ODD GRAPHS AND SELMER GROUPS OF CERTAIN ELLIPTIC CURVES

TAKESHI GOTO

Abstract. Feng and Xiong described Selmer groups of elliptic curves concerned with the congruent number problem. They used the traditional 2-descent method, and mentioned interesting relation between Selmer groups and some graphs. In this article, we give an analogous result about $\pi/3$-congruent number problem. For the proof, we use an early result given by the author.

1. Introduction

A positive integer n is called a *congruent number* (CN) if it is the area of a right triangle with rational sides. The congruent number problem means the question of determining whether a given positive integer is a CN or not. Clearly, we may assume without loss of generality that n is a squarefree natural number. 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 [14, chap.1] or Knapp [13, pp.52,53,88]).

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

Tunnell's theorem ([20]) gives a simple criterion for determining whether a given n is congruent or not. This criterion is valid if the weak form of the Birch and Swinnerton-Dyer conjecture is true. On the other hand, many mathematicians investigated the rank of E_n by so-called 2-descent method ([1], [6], [7], [11], [15], [17]). We recall some details about the 2-descent method in §2. For example, the following squarefree positive integers are non-CN's. In this article, p, p_i, q, q_j denote prime numbers and $(*/*)$ the Legendre symbol.

$$\begin{aligned}
&n = p \equiv 3 \pmod 8,\\
&n = 2p, \qquad p \equiv 5 \pmod 8,\\
&n = pq, \qquad (p,q) \equiv (3,3) \pmod 8,\\
&n = pq, \qquad (p,q) \equiv (1,3) \pmod 8, \quad (p/q) = -1,\\
&n = 2p_1 \cdots p_t, \qquad p_i \equiv 5 \pmod 8, \quad (p_j/p_i) = 1 \text{ for } i < j.
\end{aligned}$$

Recently, Feng and Xiong [5] described these non-CN's using terms of graph theory. In §3, we introduce summary of their result.

Fujiwara [3] defined the generalized concept, *θ-congruent numbers* by considering triangles with rational sides and an angle θ. In this article, we focus our attention on the case of $\theta = \pi/3$.

Definition. A natural number n is called a *$\pi/3$-congruent number* ($\pi/3$-CN) if $n\sqrt{3}$ is the area of a triangle with rational sides and an angle $\pi/3$.

The $\pi/3$-congruent number problem is also connected with the following elliptic curves:

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

Fujiwara showed that n is $\pi/3$-congruent if and only if $n = 1$ or the rank of $E_{n,\pi/3}$ is positive. Note that the regular triangle $(2, 2, 2)$ has the area $\sqrt{3}$ and the angle $\pi/3$, however, the rank of $E_{1,\pi/3}$ is zero. Fujiwara [3], Kan [12], Yoshida [21] and the author [8], [9] independently investigated the rank of $E_{n,\pi/3}$ by the 2-descent method. For example, the following squarefree positive integers are non-$\pi/3$-CN's.

$$\begin{aligned}
&n = p, && p \equiv 5, 7, 19 \pmod{24},\\
&n = 2p, && p \equiv 7, 13 \pmod{24},\\
&n = 3p, && p \equiv 5, 11, 17, 19 \pmod{24},\\
&n = pq, && (p, q) \equiv (7, 7) \pmod{24},\\
&n = pq, && (p, q) \equiv (1, 7) \pmod{24}, \quad (p/q) = -1.
\end{aligned}$$

The aim of this article is to give "$\pi/3$-analogy" of the result which is due to Feng and Xiong. In §4, we describe and prove the main result. For the proof, we use an early result given by the author, which is recalled in §2.

2. Selmer groups

In this section, we recall the definition of the Selmer group. For details, see [19, chap.3] and [18, chap.10]. We also recall some results about Selmer groups given in [8], [9]. The Selmer group is usually defined by terms of Galois cohomology:

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

however, we give simpler definition later.

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 a rational 2-torsion. It is difficult to compute the rank of this elliptic curve, however, Selmer groups are computable. Selmer groups give an upper bound of the rank by

$$\operatorname{rank} E(\mathbb{Q}) \le \dim_{\mathbb{F}_2} S^{(\varphi)}(E/\mathbb{Q}) + \dim_{\mathbb{F}_2} S^{(\varphi')}(E'/\mathbb{Q}) - 2, \tag{1}$$

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 $\varphi' \circ \varphi$ and $\varphi \circ \varphi'$ are the duplication maps. The 2-descent method means computing the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\varphi')}(E'/\mathbb{Q})$. The right hand side of (1) is often called *Selmer rank*. If the Selmer rank is zero, then so is the rank.

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

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

We call δ' the *connecting homomorphism*. We define another homomorphism $\delta : E'(\mathbb{Q}) \to \mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ similarly. Then the rank is given by the formula:

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

Let p be a prime or the infinity. We define $\delta'_p : E(\mathbb{Q}_p) \to \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ and $\delta_p : E'(\mathbb{Q}_p) \to \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ similarly. These are also called connecting homomorphisms. By the canonical map $\mathbb{Q}^\times/\mathbb{Q}^{\times 2} \to \mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$, the images $\operatorname{Im}(\delta'_p)$, $\operatorname{Im}(\delta_p)$ can be regarded as the subgroups of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$. Then the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\varphi')}(E'/\mathbb{Q})$ are given by

$$S^{(\varphi)}(E/\mathbb{Q}) = \bigcap_p \operatorname{Im}(\delta_p), \quad S^{(\varphi')}(E'/\mathbb{Q}) = \bigcap_p \operatorname{Im}(\delta'_p). \tag{3}$$

Since $\operatorname{Im}(\delta) \subset S^{(\varphi)}(E/\mathbb{Q})$, $\operatorname{Im}(\delta') \subset S^{(\varphi')}(E'/\mathbb{Q})$, the equation (2) yields the inequality (1). It is difficult to compute $\operatorname{Im}(\delta)$, $\operatorname{Im}(\delta')$, however, $\operatorname{Im}(\delta_p)$, $\operatorname{Im}(\delta'_p)$ are computable. An early result given in [8], [9], describes the images $\operatorname{Im}(\delta_p)$, $\operatorname{Im}(\delta'_p)$ explicitly. Hence we can easily calculate the Selmer groups by (3).

Now, we recall the result given in [8], [9]. For simplicity, we consider the curve

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

where α, β are non-zero distinct rational numbers. 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:

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

The discriminant of the curve is

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

Therefore 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. If p is a good prime, then

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

from a general theory. The early papers [8], [9] gave the images of connecting homomorphisms in all cases, however, we recall only required cases for the $\pi/3$-congruent number problem. In this paper, $\operatorname{ord}_p(N) = e$ means that $p^e \mid N$ and $p^{e+1} \nmid N$. We denote by $\langle c_1, \cdots, c_n \rangle$ the subgroup of $\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ or $\mathbb{Q}_p^\times/\mathbb{Q}_p^{\times 2}$ generated by $c_1, \cdots, c_n$.

Lemma 2.1. *Suppose that* $\operatorname{ord}_2(\alpha) = \operatorname{ord}_2(\beta) = 0$. *Then* $\operatorname{Im}(\delta'_2) = \langle \alpha, \beta \rangle$ *except the following three cases.*

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

Lemma 2.2. *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* $\mathrm{Im}(\delta'_2) = \langle \alpha \rangle$.

Lemma 2.3. *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* $\mathrm{Im}(\delta'_p) = \mathbb{Z}_p^\times \mathbb{Q}_p^{\times 2} / \mathbb{Q}_p^{\times 2}$.
(2) *In the other case,* $\mathrm{Im}(\delta'_p) = \mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2}$.

Lemma 2.4. *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 above lemmas immediately yield the following lemma.

Lemma 2.5. *For the curve* $E_{n,\pi/3}$, *the images* $\mathrm{Im}(\delta'_p)$ *are given as follows.*

(1) $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^\times / \mathbb{R}^{\times 2}$.

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

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

(4) *If* $p \neq 2, 3$ *and* $p \mid n$, *then*

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

In view of the following fact, 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 [2]).

Lemma 2.6. *Let* $(*, *)_p$ *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* $\mathrm{Im}(\delta_p) = \mathrm{Im}(\delta'_p)^\perp$.

From Lemmas 2.5, 2.6, we immediately have the following lemma.

Lemma 2.7. *For the curve* $E_{n,\pi/3}$, *the images* $\mathrm{Im}(\delta_p)$ *are given as follows.*

(1) $\mathrm{Im}(\delta'_\infty) = \mathbb{R}^{\times 2} / \mathbb{R}^{\times 2}$.

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

(3) $$\mathrm{Im}(\delta_3) = \begin{cases} \langle 3 \rangle, & \text{if } n \equiv 6 \pmod 9), \\ \mathbb{Q}_2^{\times 2} / \mathbb{Q}_2^{\times 2}, & \text{if } n \not\equiv 6 \pmod 9). \end{cases}$$

(4) *If* $p \neq 2, 3$ *and* $p \mid n$, *then*

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

For a squarefree positive integer $n = p_1 \cdots p_r$, we define

$$K_n = \langle -1, 2, 3, p_1, \cdots, p_r \rangle \subset \mathbb{Q}^\times / \mathbb{Q}^{\times 2}.$$

It is well-known that $S^{(\varphi)}(E_{n,\pi/3}/\mathbb{Q}) \subset K_n$ and $S^{(\varphi')}(E'_{n,\pi/3}/\mathbb{Q}) \subset K_n$. An element $d \in K_n$ belongs to $S^{(\varphi)}(E_{n,\pi/3}/\mathbb{Q})$ if and only if $d \in \mathrm{Im}(\delta_p)$ for all p. Lemmas 2.5, 2.7 are simplified as follows.

Lemma 2.8. *Suppose that $d \in K_n$. For the curve $E_{n,\pi/3}$, we have the following.*

(1) $d \in \mathrm{Im}(\delta'_\infty)$.
(2) *For $2 \mid d$, $d \in \mathrm{Im}(\delta'_2) \Leftrightarrow 2 \mid n$ and $d \equiv n \pmod 8$.*
(3) *For $2 \nmid d$, $d \notin \mathrm{Im}(\delta'_2) \Leftrightarrow n \equiv 5, \pm 2 \pmod 8$ and $d \equiv 3 \pmod 4$.*
(4) *For $3 \mid d$, $d \notin \mathrm{Im}(\delta'_3) \Leftrightarrow n \equiv 6 \pmod 9$ and $(\frac{d/3}{3}) = 1$.*
(5) *For $3 \nmid d$, $d \notin \mathrm{Im}(\delta'_3) \Leftrightarrow n \equiv 6 \pmod 9$ and $(\frac{d}{3}) = -1$.*
(6) *For $p \mid d$, $d \notin \mathrm{Im}(\delta'_p) \Leftrightarrow p \equiv 1 \pmod 3$ and $(\frac{n/d}{p}) = -1$.*
(7) *For $p \nmid d$, $d \notin \mathrm{Im}(\delta'_p) \Leftrightarrow p \equiv 1 \pmod 3$ and $(\frac{d}{p}) = -1$.*

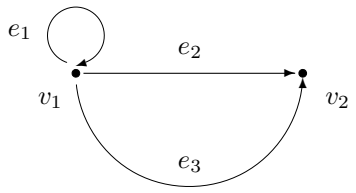
Lemma 2.9. *Suppose that $d \in K_n$. For the curve $E_{n,\pi/3}$, we have the following.*

(1) $d \in \mathrm{Im}(\delta_\infty) \Leftrightarrow d > 0$.
(2) *If $2 \mid d$, then $d \notin \mathrm{Im}(\delta_2)$.*
(3) *For $2 \nmid d$, $d \in \mathrm{Im}(\delta_2)$ if and only if one of the following conditions holds.*
   (a) $n \equiv 5 \pmod 8$.
   (b) $n \equiv \pm 1, -5 \pmod 8$ and $(\frac{-1}{d}) = 1$.
   (c) $n \equiv 2 \pmod 8$ and $(\frac{2}{d}) = 1$.
   (d) $n \equiv -2 \pmod 8$ and $(\frac{-2}{d}) = 1$.
(4) *For $3 \mid d$, $d \in \mathrm{Im}(\delta_3) \Leftrightarrow n \equiv 6 \pmod 9$ and $(\frac{d/3}{3}) = 1$.*
(5) *For $3 \nmid d$, $d \in \mathrm{Im}(\delta_p) \Leftrightarrow (\frac{d}{3}) = 1$.*
(6) *For $p \mid d$, $d \in \mathrm{Im}(\delta_p) \Leftrightarrow p \equiv 1 \pmod 3$ and $(\frac{-n/d}{p}) = 1$.*
(7) *For $p \nmid d$, $d \in \mathrm{Im}(\delta_p) \Leftrightarrow (\frac{d}{p}) = 1$.*

3. Odd graphs

In this section, we recall the definition of odd graphs and recall some result due to Feng and Xiong [5].

Let V and E be finite sets, and consider a map $\psi : E \to V \times V$. We call the pair (V, E, ψ) a *directed graph*. For example, the graph $G = (V, E, \psi)$ given by $V = \{v_1, v_2\}$, $E = \{e_1, e_2, e_3\}$, $\psi(e_1) = (v_1, v_1)$, $\psi(e_2) = (v_1, v_2)$, $\psi(e_3) = (v_1, v_2)$ is regarded as the following diagram:



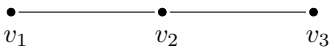
A graph $G = (V, E, \psi)$ is called *simple* if the following conditions hold.

- For any $e \in E$, $\psi(e) \notin \mathrm{diag}(V) := \{(v, v) \mid v \in V\}$.
- The map ψ is injective.

From now on, we only consider simple directed graphs, and identify $\psi(E)$ with E. We denote by $\overrightarrow{vw}$ an element $(v,w) \in E$, and by $\overline{vw}$ two elements (v,w), $(w,v) \in E$. If the condition

$$(v,w) \in E(G) \Rightarrow (w,v) \in E(G)$$

holds, then we call G a *nondirected graph*. For example, if $V(G) = \{v_1, v_2, v_3\}$, $E(G) = \{\overline{v_1v_2}, \overline{v_2v_3}\} = \{(v_1,v_2),(v_2,v_1),(v_2,v_3),(v_3,v_2)\}$, then the graph G is regarded as the following diagram.



Definition. Let $G = (V,E)$ be a simple directed graph.

- If $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \phi$, then we call $\{V_1, V_2\}$ a *partition* of V.
- A partition $\{V_1, V_2\}$ is said to be *trivial* if $V_1 = \phi$ or $V_2 = \phi$.
- A partition $\{V_1, V_2\}$ is called *odd* if there exists $v \in V_1$ such that $\#\{v \to V_2\}$ is odd, or there exists $v \in V_2$ such that $\#\{v \to V_1\}$ is odd.
- Otherwise, $\{V_1, V_2\}$ is called *even*.
- The graph G is called *odd* if any nontrivial partition is odd.
- Otherwise, G is called *even*.
- We call G a semi-odd graph if there exists only one nontrivial even partition.

Clearly, a non-connected graph is even. For example, the following graphs are odd (cf. [5]).

- A directed cycle: $V = \{v_1, \cdots, v_m\}$, $E = \{\overrightarrow{v_1v_2}, \overrightarrow{v_2v_3}, \cdots, \overrightarrow{v_{m-1}v_m}, \overrightarrow{v_mv_1}\}$.
- A non-directed cycle with $|V|$ odd:
  $V = \{v_1, \cdots, v_m\}$, $E = \{\overline{v_1v_2}, \overline{v_2v_3}, \cdots, \overline{v_{m-1}v_m}, \overline{v_mv_1}\}$.
- A complete graph with $|V|$ odd.
- A tree.

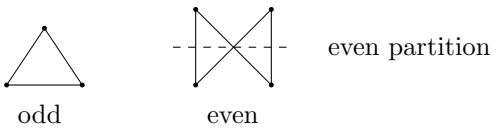


Figure 1: Non-directed cycles.

Oddness of graphs can be translated into terms of linear algebra. Let G be a directed graph with $V(G) = \{v_1, \cdots, v_m\}$ and $A(G)$ the adjacency matrix of G defined by $A(G) = (a_{ij})_{1 \le i,j \le m}$, where

$$a_{ij} = \begin{cases} 1, & \text{if } \overrightarrow{v_iv_j} \in E(G), \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, let d_i be the outdegree of the vertex v_i, namely

$$d_i = \sum_{j=1}^{m} a_{ij}.$$

The *Laplace matrix* $L(G)$ is defined by

$$L(G) = \mathrm{diag}(d_1, \cdots, d_m) - A(G).$$

By the definition, the sum of each row of $L(G)$ is zero, hence $\mathrm{rank}_{\mathbb{Z}}(L(G)) \leq m-1$.

Proposition 3.1 ([4], [5]). *Let G be a directed graph, $m = |V(G)|$ and $r = \mathrm{rank}_{\mathbb{F}_2} L(G)$. Then the number of even partitions of $V(G)$ is 2^{m-r-1}. In particular, G is odd if and only if $r = m-1$. Furthermore, G is semi-odd if and only if $r = m-2$.*

Feng and Xiong [5] noted one more interesting fact. Suppose that G is non-directed graph. A subgraph H of G is called a *spanning tree* if H is a tree and $V(G) = V(H)$. The above proposition and the Kirchhoff theorem (see [10, §1.2.4]) immediately yield the following.

Proposition 3.2 ([5]). *Suppose that G is non-directed graph. Then G is odd if and only if the number of spanning trees of G is odd.*

For example, the non-directed cycle G with $|V(G)| = 4$ is even, therefore the number of spanning trees is even.

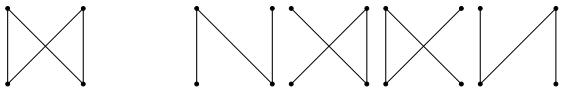


Figure 2: Spanning trees.

Now, we recall one of the results given in [5].

Definition. For an odd integer $n = p_1 \cdots p_t$, we define the directed graph $G(n)$ by

$$V(G(n)) = \{p_1, \cdots, p_t\}, \quad E(G(n)) = \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \leq i \neq j \leq t) \right\}.$$

Theorem 3.3 ([5]). *Suppose that $n \equiv 3 \pmod 8$ and $n = p_1 \cdots p_t$. The Selmer rank of E_n is zero if and only if the following two conditions hold.*

(1) $p_1 \equiv 3 \pmod 4$ *and* $p_i \equiv 1 \pmod 4$ *for* $i \geq 2$.
(2) $G(n)$ *is odd.*

Remark. The Selmer rank of E_n is even if and only if $n \equiv 1, 2$ or $3 \pmod 8$ (see [1], [16]). Feng and Xiong [5] proved similar facts for the cases that $n \equiv 1$ and $2 \pmod 8$.

4. Main results

In this section, we prove a $\pi/3$-analogy of Theorem 3.3.

Definition. For an odd integer $n = p_1 \cdots p_t$, we define the directed graphs $g(n)$, $g'(n)$ by

$$\begin{aligned} V(g(n)) &= \{-1, p_1, \cdots, p_t\}, \\ E(g(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \leq i \neq j \leq t) \right\} \\ &\quad \cup \left\{ \overrightarrow{p_i(-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \leq i \leq t) \right\}, \end{aligned}$$

$$
\begin{aligned}
V(g'(n)) &= \{-1, (-1)', p_1, \cdots, p_t\},\\
E(g'(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\}\\
&\quad \cup \left\{ \overrightarrow{p_i (-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}\\
&\quad \cup \left\{ \overrightarrow{p_i (-1)'} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}.
\end{aligned}
$$

Note that the partition $V_1 = \{-1, (-1)'\}$, $V_2 = V(g'(n)) \backslash V_1$ of $V(g'(n))$ is always even.

Theorem 4.1. *Suppose that $n \equiv 1, 7$ or $19 \pmod{24}$. The Selmer rank of $E_{n,\pi/3}$ is zero if and only if the following three conditions hold.*

(1) $\forall p \mid n,\ p \equiv 1 \pmod 3$.
(2) *$g(n)$ is odd.*
(3) *$g'(n)$ is semi-odd.*

Remark. The Selmer rank of $E_{n,\pi/3}$ is even if and only if

$$n \equiv 1, 2, 3, 5, 7, 9, 14, 15 \text{ or } 19 \pmod{24}.$$

We see this fact by investigating the "root number", namely the sign which appears in the functional equation of the Hasse-Weil L-function of $E_{n,\pi/3}$ (cf. [14], [16], [21]). We can have similar facts for the cases that $n \equiv 2, 3, 5, 9, 14$ and $15 \pmod{24}$ by using Lemmas 2.8, 2.9

For simplicity, we denote by S_n (resp. S'_n) the Selmer group $S^{(\varphi)}(E_{n,\pi/3}/\mathbb{Q})$ (resp. $S^{(\varphi')}(E'_{n,\pi/3}/\mathbb{Q})$). Then the Selmer rank of $E_{n,\pi/3}$ is $\dim_{\mathbb{F}_2} S_n + \dim_{\mathbb{F}_2} S'_n - 2$. It is clear that $\{1, n, -3n, -3\} \subset S'_n$.

Definition. For an odd integer $n = p_1 \cdots p_t q_1 \cdots q_s$ with $p_i \equiv 1 \pmod 3$, $q_j \equiv -1 \pmod 3$, we define the directed graphs $h'(n)$ by

$$
\begin{aligned}
V(h'(n)) &= \{-1, (-1)', p_1, \cdots, p_t, q_1, \cdots, q_s\},\\
E(h'(n)) &= \left\{ \overrightarrow{p_i p_j} \;\middle|\; \left(\frac{p_j}{p_i}\right) = -1 \ (1 \le i \ne j \le t) \right\}\\
&\quad \cup \left\{ \overrightarrow{p_i q_j} \;\middle|\; \left(\frac{q_j}{p_i}\right) = -1 \ (1 \le i \le t,\, 1 \le j \le s) \right\}\\
&\quad \cup \left\{ \overrightarrow{p_i (-1)} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}\\
&\quad \cup \left\{ \overrightarrow{p_i (-1)'} \;\middle|\; \left(\frac{-1}{p_i}\right) = -1 \ (1 \le i \le t) \right\}.
\end{aligned}
$$

Lemma 4.2. *Suppose that $n \equiv 1, 7$ or $19 \pmod{24}$. Then $S'_n = \{1, n, -3n, -3\}$ if and only if the graph $h'(n)$ is semi-odd.*

Proof. Suppose that $h'(n)$ is semi-odd. Then any partition $\{V_1, V_2\}$ of $V(h'(n))$ with $V_1, V_2 \ne \phi, \{-1, (-1)'\}$ is odd. Put $d = \prod V_1$. Note that $d \ne 1, n$. Since the partition is odd, we have

• there exist $p_i \in V_1$ such that $\#\{p_i \to V_2\}$ is odd, hence $(\frac{n/d}{p}) = -1$,
or
• there exist $p_i \in V_2$ such that $\#\{p_i \to V_1\}$ is odd, hence $(\frac{d}{p}) = -1$.
In both cases, $d \notin \mathrm{Im}(\delta'_p)$ from Lemma 2.8 (6),(7). We have proved that any $d \in \langle -1, p_1, \cdots, p_t, q_1, \cdots, q_s \rangle$ does not belong to S'_n. From Lemma 2.8 (2) and the fact $-3 \in S'_n$, we have $S'_n = \{1, n, -3n, -3\}$.

Suppose that the graph $h'(n)$ is not semi-odd. Then there is an even partition $\{V_1, V_2\}$ of $V(h'(n))$ with $V_1, V_2 \neq \phi, \{-1, (-1)'\}$. Put $d = \prod V_1$. Note that $d \neq 1, n$. From Lemma 2.8 (1),(3),(5),(6),(7), we have $d \in \mathrm{Im}(\delta'_\infty)$, $\mathrm{Im}(\delta'_2)$, $\mathrm{Im}(\delta'_3)$, $\mathrm{Im}(\delta'_{q_j})$. Since the partition is even, we have

• for any $p_i \in V_1$, $\#\{p_i \to V_2\}$ is even, hence $(\frac{n/d}{p}) = 1$,
and
• for any $p_i \in V_2$, $\#\{p_i \to V_1\}$ is even, hence $(\frac{d}{p}) = 1$.
Therefore, $d \in \mathrm{Im}(\delta'_{p_i})$, and it follows that $d \in S'_n$. □

In fact, we have proved the following fact:

$$\mathrm{rank}_{\mathbb{F}_2} S'_n = t + s + 2 - \mathrm{rank}_{\mathbb{F}_2} L(h'(n)).$$

If $s \geq 2$, then at least 4 rows of $L(h'(n))$ are zero, hence the Selmer rank is positive. If $s = 1$, then $n \equiv 2 \pmod 3$, a contradiction. Therefore, we need consider only the case of $s = 0$. In this case, we have $h'(n) = g'(n)$, so we have proven the following.

Lemma 4.3. *Suppose that $n \equiv 1, 7$ or $19 \pmod{24}$ and $S'_n = \{1, n, -3n, -3\}$. Then all prime divisors p of n satisfy $p \equiv 1 \pmod 3$, and the graph $g'(n)$ is semi-odd.*

In order to prove Theorem 4.1, we need one more lemma.

Lemma 4.4. *Suppose that $n \equiv 1, 7$ or $19 \pmod{24}$ and $n = p_1 \cdots p_t$ with $p_i \equiv 1 \pmod 3$. Then $S_n = \{1\}$ if and only if the graph $g(n)$ is odd.*

Proof. From Lemma 2.9 (1),(2),(4), it follows that $S_n \subset \langle p_1, \cdots, p_t \rangle$.

Suppose that $g(n)$ is odd. Then any nontrivial partition $\{V_1, V_2\}$ of $V(g(n))$ is odd. Without loss of generality, we may assume that $-1 \notin V_1$, $-1 \in V_2$. Put $d = \prod V_1$. Note that $d \neq 1$. Since the partition is odd, we have

• there exist $p_i \in V_1$ such that $\#\{p_i \to V_2\}$ is odd, hence $(\frac{-n/d}{p}) = -1$,
• there exist $p_i \in V_2$ such that $\#\{p_i \to V_1\}$ is odd, hence $(\frac{d}{p}) = -1$,
or
• $\#\{-1 \to V_1\}$ is odd, hence $(\frac{-1}{d}) = -1$.
From Lemma 2.9 (3),(6),(7), $d \notin \mathrm{Im}(\delta_p)$ or $d \notin \mathrm{Im}(\delta_2)$. In both cases, we have $d \notin S_n$.

Suppose that $g(n)$ is even. Then there exists a nontrivial even partition $\{V_1, V_2\}$ of $V(g(n))$. Without loss of generality, we may assume that $-1 \notin V_1$, $-1 \in V_2$. Put $d = \prod V_1$. Note that $d \neq 1$. From Lemma 2.9 (1), $d \in \mathrm{Im}(\delta_\infty)$. Since the partition is even, we have $d \in \mathrm{Im}(\delta_2)$, $\mathrm{Im}(\delta_{p_i})$ for any i, from the similar argument. Since $p_i \equiv 1 \pmod 3$, we have $d \equiv 1 \pmod 3$ and $d \in \mathrm{Im}(\delta_3)$. Hence $d \in S_n$. □

Lemmas 4.3, 4.4 immediately yield Theorem 4.1.

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

[4] Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture, Acta Arith. **80** (1996), 71–83.

[5] K. Feng and M. Xiong, *On elliptic curves* $y^2 = x^3 - n^2x$ *with rank zero*, J. Number Theory **109** (2004), 1-26.

[6] A. Genocchi, *Sur l'impossibilite de quelques egalites doubles*, C. R. Acad. Sci. Paris, **78** (1874), 423–436.

[7] T. Goto, *A note on the Selmer group of the elliptic curve* $y^2 = x^3 + Dx$*, Proc. Japan Acad.,* **77A** *(2001), 122–125.*

[8] 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.

[9] T. Goto, *A study on the Selmer groups of the elliptic curves with a rational* 2*-torsion*, Doctoral Thesis, Kyushu University, 2002 (available at `http://www.ma.noda.tus.ac.jp/u/tg/list-e.html`).

[10] J. M. Harris, J. L. Hirst and M. J. Mossignhoff, *Combinatorics and Graph Theory*, Undergrad. Texts Math., Springer, New York, 2000.

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

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

[13] A. Knapp, *Elliptic Curves*, Math. Notes 40, Princeton Univ. Press, Princeton, 1992.

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

[15] J. Lagrange, *Nombres congruents et courbes elliptiques*, Sém. Delange-Pisot-Poitou, 16e année, 1974/75, no. 16, 17pp.

[16] P. Monsky, *Generalizing the Birch-Stephens theorem I*, Math. Z., **221** (1996), 415–420.

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

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

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

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

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

Department of Mathematics, Faculty of Science and Technology, Tokyo University of Science, Noda, Chiba, 278-8510, Japan