 11$		110	$6 \times 7 \times 13$		546
$2 \times 5 \times 17$	-1	170	$6 \times 7 \times 17$		714
$2 \times 5 \times 23$	-1	230	$6 \times 7 \times 19$	-1	1806
$2 \times 7 \times 13$	-1	182	$6 \times 7 \times 23$	-1	966
$2 \times 7 \times 19$	1	266	$6 \times 11 \times 19$	1	1254
$2 \times 11 \times 17$	-1	374	$6 \times 11 \times 23$	-1	1518
$2 \times 11 \times 23$	-1	506	$6 \times 13 \times 13$		2886
$2 \times 13 \times 13$	-1	962	$6 \times 13 \times 17$	1	1326
$2 \times 13 \times 19$		494	$6 \times 13 \times 19$	-1	1482
$3 \times 1 \times 17$	-1	3723	$6 \times 17 \times 17$		4182
$3 \times 5 \times 5$		435	$6 \times 17 \times 23$	-1	2346
$3 \times 5 \times 13$	-1	195	$6 \times 19 \times 23$		2622
$3 \times 7 \times 23$	-1	483			

TABLE 8.

(*All* types of $n = pq$ and $2pq$ with $s_3(n) = 1$)

type	Legendre	ex.	type	Legendre	ex.
1×11	-1	803	$2 \times 1 \times 5$	-1	730
1×13	-1	949	$2 \times 1 \times 11$	-1	1606
1×17	-1	1241	$2 \times 1 \times 17$	-1	2482
1×23	-1	2231	$2 \times 1 \times 23$	-1	4462
5×7		35	$2 \times 5 \times 7$		70
5×13		65	$2 \times 5 \times 13$		130
5×17		85	$2 \times 5 \times 19$		190
5×19		95	$2 \times 7 \times 11$		154
7×17		119	$2 \times 7 \times 17$		238
7×19		133	$2 \times 7 \times 23$	-1	322
7×23		161	$2 \times 11 \times 13$		286
11×13	-1	143	$2 \times 11 \times 19$		418
11×19		209	$2 \times 13 \times 17$		442
11×23		253	$2 \times 13 \times 23$		598
13×23	-1	611	$2 \times 17 \times 19$	-1	1558
17×19		323	$2 \times 19 \times 23$		874

TABLE 9.

(*All* types of $n = pq$ and $2pq$ with $s_3(-n) = 1$)

type	Legendre	ex.	type	Legendre	ex.
1×5	-1	365	$2 \times 1 \times 5$	-1	730
1×17	-1	1241	$2 \times 1 \times 11$	-1	1606
1×19	-1	1843	$2 \times 1 \times 17$	-1	2482
1×23	-1	2231	$2 \times 1 \times 23$	-1	4462
5×13	-1	65	$2 \times 5 \times 7$	-1	70
5×19		95	$2 \times 5 \times 13$		130
5×23		115	$2 \times 5 \times 19$		190
7×11		77	$2 \times 7 \times 11$		154
7×13	-1	91	$2 \times 7 \times 17$	-1	238
7×17		119	$2 \times 7 \times 23$		322
7×23		161	$2 \times 11 \times 13$		286
11×13		143	$2 \times 11 \times 19$	1	418
11×17		187	$2 \times 13 \times 17$		442
11×19		209	$2 \times 13 \times 23$		598
13×17	-1	533	$2 \times 17 \times 19$		646
19×23		437	$2 \times 19 \times 23$		874

10. FLOWCHART

In this section, we give the flowchart for the image of the connecting homomorphism $I_p = \mathrm{Im}(\delta'_p)$, $J_p = \mathrm{Im}(\delta_p)$. Recall that our elliptic curve is

$$y^2 = x^3 + Ax^2 + Bx$$

with a discriminant $\Delta = 16B^2(A^2 - 4B)$.

For the images $I_p = \mathrm{Im}(\delta'_p)$, $J_p = \mathrm{Im}(\delta_p)$ with an odd prime p dividing the discriminant, go to Question A1.

For the images $I_2 = \mathrm{Im}(\delta'_2)$, $J_2 = \mathrm{Im}(\delta_2)$, go to Question B1.

Question A1. Does the prime p divide B?

- Yes → Go to Question A3.
- No → Go to Goal A2.

Goal A2. ($p \nmid B$) Let $a = \mathrm{ord}_p(A^2 - 4B)$. Then

- a is even and $(-2A/p) = -1 \to I_p = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.
- the other case $\to I_p = \{1\}$.

Question A3. Does the prime p divide A?

- Yes → Go to Question A5.
- No → Go to Goal A4.

Goal A4. ($p \nmid A$, $p \mid B$) Let $b = \mathrm{ord}_p(B)$. Then

- b is even and $(A/p) = -1 \to I_p = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2}/\mathbb{Q}_p^{\times 2}$.
- the other case $\to I_p = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

Question A5. ($p \mid A$, $p \mid B$) Let $a = \mathrm{ord}_p(A)$, $b = \mathrm{ord}_p(B)$. Which is your case?

- $b = 1 \rightarrow$ Go to Goal A6.
- $b = 2$, $a = 1 \rightarrow$ Go to Question A8.
- $b = 2$, $a \geq 2 \rightarrow$ Go to Question A14.
- $b \geq 3$, $a = 1 \rightarrow$ Go to Goal A7.
- $b = 3$, $a \geq 2 \rightarrow$ Go to Goal A6.

Goal A6. ($b = 1$ or $b = 3$, $a \geq 2$) In your case, $I_p = \langle B \rangle$.

Goal A7. ($b \geq 3$, $a = 1$) In your case, $I_p = \langle -A, B \rangle$.

Question A8. ($b = 2$, $a = 1$) Which is your case?

- $(A'^2 - 4B'/p) = 1 \rightarrow$ Go to Question A11.
- $(A'^2 - 4B'/p) = -1 \rightarrow$ Go to Goal A10.
- $(A'^2 - 4B'/p) = 0 \rightarrow$ Go to Goal A9.

Goal A9. In your case, $J_p = \langle 2A, A^2 - 4B \rangle$.

Goal A10. In your case, $I_p = \langle B \rangle$.

Question A11. Is B a square in $\mathbb{Q}_p$?

- Yes $\rightarrow$ Go to Goal A13.
- No $\rightarrow$ Go to Goal A12.

Goal A12. In your case, $I_p = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.

Goal A13. Let $A = pA'$, $B = p^2 B'$. Since B is a square in $\mathbb{Q}_p$, the congruence $x^2 \equiv B' \pmod{p}$ has solutions. We denote by $\sqrt{B'}$ one of such solutions. Then the image is given as follows.

- $(A' + 2\sqrt{B'}/p) = 1 \rightarrow J_p = \langle p \rangle$.
- $(A' + 2\sqrt{B'}/p) = -1 \rightarrow J_p = \langle pu \rangle$.

Question A14. ($b = 2$, $a \geq 2$) Is $-B$ a square in $\mathbb{Q}_p$?

- Yes $\rightarrow$ Go to Question A16.
- No $\rightarrow$ Go to Goal A15.

Goal A15. In your case, $I_p = \langle B \rangle$.

Question A16. Which is the value $p \mod 4$?

- $p \equiv 1 \pmod{4} \rightarrow$ Go to Goal A18.
- $p \equiv 3 \pmod{4} \rightarrow$ Go to Goal A17.

Goal A17. In your case, $I_p = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.

Goal A18. In your case, the image is given as follows.

- $(-B')^{(p-1)/4} \equiv 1 \pmod{p} \rightarrow I_p = \langle p \rangle$.
- $(-B')^{(p-1)/4} \equiv -1 \pmod{p} \rightarrow I_p = \langle pu \rangle$.

Question B1. Let $a = \mathrm{ord}_2(A)$, $b = \mathrm{ord}_2(B)$. Which is your case?

- $a = 0$, $b = 0 \to$ Go to Goal B2.
- $a = 0$, $b \geq 1 \to$ Go to Goal B8.
- $a = 1$, $b = 0 \to$ Go to Question B10.
- $a \geq 1$, $b = 1 \to$ Go to Goal B3.
- $a = 1$, $b = 2 \to$ Go to Goal B3.
- $a = 1$, $b \geq 3 \to$ Go to Goal B9.
- $a \geq 2$, $b = 0 \to$ Go to Goal B6.
- $a = 2$, $b = 2 \to$ Go to Question B14.
- $a = 2$, $b = 3 \to$ Go to Goal B4.
- $a \geq 3$, $b = 2 \to$ Go to Goal B7.
- $a \geq 3$, $b = 3 \to$ Go to Goal B5.

Goal B2. ($a = 0$, $b = 0$) In your case, the image is given as follows.

- $B \equiv 3 \pmod 4$ or $A \equiv B + 2 \pmod 8 \to I_2 = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
- the other case $\to I_2 = \langle 5 \rangle$.

Goal B3. ($a \geq 1$, $b = 1$ or $a = 1$, $b = 2$) In your case, $I_2 = \langle B, (B+1)(-A+1) \rangle$.

Goal B4. ($a = 2$, $b = 3$) In your case, $I_2 = \langle 5, B \rangle$.

Goal B5. ($a \geq 3$, $b = 3$) In your case, $I_2 = \langle B \rangle$.

Goal B6. ($a \geq 2$, $b = 0$) In your case, the image is given as follows.

- $B \equiv 3 \pmod 4$ and $A + B \equiv 7$ or $11 \pmod{16} \to I_2 = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
- the other case $\to I_2 = \langle B \rangle$.

Goal B7. ($a \geq 3$, $b = 2$) Let $B = 2^2 B'$. Then the image is given as follows.

- $a = 3$ and $B' \not\equiv 5, 9 \pmod{16} \to J_2 = \langle -B' + 4 \rangle$.
- $a = 4$ and $B' \equiv 1, 13 \pmod{16} \to J_2 = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
- $a \neq 4$ and $B' \equiv 5, 9 \pmod{16} \to J_2 = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
- the other case $\to J_2 = \langle -B' \rangle$.

Goal B8. ($a = 0$, $b \geq 1$) In your case, the image is given as the following table.

$A \bmod 8$	b	I_2
1	1	$\langle 5, B \rangle$
	2, 3	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	4	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$
	≥ 5	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
3	1	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	2	$\langle 5, B \rangle$
	3	$\langle 2, 5, B \rangle$
	≥ 4	$\langle -2, 5, B \rangle$

$A \bmod 8$	b	I_2
5	1	$\langle 5, B \rangle$
	2	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 3 : odd	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 4 : even	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$
7	1	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	2	$\langle 5, B \rangle$
	3	$\langle -2, 5, B \rangle$
	≥ 4	$\langle 2, 5, B \rangle$

Goal B9. ($a = 1$, $b \geq 3$) In your case, the image is given as the following table.

$A \mod 16$	$B \mod 32$	I_2
2	0	$\langle -1, 2, B\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle -1, 10, B\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
6	0	$\langle -2, -5, B\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle 2, -5, B\rangle$
	24	$\langle 2, -5\rangle$

$A \mod 16$	$B \mod 32$	I_2
10	0	$\langle -1, 10, B\rangle$
	8	$\langle -1, 2\rangle$
	16	$\langle -1, 2, B\rangle$
	24	$\langle -1, 10\rangle$
14	0	$\langle 2, -5, B\rangle$
	8	$\langle 2, -5\rangle$
	16	$\langle -2, -5, B\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

Question B10. ($a = 1$, $b = 0$) Which is the value $B \bmod 8$?

- $B \equiv 1 \pmod 8 \rightarrow$ Go to Goal B13.
- $B \equiv 5 \pmod 8 \rightarrow$ Go to Goal B12.
- $B \equiv 3$ or $7 \pmod 8 \rightarrow$ Go to Goal B11.

Goal B11. In your case, $I_2 = \langle B\rangle$.

Goal B12. In your case, the image is given as follows.

- If ($A \bmod 32$, $B \bmod 32$) is one of the following, then $I_2 = \mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$.
  $(2, 29), (6, 5), (6, 21), (10, 5), (14, 13), (14, 29),$
  $(18, 13), (22, 5), (22, 21), (26, 21), (30, 13), (30, 29).$
- In the other case, $I_2 = \langle 5\rangle$.

Goal B13. Let $A = 2A'$ and $C = A'^2 - B$, then the image is given as the following table.

$A' \bmod 8$	$\mathrm{ord}_2(C)$	J_2
1	3	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	4	$\langle 5, C\rangle$
	5	$\langle -2, 5, C\rangle$
	≥ 6	$\langle 2, 5, C\rangle$
3	3	$\langle 5, C\rangle$
	4	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 5 : odd	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	≥ 6 : even	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$

$A' \bmod 8$	$\mathrm{ord}_2(C)$	J_2
5	3	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	4	$\langle 5, C\rangle$
	5	$\langle 2, 5, C\rangle$
	≥ 6	$\langle -2, 5, C\rangle$
7	3	$\langle 5, C\rangle$
	4, 5	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	6	$\mathbb{Z}_2^\times \mathbb{Q}_2^{\times 2}/\mathbb{Q}_2^{\times 2}$
	≥ 7	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

Question B14. ($a = b = 2$) Let $A = 4A'$, $B = 4B'$. Which is the value $B' \bmod 8$?

- $B' \equiv 1 \pmod 8 \rightarrow$ Go to Goal B16.
- $B' \equiv 3, 5$ or $7 \pmod 8 \rightarrow$ Go to Goal B15.

Goal B15. In your case, $J_2 = \langle A'^2 - B',\ (A'^2 - B' + 1)(2A' + 1)\rangle$.

Goal B16. Let $C = A'^2 - B'$, then the image is given as the following table.

$A \mod 32$	$C \mod 32$	J_2
4	0	$\langle 2, -5, C\rangle$
	8	$\langle 2, -5\rangle$
	16	$\langle -2, -5, C\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
12	0	$\langle -1, 10, C\rangle$
	8	$\langle -1, 2\rangle$
	16	$\langle -1, 2, C\rangle$
	24	$\langle -1, 10\rangle$

$A \mod 32$	$C \mod 32$	J_2
20	0	$\langle -2, -5, C\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle 2, -5, C\rangle$
	24	$\langle 2, -5\rangle$
28	0	$\langle -1, 2, C\rangle$
	8	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$
	16	$\langle -1, 10, C\rangle$
	24	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

Acknowledgements

I would like to thank Professor Masanobu Kaneko and Professor Yutaka Sueyoshi for their many useful advices and encouragement for me.

References

[1] N. Aoki, *On the* 2*-Selmer groups of elliptic curves arising from the congruent number problem*, Comment. Math. Univ. St. Paul., **48** (1999), 77–101.
[2] N. Aoki, *Selmer groups and ideal class groups*, Comment. Math. Univ. St. Paul., **42** (1993), 209–229.
[3] B. J. Birch and N. M. Stephens, *The parity of the rank of the Mordell-Weil group*, Topology, **5** (1966), 295–299.
[4] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves I*, J. Reine Angew. Math., **212** (1963), 7–25.
[5] B. J. Birch and H. P. F. Swinnerton-Dyer, *Notes on elliptic curves II*, J. Reine Angew. Math., **218** (1965), 79–108.
[6] A. Bremner and J. W. S. Cassels, *On the equation* $Y^2 = X(X^2+p)$, Math. Comp., **42** (1984), 257–264.
[7] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge Univ. Press, Cambridge, 1997.
[8] L. E. Dickson, *History of the Theory of Numbers, Vol. II*, Chelsea Publishing Co., New York, 1966.
[9] M. Fujiwara, *θ-congruent numbers*, in: Number Theory, de Gruyter, Berlin, 1998, 235–241.
[10] T. Goto, *Calculation of Selmer groups of elliptic curves with rational 2-torsions and θ-congruent number problem*, Comment. Math. Univ. St. Paul., **50** (2001), 147–172.
[11] T. Goto, *A note on the Selmer group of the elliptic curve* $y^2 = x^3 + Dx$, Proc. Japan Acad., **77A** (2001), 122–125.
[12] R. K. Guy, *Unsolved Problems in Number Theory,* second edition, Springer, New York Berlin, 1994.
[13] T. Hibino and M. Kan, *θ-congruent numbers and Heegner points*, Arch. Math., **77** (2001), 303–308.
[14] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to* 3 *modulo* 8, Proc. Japan Acad., **72A** (1996), 168–169.
[15] M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith., **XCIV.2** (2000), 153–160.
[16] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math., **118** (1994), 331–370.
[17] A. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, 1992.
[18] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. 97, Springer, 1984.

[19] P. Monsky, *Generalizing the Birch-Stephens theorem I*, Math. Z., **221** (1996), 415–420.
[20] F. R. Nemenzo, *All congruent numbers less than* 40000, Proc. Japan Acad., **74A** (1998), 29–31.
[21] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, de Gruyter, Berlin, 1991, 227–238.
[22] J.-P. Serre, *A Course in Arithmetic*, Grad. Texts in Math. 7, Springer, New York, 1973.
[23] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Grad. Texts in Math. 106, Springer, New York, 1986.
[24] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts Math., Springer, New York, 1992.
[25] R. J. Stroeker and J. Top, *On the equation* $Y^2 = (X + p)(X^2 + p^2)$, Rocky Mountain J. Math., **24** (1994), 1135–1161.
[26] 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, Berlin, 1975.
[27] J. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. **72** (1983), 323–334.
[28] H. Wada, *On the rank of the elliptic curve* $y^2 = x^3 - 1513^2 x$, Proc. Japan Acad., **72A** (1996), 34–35.
[29] S. Yoshida, *On the equation* $y^2 = x^3 + pqx$, Comment. Math. Univ. St. Paul., **49** (2000), 23–42.
[30] S. Yoshida, *Some variants of the congruent number problem I*, Kyushu J. Math., **55** (2001), 387–404.
[31] S. Yoshida, *Some variants of the congruent number problem II*, Kyushu J. Math., to appear.