Some Variants of the Congruent Number Problem III

Shin-ichi Yoshida

0 Introduction

In the earlier papers [Yo1], [Yo2], we have studied some variants of the congruent number problem, which is called $2\pi/3$- and $2\pi/3$- congruent number problem. (See also Fujiwara [Fuj] and Kan [Kan].) According to [Yo1], the problems are reduced to studying the Mordell-Weil group of a series of elliptic curves given by

$$E_m : \quad y^2 = x(x+m)(x-3m)$$

for square-free integers m, and we have obtained that the special value $L(E_m, 1)$ of L-function for E_m is described in terms of positive definite ternary quadratic forms. It is an analogue result of Tunnell's [Tun] for the classical congruent number problem.

In this paper, we use a result of Gauss on ternary quadratic forms to give more useful criterion for non-$2\pi/3$- and non-$2\pi/3$-congruentness. Some of our results are the following.

Theorem 0.1. *Let d be a square-free integer such that $d > 1$ and $d \equiv 1 \pmod 6$. Then*

$$\frac{L(E_{2d}, 1)}{\Omega(E_{2d})} = c_{2,\tilde{d}} \cdot \{h(-8d) - N(d, 3x^2 + 4y^2 + 6z^2)\}^2$$

for some non-zero constant $c_{2,\tilde{d}}$ depending only on $\tilde{d} = d \pmod{24}$, where $\Omega(E_m)$ is the real period of E_m, $h(D)$ the class number of the quadratic orders with discriminant D, and $N(d, 3x^2 + 4y^2 + 6z^2)$ the number of representations of d by the quadratic form $3x^2 + 4y^2 + 6z^2$.

This result says that $L(E_m, 1)$ can be written in terms of more familiar number $h(D)$, and we can use many results of 2-divisibility of $h(D)$ to obtain $L(E_m, 1) \neq 0$ for various m. For instance, we will show the following.

Theorem 0.2. (1) *If p is a prime with $p \equiv 31 \pmod{48}$, then $L(E_{2p}, 1) \neq 0$ and $2p$ is not $2\pi/3$-congruent.*
(2) *Let p, q be prime numbers such that $p \equiv q \equiv 1 \pmod{12}$. Assume that*
(i) *$(q/p) = (2/p) = -1$ or*
(ii) *$(q/p) = 1$ and $(2/p) = (2/q) = -1$,*
where $(\ /\ )$ is the Legendre symbol. Then $L(E_{2pq}, 1) \neq 0$ and $2pq$ is not $2\pi/3$-congruent.
(3) *If p, q be prime numbers such that $p \equiv q \equiv 5 \pmod{24}$, then $L(E_{-pq}, 1) \neq 0$ and pq is not $\pi/3$-congruent.*

Remark. In (1), the Tate-Shafarevich group $Ш(E_{2p})$ of $E_{2p}/\mathbb{Q}$ is a non-trivial finite group. In (2), $Ш(E_{2pq})$ is a finite group of odd order and 2-part of the conjecture of Birch and Swinnerton-Dyer holds. In (3), on the one hand, the proof follows that the conjectural order of $Ш(E_{-pq})$ is odd. On the other hand, the assumption does *not* satisfy the condition of Theorem 4.1 in [Goto]. Therefore, the 2-part of $Ш(E_{-pq})$ cannot be determined if we use the descent via the isogeny $\phi_m : E_m \to E'_m = E_m/\langle(0,0)\rangle$ (see [Yo1] or [Goto]). The phenomenon comes from the fact the map $Ш(E_m)[2] \to Ш(E'_m)[\phi'_m]$ arising from ϕ_m is *not* surjective in general, where ϕ'_m is the dual isogeny of ϕ.

Another interesting application is a property on the class number of quadratic fields $\mathbb{Q}(\sqrt{-3p})$, where $p \geq 5$ is a prime number. It is well-known that

$$\begin{aligned} 2||\, h(-3p), &\quad p \equiv 5 \pmod{12} \\ 4||\, h(-12p), &\quad p \equiv 7, 11, 19 \pmod{24} \\ 8|\, h(-12p), &\quad p \equiv 23 \pmod{24} \\ 4|\, h(-3p), &\quad p \equiv 1 \pmod{12}. \end{aligned}$$

It is natural to ask

(i) when $16|\, h(-12p)$ for $p \equiv 23 \pmod{24}$, and

(ii) when $8|\, h(-3p)$ for $p \equiv 1 \pmod{12}$.

In the case (ii), we have a simple criterion. (See Proposition 4.8 in Section 4.)

The paper is organized as follows. In Section 1, we will review some properties on ternary quadratic forms. In Section 2, we will recall the result from [Yo2] with some remarks. Main theorem will be stated in Section 3. In Section 4, using the result in Section 3 and terminology of graph theory, we will show various results on $2\pi/3$-congruent and $\pi/3$-congruent number problem. Also, we will show a simple criterion whether $8|\, h(-3p)$ or not for a prime $p \equiv 1 \pmod{12}$.

1 Ternary quadratic forms and Gauss' theorem

Let d be an integer and $Q = Q(x_1, x_2, ..., x_n)$ a positive definite quadratic form of n variables. If $(a_1, a_2, ..., a_n) \in \mathbb{Z}^n$ is such that $Q(a_1, a_2, ..., a_n) = d$, then we will refer to $(a_1, a_2, ..., a_n)$ as a *representation* of d by Q. We call $(a_1, a_2, ..., a_n)$ a *primitive* representation of d by Q if $(a_1, a_2, ..., a_n)$ is a representation and the g.c.d. of $a_1, a_2, ..., a_n$ is 1. It is easy to see that all representations d by Q are primitive if d is square-free.

Let $Q = Q(x, y, z)$ be a ternary quadratic form given by

$$Q(x, y, z) = b_1x^2 + b_2y^2 + b_3z^2 + b_4yz + b_5zx + b_6xy$$

with integer coefficients b_i. Let A_Q denote the matrix

$$A_Q = \begin{pmatrix} 2b_1 & b_6 & b_5 \\ b_6 & 2b_2 & b_4 \\ b_5 & b_4 & 2b_3 \end{pmatrix}$$

with the discriminant $d_Q = \det A_Q/2$ of Q. From now on we always assume that every ternary quadratic form has integer coefficients, is primitive (i.e., the g.c.d. of coefficients is 1), and is positive definite.

Let Q be a ternary quadratic form with the matrix A_Q. A 3×3 matrix U whose entries in $\mathbb{Z}$ said to be an *automorph* of Q if $\det U = 1$ and ${}^tUA_QU = A_Q$, where ${}^tU$ denotes the transpose of U. The number of automorphs of Q is finite and define $\mathrm{aut}(Q)$ to be the number of automorphs of Q. Let d be an integer and suppose that (x_1, y_1, z_1) and (x_2, y_2, z_2) are two representations of d by Q. We say that (x_1, y_1, z_1) and (x_2, y_2, z_2) are *essentially distinct* if there is no automorph U of Q such that $(x_1, y_1, z_1) = (x_2, y_2, z_2)\ {}^tU$.

Let Q_1 and Q_2 be ternary quadratic forms with the matrices A_{Q_1} and A_{Q_2}, respectively. For $R = \mathbb{Z}, \mathbb{R}$ or $\mathbb{Z}_p$ with a prime p, we say that Q_1 and Q_2 are *equivalent over* R if there exists a 3×3 matrix U whose entries in R such that the determinant is a unit in R and that $A_{Q_2} = UA_{Q_1}{}^tU$. We simply say that Q_1 and Q_2 are *equivalent* if they are equivalent over $\mathbb{Z}$. We also say that Q_1 and Q_2 are *in the same genus* if Q_1 and Q_2 are equivalent over $\mathbb{R}$ and are equivalent over $\mathbb{Z}_p$ for all primes p.

Proposition 1.1. (p.186 of [Jon].) *Let $Q = Q(x, y, z)$ be a (positive definite, primitive) ternary quadratic forms and d an integer. Suppose that*

there is a real solution to $Q(x, y, z) = d$;

there is a solution to $Q(x, y, z) \equiv d \pmod{2^{\mathrm{ord}_2(d)+3}}$; and

there is a solution to $Q(x, y, z) \equiv d \pmod{p^{\mathrm{ord}_p(d)+1}}$ for every odd prime $p \mid d_Q$. Then there exists a ternary quadratic form Q' which is in the genus as Q such that d is represented by Q'.

Let $\{Q_1, Q_2, ..., Q_n\}$ be a complete set of representatives for the equivalence classes of forms belonging to a particular genus of (positive definite, primitive) ternary quadratic forms. (It is known that there are only finitely many of equivalence classes in a genus of ternary quadratic forms.) Let d be an integer. Recall that $N(d, Q_i)$ is the number of representation of d by Q_i. Define $\widetilde{N}(d, Q_i)$ to be the number of essentially distinct primitive representation of d by Q_i. It is easy to see that if d is square-free then

$$\widetilde{N}(d, Q_i) = N(d, Q_i)/\mathrm{aut}(Q_i).$$

We will also denote by $R(d, Q)$ the number of essentially distinct primitive representation of d by the genus containing a ternary quadratic form Q. Thus,

for any $i = 1, 2, ..., n$ we have

$$R(d, Q_i) = \sum_{j=1}^{n} \widetilde{N}(d, Q_j).$$

We will use the following deep theorem due to Gauss which relate the value of $R(d, Q)$ to the value of class numbers of the quadratic orders of imaginary quadratic fields. (For a proof, see Theorem 86 of [Jon].)

Theorem 1.2. *Let $Q = Q(x, y, z)$ be a primitive positive definite ternary quadratic form given by*

$$Q(x, y, z) = b_1x^2 + b_2y^2 + b_3z^2 + b_4yz + b_5zx + b_6xy$$

with the matrix A_Q. Assume that b_4, b_5 and b_6 are even. Put $\Delta_d = 4d_Q d/\Omega_Q^2$, where Ω_Q is the g.c.d. of two-rowed minors of A_Q. Then, for all integers $d > 1$ and prime to $2d_Q$ we have

$$R(d, Q) = \begin{cases} 2^{-u(\Delta_1)} h(-4\Delta_d)\rho & \text{if the genus of } Q \text{ represents } d, \\ 0 & \text{otherwise,} \end{cases}$$

where $h(D)$ denotes the class number of the quadratic orders with discriminant D and $\rho = \rho(Q, d)$ is given by

$$\rho = \begin{cases} 1/2 & \text{if } \Delta_d \equiv 1, 2 \pmod 4 \text{ or } 4 \pmod 8, \\ 2 & \text{if } \Delta_d \equiv 7 \pmod 8 \text{ and } \Omega_Q \text{ is odd}, \\ 1 & \text{if } \Delta_d \equiv 7 \pmod 8 \text{ and } \Omega_Q \text{ is even}, \\ 1 & \text{if } \Delta_d = 3, \\ 1 & \text{if } \Delta_d \equiv 3 \pmod 8,\ \Delta_d \neq 3 \text{ and } \mathrm{H}_2(Q)(-1)^{\mathrm{ord}_2(\Omega_Q)} = 1, \\ 1/3 & \text{if } \Delta_d \equiv 3 \pmod 8,\ \Delta_d \neq 3 \text{ and } \mathrm{H}_2(Q)(-1)^{\mathrm{ord}_2(\Omega_Q)} \neq 1, \\ 1/4 & \text{if } \Delta_d \equiv 0 \pmod 8, \end{cases}$$

where

$$\mathrm{H}_2(Q) = (-1, -d_Q/4)_2 \cdot (b_1, (b_6/2)^2 - b_1b_2)_2 \cdot (b_1b_2 - (b_6/2)^2, -d_Q/4)_2$$

denotes the Hasse symbol. Here, we will also denote $(\ ,\ )_2$ by the Hilbert symbol. Finally, we recall that $u(m)$ is the number of odd prime factors of m for an integer $m \neq 0$.

2 Notation and preliminaries

In this section, we will review some of results of [Yo2].

Let $Q = Q(x_1, \ldots, x_k)$ be a positive definite quadratic form with integer coefficients. Define the Θ-series corresponding to Q to be

$$\Theta(Q) = \Theta(Q)(\tau) = \sum_{\mathbf{x} \in \mathbb{Z}^k} q^{Q(\mathbf{x})} \quad (q = \exp(2\pi i\tau), \tau \in \mathfrak{H}).$$

Definition 2.1. Let us define several quadratic forms $Q_t^{(k)} = Q_t^{(k)}(x,y,z)$ as follows.

$$
\begin{aligned}
(1)\quad & Q_{1_1}^{(1)} = 2x^2+9y^2+9z^2+6yz,\ Q_{1_1}^{(2)} = 3x^2+6y^2+8z^2\\
(2)\quad & Q_{1_2}^{(1)} = x^2+3y^2+144z^2,\ Q_{1_2}^{(2)} = 3x^2+9y^2+16z^2,\\
& Q_{1_2}^{(3)} = 4x^2+4y^2+37z^2+2yz+4zx+4xy,\\
& Q_{1_2}^{(4)} = 7x^2+7y^2+12z^2-6yz-6zx-2xy\\
(3)\quad & Q_2^{(1)} = x^2+6y^2+12z^2,\ Q_2^{(2)} = 3x^2+4y^2+6z^2\\
(4)\quad & Q_3^{(1)} = x^2+8y^2+24z^2,\ Q_3^{(2)} = 4x^2+8y^2+9z^2+8yz+4zx\\
(5)\quad & Q_6^{(1)} = x^2+2y^2+12z^2,\ Q_6^{(2)} = 2x^2+3y^2+4z^2\\
(6)\quad & Q_{-1_1}^{(1)} = x^2+12y^2+15z^2+12yz,\\
& Q_{-1_1}^{(2)} = 3x^2+4y^2+13z^2+4yz\\
(7)\quad & Q_{-1_2}^{(1)} = 2x^2+3y^2+72z^2,\ Q_{-1_2}^{(2)} = 3x^2+8y^2+18z^2\\
(8)\quad & Q_{-2}^{(1)} = x^2+6y^2+36z^2,\ Q_{-2}^{(2)} = 4x^2+6y^2+9z^2\\
(9)\quad & Q_{-3}^{(1)} = x^2+7y^2+7z^2+2yz,\ Q_{-3}^{(2)} = 3x^2+4y^2+5z^2+4yz
\end{aligned}
$$

Definition 2.2. For $t \in \{\pm 1, \pm 2, \pm 3, 6\}$ and a positive square-free integer d, let us define $a(t,d)$ as follows.

$$
\begin{aligned}
a(1,d) =& \begin{cases} N(d, Q_{1_1}^{(1)}) - N(d, Q_{1_1}^{(2)}) & \text{if } d \equiv 11 \pmod{24} \\ N(d, Q_{1_2}^{(1)}) - N(d, Q_{1_2}^{(2)}) & \text{if } d \equiv 1,7,13 \pmod{24} \end{cases}\\
a(2,d) =& N(d, Q_2^{(1)}) - N(d, Q_2^{(2)})\\
a(3,d) =& N(d, Q_3^{(1)}) - N(d, Q_3^{(2)})\\
a(6,d) =& N(d, Q_6^{(1)}) - N(d, Q_6^{(2)})\\
a(-1,d) =& \begin{cases} N(d, Q_{-1_1}^{(1)}) - N(d, Q_{-1_1}^{(2)}) & \text{if } d \equiv 1,7,19 \pmod{24} \\ N(d, Q_{-1_2}^{(1)}) - N(d, Q_{-1_2}^{(2)}) & \text{if } d \equiv 5 \pmod{24} \end{cases}\\
a(-2,d) =& N(d, Q_{-2}^{(1)}) - N(d, Q_{-2}^{(2)})\\
a(-3,d) =& N(d, Q_{-3}^{(1)}) - N(d, Q_{-3}^{(2)})
\end{aligned}
$$

For $t \in \{\pm 1, \pm 2, \pm 3, 6\}$ and a positive square-free integer d, we put the following condition (C) on t and d.

$$
(C)\quad \begin{cases}
t = 1 & \text{and } d \equiv 1,7,11,13 \pmod{24},\\
t = 2 & \text{and } d \equiv 1 \pmod{6},\\
t = 3 & \text{and } d \equiv 1,17 \pmod{24},\\
t = 6 & \text{and } (d,6) = 1,\\
t = -1 & \text{and } d \equiv 1,5,7,19 \pmod{24},\\
t = -2 & \text{and } d \equiv 1 \pmod{6},\\
t = -3 & \text{and } d \equiv 1,3,5 \pmod{8},\ 3 \nmid d
\end{cases}
$$

For a square-free integer $m \neq 0$, let E_m be the elliptic curve (defined over $\mathbb{Q}$)given by

$$E_m : \quad y^2 = x(x+m)(x-3m).$$

Let $L(E_m, s)$ denote the L-function of E_m and $\Omega(E_m)$ the real period of E_m. For (t, d) such that the condition (C) is satisfied, put

$$Ш_{td} = \left(\frac{a(t,d)}{2^{u(d)}}\right)^2 \times \begin{cases} 1 & \text{if } t = 1 \text{ and } d \equiv 1 \pmod{12} \\ 1/16 & \text{if } t = -1,\ d \equiv 1 \pmod{24} \text{ and } d \neq 1 \\ 1/16 & \text{if } t = -3,\ d \equiv 3 \pmod{8} \text{ and } 3 \nmid d \\ 1/4 & \text{otherwise.} \end{cases}$$

In [Yo2], we have obtained the following.

Theorem 2.3. *Assume that (t, d) satisfies the condition (C). Then we have*
(1) *$L(E_{td}, 1)/\Omega(E_{td}) = c_{t,\tilde{d}} \cdot a(t, d)^2$ for some non-zero constant $c_{t,\tilde{d}}$ depending on $t, \tilde{d} = d \pmod{24}$. In particular, if $a(t, d) \neq 0$ then td is not $2\pi/3$-congruent for $t = 1, 2, 3, 6$ and $-td$ is not $\pi/3$-congruent for $t = -1, -2, -3$.*
(2) *Suppose that $a(t, d) \neq 0$. Then the Tate-Shafarevich group $Ш(E_{td})$ of $E_{td}/\mathbb{Q}$ is finite. Moreover, under the conjecture of Birch and Swinnerton-Dyer [BiSw], we have*

$$\sharp Ш(E_{td}) = Ш_{td}$$

Remark. In fact, we have not treated the case where $t = -1$ and $d \equiv 5 \pmod{24}$ in [Yo2]. In this case, by the same argument as the proof of Theorem 2.1 in [Yo2], we see that

$$\widetilde{\Phi}_{3,3} = \Theta(Q^{(1)}_{-1_2}) - \Theta(Q^{(2)}_{-1_2}) - G_3$$

is an element of $\widetilde{\Phi}_{3,3} \in S^{\perp}_{3/2}(288, \chi_3, \varphi_3)$, where $G_3(\tau) = \Phi_{6,3}(2\tau)$ (with the notation in [Yo2]). The relation between $\widetilde{\Phi}_{3,3}$ and $\Phi_{3,3}$ is given by the formula

$$\Phi_{3,3} = \widetilde{\Phi}_{3,3} - 2G_4 \in S^{\perp}_{3/2}(576, \chi_3),$$

where $G_4(\tau) = \widetilde{G}_4(2\tau)$ and $\widetilde{G}_4 = \Theta(x^2 + 24y^2 + 36z^2) - \Theta(4x^2 + 9y^2 + 24z^2)$ which is in $S^{\perp}_{3/2}(288, \chi_6)$.

Remark. Comparing the Fourier coefficients of theta series $\Phi_{3,-3}$ in [Yo2] with those of

$$\widetilde{\Phi}_{3,-3} = \frac{1}{2}\left\{\Theta(Q^{(1)}_{1_2}) - \Theta(Q^{(2)}_{1_2}) - \Theta(Q^{(3)}_{1_2}) + \Theta(Q^{(4)}_{1_2})\right\} \in S_{3/2}(576, \chi_3),$$

we have $\Phi_{3,-3} = \widetilde{\Phi}_{3,-3} \in S_{3/2}(576, \chi_3)$. Hence we have obtained that if d is a square-free integer with $d \equiv 1, 7, 13 \pmod{24}$, then

$$a(1, d) = \frac{1}{2}\left\{N(d, Q^{(1)}_{1_2}) - N(d, Q^{(2)}_{1_2}) - N(d, Q^{(3)}_{1_2}) + N(d, Q^{(4)}_{1_2})\right\}$$

This fact will be used in the next section.

3 Main result

From Preposition 3 and Proposition 4 of [Leh] (see also [Dic], [Jon]) we can check the following lemma by using a computer.

Lemma 3.1. *The quadratic forms in each of (1) $\sim$ (9) of Definition 2.1 form a genus and we have the following quantities by a direct computation, respectively.*

	$d_{Q_t^{(i)}}$	$\Omega_{Q_t^{(i)}}$	Δ_d	$\mathrm{aut}(Q_t^{(i)})$
(1)	576	24	$4d$	4
(2)	1728	12	$48d$	4
(3)	288	24	$2d$	4
(4)	768	32	$3d$	4
(5)	96	8	$6d$	4
(6)	576	12	$16d$	4
(7)	1728	24	$12d$	4
(8)	864	24	$6d$	4
(9)	192	4	$48d$	4

Remark. Some parts of this Lemma 3.1 are also obtained from [BrIn].

Using Theorem 1.2, we have obtained

Proposition 3.2. *Let $d > 1$ be a square-free integer prime to 6.*
(1) *If $d \equiv 11 \pmod{24}$, then $N(d, Q_{1_1}^{(1)}) + N(d, Q_{1_1}^{(2)}) = 12h(-d)$.*
(2) $N(d, Q_{1_2}^{(1)}) + N(d, Q_{1_2}^{(2)}) + N(d, Q_{1_2}^{(3)}) + N(d, Q_{1_2}^{(4)})$

$$= \begin{cases} 6h(-3d) & \text{if } d \equiv 1 \pmod{24} \\ 2h(-12d) & \text{if } d \equiv 7 \pmod{24} \\ 2h(-3d) & \text{if } d \equiv 13 \pmod{24}. \end{cases}$$

(3) *If $d \equiv 1 \pmod{6}$, then $N(d, Q_2^{(1)}) + N(d, Q_2^{(2)}) = 2h(-8d)$.*
(4) *If $d \equiv 1, 17 \pmod{24}$, then $N(d, Q_3^{(1)}) + N(d, Q_3^{(2)}) = 6h(-3d)$.*
(5) $N(d, Q_6^{(1)}) + N(d, Q_6^{(2)}) = h(-24d)$.
(6) $N(d, Q_{-1_1}^{(1)}) + N(d, Q_{-1_1}^{(2)})$

$$= \begin{cases} 4h(-4d) & \text{if } d \equiv 1 \pmod{24} \\ 4h(-d) & \text{if } d \equiv 7 \pmod{24} \\ 12h(-d) & \text{if } d \equiv 19 \pmod{24}. \end{cases}$$

(7) *If $d \equiv 5 \pmod{24}$, then $N(d, Q_{-1_2}^{(1)}) + N(d, Q_{-1_2}^{(2)}) = 2h(-3d)$.*
(8) *If $d \equiv 1 \pmod{6}$, then $N(d, Q_{-2}^{(1)}) + N(d, Q_{-2}^{(2)}) = h(-24d)$.*

(9) $N(d, Q_{-3}^{(1)}) + N(d, Q_{-3}^{(2)})$

$$= \begin{cases} 6h(-3d) & \text{if } d \equiv 1 \pmod 8 \\ 2h(-12d) & \text{if } d \equiv 3 \pmod 8 \\ 2h(-3d) & \text{if } d \equiv 5 \pmod 8. \end{cases}$$

Proof. Each statement of this theorem can be proved similarly, so we only give the proof for the part (4).

Let $d > 1$ be a square-free integer with $d \equiv 1, 17 \pmod{24}$. Then, it is easy to see that

$$\begin{aligned} Q_3^{(1)}(\sqrt{d}, 0, 0) &= d, \\ Q_3^{(1)}(1, 0, 0) &\equiv d \pmod 8, \\ Q_3^{(1)}(1, 0, 0) &\equiv d \pmod 3 \text{ if } d \equiv 1 \pmod{24}, \\ Q_3^{(1)}(0, 1, 0) &\equiv d \pmod 3 \text{ if } d \equiv 17 \pmod{24}. \end{aligned}$$

By Proposition 1.1, we have obtained that the genus of $Q_3^{(1)}$ represents d.

From Lemma 3.1 (4), we see that $\Delta_d = 3d \equiv 3 \pmod 8$ and $d \neq 3$ since $d \equiv 1, 17 \pmod{24}$. Moreover, since

$$\begin{aligned} \mathrm{H}_2(Q_3^{(1)}) &= (-1, -2^6 \cdot 3)_2 \cdot (1, -2^3)_2 \cdot (2^3, -2^6 \cdot 3)_2 \\ &= (-1, -3)_2 \cdot (1\_2)_2 \cdot (2\_3)_2 \\ &= 1 \cdot 1 \cdot (-1) \\ &= -1, \end{aligned}$$

we see that $\mathrm{H}_2(Q_3^{(1)}) \cdot (-1)^{\mathrm{ord}_2(\Omega_{Q_3^{(1)}})} = -1 \cdot (-1)^5 = 1$. So $\rho(Q_3^{(1)}, d) = 1/2$.

Theorem 1.2 says that

$$\left(R(d, Q_3^{(1)} =\right) \frac{1}{4} N(d, Q_3^{(1)}) + \frac{1}{4} N(d, Q_3^{(2)}) = \frac{1}{2} h(-12d).$$

Finally, by using the following lemma below, it is sasy to see that $h(-12d) = 2h(-3d)$. So the part (4) of the theorem follows. □

Lemma 3.3. *Let $D \equiv 0, 1 \pmod 4$ be a negative integer and m a positive integer. Then*

$$h(m^2 D) = \frac{h(D) m}{[\mathcal{O}^* : \mathcal{O}'^*]} \prod_{\text{prime } p \mid m} \left(1 - \left(\frac{D}{p}\right)_K \frac{1}{p}\right),$$

where $(\ /\ )_K$ is the Kronecker symbol and where $\mathcal{O}^*$ and $\mathcal{O}'^*$ are the unit group of the orders of discriminant D and $m^2 D$, respectively.

For a proof, see [Cox].

Combining Definition 2.2 with Proposition 3.2, we can easily prove the following main theorem.

Theorem 3.4. *Let $d > 1$ be a square-free integer prime to 6.*

(1) *If $d \equiv 11 \pmod{24}$, then*

$$a(1,d) = -2N(d, Q_{1_1}^{(2)}) + 12h(-d) = 2N(d, Q_{1_1}^{(1)}) - 12h(-d).$$

(2) *If $d \equiv 1, 7, 13 \pmod{24}$, then*

$$\begin{aligned} a(1,d) &= -N(d, Q_{1_2}^{(2)}) - N(d, Q_{1_3}^{(3)}) + \begin{cases} 3h(-3d) & \text{if } d \equiv 1 \pmod{24} \\ h(-12d) & \text{if } d \equiv 7 \pmod{24} \\ h(-3d) & \text{if } d \equiv 13 \pmod{24}. \end{cases} \\ &= N(d, Q_{1_2}^{(1)}) + N(d, Q_{1_2}^{(4)}) - \begin{cases} 3h(-3d) & \text{if } d \equiv 1 \pmod{24} \\ h(-12d) & \text{if } d \equiv 7 \pmod{24} \\ h(-3d) & \text{if } d \equiv 13 \pmod{24}. \end{cases} \end{aligned}$$

(3) *If $d \equiv 1 \pmod{6}$, then*

$$a(2,d) = -2N(d, Q_2^{(2)}) + 2h(-8d) = 2N(d, Q_2^{(1)}) - 2h(-8d).$$

(4) *If $d \equiv 1, 17 \pmod{24}$, then*

$$a(3,d) = -2N(d, Q_3^{(2)}) + 6h(-3d) = 2N(d, Q_3^{(1)}) - 6h(-8d).$$

(5) $a(6,d) = h(-24d) - 2N(d, Q_6^{(2)}) = 2N(d, Q_6^{(1)}) - h(-24d)$.

(6) *If $d \equiv 1, 7, 19 \pmod{24}$, then*

$$\begin{aligned} a(-1,d) &= -2N(d, Q_{-1_1}^{(2)}) + \begin{cases} 4h(-4d) & \text{if } d \equiv 1 \pmod{24} \\ 4h(-d) & \text{if } d \equiv 7 \pmod{24} \\ 12h(-d) & \text{if } d \equiv 19 \pmod{24}. \end{cases} \\ &= 2N(d, Q_{-1_1}^{(1)}) - \begin{cases} 4h(-4d) & \text{if } d \equiv 1 \pmod{24} \\ 4h(-d) & \text{if } d \equiv 7 \pmod{24} \\ 12h(-d) & \text{if } d \equiv 19 \pmod{24}. \end{cases} \end{aligned}$$

(7) *If $d \equiv 5 \pmod{24}$, then*

$$a(-1,d) = -2N(d, Q_{-1_2}^{(2)}) + 2h(-3d) = 2N(d, Q_{-1_2}^{(1)}) - 2h(-3d).$$

(8) *If $d \equiv 1 \pmod{6}$, then*

$$a(-2,d) = -2N(d, Q_{-2}^{(2)}) + h(-24d) = 2N(d, Q_{-2}^{(1)}) - h(-24d).$$

(9) *If $d \equiv 1, 3, 5 \pmod{8}$, then*

$$\begin{aligned} a(-3,d) &= -2N(d, Q_{-3}^{(2)}) + \begin{cases} 6h(-3d) & \text{if } d \equiv 1 \pmod{8} \\ 2h(-12d) & \text{if } d \equiv 3 \pmod{8} \\ 2h(-3d) & \text{if } d \equiv 5 \pmod{8}. \end{cases} \\ &= 2N(d, Q_3^{(1)}) - \begin{cases} 6h(-3d) & \text{if } d \equiv 1 \pmod{8} \\ 2h(-12d) & \text{if } d \equiv 3 \pmod{8} \\ 2h(-3d) & \text{if } d \equiv 5 \pmod{8}. \end{cases} \end{aligned}$$

Proof. If $d \equiv 1, 17 \pmod{24}$ then, by Definition 2.2, we see that

$$\begin{aligned} a(3,d) &= N(d, Q_3^{(1)}) - N(d, Q_3^{(2)}) \\ &= -2N(d, Q_3^{(2)}) + (N(d, Q_3^{(1)}) + N(d, Q_3^{(2)})) \\ &= 2N(d, Q_3^{(1)}) - (N(d, Q_3^{(1)}) + N(d, Q_3^{(2)})). \end{aligned}$$

So the part (4) follows from Proposition 3.2(4). Other parts can be obtained by the same argument. Note that one also uses the last remark in Section 2 to prove the part (2). □

Theorem 0.1 follows from Theorem 3.4(3) and Theorem 2.3.

4 Application

Recently, one can find a lot of paper on the size of Selmer groups of elliptic curves by using terminology of graph theory. For instance, see [Feng], [FeXi], [FaJa], [BCJKLR], [Zha1], [Zha2], and [Zha3] in the case of the congruent number elliptic curves $y^2 = x^3 - m^2x$, and [Goto] in the case of $\pi/3$-congruent number elliptic curves E_{-m} $(m > 0)$.

Following [Feng], we will use graph theory to obtain various non-vanishing results of the special value of L-series of E_m. We also mention that if $L(E_m, 1) \neq 0$ then both $E_m(\mathbb{Q})$ and $Ш(E_m)$ are finite by the deep result of Kolyvagin [Kol1], [Kol2].

We begin with the work of Rédei and Reichardt [Réd], [RR].

Let D be a discriminant of a imaginary quadratic field k. Let $\mathrm{Cl}(k)$ denote the ideal class group of k, $\mathrm{Cl}(k)[2^\infty]$ its 2-Sylow subgroup. We define non-negative integers e_j $(j = 1, 2, \ldots)$ by the formula

$$\sharp(\mathrm{Cl}(k)[2^\infty]/(\mathrm{Cl}(k)[2^\infty])^{2^j}) = 2^{e_1+e_2+\cdots+e_j}.$$

In particular, e_2 is the *4-rank* of $\mathrm{Cl}(k)$.

We say that an unordered pair $\{D_1, D_2\}$ is *D-splitting* if both D_1 and D_2 are discriminants of quadratic fields and $D = D_1D_2$. For this purpose, we allow to say that $\{1, D\} = \{D, 1\}$ is also D-splitting, called the *trivial* D-splitting. By definition, a D-splitting $\{D_1, D_2\}$ is called *of second kind* if

$$\begin{aligned} \left(\frac{D_1}{p}\right)_K &= 1 \quad \text{for any prime } p \mid D_2 \text{ and} \\ \left(\frac{D_2}{p}\right)_K &= 1 \quad \text{for any prime } p \mid D_1 \ , \end{aligned}$$

where, as before, we denote by $(\ /\ )_K$ the Kronecker symbol.

By the genus theory of Gauss, the number of all D-splittings is equal to $2^{e_1} = 2^{m-1}$,where m is the number of prime factors of D. The theorem of Rédei and Reichardt as follows.

Theorem 4.1. *The number of D-splittings of second kind is* 2^{e_2}.

We recall standard terminology of graph theory.
Let $G = (V, E)$ be a simple directed graph, $V = \{v_1, \ldots, v_m\}$ the vertices of G, and $E \subset V \times V$ the arcs of G. The *adjacency matrix* $A(G) = (a_{ij})_{1 \le i,j \le m}$ of G is defined by

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } \overrightarrow{v_i v_j} := (v_i, v_j) \in E \\ 0 & \text{otherwise} \end{cases}$$

Set $d_i = \sum_{j=1}^{m} a_{ij}$ $(i = 1, \ldots, m)$ and $M(G) = \mathrm{diag}(d_1, \ldots, d_m) - A(G)$. Let $r_2(G)$ be the $\mathbb{F}_2$-rank of $M(G)$. It is easy to see that $r_2(G) \le \mathrm{rank}_{\mathbb{Q}} M(G) \le m - 1$.

Definition 4.2. Let $G = (V, E)$ be a directed graph.
(1) We say that $V = V_1 \cup V_2$ is a *partition* of V if $V_1 \cap V_2 = \emptyset$. A partition $V = V_1 \cup V_2$ is called *trivial* if $V_1 = V$ or $V_2 = V$.
(2) A partition $V = V_1 \cup V_2$ of V is called *odd* if
· there exists $w_1 \in V_1$ such that $\sharp\{w_2 \in V_2 |\ \overrightarrow{w_1 w_2} \in E\}$ is odd, or
· there exists $w_2 \in V_2$ such that $\sharp\{w_1 \in V_1 |\ \overrightarrow{w_2 w_1} \in E\}$ is odd.
Otherwise the partition is called *even*.
(3) G is called *odd* if each non-trivial partition of V is odd.

The following proposition is known. (For example, see [Feng].)

Proposition 4.3. *Let $G = (V, E)$ be a directed graph with m vertices. Then the number of even partitions of V is $2^{m - r_2(G) - 1}$. In particular, G is an odd graph if and only if $r_2(G) = m - 1$.*

Let D be a discriminant of a imaginary quadratic field. It is well-known that any discriminant (of a quadratic field) factors uniquely into a product of prime discriminants. Here the prime discriminants are $(-1)^{(p-1)/2} p$ for an odd prime, together with $-4, -8, 8$. Prime discriminants will be denoted by p^*; associate to a prime discriminant its unique prime divisor p. Suppose the discriminant $D = p_1^* p_2^* \cdots p_m^*$ factors into a product of m distinct prime discriminants.

Following [Réd], [RR], let us define a graph $G(D) = (V(D), E(D))$ as follows.
(1) The set of vertices: $V(D) = \{p_1, \ldots p_m\}$.
(2) The set of arcs:

$$E(D) = \left\{ \overrightarrow{p_i p_j} \;\middle|\; 1 \le i, j \le m, \left(\frac{p_i^*}{p_j}\right)_K = -1 \right\}$$

Let $A(G(D)) = (a_{ij})_{1 \le i,j \le m}$ be the adjacency matrix of $G(D)$, that is,

$$a_{ij} = \begin{cases} 1 & \text{if } i \neq j \text{ and } (p_i^*/p_j)_K = -1 \\ 0 & \text{otherwise.} \end{cases}$$

As before, set $d_i = \sum_{j=1}^{m} a_{ij}$ $(i = 1, \ldots, m)$ and $M(G(D)) = \mathrm{diag}(d_1, \ldots, d_m) - A(G(D))$. Let $r_2(G(D))$ be the $\mathbb{F}_2$-rank of $M(G(D))$.

Redéi [Réd] shows that the system of linear equations

$$\sum_{i=1}^{m} a_{ij}(x_i + x_j) = 0 \quad (1 \leq j \leq m)$$

viewed over $\mathbb{F}_2$ has rank exactly $m - e_2 - 1$. Note that the coefficient matrix of the system of linear equations is equals to $M(G(D))$ over $\mathbb{F}_2$. Hence, comparing with Proposition 4.3, we have obtained the following.

Theorem 4.4. *In the above notation, we have $e_2 = r_2(G(D))$. In particular, $e_2 = 0$, that is, $2^{m-1} \parallel h(D)$ if and only if $G(D)$ is an odd graph.*

We are ready to prove various results on $2\pi/3$- and $\pi/3$-congruent number problem. We have the following result which the author could not prove in [Yo2]. (See the last remark of section 3 of [Yo2].)

Theorem 4.5. *Let p be a prime number such that $p \equiv 11, 19 \pmod{24}$. Then $L(E_{-3p}, 1) \neq 0$. In particular, $3p$ is not $\pi/3$-congruent. Moreover, $\sharp Ш(E_{-3p})$ and $Ш_{-3p}$ are odd, so the 2-part of the Birch and Swinnerton-Dyer conjecture for E_{-3p} is true.*

Proof. By the quadratic reciprocity laws, we have $(-4/p)_K = (-p/2)_K = -1$, $(-3/p)_K \cdot (-p/3)_K = -1$ and $(-4/3)_K = (-3/2)_K = -1$. Hence we see that the graph $G(-12p)$ is odd. It follows from Theorem 4.4 that $h(-12p) \equiv 4 \pmod{8}$.

Since $p \equiv 3 \pmod{4}$, it is easy to see that

$$\begin{aligned}
& N(p, Q_{-3}^{(2)}) \\
= \; & N(p, 3x^2 + (2y+z)^2 + 4z^2) \\
\equiv \; & \sharp\{(x,y,z) \mid \; 3x^2 + (2y+z)^2 + 4z^2 = p, (2y+z)z = 0\} \pmod{8} \\
= \; & \sharp\{(x,y,z) \mid \; 3x^2 + 4y^2 = p\} + \sharp\{(x,y,z) \mid \; 3x^2 + 16y^2 = p\} \\
= \; & \begin{cases} 0 & \text{if } p \equiv 11 \pmod{24} \\ 4+4 & \text{if } p \equiv 19 \pmod{24} \end{cases} \\
\equiv \; & 0 \pmod{8}
\end{aligned}$$

Therefore we have obtained that

$$\frac{a(-3,p)}{2} = -N(p, Q_{-3}^{(2)}) + h(-12p) \equiv 4 \pmod{8}$$

by Theorem 3.4(9). In particular, $L(E_{-3p}, 1)/\Omega(E_{-3p}) = c_{-3,p} a(-3,p)^2 \neq 0$ and $3p$ is not $\pi/3$-congruent by Theorem 2.3(1). Moreover, the above congruence shows that $Ш_{-3p}$ is odd because of Theorem 2.3(2). The oddness of $Ш(E_{-3p})$ follows from Table 1 of [Yo1]. □

Let us prove Theorem 0.2.

Proof of Theorem 0.2 (1) Since $p \equiv 15 \pmod{16}$, a result of Pizer [Piz] says that $8 \mid h(-8p)$. We also see that

$$\begin{aligned} N(p, Q_2^{(2)}) &= N(p, 3x^2+4y^2+6z^2) \\ &\equiv \sharp\{(x,y,z) \mid 3x^2+4y^2 = p\} \pmod 8 \\ &= 4 \end{aligned}$$

since $p \equiv 7 \pmod{12}$. Therefore we have obtained that

$$\frac{a(2,p)}{2} = -N(p, Q_2^{(2)}) + h(-8p) \equiv 4 \pmod 8$$

by Theorem 3.4(3). In particular, $L(E_{2p},1)/\Omega(E_{2p}) = c_{2,p}a(2,p)^2 \neq 0$ and $2p$ is not $2\pi/3$-congruent by Theorem 2.3(1). This proves (1). We remark that the above congruence shows that $4 \parallel Ш_{2p}$ because of Theorem 2.3(2). The non-triviality of $Ш(E_{2p})$ follows from Table 1 of [Yo1].

(2) From the assumption, the same argument as Theorem 4.5 shows that the graph $G(-8pq)$ is odd and hence $h(-8pq) \equiv 4 \pmod 8$.

$$\begin{aligned} N(pq, Q_2^{(2)}) &= N(pq, 3x^2+4y^2+6z^2) \\ &\equiv \sharp\{(x,y,z) \mid 3x^2+4y^2 = pq\} \pmod 8 \\ &= 0 \end{aligned}$$

since $pq \equiv 1 \pmod 4$. Therefore we have obtained that

$$\frac{a(2,pq)}{2} = -N(pq, Q_2^{(2)}) + h(-8p) \equiv 4 \pmod 8$$

by Theorem 3.4(3). Moreover, the above congruence shows that $Ш_{2pq}$ is odd because of Theorem 2.3(2). The oddness of $Ш(E_{2pq})$ follows by the 2-descent method as in [Yo1].

(3) First we see that

$$N(pq, Q_{-1_1}^{(2)}) = \sharp\{(x,y,z) | pq = x_1^2 + 12y_1^2 + 12z^2;\ y_1, z : \text{odd}\}$$

since $pq \equiv 1 \pmod{24}$ and the correspondence $(x_1, y_1) = (2y+z, x/2)$. Hence we use the condition $pq \equiv 1 \pmod{24}$ again to obtain that

$$\begin{aligned} N(pq, Q_{-1_1}^{(2)}) &= N(pq, x^2+12y^2+12z^2) - N(pq, x^2+48y^2+48z^2) \\ &\equiv 2N(pq, x^2+12y^2) + 2N(pq, x^2+24y^2) \\ &\qquad -2N(pq, x^2+48y^2) - 2N(pq, x^2+96y^2) \pmod{16} \\ &= 2N(pq, x^2+24y^2) - 2N(pq, x^2+96y^2). \end{aligned}$$

(The last equality follows from $p \equiv q \equiv 2 \pmod 3$.)

Next we will show that $N(pq, x^2+24y^2) = 8, N(pq, x^2+96y^2) = 4$. In fact, we can write $p = 2a^2+3b^2, q = 2c^2+3d^2$ with odd positive integers a, b, c, d since $p \equiv q \equiv 5 \pmod{24}$. Then $pq = (2ac+3bd)^2 + 6(ad-bc)^2$ and any solution

of the equation $x^2 + 6y^2 = pq$ (in integers) has $y = \pm(ad - bc), \pm(ad + bc)$. Since a, b, c, d are all odd, we easily have $N(pq, x^2 + 24y^2) = 8$. Moreover, either $4 \mid ad - bc$ or $4 \mid ad + bc$ is satisfied and we have $N(pq, x^2 + 96y^2) = 4$. Since $G(-4pq)$ is an even graph from the assumption, $h(-4pq) \equiv 0 \pmod 8$. Theorem 3.4(6) gives

$$\begin{aligned} \frac{a(-1, pq)}{4} &= h(-4pq) - \frac{1}{2}N(pq, Q^{(2)}_{-1_1}) \\ &\equiv h(-4pq) - N(pq, x^2 + 24y^2) + N(pq, x^2 + 96y^2) \pmod 8 \\ &\equiv 4 \pmod 8. \end{aligned}$$

Therefore we have $L(E_{-pq}, 1) \neq 0$ and pq is not $\pi/3$-congruent.
This completes the proof. □

Remark. Let $p, q \geq 5$ be distinct prime numbers and let $t \in \{\pm 1, \pm 2, \pm 3, 6\}$. By an argument similar to Theorem 0.2 (2), we can show that $L(E_{tpq}, 1) \neq 0$ for a lot of "two prime factors" cases where the 2-torsion part of $Ш(E_{tpq})$ is trivial. For example, we have the following.

Theorem 4.6. *Let $p, q \geq 5$ be distinct prime numbers.*
(1) *For the following integer m, $L(E_m, 1) \neq 0$ and m is not a $2\pi/3$-congruent number.*

(i) $m = pq$, $pq \equiv 11 \pmod{24}$, $(p/q) = -1$.
(ii) $m = pq$, $p \equiv 1 \pmod{24}$, $q \equiv 7 \pmod{24}$, $(p/q) = -1$.
(iii) $m = 2pq$, $p \equiv q \equiv 5, 13 \pmod{24}$.
(iv) $m = 3pq$, $pq \equiv 17 \pmod{24}$, $(p/q) = -1$.
(v) $m = 6pq$, *$G(-24pq)$ is an odd graph.*

(2) *For the following integer m, $L(E_m, 1) \neq 0$ and $|m|$ is not a $\pi/3$-congruent number.*

(i) $m = -pq$, $pq \equiv 7 \pmod{12}$, $(p/q) = -1$.
(ii) $m = -pq$, $p \equiv q \equiv 7, 11, 19 \pmod{24}$, $(p/q) = -1$.
(iii) $m = -2pq$, $p \equiv q \equiv 13 \pmod{24}$.
(iv) $m = -3pq$, $p \equiv q \equiv 5, 17 \pmod{24}$.

Let $p \geq 5$ be a prime number. By an argument similar to the above proof of Theorem 0.2(1), we can also obtain that $L(E_{tp}, 1) \neq 0$ and $Ш(E_{tp})$ is a non-trivial finite group.

Theorem 4.7. *Let p be a prime number such that $p \equiv 1 \pmod{24}$.*
For the following integer m, $L(E_m, 1) \neq 0$ and m is not a $2\pi/3$-congruent number and $Ш(E_m)$ is non-trivial finite group.

(i) $m = 2p$, $(2/p)_4 = -1$, *where $(\ /\ )_4$ denotes the quartic residue symbol.*
(ii) $m = 3p$, *There exist $x, y \in \mathbb{Z}$ such that $p = 9x^2 + 16z^2$.*

Proof. (i) Theorem 3.4 and easy argument give that

$$\begin{aligned}\frac{a(2,p)}{2} &= h(-8p) - N(p, Q_2^{(2)}) \\ &\equiv h(-8p) \pmod 8.\end{aligned}$$

From a result of [Piz], we see that

$$h(-4p) + h(-8p) \equiv \frac{p-1}{2} \pmod 8.$$

Since $p \equiv 1 \pmod 8$, we can write $p = a^2 + 16b^2$ with $a, b \in \mathbb{Z}$. Then one uses the result of [Bro] to obtain

$$h(-4p) \equiv \frac{p-1}{2} + 4b \pmod 8.$$

Combining these congruences, we have

$$\frac{a(2,p)}{2} \equiv 4b \pmod 8.$$

It is well-known that b is odd if and only if $(2/p)_4 = -1$. (For example, see p.318 of [Sil].) Hence it follows from the assumption that $L(E_{2p}, 1) \neq 0$ and $2p$ is not a $2\pi/3$-congruent number. The non-triviality of $Ш(E_{2p})$ follows from Table 1 of [Yo1].
(ii) By the same argument and Proposition 4.8 below, we have

$$\begin{aligned}\frac{a(3,p)}{2} &\equiv h(-3p) \pmod 8 \\ &\equiv 4 \pmod 8.\end{aligned}$$

The remaining also follows from Table 1 of [Yo1]. □

Let p be a prime number such that $p \equiv 1 \pmod{12}$. Using Theorem 4.4 or a result of [Piz], we see that $h(-3p) \equiv 0 \pmod 4$. It may be well-known for experts that the following criterion, however, the method of proof below is interesting to the author.

Proposition 4.8. *Let p be a prime number such that $p \equiv 1 \pmod{12}$. Then the following two conditions are equivalent each other.*
(1) $h(-3p) \equiv 4 \pmod 8$.
(2) *There exist $x, y \in \mathbb{Z}$ such that $p = 9x^2 + 16z^2$.*

Remark. The above conditions are also equivalent that $(-3/p)_4 = -1$.

Proof. First, we will give the proof in the case where $p \equiv 1 \pmod{24}$. From Definition 2.2 and Theorem 3.4, we see that

$$\begin{aligned}a(1,p) &= N(p, Q_{1_2}^{(1)}) - N(p, Q_{1_3}^{(2)}) \\ a(1,p) &= -N(p, Q_{1_2}^{(2)}) - N(p, Q_{1_3}^{(3)}) + 3h(-3p).\end{aligned}$$

By the first equality, one finds that

$$\begin{aligned} a(1,p) &\equiv N(p,x^2+144y^2)+N(p,x^2+3y^2) \\ &\quad -N(p,9y^2+16z^2)-N(p,3x^2+16z^2) \pmod 8 \\ &= N(p,x^2+144y^2)+4-N(p,9y^2+16z^2)+0 \\ &= N(p,x^2+144y^2)-N(p,9y^2+16z^2)+4, \end{aligned}$$

since $p \equiv 1 \pmod{24}$. Moreover, one can easily see that either $N(p,x^2+144y^2)=4$ or $N(p,9y^2+16z^2)=4$. Hence we have $a(1,p) \equiv 0 \pmod 8$. On the other hand, from the second form of $a(1,p)$ above, one finds that

$$\begin{aligned} a(1,p) &\equiv -N(p,9x^2+16y^2)-N(p,3x^2+16y^2) \\ &\quad -N(p,(2x+z)^2+36z^2)+3h(-3p) \pmod 8 \\ &= -N(p,9x^2+16y^2)-0-0+3h(-3p), \\ &= -N(p,9x^2+16y^2)+h(-3p) \end{aligned}$$

since $p \equiv 1 \pmod{24}$ and $h(-3p) \equiv 0 \pmod 4$. Here, we also use the fact that

$$\begin{aligned} Q_{1_2}^{(3)} &= 4x^2+4y^2+37z^2+2yz+4zx+4xy \\ &= (2x+y+z)^2+3y^2+36z^2. \end{aligned}$$

Therefore, we have $h(-3p) \equiv N(p,9x^2+16y^2) \pmod 8$ and the half of the proposition follows.

Secondly, we will give the proof in the case $p \equiv 13 \pmod{24}$. From Theorem 3.4, we see that

$$a(1,p) = -N(p,Q_{1_2}^{(2)})-N(p,Q_{1_3}^{(3)})+h(-3p).$$

By the proof of Theorem 3.8 in [Yo2], we see that $a(1,p) \equiv 4 \pmod 8$ and $N(p,Q_{1_2}^{(2)}) \equiv 0 \pmod 8$. Therefore,

$$4 \equiv -N(p,(2x+z)^2+36z^2)+h(-3p) \pmod 8.$$

It is easy to see that $N(p,(2x+z)^2+36z^2)$ is equal to 0 or 4. Since $p \equiv 5 \pmod 8$, we can show that

$$N(p,(2x+z)^2+36z^2) = N(p,w^2+36z^2)$$

So the above congruence gives that

$$h(-3p) \equiv 4 \pmod 8 \iff N(p,w^2+36z^2)=0$$

Finally, from the fact that $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$, one can see that

$$N(p,w^2+36z^2)+N(p,9w^2+4z^2) = N(p,w^2+4z^2) = 4.$$

Hence, we have

$$h(-3p) \equiv 4 \pmod 8 \iff N(p,9w^2+4z^2)=4.$$

So the remaining of the proposition is proved. □

Using a recent result on quaternary quadratic forms, one can obtain non-$2\pi/3$-congruentness result for a "three prime factors" case.

Theorem 4.9. *Let p, q, r be distinct primes. Suppose that $p \equiv 1 \pmod 6$, $q \equiv r \equiv 5 \pmod 6$ and that the graph $G(-8pqr)$ is odd. Then $L(E_{2pqr}, 1) \neq 0$ and $2pqr$ is not $2\pi/3$-congruent.*

Proof. The following result is due to Corollary 7.1(i) of [AALW].

$$N(d, x^2+6y^2+6z^2+12w^2) = \sum_{0<l|d} \frac{d}{l}\left(\frac{12}{l}\right)_K + \frac{1}{2}\sum_{\substack{,j\in\mathbb{Z}_{>0}\\ i,j \text{ odd}\\ 4d=i^2+3j^2}} (-1)^{\frac{i-1}{2}} i + \frac{1}{2}\sum_{\substack{,j\in\mathbb{Z}_{>0}\\ i,j \text{ odd}\\ 4d=i^2+3j^2}} (-1)^{\frac{j-1}{2}} j$$

if $d \equiv 1 \pmod 6$.

Put $d = pqr$. First, from the fact that $q \equiv r \equiv 5 \pmod 6$, it is easy to see that $N(4pqr, x^2+3y^2) = 0$. Hence we can check that

$$\begin{aligned} & N(pqr, x^2+6y^2+6z^2+12w^2) \\ &= \sum_{0<l|d} \frac{pqr}{l}\left(\frac{12}{l}\right)_K \\ &= \left\{p+\left(\frac{12}{p}\right)_K\right\}\left\{q+\left(\frac{12}{q}\right)_K\right\}\left\{r+\left(\frac{12}{r}\right)_K\right\} \\ &\equiv 0 \pmod{32}. \end{aligned}$$

Next one can verify that

$$\begin{aligned} & N(pqr, x^2+6y^2+6z^2+12w^2) \\ \equiv\ & \sharp\{(x,y,z,w) | x^2+6y^2+6z^2+12w^2 = pqr,\ xyzw = 0\} \pmod{32} \\ =\ & 2N(pqr, x^2+6y^2+12z^2) + N(pqr, x^2+6y^2+6z^2) \\ & -2N(pqr, x^2+6y^2) - N(pqr, x^2+12y^2). \end{aligned}$$

Using Theorem 1.2 and the fact that the ternary quadratic form $x^2+6y^2+6z^2$ forms a genus, we obtain that

$$\frac{1}{8}N(pqr, x^2+6y^2+6z^2) = \begin{cases} h(-4pqr)/2 & \text{if } pqr \equiv 1 \pmod{12} \\ h(-pqr) & \text{if } pqr \equiv 7 \pmod{24} \\ 0 & \text{if } pqr \equiv 19 \pmod{24}. \end{cases}$$

In any case, we have $N(pqr, x^2+6y^2+6z^2) \equiv 0 \pmod{32}$ by the genus theory of quadratic fields. Considering that the integer pqr factors into a product of prime ideals in $\mathbb{Q}(\sqrt{-24})$, we see that $N(pqr, x^2+6y^2+12z^2)$ is either 16 or 0. We see also that $N(pqr, x^2+12y^2) = 0$ since $q \equiv r \equiv 2 \pmod 3$.
Therefore,

$$2N(pqr, x^2+6y^2+12z^2) \equiv 0 \pmod{32}.$$

By (3) of Theorem 3.4, we obtain that

$$\begin{aligned} a(2,pqr) &= 2N(pqr, x^2+6y^2+12z^2) - 2h(-8pqr) \\ &\equiv -2h(-8pqr) \pmod{32}. \end{aligned}$$

From the assumption that $G(-8pqr)$ is odd, it completes the proof of the theorem. □

References

[AALW] A. Alaca, Ş. Alaca, M. F. Lemire, K. S. Williams Theta function identities and representations by certain quaternary quadratic forms II, *International Mathematical Forum* **3** (2008), 539–579.

[BiSw] B. J. Birch and H. P. F. Swinnerton-Dyer, Notes on elliptic curves II, *J. reine angew. Math.* **218** (1965), 79–108.

[BrIn] H. Brandt and O. Intrau, *Tabellen reduzierter positiver ternärer quadratischer Formen,* Abh. Sächs. Akad. Wiss. Math.-Nat. Kl. 45, Heft 4, 1958.

[Bro] E. Brown, The class number of $\mathbb{Q}(\sqrt{-p})$ for $p \equiv 1 \pmod 8$ a prime, *Proc. Amer. Math. Soc.* **31** (1972), 381–383.

[BCJKLR] M. V. Brown,N. J. Calkin,K. James,A. J. King, S. Lockard and R. C. Rhoades, Trivial Selmer groups and even partitions of a graph, *Integers: Electronic Journal of Combinatorial Number Theory* **6** (2006), ♯A33, 17pp.

[Cox] D. A. Cox, *Primes of the Form x^2+ny^2, Fermat, Class Field Theory, and Complex Multiplication,* Wiley, 1997

[Dic] L. E. Dickson, *Studies in the Theory of Numbers* Chelsea Pub.Co., 1957.

[FaJa] B. Faulkner and K. James, A graphical approach to computing Selmer groups of congruent number curves, *Ramanujan J.* **14** (2007), 107–129.

[Feng] K. Feng, Non-congruent numbers, odd graphs and the Birch and Swinnerton-Dyer conjecture, *Acta Arith.* **LXXV.1** (1996), 71–83.

[FeXi] K. Feng and M. Xiong, Elliptic curves $y^2 = x^3 - n^2x$ with rank zero, *Journal of Number Theory* **109** (2004), 1–26.

[Fuj] M. Fujiwara, θ-congruent numbers, in: *Number Theory*, (György, Pethó, Sós eds.), Walter de Gruyter, 1997, pp.235–241.

[Goto] T. Goto, Odd graphs and Selmer groups of certain elliptic curves, Algebra and Computation, report collection **6** (2005), 10pp.

[Jon] B. W. Jones, *The Arithmetic Theory of Quadratic Forms,* Mathematical Association of America, 1950.

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

[Kol1] V. A. Kolyvagin, Finiteness of $E(\mathbb{Q})$ and Ш$(E/\mathbb{Q})$ for a subclass of Weil curves, *Math. USSR. Izv.* **32** (1989), 523–542.

[Kol2] ———, Euler systems, in: *The Grothendieck Festschrift vol.II*, (P. Cartier, L. Illusie, et al, eds.), Progr. in Math. 87, Birkhäuser, 1990, pp.435–483.

[Leh] J. L. Lehman, Levels of positive definite ternary quadratic forms, *Math. Comp.* **58** (1992), 399–417.

[Piz] A. Pizer, On the 2-part of the class number of imaginary quadratic number fields, *Journal of Number Theory* **8** (1976), 184–192.

[Réd] L. Rédei, Arithmetische Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.* **171** (1934), 55–60.

[RR] L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.* **170** (1933), 69–74.

[Sil] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer-Verlag, New York, 1985.

[Tun] J. B. Tunnell, A classical diophantine problem and moduler forms of weight 3/2, *Invent. Math.* **72** (1983), 323–334.

[Yo1] S. Yoshida, Some variants of the congruent number problem I, *Kyushu J. of Math.* **55** (2001), 387-404.

[Yo2] ———, Some variants of the congruent number problem II, *Kyushu J. of Math.* **56** (2002), 147-165.

[Zha1] C. Zhao A criterion for elliptic curves with lowest 2-power in $L(1)$, *Math. Proc. Camb. Phil. Soc.* **121** (1997), 385-400.

[Zha2] ———, A criterion for elliptic curves with second lowest 2-power in $L(1)$, *Math. Proc. Camb. Phil. Soc.* **131** (2001), 385-404.

[Zha3] ———, A criterion for elliptic curves with second lowest 2-power in $L(1)$ (II), *Acta Math. Sinica, English Ser.* **21** (2005), 961-976.

Department of Mathematics and Informatics
Graduate School of Science and Technology

Chiba University
1-33 Yayoi-cho, Inage-ku, Chiba-shi, 263-8522
Japan

E-mail address: myoshida@math.s.chiba-u.ac.jp