ON NON-CONGRUENT NUMBERS WITH 1 MODULO 4 PRIME FACTORS

YI OUYANG AND SHENXING ZHANG

Abstract. In this paper, we use the 2-decent method to find a series of odd non-congruent numbers $\equiv 1 \pmod 8$ whose prime factors are $\equiv 1 \pmod 4$ such that the congruent elliptic curves have second lowest Selmer groups, which includes Li and Tian's result [LT00] as special cases.

Contents

1. Introduction

The congruent number problem is about when a positive integer can be the area of a rational right triangle. A positive integer n is a non-congruent number if and only if the congruent elliptic curve

$$E := E^{(n)} : y^2 = x^3 - n^2 x$$

has Mordell-Weil rank zero. In [Keq08] and [Fen97], Feng obtained several series of non-congruent numbers for $E^{(n)}$ with the lowest Selmer groups. In [LT00], Li and Tian obtained a series of non-congruent numbers whose prime factors are $\equiv 1 \pmod 8$ such that $E^{(n)}$ has second lowest Selmer groups. The essential tool of the above results is the 2-descend method of elliptic curves. In this paper, we will use this method to get a series of odd non-congruent numbers whose prime factors are $\equiv 1 \pmod 4$ such that $E^{(n)}$ has second lowest Selmer groups, which includes Li and Tian's result as special cases.

Date: January 7th, 2013.
2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 11D25.
Research partially supported by Project 11171317 from NSFC.

Suppose n is a square-free integer such that $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and primes $p_i \equiv 1 \pmod 4$, then by quadratic reciprocity law $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_i}\right)$.

Definition 1.1. Suppose $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and $p_i \equiv 1 \pmod 4$. The graph $G(n) := (V, A)$ associated to n is a simple undirected graph with vertex set $V := \{\text{prime } p \mid n\}$ and edge set $A := \{\overline{pq} : \left(\frac{p}{q}\right) = -1\}$.

Recall for a simple undirected graph $G = (V, A)$, a partition $V = V_0 \cup V_1$ is called *even* if for any $v \in V_i$ $(i = 0, 1)$, $\#\{v \to V_{1-i}\}$ is even. G is called an *odd graph* if the only even partition is the trivial partition $V = \emptyset \cup V$. Then our main result is:

Theorem 1.2. *Suppose $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and $p_i \equiv 1 \pmod 4$. If the graph $G(n)$ is odd and $\delta(n)$ (as given by (4.2)) is 1, then for the congruent elliptic curve $E = E^{(n)}$,*

$$\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0 \text{ and } Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

As a consequence, n is a non-congruent number.

The following Corollary is Li and Tian's result, cf. [LT00]:

Corollary 1.3. *Suppose $n = p_1 \cdots p_k$ and $p_i \equiv 1 \pmod 8$. If the graph $G(n)$ is odd and the Jacobi symbol $\left(\frac{1+\sqrt{-1}}{n}\right) = -1$, then for $E = E^{(n)}$,*

$$\mathrm{rank}_{\mathbb{Z}}(E(\mathbb{Q})) = 0 \text{ and } Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2.$$

As a consequence, n is a non-congruent number.

2. Review of 2-descent method

In this section, we recall the 2-descent method of computing the Selmer groups of elliptic curves. This section follows [LT00] pp 232–233, also cf. [BSD65] §5 and [Sil09] X.4.

For an isogeny $\varphi : E \to E'$ of elliptic curves defined over a number field K, one has the following fundamental exact sequence

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

Moreover, if $\psi : E' \to E$ is another isogeny, for the composition $\psi \circ \varphi : E \to E$, then the following diagram of exact sequences commutes (cf. [XZ09] p 5):

$$\begin{tikzcd}
 & 0 \arrow[d, dotted, "\iota_1"] & 0 \arrow[d, dotted, "\iota_2"] & 0 \arrow[d] & \\
0 \arrow[r] & E'(K)/\varphi E(K) \arrow[r] \arrow[d, "\psi"] & S^{(\varphi)}(E/K) \arrow[r] \arrow[d] & Ш(E/K)[\varphi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K)/\psi\varphi E(K) \arrow[r] \arrow[d] & S^{(\psi\varphi)}(E/K) \arrow[r] \arrow[d] & Ш(E/K)[\psi\varphi] \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & E(K)/\psi E'(K) \arrow[r] \arrow[d] & S^{(\psi)}(E'/K) \arrow[r] & Ш(E'/K)[\psi] \arrow[r] & 0 \\
 & 0 & & &
\end{tikzcd}$$

Now suppose n is a fixed odd positive square-free integer, $K=\mathbb{Q}$, and $E/\mathbb{Q}$, $E'/\mathbb{Q}$, φ, $\psi=\varphi^\vee$ are given by

$$E=E^{(n)}: y^2=x^3-n^2x,\quad E'=\widehat{E^{(n)}}: y^2=x^3+4n^2x,$$
$$\varphi: E\to E',\ (x,y)\mapsto(\frac{y^2}{x^2},\frac{y(x^2+n^2)}{x^2}),$$
$$\psi: E'\to E,\ (x,y)\mapsto(\frac{y^2}{4x^2},\frac{y(x^2-4n^2)}{8x^2}).$$

Then $\varphi\psi=[2],\psi\varphi=[2]$. In this case ι_1 and ι_2 are exact. Let $\tilde{S}^{(\psi)}(E'/\mathbb{Q})$ denote the image of $S^{(\psi\varphi)}(E/\mathbb{Q})$ in $S^{(\psi)}(E'/\mathbb{Q})$. Then

$$\#Ш(E/\mathbb{Q})[\varphi]=\frac{\#S^{(\varphi)}(E/\mathbb{Q})}{\#E'(\mathbb{Q})/\varphi E(\mathbb{Q})},\quad \#Ш(E'/\mathbb{Q})[\psi]=\frac{\#S^{(\psi)}(E'/\mathbb{Q})}{\#E(\mathbb{Q})/\psi E'(\mathbb{Q})},$$

and

$$\#Ш(E/\mathbb{Q})[2]=\frac{\#S^{(\varphi)}(E/\mathbb{Q})\cdot\#\tilde{S}^{(\psi)}(E'/\mathbb{Q})}{\#E'(\mathbb{Q})/\varphi E(\mathbb{Q})\cdot\#E(\mathbb{Q})/\psi E'(\mathbb{Q})}. \tag{2.2}$$

Similarly, for $[2]=\varphi\circ\psi: E'\to E'$, ι_1 and ι_2 are exact, and

$$\#Ш(E'/\mathbb{Q})[2]=\frac{\#S^{(\psi)}(E'/\mathbb{Q})\cdot\#\tilde{S}^{(\varphi)}(E/\mathbb{Q})}{\#E(\mathbb{Q})/\psi E'(\mathbb{Q})\cdot\#E'(\mathbb{Q})/\varphi E(\mathbb{Q})}. \tag{2.3}$$

The 2-descent method to compute the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\psi)}(E'/\mathbb{Q})$ is as follows (cf. [Sil09] for general elliptic curves). Let

$$S=\{\text{prime factors of } 2n\}\cup\{\infty\},$$
$$\mathbb{Q}(S,2)=\{b\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}: 2\mid \operatorname{ord}_p(b),\forall p\notin S\}.$$

Note that $\mathbb{Q}(S,2)$ is represented by factors of $2n$ and we identify these two sets. By the exact sequence

$$0\to E'(\mathbb{Q})/\varphi E(\mathbb{Q})\xrightarrow{i}\mathbb{Q}(S,2)\xrightarrow{j} WC(E/\mathbb{Q})[\varphi],$$

where

$$i:\ (x,y)\mapsto x,\ O\mapsto 1,\ (0,0)\mapsto 4n^2,\qquad j: d\mapsto\{C_d/\mathbb{Q}\}$$

and $C_d/\mathbb{Q}$ is the homogeneous space for $E/\mathbb{Q}$ defined by the equation

$$C_d: dw^2=d^2+4n^2z^4, \tag{2.4}$$

the φ-Selmer group $S^{(\varphi)}(E/\mathbb{Q})$ is then

$$S^{(\varphi)}(E/\mathbb{Q})\cong\{d\in\mathbb{Q}(S,2): C_d(\mathbb{Q}_p)\neq\emptyset,\ \forall p\in S\}.$$

Similarly, suppose

$$C'_d: dw^2=d^2-n^2z^4. \tag{2.5}$$

The ψ-Selmer group $S^{(\psi)}(E'/\mathbb{Q})$ is then

$$S^{(\psi)}(E'/\mathbb{Q})\cong\{d\in\mathbb{Q}(S,2): C'_d(\mathbb{Q}_p)\neq\emptyset,\ \forall p\in S\}.$$

The method to compute $\tilde{S}^{(\varphi)}(E/\mathbb{Q})$ follows from [BSD65] §5, Lemma 10:

Lemma 2.1. *Let $d\in S^{(\varphi)}(E/\mathbb{Q})$. Suppose (σ,τ,μ) is a nonzero integer solution of $d\sigma^2=d^2\tau^2+4n^2\mu^2$. Let $\mathcal{M}_b$ be the curve corresponding to $b\in\mathbb{Q}^\times/\mathbb{Q}^{\times 2}$ given by*

$$\mathcal{M}_b:\ dw^2=d^2t^4+4n^2z^4,\quad d\sigma w-d^2\tau t^2-4n^2\mu z^2=bu^2. \tag{2.6}$$

Then $d\in\tilde{S}^{(\varphi)}(E/\mathbb{Q})$ if and only if there exists $b\in\mathbb{Q}(S,2)$ such that $\mathcal{M}_b$ is locally solvable everywhere.

Note that the existence of σ, τ, μ follows from Hasse-Minkowski theorem (cf. [Ser73]).

3. Local computation

We need a modification of the Legendre symbol. For $x \in \mathbb{Q}_p$ or $\in \mathbb{Q}$ such that $\mathrm{ord}_p(x)$ is even, we set

$$\left(\frac{x}{p}\right) := \left(\frac{xp^{-\mathrm{ord}_p(x)}}{p}\right). \tag{3.1}$$

Thus $(\frac{\cdot}{p})$ defines a homomorphism from $\{x \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \mathrm{ord}_p(x) \text{ is even}\}$ to $\{\pm 1\}$.

3.1. **Computation of Selmer groups.** In this subsection, we will find the conditions when C_d or C'_d is locally solvable. We will not give details since one only need to consider the valuations and quadratic residue.

Lemma 3.1. *$d \in S^{(\varphi)}(E/\mathbb{Q})$ if and only if d satisfies*

(1) *$d > 0$ has no prime factor $p \equiv 3 \pmod 4$;*
(2) *$\left(\frac{n/d}{p}\right) = 1$ for all odd $p \mid d$;*
(3) *$\left(\frac{d}{p}\right) = 1$ for all odd $p \mid (2n/d)$;*
(4) *if $2 \mid d$, $n \equiv \pm 1 \pmod 8$.*

Proof. In this case $C_d : dw^2 = d^2t^4 + 4n^2z^4$. It is obvious that $C_d(\mathbb{R}) \neq \emptyset \Leftrightarrow d > 0$. Assume $d > 0$.

(i) If $2 \nmid d \mid n$, then $C_d : w^2 = d(t^4 + 4(n/d)^2 z^4)$.

- $p = 2$. $C_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv 1 \pmod 4$.
- $p \mid d$. $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ and $p \equiv 1 \pmod 4$.
- $p \nmid d$. $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$.

(ii) If $2 \mid d \mid 2n$, then $C_d : w^2 = d(t^4 + (2n/d)^2 z^4)$.

- $p = 2$. $C_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv 2 \pmod 8,\ n \equiv \pm 1 \pmod 8$.
- $2 \neq p \mid d$. $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ and $p \equiv 1 \pmod 4$.
- $p \nmid d$. $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$.

Combining (i) and (ii) follows the lemma. □

Lemma 3.2. *$d \in S^{(\psi)}(E'/\mathbb{Q})$ if and only if d satisfies*

(1) *$d \equiv \pm 1 \pmod 8$ or $n/d \equiv \pm 1 \pmod 8$*
(2) *$\left(\frac{n/d}{p}\right) = 1$ for all $p \mid d, p \equiv 1 \pmod 4$;*
(3) *$\left(\frac{d}{p}\right) = 1$ for all $p \mid (n/d), p \equiv 1 \pmod 4$.*

Proof. In the case $C'_d : dw^2 = d^2t^4 - n^2z^4$.

(i) If $2 \mid d$, consider the 2-valuation of each side, we see $C'_d(\mathbb{Q}_2) = \emptyset$.

(ii) If $2 \nmid d \mid n$, then $C'_d : w^2 = d(t^4 - (n/d)^2 z^4)$.

- $p = 2$. $C'_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv \pm 1 \pmod 8$ or $n/d \equiv \pm 1 \pmod 8$.
- $p \mid d$. $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ or $\left(\frac{-n/d}{p}\right) = 1$.
- $p \nmid d$. $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$ or $\left(\frac{-d}{p}\right) = 1$.

Combining (i) and (ii) follows the lemma. □

3.2. **Computation of the images of Selmer groups.** Suppose $0 < 2d \in S^{(\varphi)}(E/\mathbb{Q})$, d is odd with no $\equiv 3 \pmod 4$ prime factor, we want to find a necessary condition for $2d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$. Write $2d = \tau^2 + \mu^2$ and select the triple (σ, τ, μ) in Lemma 2.1 to be $(2n, n\tau/d, \mu)$. Then the defining equations of $\mathcal{M}_{4ndb}$ in (2.6) can be written as

$$w^2 = 2d(t^4 + (n/d)^2 z^4), \quad w - \tau t^2 - (n/d)\mu z^2 = bu^2. \tag{3.2}$$

By abuse of notations, we denote the above curve by $\mathcal{M}_b$. We use the notation $O(p^m)$ to denote a number with p-adic valuation $\geq m$.

The case $p \mid d$. For $i_p \equiv \tau/\mu \pmod{p\mathbb{Z}_p}$, $i_p \in \mathbb{Z}_p$ and $i_p^2 = -1$, then

$$p \mid (\tau - i_p\mu), \quad p \nmid (\tau + i_p\mu).$$

It's easy to see $v(t) = v(z)$, we may assume that $z = 1$, $t^2 \equiv \pm\frac{i_p n}{d} \pmod p$, then $\mathcal{M}_b$ is given by

$$\mathcal{M}_b: \quad w^2 = 2d(t^4 + (n/d)^2), \quad w - \tau t^2 - (n/d)\mu = bu^2.$$

(i) If $v(bu^2) = m \geq 3$, then by $w^2 = (\tau t^2 + \frac{n\mu}{d} + O(p^m))^2 = 2d(t^4 + \frac{n^2}{d^2})$,

$$\left(\mu t^2 - \frac{n\tau}{d}\right)^2 = O(p^m).$$

Let $t^2 = \frac{n\tau}{d\mu} + \beta$, where $v(\beta) = \alpha \geq \frac{m}{2}$, then

$$\begin{aligned} w^2 =& 2d\left((\frac{n}{d})^2 + (\frac{n\tau}{d\mu})^2 + 2\frac{n\tau}{d\mu}\beta + \beta^2\right) \\ =& \frac{4n^2}{\mu^2}(1 + \frac{\tau\mu}{n}\beta + \frac{d\mu^2}{2n^2}\beta^2), \end{aligned}$$

Take the square root on both sides, then

$$\begin{aligned} w =& \pm\frac{2n}{\mu}\left(1 + \frac{1}{2}(\frac{\tau\mu}{n}\beta + \frac{d\mu^2}{2n^2}\beta^2) - \frac{1}{8}(\frac{\tau\mu}{n}\beta)^2 + O(p^{3\alpha-3})\right) \\ =& \pm\left(\frac{2n}{\mu} + \tau\beta + n\mu(\frac{\mu\beta}{2n})^2 + O(p^{3\alpha-2})\right), \end{aligned}$$

but on the other hand,

$$w = \tau t^2 + \frac{n\mu}{d} + bu^2 = \frac{2n}{\mu} + \tau\beta + bu^2.$$

The sign must be positive and

$$bu^2 = n\mu(\frac{\mu\beta}{2n})^2 + O(p^{3\alpha-2}),$$

thus $p \mid b$, $\left(\frac{b/p}{p}\right) = \left(\frac{n\mu/p}{p}\right)$, $\left(\frac{n/b}{p}\right) = \left(\frac{\mu}{p}\right) = \left(\frac{2\tau}{p}\right)$.

(ii) If $v(bu^2) = m \leq 2$ and $t^2 \equiv \frac{i_p n}{d} \pmod p$, let $t^2 = \frac{i_p n}{d} + p\alpha i_p$, then

$$w^2 = 2d \cdot p\alpha i_p \cdot \left(\frac{2i_p n}{d} + p\alpha i_p\right) = -4p^2 \cdot \frac{n\alpha}{p}\left(1 + \frac{pd\alpha}{2n}\right),$$

and

$$\begin{aligned}
w_1 =& \frac{w}{p} = \pm 2i_p\sqrt{\frac{n\alpha}{p}}\Big(1+\frac{pd\alpha}{4n}+O(p^2)\Big),\\
bu^2 =& w-\tau t^2-\frac{n\mu}{d}\\
=& \pm 2pi_p\sqrt{\frac{n\alpha}{p}}\Big(1+\frac{pd\alpha}{4n}\Big)-\frac{i_p\tau n}{d}-\frac{n\mu}{d}-\tau\alpha i_p p+O(p^3)\\
=& -\frac{p^2i_p\tau}{n}\Big(\sqrt{\frac{n\alpha}{p}}\mp\frac{n}{p\tau}\Big)^2-\frac{ni_p}{2d\tau}(\tau-i_p\mu)^2\pm 2p^2i_p\sqrt{\frac{n\alpha}{p}}\frac{d\alpha}{4n}+O(p^3).
\end{aligned}$$

If $v(bu^2)=2$, then $\sqrt{\frac{n\alpha}{p}}\equiv\pm\frac{n}{p\tau}\pmod p$, and

$$\begin{aligned}
bu^2 =& -\frac{ni_p}{2d\tau}(\tau-i_p\mu)^2\pm 2p^2i_p\sqrt{\frac{n\alpha}{p}}\frac{d\alpha}{4n}+O(p^3)\\
=& \frac{-ni_p(\tau-i_p\mu)^3(3\tau+i_p\mu)}{8d\tau^3}+O(p^3)\\
=& \frac{-ni_p(\tau-i_p\mu)^3}{2d\tau^2}+O(p^3)=O(p^3),
\end{aligned}$$

which is impossible! Thus $v(bu^2)=1$ and $p\mid b$,

$$\left(\frac{b/p}{p}\right)=\left(\frac{-pi_p\tau/n}{p}\right)=\left(\frac{2p\tau/n}{p}\right),\ \text{or}\ \left(\frac{n/b}{p}\right)=\left(\frac{2\tau}{p}\right).$$

(iii) If $v(bu^2)=m\le 2$ and $t^2\equiv -i_p(n/d)\pmod p$, then

$$\begin{aligned}
bu^2 =& w-\tau t^2-(n/d)\mu=(\tau i_p-\mu)n/d+O(p)\\
=& 2i_p\tau n/d+O(p)=(1+i_p)^2\cdot\frac{n}{d}\cdot\tau+O(p),
\end{aligned}$$

thus $p\nmid b$ and $\left(\frac{b}{p}\right)=\left(\frac{\tau}{p}\right)\left(\frac{n/d}{p}\right)$.

Note that $2\tau\equiv\tau+\mu i_p\pmod p$ and $\left(\frac{2n/d}{p}\right)=1$, hence we have

Lemma 3.3. *The curve $\mathcal{M}_b$ defined by (3.2) is locally solvable at $p\mid d$ if and only if*

$$\textit{either}\ \ p\mid b,\ \left(\frac{n/b}{p}\right)=\left(\frac{\tau+\mu i_p}{p}\right);\quad \textit{or}\ \ p\nmid b,\ \left(\frac{b}{p}\right)=\left(\frac{\tau+\mu i_p}{p}\right).$$

The case $p\mid\frac{n}{d}$. In this case t is a p-adic unit if and only if w is so.

(i) If $v(w)=v(t)=0$, then $w\equiv\pm\sqrt{2d}t^2\pmod p$ and $(\pm\sqrt{2d}-\tau)t^2\equiv bu^2\pmod p$. Since $(\sqrt{2d}-\tau)(\sqrt{2d}+\tau)=2d-\tau^2=\mu^2$ and $\sqrt{2d}\pm\tau$ are co-prime, $\mathrm{ord}_p(\sqrt{2d}-\tau)$ is even and $\left(\frac{\sqrt{2d}-\tau}{p}\right)$ is well defined. Then $\mathcal{M}_b$ is locally solvable if and only if

$$p\nmid b,\left(\frac{2d}{p}\right)=1\ \text{and}\ \left(\frac{b}{p}\right)=\left(\frac{\sqrt{2d}-\tau}{p}\right).$$

(ii) If $v(z)=0$ and $w=pw_1, t=pt_1$, then $w_1^2=2d(p^2t_1^2+(\frac{n}{pb})^2z^4)$, $w_1\equiv\pm\sqrt{2d}\frac{n}{pd}z^2\pmod p$ and $bu^2/p\equiv(\pm\sqrt{2d}-\mu)\frac{n}{pd}z^2\pmod p$. Thus $\mathcal{M}_b$ is locally solvable if and only if

$$p \mid b, \left(\frac{2d}{p}\right) = 1 \text{ and } \left(\frac{n/(db)}{p}\right) = \left(\frac{\sqrt{2d}-\mu}{p}\right).$$

Note that

$$2(\sqrt{2d}-\tau)(\sqrt{2d}-\mu) = (\tau+\mu-\sqrt{2d})^2 \Rightarrow \left(\frac{\sqrt{2d}-\mu}{p}\right) = \left(\frac{2(\sqrt{2d}-\tau)}{p}\right).$$

From now on, suppose $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and $p_i \equiv 1 \pmod 4$. Pick $i_p \in \mathbb{Z}_p$ such that $i_p^2 = -1$, then

$$\sqrt{2d} - \tau = -(\tau + \mu i_p) \cdot \frac{1}{2}\Big(1 - \frac{\sqrt{2d}}{\tau + \mu i_p}\Big)^2.$$

Note that $\left(\frac{2d}{p}\right) = 1$, we have

Lemma 3.4. *$\mathcal{M}_b$ defined by (3.2) is locally solvable at $p \mid \frac{n}{d}$ if and only if*

$$\begin{aligned} p \mid b, \quad & \left(\frac{2d}{p}\right) = 1 \text{ and } \left(\frac{n/b}{p}\right) = \left(\frac{\tau+\mu i_p}{p}\right)\left(\frac{2}{p}\right), \\ \text{or } p \nmid b, \quad & \left(\frac{2d}{p}\right) = 1 \text{ and } \left(\frac{b}{p}\right) = \left(\frac{\tau+\mu i_p}{p}\right)\left(\frac{2}{p}\right). \end{aligned}$$

By Lemmas 2.1, 3.1, 3.3 and 3.4, we have

Proposition 3.5. *Suppose $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and $p_i \equiv 1 \pmod 4$, then $2d \in S^{(\varphi)}(E/\mathbb{Q})$ if and only if $d > 0$ and $\left(\frac{2n/d}{p}\right) = 1$ for $p \mid d$, $\left(\frac{2d}{p}\right) = 1$ for $p \mid \frac{n}{d}$. In this case $2d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$ only if there exists $b \in \mathbb{Q}(S,2)$ satisfying:*

(1) If $p \mid d$, $i_p \equiv \tau/\mu \pmod{p\mathbb{Z}_p}$, $i_p^2 = -1$,

$$p \mid b, \ \left(\frac{n/b}{p}\right) = \left(\frac{\tau+\mu i_p}{p}\right), \quad \text{or} \quad p \nmid b, \quad \left(\frac{b}{p}\right) = \left(\frac{\tau+\mu i_p}{p}\right).$$

(2) If $p \mid \frac{n}{d}$, $i_p^2 = -1$,

$$p \mid b, \ \left(\frac{n/b}{p}\right) = \left(\frac{2(\tau+\mu i_p)}{p}\right), \quad \text{or} \quad p \nmid b, \quad \left(\frac{b}{p}\right) = \left(\frac{2(\tau+\mu i_p)}{p}\right).$$

4. Proof of the main result

4.1. **Some facts about graph theory.** We now recall some notations and results in graph theory, cf. [Fen97, Keq08].

Definition 4.1. Let $G = (V, A)$ be a simple undirected graph. Suppose $\#V = k$. The *adjacency matrix* $M(G) = (a_{ij})$ of G is the $k \times k$ matrix defined as

$$a_{ij} := \begin{cases} 0, & \text{if } \overline{v_i v_j} \notin A; \\ 1, & \text{if } \overline{v_i v_j} \in A. \end{cases} \tag{4.1}$$

The *Laplace matrix* $L(G)$ of G is defined as

$$L(G) = \operatorname{diag}\{d_1, \ldots, d_k\} - M(G)$$

where d_i is the degree of v_i.

Theorem 4.2. *Let G be a simple undirected graph and $L(G)$ its Laplace matrix.*

(1) *The number of even partitions of V is 2^{k-1-r}, where $r = \operatorname{rank}_{\mathbb{F}_2} L(G)$.*
(2) *The graph G is odd if and only if $r = k-1$.*
(3) *If G is odd, then the equations*

$$L(G)\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix}$$

has solutions if and only if $t_1 + \cdots + t_k = 0$.

Proof. The proof of the first two parts follows from [Keq08]. We have a bijection

$$\mathbb{F}_2^k/\{(0,\cdots,0),(1,\cdots,1)\} \xrightarrow{\sim} \{\text{partitions of } V\}$$
$$(c_1,\dots,c_k) \longmapsto (V_0, V_1)$$

where $V_i = \{v_j : c_j = i \ (1 \le j \le k)\},\ i \in \{0,1\}$.

Regard $L(G) = \operatorname{diag}\{d_1,\dots,d_k\} - (a_{ij})$ as a matrix over $\mathbb{F}_2$. If

$$L(G)\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_k \end{pmatrix} \in \mathbb{F}_2^k,$$

then if $v_i \in V_t, t \in \{0,1\}$,

$$\begin{aligned} b_i &= d_i c_i + \sum_{j=1}^k a_{ij} c_j = \sum_{j=1}^k a_{ij}(c_i + c_j) \\ &= \sum_{j=1}^k a_{ij}(t + c_j) = \sum_{c_j = 1-t} a_{ij} = \#\{v_i \to V_{1-t}\} \in \mathbb{F}_2. \end{aligned}$$

(1) The number of even partitions is

$$\frac{1}{2}\#\left\{(c_1,\dots,c_k) \in \mathbb{F}_2^n : L(G)\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\right\} = 2^{k-1-r}.$$

(2) follows from (1) easily.

(3) Since L is of rank $k-1$, the image space of L is of dimensional $k-1$, but it lies in the hyperplane $x_1 + \cdots + x_k = 0$, thus they coincide and the result follows. □

4.2. **Graph $G(n)$ and Selmer groups of E and E'.** From now on, we suppose $n = p_1 \cdots p_k \equiv 1 \pmod 8$ and $p_i \equiv 1 \pmod 4$. Recall for an integer a prime to n, the Jacobi symbol $\left(\frac{a}{n}\right) = \prod_{p|n}\left(\frac{a}{p}\right)$, which is extended to a multiplicative homomorphism from $\{a \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \operatorname{ord}_p(a) \text{ even for } p \mid n\}$ to $\{\pm 1\}$. Set

$$\left[\frac{a}{n}\right] := \frac{1}{2}\left(1 - \left(\frac{a}{n}\right)\right).$$

The symbol $[\frac{-}{n}]$ is an additive homomorphism from $\{a \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \operatorname{ord}_p(a) \text{ even for } p \mid n\}$ to $\mathbb{F}_2$.

By definition, the adjacency matrix $M(G(n))$ has entries $a_{ij} = \left[\frac{p_i}{p_j}\right]$. For $0 < d \mid n$, we denote by $\{d, \frac{n}{d}\}$ the partition $\{p : p \mid d\} \cup \{p : p \mid \frac{n}{d}\}$ of $G(n)$.

The following proposition is a translation of results in Lemma 3.1 and Lemma 3.2:

Proposition 4.3. *Given a factor d of n.*

(1) For the Selmer group $S^{(\varphi)}(E/\mathbb{Q})$,

(1-a) *$d \in S^{(\varphi)}(E/\mathbb{Q})$ if and only if $d > 0$ and $\{d, n/d\}$ is an even partition of $G(n)$;*

(1-b) *Suppose*

$$c_i = \begin{cases} 1, & \text{if } p_i \mid d, \\ 0, & \text{if } p_i \mid \frac{n}{d}; \end{cases} \qquad t_i = \left[\frac{2}{p_i}\right].$$

Then $2d \in S^{(\varphi)}(E/\mathbb{Q})$ if and only if $d > 0$ and

$$L(G)\begin{pmatrix} c_1 \\ \vdots \\ c_k \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_k \end{pmatrix}.$$

(2) For the Selmer group $S^{(\psi)}(E'/\mathbb{Q})$,

(2-a) *$d \in S^{(\psi)}(E'/\mathbb{Q})$ if and only if $d \equiv \pm 1 \pmod 8$ and $\{d, n/d\}$ is an even partition of $G(n)$;*

(2-b) *$2d \notin S^{(\psi)}(E'/\mathbb{Q})$.*

Proof. One only has to show (1-b), the rest is easy. For any i, let $[i]$ be the set of j such that p_i and p_j are both prime divisors of d or n/d. Then

$$d_i c_i + \sum_{j \neq i} a_{ij} c_j = \sum_{j \neq i} a_{ij}(c_i + c_j) = \sum_{j \notin [i]} a_{ij} = \left[\frac{d}{p_i}\right] \text{ or } \left[\frac{n/d}{p_i}\right].$$

Then (1-b) follows from Lemma 3.1. □

Applying Theorem 4.2(3) to Proposition 4.3, then we have

Corollary 4.4. *If $G(n)$ is odd, there exists a unique factor $0 < d < \sqrt{2n}$ of n such that*

$$S^{(\varphi)}(E/\mathbb{Q}) = \{1, 2d, 2n/d, n\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

and

$$S^{(\psi)}(E'/\mathbb{Q}) = \{\pm 1, \pm n\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

For the d given in Corollary 4.4, write $2d = \tau^2 + \mu^2$. If $2d \in \tilde{S}^{(\varphi)}(E/\mathbb{Q})$, we suppose b satisfies the condition that $\mathcal{M}_b$ defined by (3.2) is locally solvable everywhere. Suppose $c' = (c_1', \cdots, c_k')^T$ and $t' = (t_1', \cdots t_k')^T$ are given by

$$c_j' = \begin{cases} 1, & \text{if } p_j \mid b, \\ 0, & \text{if } p_j \nmid b; \end{cases} \qquad t_j' = \begin{cases} \left[\dfrac{\tau + \mu i_{p_j}}{p_j}\right], & \text{if } p_j \mid d, \\ \left[\dfrac{2(\tau + \mu i_{p_j})}{p_j}\right], & \text{if } p_j \mid \frac{n}{d}. \end{cases}$$

By Proposition 3.5, $Lc' = t'$, i.e., $Lv = t'$ has a solution $v = c'$, which means that the summation of t_j' must be zero in $\mathbb{F}_2$ by Theorem 4.2(3).

Definition 4.5. Suppose n is given such that $G(n)$ is an odd graph. For the unique factor d given in Corollary 4.4, write $2d = \tau^2 + \mu^2$ and $\frac{2n}{d} = \tau'^2 + \mu'^2$. Let $i \in \mathbb{Z}/n\mathbb{Z}$ be defined by

$$i \equiv \frac{\tau}{\mu} \pmod d, \quad i \equiv \frac{\tau'}{\mu'} \pmod{\frac{n}{d}}.$$

We define

$$\delta(n) := \left[\frac{\tau + \mu i}{n}\right] + \left[\frac{2}{d}\right] \in \mathbb{F}_2. \tag{4.2}$$

Then the following is a consequence of Proposition 3.5.

Corollary 4.6. *If $G(n)$ is odd and $\delta(n) = 1$, then*

$$\tilde{S}^{(\varphi)}(E/\mathbb{Q}) = \{1\}.$$

Proof. Let λ^* be the $\mathbb{F}_2$-rank of $\tilde{S}^{(\varphi)}(E/\mathbb{Q})$, λ be the $\mathbb{F}_2$-rank of $S^{(\varphi)}(E/\mathbb{Q})$, then $\lambda = 2$. The existence of the Cassels' skew-symmetric bilinear form on Ш implies that the difference $\lambda - \lambda^*$ is even.

By the above analysis, $\delta(n) = \sum_j t'_j \neq 0$, thus $2d \notin \tilde{S}^{(\varphi)}(E/\mathbb{Q})$, we have $\lambda^* < \lambda$, $\lambda^* = 0$. $\square$

Remark. If we replace d by $\frac{n}{d}$ in the definition, $\delta(n)$ is invariant. Indeed, $[\frac{2}{d}] = [\frac{2}{n/d}]$. For the other term,

$$\left[\frac{\tau + \mu i}{n}\right] = \left[\frac{\tau + \mu i}{d}\right] + \left[\frac{\tau + \mu i'}{n/d}\right]$$

where $i \equiv \tau/\mu \pmod{d}$, $i' \equiv \tau'/\mu' \pmod{n/d}$. Let $u = (\tau\tau' - \mu\mu')/2$, $v = (\tau\mu' - \mu\tau')/2$, then

$$\begin{aligned} u + vi =&(\tau + \mu i)(\tau' + \mu' i)/2 \equiv \tau(\tau' + \mu' \cdot \frac{\tau}{\mu}) \\ \equiv&\tau\mu(\tau'\mu + \tau\mu')/\mu^2 \equiv (\tau + \mu)^2/\mu^2 \cdot v/2 \pmod{d}. \end{aligned}$$

Similarly, $u + vi' \equiv (\tau' + \mu')^2/\mu'^2 \cdot v/2 \pmod{(n/d)}$. If we interchange d and n/d, $\delta(n)$ will differ

$$\begin{aligned} &\left[\frac{\tau + \mu i}{d}\right] + \left[\frac{\tau + \mu i'}{n/d}\right] + \left[\frac{\tau' + \mu' i'}{n/d}\right] + \left[\frac{\tau' + \mu' i}{d}\right] \\ =&\left[\frac{2(u + vi)}{d}\right] + \left[\frac{2(u + vi')}{n/d}\right] = \left[\frac{v}{d}\right] + \left[\frac{v}{n/d}\right] \\ =&\left[\frac{v}{n}\right] = \left[\frac{n}{v}\right] = \left[\frac{u^2 + v^2}{v}\right] = 0 \in \mathbb{F}_2. \end{aligned}$$

Thus $\delta(n)$ does not change, which implies that $\delta(n)$ does not depend on the choice of d, τ, μ and only depend on n.

4.3. **Proof of the main result.**

Proof of Theorem 1.2. We shall use the fundamental exact sequence (2.1) and the commutative diagram in §2 frequently.

Since $E(\mathbb{Q})_{\mathrm{tor}} \cap \psi E'(\mathbb{Q}) = \{O\}$ and $\#E(\mathbb{Q})_{\mathrm{tor}} = 4$, $\#E(\mathbb{Q})/\psi E'(\mathbb{Q}) \geq 4$. Since $G(n)$ is odd, $\#S^{(\psi)}(E'/\mathbb{Q}) = 4$ and $\#E(\mathbb{Q})/\psi E'(\mathbb{Q}) = 4$, by (2.1), $\text{Ш}(E'/\mathbb{Q})[\psi] = 0$. Apparently $\tilde{S}^{(\psi)}(E'/\mathbb{Q}) \supseteq E(\mathbb{Q})/\psi E'(\mathbb{Q})$ and thus $\#\tilde{S}^{(\psi)}(E'/\mathbb{Q}) = 4$.

By Corollary 4.6, $\tilde{S}^{(\varphi)}(E/\mathbb{Q}) = \{1\}$, then $\#E'(\mathbb{Q})/\varphi E(\mathbb{Q}) = 1$. The facts that $\#E(\mathbb{Q})/\psi E'(\mathbb{Q}) = 4$ and $E(\mathbb{Q})_{\mathrm{tor}} \cong (\mathbb{Z}/2\mathbb{Z})^2$ imply that $\#E(\mathbb{Q})/2E(\mathbb{Q}) = 4$ and

$$\operatorname{rank}_{\mathbb{Z}} E(\mathbb{Q}) = \operatorname{rank}_{\mathbb{Z}} E'(\mathbb{Q}) = 0.$$

From $\text{Ш}(E'/\mathbb{Q})[\psi] = E'(\mathbb{Q})/\varphi E(\mathbb{Q}) = 0$, the diagram tells us that

$$\text{Ш}(E/\mathbb{Q})[2] \cong \text{Ш}(E/\mathbb{Q})[\varphi] \cong S^{(\varphi)}(E/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z},$$

and (2.3) tells us that

$$\text{Ш}(E'/\mathbb{Q})[2] \cong \text{Ш}(E'/\mathbb{Q})[\psi] \cong 0.$$

Hence $Ш(E'/\mathbb{Q})[2^\infty] = 0$ and $Ш(E'/\mathbb{Q})[2^k\psi] = 0$. By the exact sequence

$$0 \to Ш(E/\mathbb{Q})[\varphi] \to Ш(E/\mathbb{Q})[2^k] \to Ш(E'/\mathbb{Q})[2^{k-1}\psi],$$

we have for every $k \in \mathbb{N}_+$,

$$Ш(E/\mathbb{Q})[2^k] \cong Ш(E/\mathbb{Q})[\varphi] \cong (\mathbb{Z}/2\mathbb{Z})^2,$$

and thus $Ш(E/\mathbb{Q})[2^\infty] \cong (\mathbb{Z}/2\mathbb{Z})^2$. □

Proof of Corollary 1.3. In this case, $d = 1$ and $\tau = \mu = 1$, $\delta(n) = \left[\frac{1+\sqrt{-1}}{n}\right]$, thus the result follows. □

Acknowledgement. This paper was prepared when the authors were visiting the Academy of Mathematics and Systems Science and the Morningside Center of Mathematics of Chinese Academy of Sciences, and was grew out of a project proposed by Professor Ye Tian to the second author. We would like to thank Professor Ye Tian for his vision, insistence and generous hospitality. We also would like to thank Jie Shu and Jinbang Yang for many helpful discussions.

References

[BSD65] B. J. Birch and H. P. F. Swinnerton-Dyer. Notes on elliptic curves. II. *J. Reine Angew. Math.*, 218:79–108, 1965.

[Fen97] Keqin Feng. Non-congruent number, odd graph and the BSD conjecture on $y^2 = x^3 - n^2x$. In *Singularities and complex geometry (Beijing, 1994)*, volume 5 of *AMS/IP Stud. Adv. Math.*, pages 54–66. Amer. Math. Soc., Providence, RI, 1997.

[Keq08] Feng Keqin. *Non-congruent Numbers and Elliptic Curves with Rank Zero*. Press of University of Science and Technology of China, 1 edition, 2008.

[LT00] Delang Li and Ye Tian. On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D\colon y^2 = x^3 - D^2x$. *Acta Math. Sin. (Engl. Ser.)*, 16(2):229–236, 2000.

[Ser73] J.-P. Serre. *A course in arithmetic*. Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French.

[Sil09] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[XZ09] Maosheng Xiong and Alexandru Zaharescu. Selmer groups and Tate-Shafarevich groups for the congruent number problem. *Comment. Math. Helv.*, 84(1):21–56, 2009.

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China
Email address: yiouyang@ustc.edu.cn

Wu Wen-Tsun Key Laboratory of Mathematics, School of Mathematical Sciences, University of Science and Technology of China, Hefei, Anhui 230026, China
Email address: zsxqq@mail.ustc.edu.cn