Volume 57 Number 3 March 2014 443–664

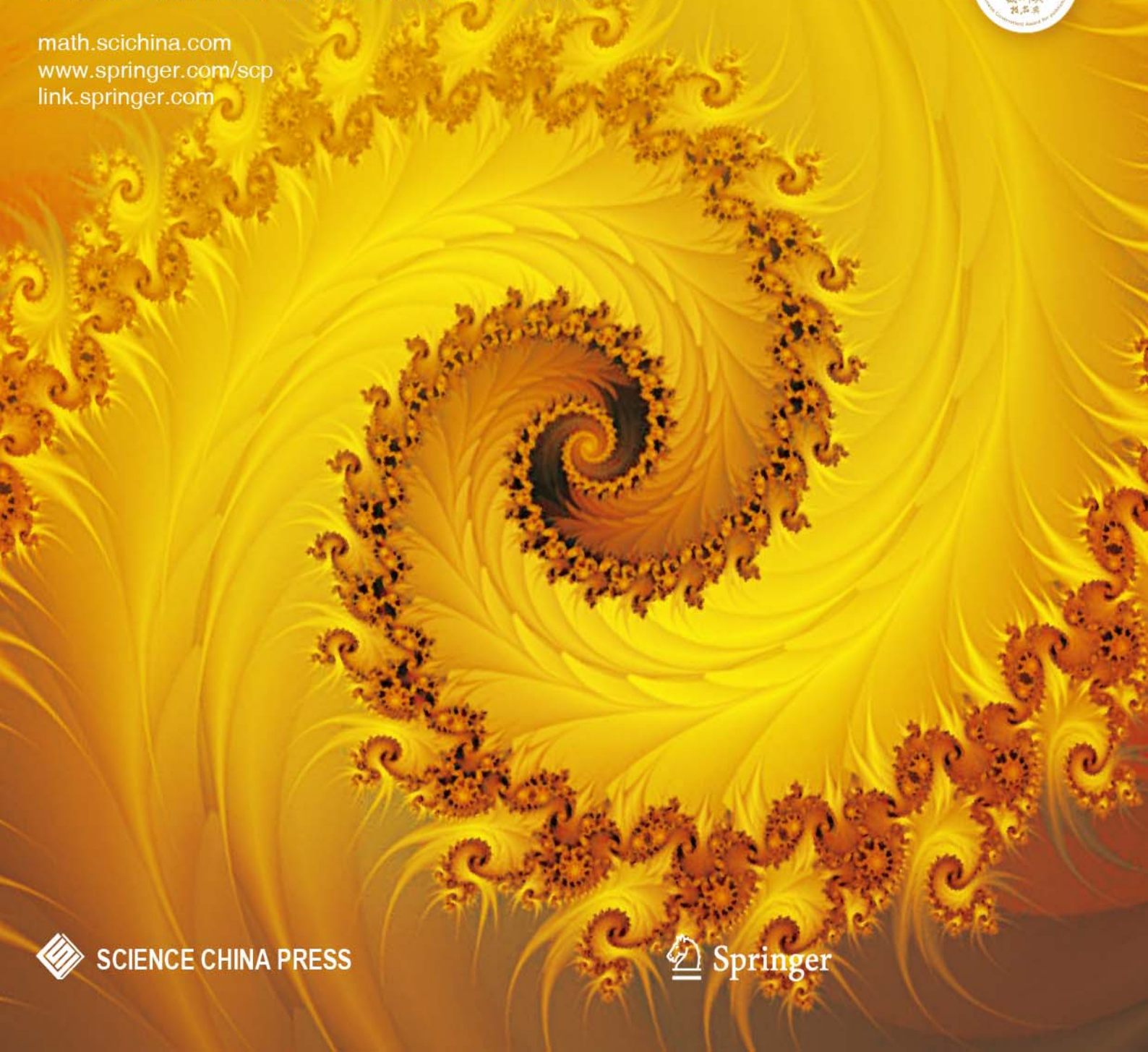
ISSN 1674-7283 CN 11-5837/O1

中国科学：数学

SCIENCE CHINA
Mathematics

Sponsored by
CHINESE ACADEMY OF SCIENCES
NATIONAL NATURAL SCIENCE FOUNDATION OF CHINA

math.scichina.com
www.springer.com/scp
link.springer.com



SCIENCE CHINA PRESS

Springer

Editorial Board

Supported by NSFC

SCIENCE CHINA
Mathematics

• ARTICLES •

March 2014 Vol. 57 No. 3: 649–658
doi: 10.1007/s11425-013-4705-y

On non-congruent numbers with 1 modulo 4 prime factors

OUYANG Yi & ZHANG ShenXing*

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

Received September 11, 2012; accepted December 28 2012; published online September 4, 2013

Abstract In this paper, we use the 2-descent 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 include Li and Tian's result as special cases.

Keywords non-congruent number, 2-descent, second 2-descent

MSC(2010) 11G05, 11D25

Citation: Ouyang Y, Zhang S X. On non-congruent numbers with 1 modulo 4 prime factors. Sci China Math, 2014, 57: 649–658, doi: 10.1007/s11425-013-4705-y

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

$$E := E^{(n)} : y^2 = x^3 - n^2 x \tag{1.1}$$

has Mordell-Weil rank zero. In [3,4], Feng obtained several series of non-congruent numbers for $E^{(n)}$ with the lowest Selmer groups. In [5], 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-descent 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 include Li and Tian's result as special cases.

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 $(\frac{p_i}{p_j}) = (\frac{p_j}{p_i})$.

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 with n is a simple undirected graph with vertex set $V := \{\text{prime } p \mid n\}$ and edge set $A := \{\overline{pq} : (\frac{p}{q}) = -1\}$.

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:

*Corresponding author

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 will be given by (4.5)) is 1, then for the congruent elliptic curve $E = E^{(n)}$,*

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

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

The following corollary is Li and Tian's result [5]:

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 $(\frac{1+\sqrt{-1}}{n}) = -1$, then for $E = E^{(n)}$,*

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

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 [5, pp. 232–233], also cf. [1, Section 5] and [7, Chapter 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. [8, 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

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

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,

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

The 2-descent method to compute the Selmer groups $S^{(\varphi)}(E/\mathbb{Q})$ and $S^{(\psi)}(E'/\mathbb{Q})$ is as follows (cf. [7] for general elliptic curves): Let

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

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

$$S^{(\varphi)}(E/\mathbb{Q}) \cong \{d \in \mathbb{Q}(S,2) : C_d(\mathbb{Q}_p) \neq \emptyset,\ \forall\, p \in S\}. \tag{2.5}$$

Similarly, suppose

$$C'_d : dw^2 = d^2 - n^2z^4. \tag{2.6}$$

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

$$S^{(\psi)}(E'/\mathbb{Q}) \cong \{d \in \mathbb{Q}(S,2) : C'_d(\mathbb{Q}_p) \neq \emptyset,\ \forall\, p \in S\}. \tag{2.7}$$

The method to compute $\tilde{S}^{(\varphi)}(E/\mathbb{Q})$ follows from [1, Section 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*

$$\mathcal{M}_b :\ dw^2 = d^2t^4 + 4n^2z^4, \quad d\sigma w - d^2\tau t^2 - 4n^2\mu z^2 = bu^2. \tag{2.8}$$

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. [6]).

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 the details since we 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)*$(\frac{n/d}{p}) = 1$ for all odd $p \mid d$;*

(3) *$(\frac{d}{p}) = 1$ 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 $C_d : w^2 = d(t^4 + 4(n/d)^2z^4)$.

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

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

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

Combining (i) and (ii) completes the proof of 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) *$(\frac{n/d}{p}) = 1$ for all $p \mid d, p \equiv 1 \pmod 4$;*

(3) *$(\frac{d}{p}) = 1$ for all $p \mid (n/d), p \equiv 1 \pmod 4$.*

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

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

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

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

Combining (i) and (ii) completes the proof of 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 prime factor $\equiv 3 \pmod 4$. 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 (2.8) can be written as

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

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 $\geqslant m$.

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 is 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

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

(i) If $v(bu^2) = m \geqslant 3$, 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 $v(\beta) = \alpha \geqslant \frac{m}{2}$, then

$$w^2 = 2d\left(\left(\frac{n}{d}\right)^2 + \left(\frac{n\tau}{d\mu}\right)^2 + 2\frac{n\tau}{d\mu}\beta + \beta^2\right) = \frac{4n^2}{\mu^2}\left(1 + \frac{\tau\mu}{n}\beta + \frac{d\mu^2}{2n^2}\beta^2\right).$$

Take the square root on both sides, then

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

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

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

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

(ii) If $v(bu^2) = m \leqslant 2$ 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

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

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

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

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

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

(iii) If $v(bu^2) = m \leqslant 2$ 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 $(\frac{b}{p}) = (\frac{\tau}{p})(\frac{n/d}{p})$.

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

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

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 $(\frac{\sqrt{2d}-\tau}{p})$ is well defined. We may assume $p \nmid \sqrt{2d}+\tau$. If $w \equiv -\sqrt{2d} \pmod p$ or $v(\mu) = 0$, then $p \nmid b, (\frac{b}{p}) = (\frac{-\sqrt{2d}-\tau}{p})$. Otherwise $v(\mu) \geqslant 1, w \equiv \sqrt{2d} \pmod p$, $v(bu^2) \geqslant 1$,

$$\begin{aligned} w^2 &= (\tau t^2 + \mu n/d + bu^2)^2 = 2d(t^4 + (n/d)^2), \\ (\mu t^2 - n\tau/d)^2 &= bu^2(2w - bu^2) = bu^2(2\tau t^2 + O(p)), \end{aligned}$$

thus $p \nmid b, (\frac{b}{p}) = (\frac{2\tau}{p}) = (\frac{\sqrt{2d}+\tau}{p})$. Then $\mathcal{M}_b$ is locally solvable if and only if

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

(ii) If $v(z) = 0$ and $w = pw_1, t = pt_1$, then $w_1^2 = 2d(p^2t_1^4 + (\frac{n}{pd})^2 z^4)$, $w_1 \equiv \pm\sqrt{2d}\frac{n}{pd}z^2 \pmod p$ 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

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

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

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

Note that $(\frac{2d}{p}) = 1$, 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*

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

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 $(\frac{2n/d}{p}) = 1$ for $p \mid d$, $(\frac{2d}{p}) = 1$ 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. [3, 4].

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

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

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

$$L(G) = \operatorname{diag}\{d_1, \ldots, d_k\} - M(G), \tag{4.2}$$

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 [3]. We have a bijection

$$\begin{aligned} \mathbb{F}_2^k / \{(0, \ldots, 0), (1, \ldots, 1)\} &\xrightarrow{\sim} \{\text{partitions of } V\} \\ (c_1, \ldots, c_k) &\longmapsto (V_0, V_1), \end{aligned}$$

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

Regard $L(G) = \operatorname{diag}\{d_1, \ldots, d_k\} - (a_{ij})$ 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 $v_i \in V_t, t \in \{0, 1\}$,

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

(1) The number of even partitions is

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

(2) follows from (1) easily.

(3) Since L is of rank $k - 1$, the image space of L is of dimension $k - 1$, 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

$$n = p_1 \cdots p_k \equiv 1 \pmod 8 \quad \text{and} \quad p_i \equiv 1 \pmod 4.$$

Recall for an integer a prime to n, the Jacobi symbol $(\frac{a}{n}) = \prod_{p|n}(\frac{a}{p})$, which is extended to a multiplicative homomorphism from $\{a \in \mathbb{Q}^\times/\mathbb{Q}^{\times 2} : \mathrm{ord}_p(a) \text{ even for } p \mid n\}$ to $\{\pm 1\}$. Set

$$\left[\frac{a}{n}\right] := \frac{1}{2}\left(1 - \left(\frac{a}{n}\right)\right). \tag{4.3}$$

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

By definition, the adjacency matrix $M(G(n))$ has entries $a_{ij} = [\frac{p_i}{p_j}]$. 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 Lemmas 3.1 and 3.2:

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

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

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

(1b) *Suppose*

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

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 $S^{(\psi)}(E'/\mathbb{Q})$,*

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

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

Proof. One only shows (1b), 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 (1b) follows from Lemma 3.1. □

Applying Theorem 4.2(3) to Proposition 4.3, 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 $c' = (c'_1, \ldots, c'_k)^{\mathrm{T}}$ and $t' = (t'_1, \ldots t'_k)^{\mathrm{T}}$ are given by

$$c'_j = \begin{cases} 1, & \text{if} \quad p_j \mid b, \\ 0, & \text{if} \quad p_j \nmid b; \end{cases} \qquad t'_j = \begin{cases} \left[\dfrac{\tau + \mu i_{p_j}}{p_j}\right], & \text{if} \quad p_j \mid d, \\ \left[\dfrac{2(\tau + \mu i_{p_j})}{p_j}\right], & \text{if} \quad p_j \mid \dfrac{n}{d}. \end{cases}$$

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

$$i \equiv \frac{\tau}{\mu} \pmod{d}, \quad i \equiv \frac{\tau'}{\mu'}\left(\bmod \frac{n}{d}\right). \tag{4.4}$$

We define

$$\delta(n) := \left[\frac{\tau + \mu i}{n}\right] + \left[\frac{2}{d}\right] \in \mathbb{F}_2. \tag{4.5}$$

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 $\lambda^* < \lambda$, $\lambda^* = 0$. □

Remark 4.7. 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

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

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 choices of d, τ, μ and only depends 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 Section 2 frequently.

Since $E(\mathbb{Q})_{\text{tor}} \cap \psi E'(\mathbb{Q}) = \{O\}$ and $\#E(\mathbb{Q})_{\text{tor}} = 4$, $\#E(\mathbb{Q})/\psi E'(\mathbb{Q}) \geqslant 4$. Since $G(n)$ is odd, $\#S^{(\psi)}(E'/\mathbb{Q}) = 4$ and $\#E(\mathbb{Q})/\psi E'(\mathbb{Q}) = 4$, by (2.1), $Ш(E'/\mathbb{Q})[\psi] = 0$. 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 $E(\mathbb{Q})_{\text{tor}} \cong (\mathbb{Z}/2\mathbb{Z})^2$ 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 $Ш(E'/\mathbb{Q})[\psi] = E'(\mathbb{Q})/\varphi E(\mathbb{Q}) = 0$, the diagram tells us that

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

and (2.3) tells us that

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

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 $\tau = \mu = 1$, $\delta(n) = [\frac{1+\sqrt{-1}}{n}]$, thus the result follows. □

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 11171317) and National Key Basic Research Program of China (Grant No. 2013CB834202). 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

1 Birch B, Swinnerton-Dyer H P F. Notes on ellptic curves (II). J Reine Angrew Math, 1965, 218: 79–108
2 Cassels J W S. Arithmetic on curves of genus 1, (IV) proof of the Hauptvermutung. J Reine Angrew Math, 1962, 211: 95–112
3 Feng K. Non-congruent Numbers and Elliptic Curves with Rank Zero. Hefei: Press of University of Science and Technology of China, 2008, 25–29
4 Feng K. Non-congruent number, odd graphs and the BSD conjecture. Acta Arith, 1996, 80
5 Li D, Tian Y. On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D : y^2 = x^3 - D^2x$. Acta Math Sinica, 2000, 16: 229–236
6 Serre J P. A Course in Arithmetic. Berlin: Springer-Verlag, 1973
7 Silverman J H. The Arithmetic of Elliptic Curves. GTM 106. New York: Springer-Verlag, 1986
8 Xiong M, Zaharescu A. Selmer groups and Tate-Shararevich groups for the congruent number problem. Comment Math Helv, 2009, 84: 21–56

Information for authors

SCIENCE CHINA Mathematics, a peer-reviewed mathematical journal cosponsored by Chinese Academy of Sciences and National Natural Science Foundation of China, and published monthly in both print and electronic forms by Science China Press and Springer, is committed to publishing high-quality, original results in both basic and applied research.

Categories of articles:

Reviews summarize representative results and achievements in a particular topic or an area, comment on the current state of research, and advise on the research directions. The author's own opinion and related discussion are requested.

Articles report on important original results in all areas of mathematics.

Brief reports present short reports in a timely manner of the latest important results.

Authors are recommended to use the online submission services. To submit a manuscript, please visit http://mc03.manuscriptcentral.com/scmath, get an account, and follow the instructions to upload the text and image/table files.

Authors should also submit such accompanying materials as a short statement on the research background, area/subarea and significance of the work, a brief introduction to the first and corresponding authors including their mailing address, post code, telephone number, fax number, and email address. Authors may suggest several referees (please supply full names, addresses, phone, fax and email), and/or request the exclusion of specific reviewers.

All submissions will be reviewed by referees selected by the editorial board. The decision of acceptance or rejection of a manuscript is made by the editorial board based on the referees' reports. The entire review process may take 90 to 180 days, and the editorial office will inform the author of the decision as soon as the process is completed.

Authors should guarantee that their submitted manuscript has not been published before, and has not been submitted elsewhere for print or electronic publication consideration.

Submission of a manuscript is taken to imply that all the named authors are aware that they are listed as co-authors, and they have seen and agreed to the submitted version of the paper. No change in the order of listed authors can be made without an agreement signed by all the authors.

Once a manuscript is accepted, the authors should send a copyright transfer form signed by all authors to Science China Press. Authors of one published paper will be presented one sample copy. If offprints and more sample copies are required, please contact the managing editor and pay the extra fee. The full text in Chinese and in English opens freely to the readers in China at www.scichina.com, and the full text in English is available to overseas readers at link.springer.com.

Subscription information

ISSN print edition: 1674-7283
ISSN electronic edition: 1869-1862

Subscription rates:
For information on subscription rates please contact:
Customer Service
China: sales@scichina.org
North and South America:
journals-ny@springer.com
Outside North and South America:
subscriptions@springer.com

Orders and inquiries:
China
Science China Press
16 Donghuangchenggen North Street,
Beijing 100717, China
Tel: 86-10-64016232
Fax: 86-10-64016350
Email: sales@scichina.org
North and South America
Springer New York, Inc.
Journal Fulfillment
P.O. Box 2485
Secaucus, NJ 07096, USA
Tel: 1-800-SPRINGER or 1-201-348-4033
Fax: 1-201-348-4505
Email: journals-ny@springer.com
Outside North and South America
Springer Distribution Center
Customer Service Journals
Haberstr. 7, 69126
Heidelberg, Germany
Tel: 49-6221-345-0, Fax: 49-6221-345-4229
Email: subscriptions@springer.com

Cancellations must be received by September 30 to take effect at the end of the same year.

Changes of address: Allow for six weeks for all changes to become effective. All communications should include both old and new addresses (with postal codes) and should be accompanied by a mailing label from a recent issue. According to § 4 Sect. 3 of the German Postal Services Data Protection Regulations, if a subscriber's address changes, the German Federal Post Office can inform the publisher of the new address even if the subscriber has not submitted a formal application for mail to be forwarded. Subscribers not in agreement with this procedure may send a written complaint to Customer Service Journals, Karin Tiks, within 14 days of publication of this issue.

Microform editions are available from: ProQuest. Further information available at http://www.il.proquest.com/uni.

Electronic edition:
An electronic version is available at link.springer.com.

Production:
Science China Press
16 Donghuangchenggen North Street, Beijing 100717, China
Tel: 86-10-64016232
Fax: 86-10-64016350
Printed in the People's Republic of China

Jointly Published by
Science China Press and Springer

SCIENCE CHINA

Mathematics

CONTENTS

Vol. 57 No. 3 March 2014

Progress of Projects Supported by NSFC

Articles

math.scichina.com

www.springer.com/scp

Indexed by:
SCI-CD
MR
Z Math
MathSciNet

ISSN 1674-7283