数理解析研究所講究録 1319 巻 2003 年 183-192

Calculation of Selmer groups of elliptic curves with a rational 2-torsion

TAKESHI GOTO (Faculty of Mathematics, Kyushu University)
後藤丈志 (九州大学数理学府)

ABSTRACT

In this article, we give explicit formulae for the Selmer groups associated to the 2-isogenies, for any elliptic curves with a rational 2-torsion. Furthermore, we give a formula for the 2-Selmer group, in some special cases. Using this formula, we can obtain some results about $\pi/3$-congruent number problem.

1 Introduction

Let E be an elliptic curve with a rational 2-torsion, that is a curve defined by

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

where A, B are integers, and the discriminant $16B^2(A^2-4B)$ is not zero. The point $(0,0)$ on this curve is the rational 2-torsion. It is difficult to compute the rank of this elliptic curve, but Selmer groups are computable, and give an upper bounds of the rank by

$$\operatorname{rank} E(\mathbb{Q}) \leq \log_2 |S^{(\varphi)}(E/\mathbb{Q})| \cdot |S^{(\varphi')}(E'/\mathbb{Q})| - 2, \tag{1}$$

where E' is the curve defined by

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

and φ, φ' are isogenies of degree 2 such that $\varphi' \circ \varphi = [2]_E$, $\varphi \circ \varphi' = [2]_{E'}$. If E has three rational 2-torsions, then the Selmer group $S^{(2)}(E/\mathbb{Q})$ gives a better upper bound of the rank.

Many mathematicians have studied the Selmer groups. For example, Monsky (Appendix in [5]) and Aoki [1] calculated the group for $y^2 = x^3 - n^2x$ (n is an integer), Yoshida [12] did for $y^2 = x^3 + pqx$ (p, q are primes), Schmitt [9] did for $y^2 = x^3 - 2nx^2 + 2n^2x$ (n is an integer), Fujiwara [3], Kan [6], and Yoshida [13] did for $y^2 = x^3 + 2nx^2 - 3n^2x$ ($n = p, 2p, 3p, 6p$ for a prime p). Though there is an algorithm to calculate the Selmer group of a given elliptic curve (cf. [10], [2]), no general formula seems to have been discovered.

Theorem 1 *The Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$, $S^{(\varphi')}(E'/\mathbb{Q})$ are given by*

$$S^{(\varphi)}(E/\mathbb{Q}) = \bigcap_{p \in M_{\mathbb{Q}}} \operatorname{Im}(\delta_p), \quad S^{(\varphi')}(E'/\mathbb{Q}) = \bigcap_{p \in M_{\mathbb{Q}}} \operatorname{Im}(\delta'_p),$$

where $M_{\mathbb{Q}} = \{primes\} \cup \{\infty\}$. The groups $\operatorname{Im}(\delta_p)$, $\operatorname{Im}(\delta'_p)$ are given in §4.

This theorem is a generalized result of some earlier studies. The method owes its origin to Aoki [1]. In [4], an explicit procedure to calculate the Selmer group is described.

Let E_n and $E_{n,\pi/3}$ be elliptic curves defined by

$$E_n \;:\; y^2 = x^3 - n^2x,$$
$$E_{n,\pi/3} \;:\; y^2 = x^3 + 2nx^2 - 3n^2x.$$

Note that these curves have three rational 2-torsions. The curve E_n is connected to *congruent number problem* ([7]), and the curve $E_{n,\pi/3}$ is connected to $\pi/3$-*congruent number problem* ([3]).

Theorem 2 *Let $E = E_n$ or $E_{n,\pi/3}$. The Selmer group $S^{(2)}(E/\mathbb{Q})$ is given by*

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

The groups $\mathrm{Im}(\bar{\delta}_p)$ are given in §2.

2 Definition of the Selmer group

In this section, we recall the definition of the Selmer group. For details, see [11, chap.3] and [10, chap.10]. The Selmer group is usually defined by Galois cohomology:

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

But we will give simpler definition.

Let $\delta' : E(\mathbb{Q}) \to \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ be the following map:

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

This is called the *connecting homomorphism.* We define another homomorphism $\delta : E'(\mathbb{Q}) \to \mathbb{Q}_2^\times/\mathbb{Q}_2^\times$ similarly. Then the rank is given by the formula:

$$\mathrm{rank}\, E(\mathbb{Q}) = \log_2 |\mathrm{Im}(\delta)| \cdot |\mathrm{Im}(\delta')| - 2. \tag{2}$$

Let p be a prime or infinity, then $\delta'_p : E(\mathbb{Q}_p) \to \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ and $\delta_p : E'(\mathbb{Q}_p) \to \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ are defined similarly. These are also called connecting homomorphism.

When we regard the images $\mathrm{Im}(\delta_p)$ as subgroups of $\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$, we have $\mathrm{Im}(\delta) \subset \cap_p \mathrm{Im}(\delta_p)$, From (2), we have the inequality:

$$\mathrm{rank}\, E(\mathbb{Q}) \le \log_2 |\cap \mathrm{Im}(\delta_p)| \cdot |\cap \mathrm{Im}(\delta'_p)| - 2.$$

The Selmer groups are given by

$$S^{(\varphi)}(E/\mathbb{Q}) = \bigcap \mathrm{Im}(\delta_p), \quad S^{(\varphi')}(E'/\mathbb{Q}) = \bigcap \mathrm{Im}(\delta'_p),$$

hence we have the inequality (1). Note that we can calculate the Selmer group easily when the images are given. In §4, we will give the images for *all cases*.

Next, we consider the group $S^{(2)}(E/\mathbb{Q})$. Here, we restrict our elliptic curve to one with three rational 2-torsions, and let E be a curve defined by

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

where α, β are integers. Let $\bar{\delta_p} : E(\mathbb{Q}) \to \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2} \times \mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$ be the following map:

$$\bar{\delta}(P) = \begin{cases} (x, x-\alpha), & \text{if } P \neq (\alpha,0),(0,0),\mathcal{O}, \\ (\alpha, \alpha(\alpha-\beta)), & \text{if } P = (\alpha,0), \\ (\alpha\beta, -\alpha), & \text{if } P = (0,0), \\ (1,1), & \text{if } P = \mathcal{O}. \end{cases}$$

Then the Selmer group is given by

$$S^{(2)}(E/\mathbb{Q}) = \bigcap \mathrm{Im}(\bar{\delta_p}),$$

and this gives a better upper bound, that is,

$$\begin{aligned} \operatorname{rank} E(\mathbb{Q}) &\leq \log_2 |S^{(2)}(E/\mathbb{Q})| - 2 \\ &\leq \log_2 |S^{(\varphi)}(E/\mathbb{Q})| \cdot |S^{(\varphi')}(E'/\mathbb{Q})| - 2. \end{aligned} \tag{3}$$

If the images $\mathrm{Im}(\bar{\delta_p})$ are given, we can calculate the Selmer group $S^{(2)}(E/\mathbb{Q})$. If p is a prime not dividing the discriminant, then $\mathrm{Im}(\bar{\delta_p}) = \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \times \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

Theorem 2' *For the curve E_n, the images $\mathrm{Im}(\bar{\delta_p})$ are given as follows.*

1. $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1),(-1,1)\}$.
2. *If p is an odd prime dividing n, then* $\mathrm{Im}(\bar{\delta}_p) = \{(1,1),\ (n,2n),\ (-n,2),\ (-1,n)\}$.
3. *If n is odd, then* $\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1),\ (1,5),\ (n,2n),\ (n,10n), \\ (-n,2),\ (-n,10),\ (-1,n),\ (-1,5n) \end{array} \right\}$.
4. *If $n \equiv 2 \pmod 8$, then* $\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1),\ (5,-1),\ (n,2n),\ (-n,2), \\ (5n,-2n),\ (-5n,-2),\ (-5,-n),\ (-1,n) \end{array} \right\}$.
5. *If $n \equiv 6 \pmod 8$, then* $\mathrm{Im}(\bar{\delta}_2) = \left\{ \begin{array}{l} (1,1),\ (5,-5),\ (n,2n),\ (-n,2), \\ (5n,-10n),\ (-5n,-10),\ (-5,-5n),\ (-1,n,) \end{array} \right\}$.

For the curve $E_{n,\pi/2}$, the images $\mathrm{Im}(\bar{\delta_p})$ are given as follows.

1. *If $n > 0$, then* $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1),(-1,1)\}$.
2. *If $n < 0$, then* $\mathrm{Im}(\bar{\delta}_\infty) = \{(1,1),(-1,-1)\}$.
3. *If p is a prime greater than 3, then* $\mathrm{Im}(\bar{\delta}_p) = \{(1,1),\ (n,n),\ (-3n,3),\ (-3,3n)\}$.
4. *If $n \equiv 1 \pmod 3$, then* $\mathrm{Im}(\bar{\delta}_3) = \{(1,1),(-1,-1),(3,-3),(-3,3)\}$.
5. *If $n \equiv 2 \pmod 3$, then* $\mathrm{Im}(\bar{\delta}_3) = \{(1,1),(-1,-1),(3,3),(-3,-3)\}$.
6. *If $3 \mid n$, then* $\mathrm{Im}(\bar{\delta}_3) = \{(1,1),(n,n),(-3n,3),(-3,3n)\}$.

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

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

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

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

3 Congruent number problem

If the rank of the curve $E_{n,\pi/3}$ is positive, the integer n is called a *$\pi/3$-congruent number.* If $|S^{(2)}(E_{n,\pi/3}/\mathbb{Q})| = 4$, then the rank is 0, by (3).

Theorem 3 **([3],[6],[13],[4])** *Let p be a prime.*

1. *If* $p \equiv 5, 7$ *or* $19 \pmod{24}$, *then* p *is not* $\pi/3$*-congruent.*
2. *If* $p \equiv 7$ *or* $13 \pmod{24}$, *then* $2p$ *is not* $\pi/3$*-congruent.*
3. *If* $p \equiv 5, 11, 17$ *or* $19 \pmod{24}$, *then* $3p$ *is not* $\pi/3$*-congruent.*

Using Theorem 2, we can obtain more analogous facts.

TABLE 1.
(Types of $n = pq, 2pq, 3pq$ and $6pq$ with rank $E_{n,\pi/3}(\mathbb{Q}) = 0$)

$p \times q$ mod 24	(p/q)	ex.	$p \times q$ mod 24	(p/q)	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

Serf [8] construct such a table for the curve E_n. Using Theorem 2, we can complement Serf's table.

4 Flowchart

In this section, we describe the flowchart giving the groups $\mathrm{Im}(\delta'_p)$, $\mathrm{Im}(\delta_p)$, without proof (see [4] for some special cases). Recall that our elliptic curve is

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

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

In the rest of this article, we denote by $\langle c_1, \cdots, c_n \rangle$ the subgroup of $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, generated by $c_1, \cdots, c_n$, and by u a non-square element modulo p. In view of the following well-known fact, if one of the groups $\mathrm{Im}(\delta_p)$, $\mathrm{Im}(\delta'_p)$ is given, the other group is automatically given.

Theorem 4 *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 $V^\perp = \{x \in \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2} \,|\, (x, y)_p = 1$ for all $y \in V\}$. Then*

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

From the locus $E(\mathbb{R})$, the images $\mathrm{Im}(\delta'_\infty)$, $\mathrm{Im}(\delta_\infty)$ 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, $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times/\mathbb{R}^{\times 2}$, $\mathrm{Im}(\delta_\infty) = \{1\}$.

If p is a prime not dividing the discriminant, then $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, $\mathrm{Im}(\delta_p) = \mathbb{Z}_p^\times\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$. For the groups $I_p = \mathrm{Im}(\delta'_p)$, $J_p = \mathrm{Im}(\delta_p)$ with an odd prime p dividing the discriminant, go to Question A1. For the groups $I_2 = \mathrm{Im}(\delta'_2)$, $J_2 = \mathrm{Im}(\delta_2)$, go to Question B1.

A1 Does the prime p divide B?
- Yes → Go to A3.
- No → Go to A2.

A2 ($p \not| B$) 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 $\to I_p = \{1\}$.

A3 Does the prime p divide A?
- Yes → Go to A5.
- No → Go to A4.

A4 ($p \not| A$, $p \,|\, B$) 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 $\to I_p = \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$.

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

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

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

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

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

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

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

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

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

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

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

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.

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

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

- Yes $\to$ Go to A16.
- No $\to$ Go to A15.

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

A16 Which is the value $p \bmod 4$?

- $p \equiv 1 \pmod 4 \to$ Go to A18.
- $p \equiv 3 \pmod 4 \to$ Go to A17.

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

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

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

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

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

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 $\to I_2 = \langle 5 \rangle$.

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

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

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

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 $\to I_2 = \langle B \rangle$.

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 $\to J_2 = \langle -B' \rangle$.

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	$\langle 2, 5, B\rangle$

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

$A \bmod 16$	$B \bmod 32$	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	$\langle 2, -5\rangle$

$A \bmod 16$	$B \bmod 32$	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	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

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

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

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

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, $I_2 = \langle 5\rangle$.

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	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

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

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

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

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

$A \bmod 32$	$C \bmod 32$	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	$\langle -1, 10\rangle$

$A \bmod 32$	$C \bmod 32$	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	$\mathbb{Q}_2^\times/\mathbb{Q}_2^{\times 2}$

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] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, second edition, Cambridge Univ. Press, Cambridge, 1997.

[3] M. Fujiwara, *θ-congruent numbers*, in: Number Theory, de Gruyter, Berlin, 1998, 235–241.

[4] 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.

[5] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II*, Invent. Math., **118** (1994), 331–370.

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

[7] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Grad. Texts in Math. 97, Springer, 1984.

[8] P. Serf, *Congruent numbers and elliptic curves*, in: Computational Number Theory, de Gruyter, Berlin, 1991, 227–238.

[9] S. Schmitt, *Computation of the Selmer groups of certain parametrized elliptic curves*, Acta Arith., **LXXVIII.3** (1997), 241–254.

[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, New York, 1986.

[11] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergrad. Texts Math., Springer, New York, 1992.

[12] S. Yoshida, *On the equation $y^2 = x^3 + pqx$*, Comment. Math. Univ. St. Paul., **49** (2000), 23–42.

[13] S. Yoshida, *Some variants of the congruent number problem I*, Kyushu J. Math., **55** (2001), 387–404.

Takeshi Goto
Faculty of Mathematics
Kyushu University 33
Fukuoka 812-8581, Japan
e-mail address: tgoto@math.kyushu-u.ac.jp