Comment. Math. Helv. 84 (2009), 21–56 **Commentarii Mathematici Helvetici**

Selmer groups and Tate–Shafarevich groups for the congruent number problem

Maosheng Xiong and Alexandru Zaharescu*

Abstract. We study the distribution of the sizes of the Selmer groups arising from the three 2-isogenies and their dual 2-isogenies for the elliptic curve $E_n : y^2 = x^3 - n^2x$. We show that three of them are almost always trivial, while the 2-rank of the other three follows a Gaussian distribution. It implies three almost always trivial Tate–Shafarevich groups and three large Tate–Shafarevich groups. When combined with a result obtained by Heath-Brown, we show that the mean value of the 2-rank of the large Tate–Shafarevich groups for square-free positive odd integers $n \leq X$ is $\frac{1}{2}\log\log X + O(1)$, as $X \to \infty$.

Mathematics Subject Classification (2000). 11G05, 14H52, 11L40, 11N45.

Keywords. Elliptic curves, congruent number problem, Selmer group, Tate–Shafarevich group, Erdös–Kac Theorem.

1. Introduction

A positive integer n is called a "congruent number" if n equals the area of a rational right triangle, where "rational" means that the lengths of the three sides of this triangle are rational numbers. Although Tunnell ([38]) presented an elementary criterion via the theory of modular forms, strictly speaking the problem of deciding whether or not a given integer is a congruent number is still open. Clearly one may restrict attention to positive square-free integer n. It is a well-known fact that n is a congruent number if and only if the elliptic curve $E_n : y^2 = x^3 - n^2x$ has positive rank over $\mathbb{Q}$ ([25]). Partly because of this relation and among other things, this family of elliptic curves E_n has attracted a lot of attention and its arithmetic properties, such as the rank, the associated L-functions, the Selmer groups and Tate–Shafarevich groups related to this curve have been studied extensively (see [1], [4], [5], [8], [11], [13], [14], [15], [16], [20], [21], [23], [27], [29], [30], [32], [33], [34], [35], [37], [38], [42], [43]).

Let $\phi : E \to E'$ be an isogeny between two elliptic curves E and E' over $\mathbb{Q}$. For the cases of interest to us, ϕ is defined over $\mathbb{Q}$ and $E[\phi]$, the kernel of ϕ consists of

*The second author was supported by NSF grant number DMS-0456615, and by CNCSIS grant GR106/2007, code 1116, of the Romanian Ministry of Education and Research.

$\mathbb{Q}$-rational points. Via Galois cohomology the exact sequence

$$0 \longrightarrow E[\phi] \longrightarrow E \xrightarrow{\phi} E' \longrightarrow 0$$

gives us the following commutative diagram (for details, please see chapter X in [36]):

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} & \longrightarrow & \mathrm{Sel}^{(\phi)}(E/\mathbb{Q}) & \longrightarrow & Ш(E/\mathbb{Q})[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \frac{E'(\mathbb{Q})}{\phi(E(\mathbb{Q}))} & \longrightarrow & H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[\phi]) & \longrightarrow & H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E)[\phi] & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & 0 & \longrightarrow & \prod_v H^1(G_v, E) & \longrightarrow & \prod_v H^1(G_v, E) & \longrightarrow & 0,
\end{array}$$

where $\mathrm{Sel}^{(\phi)}(E/\mathbb{Q})$ is the ϕ-Selmer group and $Ш(E/\mathbb{Q})$ is the Tate–Shafarevich group.

While the Selmer group is relatively easy to handle, the Tate–Shafarevich group is more mysterious. It appears naturally in the Birch and Swinnerton-Dyer conjecture, and measures the degree of deviation from the Hasse principle. Even the finiteness of the group is not known in general. Various families of elliptic curves with large Tate–Shafarevich groups were identified by a number of authors (see [2], [3], [6], [7], [24], [26], [28], [30]). Moments ([10]), heuristic results ([9]), and upper bounds ([17], [18]) on the order of Tate–Shafarevich groups were also considered.

For the elliptic curve E_n, Heath-Brown ([20], [21]) employed a method based on character sums to obtain deep results on the behavior of the size of the Selmer group $\mathrm{Sel}^{(2)}(E_n/\mathbb{Q})$ arising from the isogeny $[2]\colon E_n \to E_n$. For $h = 1, 3, 5, 7$, denote

$$S(X, h) = \{1 \le n \le X : n \equiv h \pmod 8 \text{ and } n \text{ is square-free}\}, \tag{1}$$

and for $n \in S(X, h)$, let

$$\#\mathrm{Sel}^{(2)}(E_n/\mathbb{Q}) = 2^{s(n)+2}.$$

In Theorem 1 of [21] he proved that for any fixed positive integer k

$$\sum_{n \in S(X,h)} 2^{ks(n)} = c_k \#S(X, h) + o_k(X) \tag{2}$$

as $X \to \infty$, where $c_k = \prod_{j=1}^{k}(1 + 2^j)$. He further derived the following result. Let

$$\lambda = \prod_{n=1}^{\infty}(1 + 2^{-n})^{-1} = 0.4194\ldots,$$

and

$$d_r = \lambda \frac{2^r}{\prod_{1\le j\le r}(2^j-1)} \quad (r = 0, 1, 2, \ldots).$$

Then if $h = 1$ or 3 and r is even, or if $h = 5$ or 7 and r is odd, one has

$$\#\{n \in S(X,h) : s(n) = r\} \sim d_r \#S(X,h),$$

as $X \to \infty$. This is Theorem 2 in [21], and it shows that the probability that the 2-rank of the Selmer group $\mathrm{Sel}^{(2)}(E_n/\mathbb{Q})$ equals any given non-negative integer is always positive.

Heath-Brown also obtained the asymptotic formula (see Corollary 2, [21])

$$\sum_{n\in S(X,h)} s(n) = c'_h \#S(X,h) + o(X) \tag{3}$$

as $X \to \infty$, where

$$c'_h = \begin{cases} 1.2039\ldots & \text{if } h = 1, 3, \\ 1.3250\ldots & \text{if } h = 5, 7. \end{cases}$$

Notice that since the rank of the elliptic curve satisfies $r(E_n/\mathbb{Q}) \le s(n)$, the above asymptotic formula yields a sharp upper bound on the average rank of the elliptic curves in this family (see Corollary 3 and 4 in [21]). Heath-Brown's method was generalized by G. Yu ([39], [40], [41]) to broader families of elliptic curves with full 2-torsion points and with a 2-torsion point in $\mathbb{Q}$, and he obtained sharp upper bounds on the average rank of the elliptic curves in those families.

In this paper we also focus on the family of elliptic curves E_n. For the three different 2-isogenies ϕ_1, ϕ_2, ϕ_3 defined by

$$\begin{aligned} \phi_1 \colon E_n &\longrightarrow E_{1,n} : y^2 = x^3 + 4n^2x, \\ (x,y) &\longmapsto (y^2/x^2, -y(n^2+x^2)/x^2), \end{aligned}$$

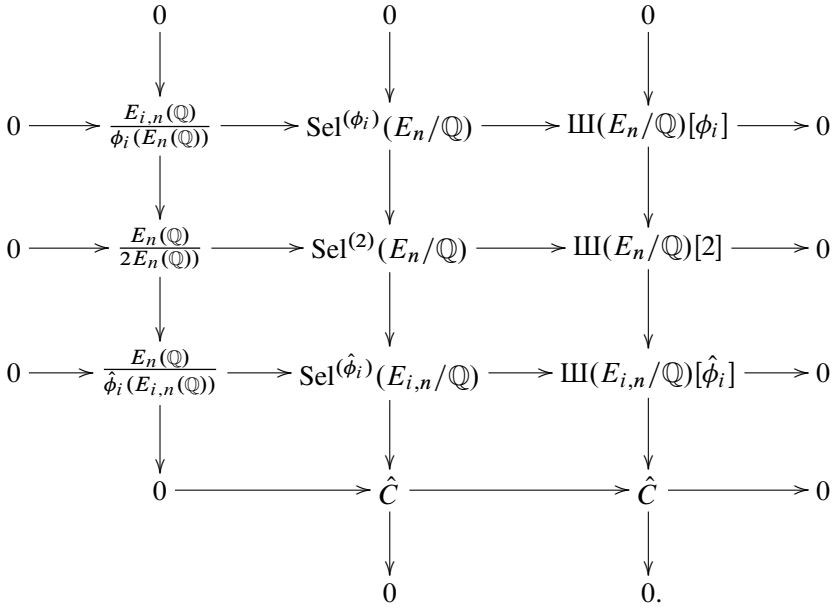
$$\begin{aligned} \phi_2 \colon E_n &\longrightarrow E_{2,n} : y^2 = x(x^2 - 6nx + n^2), \\ (x,y) &\longmapsto (y^2/(x+n)^2, y(2n^2 - (x+n)^2)/(x+n)^2), \end{aligned}$$

and

$$\begin{aligned} \phi_3 \colon E_n &\longrightarrow E_{3,n} : y^2 = x(x^2 + 6nx + n^2), \\ (x,y) &\longmapsto (y^2/(x-n)^2, y(2n^2 - (x-n)^2)/(x-n)^2), \end{aligned}$$

let $\hat{\phi}_1 \colon E_{1,n} \to E_n$, $\hat{\phi}_2 \colon E_{2,n} \to E_n$ and $\hat{\phi}_3 \colon E_{3,n} \to E_n$ be their dual 2-isogenies respectively. Hence $\hat{\phi}_i \circ \phi_i = [2]$ for $i = 1, 2, 3$, and one has the following

commutative diagrams (see pp. 97, [1]):



The first three rows are basic short exact sequences in the arithmetic of elliptic curves coming from Galois cohomology; the exactness in the first column comes from the fact that E_n contains full 2-torsion in $\mathbb{Q}$, and the rest come from the Snake lemma.

Here one may apply Heath-Brown's method to obtain asymptotic formulas for the average of the sizes of the two Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$, and this may reveal some interesting distribution phenomena. Moreover, by comparing such results on $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$ and the result on $\mathrm{Sel}^{(2)}(E_n/\mathbb{Q})$ obtained by Heath-Brown, one may be able to obtain new information on the Tate–Shafarevich groups in the third column of the commutative diagrams. As we will see below, this is precisely the case. We will prove the following results. Let $S(X,h)$ be the set of integers defined in (1).

Theorem 1. *Let $h = 1, 3, 5$ or 7 and $i = 1, 2$ or 3. For $n \in S(X,h)$, denote*

$$\#\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q}) = 2^{s(n,\phi_i)}, \quad \#\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q}) = 2^{s(n,\hat{\phi}_i)+2}.$$

Then $s(n,\phi_i) = 0$ for almost all $n \in S(X,h)$ as $X \to \infty$, and $s(n,\hat{\phi}_i)$ follows a Gaussian distribution. More precisely, for any integer $k \geq 0$, one has

$$\lim_{X\to\infty} \frac{1}{\#S(X,h)} \sum_{n\in S(X,h)} s(n,\phi_i)^k = 0,$$

and for any $\gamma \in \mathbb{R}$,

$$\lim_{X\to\infty} \frac{1}{\#S(X,h)} \#\left\{ n \in S(X,h) : \frac{s(n,\hat{\phi}_i) - \frac{1}{2}\log\log n}{\sqrt{\frac{1}{2}\log\log n}} \le \gamma \right\} = G(\gamma),$$

where the function G *is defined by*

$$G(\gamma) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}}\, \mathrm{d}t.$$

We note that the sizes of the three Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$, $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$ and $\mathrm{Sel}^{(2)}(E_n/\mathbb{Q})$ behave very differently. While the first is almost always trivial and the 2-rank of the second follows a Gaussian distribution, the probability that the 2-rank of the third equals any non-negative integer is always positive. It also implies that the map $\phi_i : E_n(\mathbb{Q}) \to E_{i,n}(\mathbb{Q})$ is almost always surjective for $n \in S(X,h)$ as $X \to \infty$.

Theorem 2. *Let* $h = 1, 3, 5$ *or* 7 *and* $i = 1, 2$ *or* 3. *For* $n \in S(X,h)$, *denote*

$$\#Ш(E_n/\mathbb{Q})[\phi_i] = 2^{t(n,\phi_i)}, \quad \#Ш(E_{i,n}/\mathbb{Q})[\hat{\phi}_i] = 2^{t(n,\hat{\phi}_i)}.$$

Then $t(n,\phi_i) = 0$ *for almost all* $n \in S(X,h)$ *as* $X \to \infty$. *Moreover, for any positive integer* k, *one has*

$$\frac{1}{\#S(X,h)} \sum_{n\in S(X,h)} t(n,\phi_i)^k = O_k\big((\log X)^{-1/5}\big),$$

and

$$\frac{1}{\#S(X,h)} \sum_{n\in S(X,h)} t(n,\hat{\phi}_i)^k = \left(\frac{\log\log X}{2}\right)^k + O_k\big((\log\log X)^{k-1}\big).$$

In particular when $k = 1$, it shows that the mean value of the 2-rank of the large Tate–Shafarevich groups is $\frac{1}{2}\log\log X + O(1)$. Notice that $Ш(E_{i,n}/\mathbb{Q})[\hat{\phi}_i] \subset Ш(E_{i,n}/\mathbb{Q})[2]$, Theorem 2 implies that the 2-part of the Tate–Shafarevich group $Ш(E_{i,n}/\mathbb{Q})$ can be arbitrarily large for any $i = 1, 2$ or 3.

There are three main ingredients in the proofs of the above results. First, we use a graph method to determine the sizes of the Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$ separately. This will reveal a simple relation, which is essential in reducing the complexity of the problem. Second, we employ Heath-Brown's method based on character sums in order to obtain asymptotic formulas for the average of

the size of the Selmer group. This will yield the distribution results. Third, by combining our results, the full strength of the results obtain by Heath-Brown and the above commutative diagrams, we derive information on the corresponding Tate–Shafarevich groups.

Acknowledgement. The authors are very grateful to the referee for many useful comments and suggestions.

2. Preliminaries

2.1. 2-descent and Selmer groups. The 2-descent method is explained in the last chapter of Silverman's book ([36]) in general. For our particular case of E_n, this was specified in [13], [14] and [15] as follows.

For a square-free positive integer n, let $n = p_1 \dots p_t$, where $p_1, \dots, p_t$ are the distinct odd prime factors of n. Define a set S of prime divisors of the rational number field $\mathbb{Q}$ by

$$S = \{\infty, 2, p_1, \dots, p_t\}$$

and a subgroup M of the multiplicative group $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by the elements $-1, 2, p_1, \dots, p_t$. For $i = 1, 2, 3$, for each $d \in M$ we have homogeneous spaces $C_{i,d}$ and $C'_{i,d}$ corresponding to the isogenies ϕ_i and $\hat{\phi}_i$ respectively. They are defined as

$$\begin{aligned}
C_{1,d}\colon &\quad dw^2 = t^4 + (2n/d)^2 z^4,\\
C'_{1,d}\colon &\quad dw^2 = t^4 - (n/d)^2 z^4,\\
C_{2,d}\colon &\quad dw^2 = t^4 - 6(n/d)t^2z^2 + (n/d)^2 z^4,\\
C'_{2,d}\colon &\quad dw^2 = t^4 + 3(n/d)t^2z^2 + 2(n/d)^2 z^4,\\
C_{3,d}\colon &\quad dw^2 = t^4 + 6(n/d)t^2z^2 + (n/d)^2 z^4,\\
C'_{3,d}\colon &\quad dw^2 = t^4 - 3(n/d)t^2z^2 + 2(n/d)^2 z^4.
\end{aligned}$$

The Selmer group $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ ($\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$) measures the possibility of $C_{i,d}$ ($C'_{i,d}$) having non-trivial solutions in the local field $\mathbb{Q}_v$ for all $v \in S$. Namely,

$$\begin{aligned}
\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q}) &\cong \left\{d \in M : C_{i,d}(\mathbb{Q}_v) \neq \phi \text{ for all } v \in S\right\},\\
\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q}) &\cong \{d \in M : C'_{i,d}(\mathbb{Q}_v) \neq \phi \text{ for all } v \in S\},
\end{aligned}$$

where $C_{i,d}(\mathbb{Q}_v) \neq \phi$ ($C'_{i,d}(\mathbb{Q}_v) \neq \phi$) means that the homogeneous space $C_{i,d}$ ($C'_{i,d}$) has non-trivial solutions $(w, t, z) \neq (0, 0, 0)$ in $\mathbb{Q}_v$. The Selmer groups

$\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$ can be considered as subgroups of M. Notice that $\{\pm 1, \pm n\} \subseteq \mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q})$, $\{1, 2, -n, -2n\} \subseteq \mathrm{Sel}^{(\hat{\phi}_2)}(E_{2,n}/\mathbb{Q})$ and $\{1, 2, n, 2n\} \subseteq \mathrm{Sel}^{(\hat{\phi}_3)}(E_{3,n}/\mathbb{Q})$, since the corresponding homogeneous spaces have global non-trivial solutions in $\mathbb{Q}$.

2.2. A graph method. We use standard terminology in graph theory ([19]). Let $G = (V, A)$ be a simple directed graph where $V = V(G) = \{v_1, \ldots, v_m\}$ is the set of vertices of G, and $A = A(G)$ is the set of arcs in G. We denote an arc $(v_i, v_j) \in A$ by $\overrightarrow{v_i v_j}$. The adjacency matrix of G is defined by

$$M(G) = (a_{ij})_{1 \leqslant i,j \leqslant m},$$

where

$$a_{ij} = \begin{cases} 1 & \text{if } \overrightarrow{v_i v_j} \in A \ \ (1 \leqslant i \neq j \leqslant m), \\ 0 & \text{otherwise.} \end{cases}$$

For the vertex v_i, $1 \leq i \leq m$, let $d_i = \sum_{j=1}^{m} a_{ij}$. The Laplace matrix of the graph G is defined by

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

The term "odd graph" has been used by K. Feng, Y. Xue and one of the authors in their study of new families of non-congruent numbers ([13], [14], [15]).

Definition 1. Let $G = (V, A)$ be a directed graph. A partition of vertices $V_1 \cup V_2 = V$ is called odd if either there exists a vertex $v_1 \in V_1$ such that $\#\{v_1 \to V_2\}$, the total number of arcs from v_1 to vertices in V_2 is odd, or there exists $v_2 \in V_2$ such that $\#\{v_2 \to V_1\}$ is odd. Otherwise the partition $V_1 \cup V_2 = V$ is called even. The graph G is called odd if all non-trivial partitions $\{V_1, V_2\} \neq \{V, \phi\}$ of V are odd.

We need the following counting lemma, which can be derived by the same idea used in the proof of Lemma 2.2 in [13].

Lemma 1. *Let $G = (V, A)$ be a directed graph, $V = \{v_1, \ldots, v_{s+t}\}$ $(s, t \geq 0)$. Then the number of even partition $\{V_1, V_2\}$ of V such that $\{v_{s+1}, \ldots, v_{s+t}\} \subset V_2$ is equal to the number of vectors $(x_1, \ldots, x_s) \in \mathbb{F}_2^s$ such that $L(G) \cdot (x_1, \ldots, x_s, 0, \ldots, 0)^T = \mathbf{0}$.*

3. Explicit formulas for the Selmer groups

The problem of finding the sizes of the Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ (respectively $\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q})$) is equivalent to the problem of determining how many homogeneous spaces $C_{i,d}$ (respectively $C'_{i,d}$) have non-trivial solutions over certain local fields.

While the solvability conditions can be found by using Hensel's lemma, one still needs a clever combinatoric method to piece them together. We will interpret these solvability conditions as certain "even partitions" of a graph, and use Lemma 1 to find the number of such partitions.

3.1. The sizes of $\mathbf{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$ and $\mathbf{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q})$. We collect the solvability conditions for $C_{1,d}$ and $C'_{1,d}$ over local fields as follows.

Lemma 2 (Lemma 3.1, [14]). *Suppose that $n = p_1 \dots p_t$ ($t \geq 1$) is a square-free odd integer, $d \in M = \langle -1, 2, p_1, \dots, p_t \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$, $v \in S = \{\infty, 2, p_1, \dots, p_t\}$. Let p denote an odd prime number. One has*

(1) $C_{1,d}(\mathbb{Q}_\infty) = \phi \iff d < 0$;

(2) *For $p \mid d$, $C_{1,d}(\mathbb{Q}_p) \neq \phi \iff \left(\frac{-1}{p}\right) = 1$ and $\left(\frac{n/d}{p}\right) = 1$;*

(3) *For $p \mid \frac{n}{d}$, $C_{1,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{d}{p}\right) = -1$;*

(4) *If $n \equiv \pm 3 \pmod 8$ and $2 \mid d$, then $C_{1,d}(\mathbb{Q}_2) = \phi$;*

(5) *$d \equiv 1 \pmod 4 \Longrightarrow C_{1,d}(\mathbb{Q}_2) \neq \phi$;*

(6) *If $n \equiv \pm 1 \pmod 8$, $d = 2d' \mid 2n$ and $d' \equiv 1 \pmod 4$, then $C_{1,d}(\mathbb{Q}_2) \neq \phi$.*

Lemma 3 (Lemma 3.2, [14]). *Under the same assumptions one has*

(1) $2 \mid d \Longrightarrow C'_{1,d}(\mathbb{Q}_2) = \phi$;

(2) *If $2 \nmid d$, then $C'_{1,d}(\mathbb{Q}_2) = \phi \iff d \equiv \pm 3 \pmod 8$ and $\frac{n}{d} \equiv \pm 3 \pmod 8$;*

(3) *If $p \mid d$, then $C'_{1,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{-1}{p}\right) = 1$ and $\left(\frac{n/d}{p}\right) = -1$;*

(4) *If $p \mid \frac{n}{d}$, then $C'_{1,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{-1}{p}\right) = 1$ and $\left(\frac{d}{p}\right) = -1$.*

For a square-free positive odd integer n, let

$$n = p_1 \dots p_t q_1 \dots q_s$$

be its prime factorization, where

$$\begin{cases} p_i \equiv 1 \pmod 4, & 1 \leq i \leq t, \\ q_j \equiv 3 \pmod 4, & 1 \leq j \leq s. \end{cases}$$

If $n \equiv \pm 3 \pmod 8$, we construct a graph $\widehat{G}_1(n) = (V, A)$ by assigning

$$V = \{p_1, \dots, p_t, q_1, \dots, q_s\},$$

$$A = \left\{\overrightarrow{pq} \,:\, \left(\frac{q}{p}\right) = -1,\ p \mid n,\ q \mid n\right\}.$$

By (1), (2) and (3) of Lemma 2 one has $\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q}) \subset \langle p_1, \ldots, p_t\rangle$. For any $d = p_1 \ldots p_r \in \langle p_1, \ldots, p_t\rangle$, it is easy to see from Lemma 2 that $d \in \mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$ if and only if the partition

$$\{p_1, \ldots, p_r\} \cup \{p_{r+1}, \ldots, p_s, q_1, \ldots, q_s\} = V$$

is an even partition. Let $L(\widehat{G}_1(n)$ be the Laplace matrix of the graph $\widehat{G}_1(n)$. Then by Lemma 1, the number of such even partitions, as well as the size of the Selmer group $\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$ is

$$2^{t-\mathrm{rank}_{\mathbb{F}_2} L(\widehat{G}_1(n))}.$$

For the Selmer group $\mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q})$ and $n \equiv \pm 3 \pmod 8$, we construct another graph $G_1(n) = (V, A)$ by assigning

$$V = \{p_1, \ldots, p_t, q_1, \ldots, q_s\},$$

$$\begin{aligned} A = &\left\{\overline{p_i\, p_j} \,:\, \left(\frac{p_j}{p_i}\right) = -1,\ 1 \le i \ne j \le t\right\} \\ &\cup \left\{\overrightarrow{p_i q_r} \,:\, \left(\frac{q_r}{p_i}\right) = -1,\ 1 \le i \le t,\ 1 \le r \le s\right\}. \end{aligned}$$

We know from Lemma 3 that for any $d = p_1 \ldots p_r q_1 \ldots q_l \in \langle p_1, \ldots, p_t, q_1, \ldots, q_s\rangle$, $d \in \mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q})$ if and only if the partition

$$\{p_1, \ldots, p_r, q_1, \ldots, q_l\} \cup \{p_{r+1}, \ldots, p_s, q_{l+1}, \ldots, q_s\} = V$$

is an even partition. By Lemma 1, the size of the Selmer group, which is twice the number of such even partitions is

$$2^{t+s+1-\mathrm{rank}_{\mathbb{F}_2} L(G_1(n))}.$$

Here $L(G_1(n))$ denotes the Laplace matrix of the graph $G_1(n)$. One sees that

$$\mathrm{rank}_{\mathbb{F}_2} L(\widehat{G}_1(n)) = \mathrm{rank}_{\mathbb{F}_2} L(G_1(n).$$

Therefore

$$\#\mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q}) = \#\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q}) \cdot 2^{s+1}.$$

In the case when $n \equiv \pm 1 \pmod 8$ the computation is similar and we omit the details. We have in conclusion the following result.

Theorem 3. *For any square-free positive odd integer n, let*

$$n = p_1 \dots p_t q_1 \dots q_s$$

be its prime factorization, where

$$\begin{cases} p_i \equiv 1 \pmod 4, & 1 \le i \le t, \\ q_j \equiv 3 \pmod 4, & 1 \le j \le s. \end{cases}$$

Let $s(n,\phi_1)$ and $s(n,\hat{\phi}_1)$ be the 2-rank of the Selmer groups $\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q})$ respectively, i.e.,

$$\#\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q}) = 2^{s(n,\phi_1)}, \quad \#\mathrm{Sel}^{(\hat{\phi}_1)}(E_{1,n}/\mathbb{Q}) = 2^{s(n,\hat{\phi}_1)+2}.$$

If $n \equiv \pm 3 \pmod 8$, we construct a graph $G_1(n) = (V, A)$ by

$$V = \{p_1, \dots, p_t, q_1, \dots, q_s\},$$

$$\begin{aligned} A = &\left\{\overline{p_i\, p_j} \,:\, \left(\frac{p_j}{p_i}\right) = -1,\ 1 \le i \ne j \le t\right\} \\ &\cup \left\{\overrightarrow{p_i q_r} \,:\, \left(\frac{q_r}{p_i}\right) = -1,\ 1 \le i \le t,\ 1 \le r \le s\right\}. \end{aligned}$$

Let $M_1(n)$ be the Laplace matrix of the graph $G_1(n)$. Then

$$s(n,\phi_1) = t - \mathrm{rank}_{\mathbb{F}_2} M_1(n), \quad s(n,\hat{\phi}_1) = s - 1 + t - \mathrm{rank}_{\mathbb{F}_2} M_1(n).$$

If $n \equiv \pm 1 \pmod 8$, we construct a graph $G_1'(n) = (V, A)$ by

$$V = \{p_1, \dots, p_t, q_1, \dots, q_s, -1\},$$

$$\begin{aligned} A = &\left\{\overline{p_i\, p_j} \,:\, \left(\frac{p_j}{p_i}\right) = -1,\ 1 \le i \ne j \le t\right\} \\ &\cup \left\{\overrightarrow{p_i q_r} \,:\, \left(\frac{q_r}{p_i}\right) = -1,\ 1 \le i \le t,\ 1 \le r \le s\right\} \\ &\cup \left\{\overrightarrow{(-1)\, p} \,:\, p \equiv \pm 3 \pmod 8,\ p \in V\right\}. \end{aligned}$$

Let $M_1'(n)$ be the Laplace matrix of the graph $G_1'(n)$. Then

$$s(n,\phi_1) = t + 1 - \mathrm{rank}_{\mathbb{F}_2} M_1'(n), \quad s(n,\hat{\phi}_1) = s - 1 + t - \mathrm{rank}_{\mathbb{F}_2} M_1'(n).$$

These explicit formulas reveal a simple relation between these two Selmer groups, which are crucial in determining the distribution of the 2-rank of one of them. They are essentially the same as the ones obtained by N. Aoki (Theorem 2.1, [1]).

3.2. The sizes of $\mathrm{Sel}^{(\phi_2)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_2)}(E_{2,n}/\mathbb{Q})$. The solvability conditions of homogeneous spaces $C_{2,d}$ and $C'_{2,d}$ over local fields can be derived from Hensel's lemma, and the proofs are very similar to those leading to Lemmas 2 and 3 above. Thus we omit the proofs and collect the results below.

Lemma 4. *Suppose that $n = p_1 \dots p_t$ $(t \geq 1)$ is a square-free odd integer, $d \in M = \langle -1, 2, p_1, \dots, p_t \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$, $v \in S = \{\infty, 2, p_1, \dots, p_t\}$. Let p denote an odd prime number. One has*

(1) $2 \mid d \Longrightarrow C_{2,d}(\mathbb{Q}_2) = \phi$;

(2) *For $p \mid d$, $C_{2,d}(\mathbb{Q}_p) \neq \phi \Longleftrightarrow \left(\frac{2}{p}\right) = 1$ and $\left(\frac{n/d}{p}\right) = 1$;*

(3) *For $p \mid \frac{n}{d}$, $C_{2,d}(\mathbb{Q}_p) = \phi \Longleftrightarrow \left(\frac{d}{p}\right) = -1$;*

(4) $C_{2,d}(\mathbb{Q}_\infty) \neq \phi \Longleftrightarrow d > 0$;

(5) $C_{2,d}(\mathbb{Q}_2) \neq \phi \Longleftrightarrow n \equiv 3 \pmod 4, d \equiv \pm 1 \pmod 8$ *or* $n \equiv 1 \pmod 4$, $d \equiv 1 \pmod 8$.

Lemma 5. *Under the same assumptions one has*

(1) $C'_{2,d}(\mathbb{Q}_\infty) \neq \phi$;

(2) $2 \nmid d$, $C'_{3,d}(\mathbb{Q}_2) \neq \phi \Longleftrightarrow d \equiv 1 \pmod 4$ *or* $\frac{n}{d} \equiv 3 \pmod 4$;

(3) *If $p \mid d$, $C'_{2,d}(\mathbb{Q}_p) = \phi \Longleftrightarrow \left(\frac{2}{p}\right) = 1$ and $\left(\frac{-n/d}{p}\right) = -1$;*

(4) *If $p \mid \frac{n}{d}$, $C'_{2,d}(\mathbb{Q}_p) = \phi \Longleftrightarrow \left(\frac{2}{p}\right) = 1$ and $\left(\frac{d}{p}\right) = -1$.*

By the same graph method one can compute explicitly the sizes of the Selmer groups $\mathrm{Sel}^{(\phi_2)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_2)}(E_{2,n}/\mathbb{Q})$.

Theorem 4. *For any square-free positive odd integer n, let*

$$n = P_1 \dots P_t p_1 \dots p_{t'} \mathbb{Q}_1 \dots \mathbb{Q}_s q_1 \dots q_{s'}$$

be its prime factorization, where $P_i \equiv 1 \pmod 8$, $p_j \equiv 7 \pmod 8$, $\mathbb{Q}_r \equiv 3 \pmod 8$, $q_m \equiv 5 \pmod 8$, $t, t', s, s' \geq 0$. Let $s(n, \phi_2)$ and $s(n, \hat{\phi}_2)$ be the 2-rank of the Selmer groups $\mathrm{Sel}^{(\phi_2)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_2)}(E_{2,n}/\mathbb{Q})$ respectively, i.e.,

$$\#\mathrm{Sel}^{(\phi_2)}(E_n/\mathbb{Q}) = 2^{s(n,\phi_2)}, \quad \#\mathrm{Sel}^{(\hat{\phi}_2)}(E_{2,n}/\mathbb{Q}) = 2^{s(n,\hat{\phi}_2)+2}.$$

If $n \equiv 1 \pmod 4$, construct a graph $G_2(n) = (V, A)$ by

$$V = \{p : p \mid n\} \cup \{-1\},$$

$$A = \left\{\overrightarrow{pq} : \left(\frac{q}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n,\ q \mid n\right\}$$
$$\cup \left\{\overrightarrow{p(-1)} : \left(\frac{-1}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n\right\}.$$

Let $M_2(n)$ be the Laplace matrix of the graph $G_2(n)$. Then

$$s(n, \phi_2) = t + t' - \operatorname{rank}_{\mathbb{F}_2} M_2(n),\ s(n, \hat{\phi}_2) = s + s' + t + t' - \operatorname{rank}_{\mathbb{F}_2} M_2(n).$$

If $n \equiv 3 \pmod 4$, construct a graph $G_2'(n) = (V, A)$ by

$$V = \{p : p \mid n\} \cup \{-1, \epsilon\},$$

$$A = \left\{\overrightarrow{pq} : \left(\frac{q}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n,\ q \mid n\right\}$$
$$\cup \left\{\overrightarrow{p(-1)} : \left(\frac{-1}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n\right\}$$
$$\cup \left\{\overrightarrow{\epsilon p} : \left(\frac{-1}{p}\right) = -1,\ p \mid n\right\}.$$

Let $M_2'(n)$ be the Laplace matrix of the graph $G_2'(n)$. Then

$$s(n, \phi_2) = t + t' + 1 - \operatorname{rank}_{\mathbb{F}_2} M_2'(n), \quad s(n, \hat{\phi}_2) = s + s' + t + t' - \operatorname{rank}_{\mathbb{F}_2} M_2'(n).$$

3.3. The sizes of $\mathrm{Sel}^{(\phi_3)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_3)}(E_{3,n}/\mathbb{Q})$

Lemma 6 (Lemma 4.1, [15]). *Suppose that $n = p_1 \dots p_t$ $(t \geq 1)$ is a square-free odd integer, $d \in M = \langle -1, 2, p_1, \dots, p_t\rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$, $v \in S = \{\infty, 2, p_1, \dots, p_t\}$. Let p denote an odd prime number. One has*

(1) $2 \mid d \Longrightarrow C_{3,d}(\mathbb{Q}_2) = \phi$;

(2) *For $p \mid d$, $C_{3,d}(\mathbb{Q}_p) \neq \phi \iff \left(\frac{2}{p}\right) = 1$ and $\left(\frac{-n/d}{p}\right) = 1$;*

(3) *For $p \mid \frac{n}{d}$, $C_{3,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{d}{p}\right) = -1$;.*

(4) $C_{3,d}(\mathbb{Q}_\infty) \neq \phi$;

(5) $C_{3,d}(\mathbb{Q}_2) \neq \phi \iff n \equiv 3 \pmod 4, d \equiv 1 \pmod 8$ *or* $n \equiv 1 \pmod 4, d \equiv \pm 1 \pmod 8$.

Lemma 7 (Lemma 4.1, [15]). *Under the same assumptions one has*

(1) $d < 0 \iff C'_{3,d}(\mathbb{Q}_\infty) = \phi$;

(2) $2 \nmid d$, $C'_{3,d}(\mathbb{Q}_2) \neq \phi \iff d \equiv 1 \pmod 4$ *or* $\frac{n}{d} \equiv 1 \pmod 4$;

(3) *If $p \mid d$, $C'_{3,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{2}{p}\right) = 1$ and $\left(\frac{n/d}{p}\right) = -1$;*

(4) *If* $p \mid \frac{n}{d}$, $C'_{3,d}(\mathbb{Q}_p) = \phi \iff \left(\frac{2}{p}\right) = 1$ *and* $\left(\frac{d}{p}\right) = -1$.

We use the same graph method to compute explicitly the sizes of the Selmer groups $\mathrm{Sel}^{(\phi_3)}(E_n/\mathbb{Q})$ and $\mathrm{Sel}^{(\hat{\phi}_3)}(E_{3,n}/\mathbb{Q})$.

Theorem 5. *For any square-free positive odd integer* n, *let*

$$n = P_1 \dots P_t p_1 \dots p_{t'} \mathbb{Q}_1 \dots \mathbb{Q}_s q_1 \dots q_{s'}$$

be its prime factorization, where $P_i \equiv 1 \pmod 8$, $p_j \equiv 7 \pmod 8$, $\mathbb{Q}_r \equiv 3 \pmod 8$, $q_m \equiv 5 \pmod 8$, $t, t', s, s' \geq 0$. *Let* $s(n, \phi_3)$ *and* $s(n, \hat{\phi}_3)$ *be the* 2*-rank of the Selmer groups* $\mathrm{Sel}^{(\phi_3)}(E_n/\mathbb{Q})$ *and* $\mathrm{Sel}^{(\hat{\phi}_3)}(E_{3,n}/\mathbb{Q})$ *respectively, i.e.,*

$$\#\mathrm{Sel}^{(\phi_3)}(E_n/\mathbb{Q}) = 2^{s(n,\phi_3)}, \quad \#\mathrm{Sel}^{(\hat{\phi}_3)}(E_{3,n}/\mathbb{Q}) = 2^{s(n,\hat{\phi}_3)+2}.$$

If $n \equiv 3 \pmod 4$, *construct a graph* $G_3(n) = (V, A)$ *by*

$$V = \{p : p \mid n\},$$

$$A = \left\{\overrightarrow{pq} : \left(\frac{q}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n,\ q \mid n\right\}.$$

Let $M_3(n)$ *be the Laplace matrix of the graph* $G_3(n)$. *Then*

$$s(n, \phi_3) = t + t' - \mathrm{rank}_{\mathbb{F}_2} M_3(n), \quad s(n, \hat{\phi}_3) = s + s' + t + t' - 1 - \mathrm{rank}_{\mathbb{F}_2} M_3(n).$$

If $n \equiv 1 \pmod 4$, *construct a graph* $G'_3(n) = (V, A)$ *by*

$$V = \{p : p \mid n\} \cup \{-1\},$$

$$A = \left\{\overrightarrow{pq} : \left(\frac{q}{p}\right) = -1 \text{ and } \left(\frac{2}{p}\right) = 1,\ p \mid n,\ q \mid n\right\}$$
$$\cup \left\{\overrightarrow{(-1)p} : \left(\frac{-1}{p}\right) = -1,\ p \mid n\right\}.$$

Let $M'_3(n)$ *be the Laplace matrix of the graph* $G'_3(n)$. *Then*

$$s(n, \phi_3) = t + t' + 1 - \mathrm{rank}_{\mathbb{F}_2} M'_3(n), \quad s(n, \hat{\phi}_3) = s + s' + t + t' - 1 - \mathrm{rank}_{\mathbb{F}_2} M'_3(n).$$

4. Averaging the Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$

First we consider the Selmer group $\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$. From Lemma 2, if $n \equiv \pm 3 \pmod 8$ one has

$$2^{s(n,\phi_1)} = \sum_{n=dd'} \prod_{p \mid d} \frac{1}{4}\left(\left(\frac{-1}{p}\right) + 1\right)\left(\left(\frac{d'}{p}\right) + 1\right) \prod_{p \mid d'} \frac{1}{2}\left(\left(\frac{d}{p}\right) + 1\right),$$

and if $n \equiv \pm 1 \pmod 8$,

$$2^{s(n,\phi_1)} = \sum_{n=dd'} \prod_{p|d} \frac{1}{4}\left(\left(\frac{-1}{p}\right)+1\right)\left(\left(\frac{d'}{p}\right)+1\right) \prod_{p|d'} \frac{1}{2}\left(\left(\frac{d}{p}\right)+1\right)$$
$$+ \sum_{n=dd'} \prod_{p|d} \frac{1}{4}\left(\left(\frac{-1}{p}\right)+1\right)\left(\left(\frac{2d'}{p}\right)+1\right) \prod_{p|d'} \frac{1}{2}\left(\left(\frac{2d}{p}\right)+1\right).$$

4.1. The case $n \equiv \pm 3 \pmod 8$. We consider this simpler case first. Let $h = 3$ or 5 and $n \in S(X,h)$. Expanding the product in the formula for $2^{s(n,\phi_1)}$ one has

$$2^{s(n,\phi_1)} = \sum_{n=D_0D_1D_2D_3D_4D_5} 4^{-\omega(D_0D_1D_2D_3)} 2^{-\omega(D_4D_5)} \left(\frac{-1}{D_1D_2}\right)\left(\frac{D_4}{D_1}\right)\left(\frac{D_1}{D_4}\right)$$
$$\times \left(\frac{D_4}{D_3}\right)\left(\frac{D_3}{D_4}\right)\left(\frac{D_5}{D_1}\right)\left(\frac{D_5}{D_3}\right)\left(\frac{D_0}{D_4}\right)\left(\frac{D_2}{D_4}\right) = \sum_{\boldsymbol{D}} g(\boldsymbol{D}),$$

where the vector $\boldsymbol{D} = (D_0, D_1, D_2, D_3, D_4, D_5)$ is subject to the condition that $n = D_0D_1D_2D_3D_4D_5$. Here ω is the additive function counting the number of distinct prime divisors.

The authors would like to remark that the above formula, which runs over 6-dimensional vectors $\boldsymbol{D}$, is intrinsically much simpler than the corresponding formula for the cardinality of $S^{(2)}(E_n/\mathbb{Q})$ of [20], which runs over vectors $\boldsymbol{D}$ which are 16-dimensional (see Lemma 3 on page 177 of [20]).

Our goal is to estimate

$$\sum_{n \in S(X,h)} 2^{s(n,\phi_1)}.$$

We sum over the six variables D_i, subject to the conditions that each D_i is square-free, that they are coprime in pairs, and that their product n satisfies

$$n \le X, \quad n \equiv h \pmod 8.$$

We divide the range of each variable D_i into intervals $[A_i, 2A_i)$, where A_i runs over powers of 2. There are $O(\log^6 X)$ many non-empty subsums, which we shall write in the form $S(\boldsymbol{A})$, where $\boldsymbol{A} = (A_0, A_1, A_2, A_3, A_4, A_5)$. Here we may assume that

$$1 \le \prod_{i=1}^{5} A_i \ll X.$$

Following Heath-Brown, we shall describe the variables D_i and D_j as being "linked" if exactly one of the Jacobi symbols

$$\left(\frac{D_i}{D_j}\right), \quad \left(\frac{D_j}{D_i}\right)$$

occurs in the expression for $g(\boldsymbol{D})$. It is easy to see that (D_1, D_5), (D_3, D_5), (D_0, D_4) and (D_2, D_4) are all the pairs of linked variables.

4.1.1. Case one. For the linked variables D_1, D_5. Suppose $A_1, A_5 \geq (\log X)^{224}$. We may write $g(\boldsymbol{D})$ in the form

$$g(\boldsymbol{D}) = \left(\frac{D_5}{D_1}\right) a(D_5)b(D_1),$$

where the function $a(D_5)$ depends on all other variables D_i except D_1, and similarly for the function $b(D_1)$. Moreover we have

$$|a(D_5)|, |b(D_1)| \leq 1.$$

We can now write

$$|S(\boldsymbol{A})| = \sum_{D_0, D_2, D_3, D_4} \left| \sum_{D_1, D_5} \left(\frac{D_5}{D_1}\right) a(D_5)b(D_1) \right|.$$

We need the following result.

Lemma 8 (Lemma 4, [20]). *Let a_m, b_n be complex numbers of modulus at most* 1. *Let an odd number h be given and let $M, N, X \gg 1$. Then*

$$\sum_{m,n} \left(\frac{n}{m}\right) a_m b_n \ll MN \{\min(M, N)\}^{-1/32},$$

uniformly in X, where the sum runs over square-free m, n satisfying $M \leq m < 2M$, $N \leq n < 2N, mn \leq X$ and $mn \equiv h \pmod 8$.

As a consequence of this lemma one finds that

$$S(\boldsymbol{A}) \ll D_0 D_2 D_3 D_4 D_1 D_5 \{\min(D_1, D_5)\}^{-1/32} \ll X(\log X)^{-7}.$$

Similar results hold for other linked variables. Therefore one has

Lemma 9. *We have*

$$S(\boldsymbol{A}) \ll X(\log X)^{-7}$$

whenever there is a pair of linked variables with $A_i, A_j \geq (\log X)^{224}$.

4.1.2. Case two. We now examine the case when $A_1 \geq (\log X)^{224}$ while $A_5 < (\log X)^{224}$. Using quadratic reciprocity we put $g(\boldsymbol{D})$ in the form

$$g(\boldsymbol{D}) = 4^{-\omega(D_1)} \left(\frac{D_1}{D_5}\right) \chi(D_1)c,$$

where χ is a character modulo 8, which may depend on the variables D_i other than D_1, and the factor c is independent of D_1 and satisfies $|c| \leq 1$. It follows that

$$|S(\boldsymbol{A})| \leq \sum_{D_0,D_2,D_3,D_4,D_5} \left| \sum_{D_1} 4^{-\omega(D_1)} \left(\frac{D_1}{D_5}\right) \chi(D_1) \right|, \tag{4}$$

where the inner sum is restricted by the conditions that D_1 must be square-free and coprime to all the other variables D_0, D_2, D_3, D_4, D_5. Next, we employ the following result, which slightly generalizes Lemma 4 in [20].

Lemma 10 (Lemma 4.2, [39]). *Suppose s is a fixed rational number. Let N be sufficiently large. Then for arbitrary positive integers q, r and any nonprincipal character $\chi \pmod q$, we have*

$$\sum_{n \leq X, \gcd(n,r)=1} \mu^2(n) s^{\omega(n)} \chi(n) \ll X\tau(r) \exp(-\eta\sqrt{\log X})$$

with a positive constant $\eta = \eta_{s,N}$, uniformly for $q \leq \log^N X$. Here τ is the usual divisor function and μ is the Möbius function.

To use this result we remove the condition $D_1 \equiv h' \pmod 8$ from the inner sum on the right side of (4) and insert instead a factor

$$\frac{1}{4} \sum_{\psi \pmod 8} \psi(D_1)\overline{\psi(h')}.$$

One has

$$\begin{aligned} S(\boldsymbol{A}) &\ll A_1 \exp(-\eta\sqrt{\log A_1}) \sum_{D_0,D_2,D_3,D_4,D_5} \tau(D_0D_2D_3D_4D_5) \\ &\ll A_1 \exp(-\eta\sqrt{\log A_1}) \prod_{D_i, i\neq 1} \sum_{D_i} \tau(D_i) \\ &\ll A_1 \exp(-\eta\sqrt{\log A_1}) \prod_{D_i, i\neq 1} A_i \log X \\ &\ll X(\log X)^5 \exp(-\eta\sqrt{\log A_1}), \end{aligned}$$

provided that $D_5 \neq 1$ and $8D_5 \ll \log^N A_1$ for some $N > 0$. We summarize the above results as follows.

Lemma 11. *For any constant κ with $0 < \kappa < 1$ one has*

$$S(\boldsymbol{A}) \ll X(\log X)^{-7}$$

whenever there are linked variables D_i, D_j for which

$$A_i \geq \exp\{(\log X)^{\kappa}\}$$

and $D_j > 1$.

4.1.3. Case three. For any $0 < \kappa < 1$ denote

$$C = \exp\{(\log X)^{\kappa}\}. \tag{5}$$

Let $\sum'$ indicate the condition that $A_0, A_1, A_2, A_3 \leq C$, $A_4 \leq C$ or $A_5 \leq C$. Then

$$\sum_{\boldsymbol{A}}{}' |S(\boldsymbol{A})| \leq 2 \sum_{D_i \leq 2C, 0 \leq i \leq 4} 4^{-\omega(D_0)} \dots 4^{-\omega(D_3)} 2^{-\omega(D_4)} \sum_{D_5 \leq \frac{X}{D_0 \dots D_4}} 2^{-\omega(D_5)}.$$

We now use the bounds

$$\sum_{n \leq X} \gamma^{\omega(n)} \ll X(\log X)^{\gamma - 1},$$

and

$$\sum_{n \leq X} \frac{\gamma^{\omega(n)}}{n} \leq \prod_{p \leq X} \left(1 + \frac{\gamma}{p}\right) \ll (\log X)^{\gamma},$$

which are valid for any fixed $\gamma > 0$. Since

$$\frac{X}{D_0 \dots D_4} \gg XC^{-5} \gg X^{1/2},$$

one has $\log(XC^{-5}) \gg \log X$. Therefore

$$\begin{aligned}
\sum_{\boldsymbol{A}}{}' |S(\boldsymbol{A})| &\ll \sum_{D_i \leq 2C, 0 \leq i \leq 4} 4^{-\omega(D_0)} \dots 4^{-\omega(D_3)} 2^{-\omega(D_4)} \frac{X}{D_0 \dots D_4} (\log X)^{-1/2} \\
&\ll X(\log X)^{-1/2} \Big(\sum_{n \leq 2C} \frac{4^{-\omega(n)}}{n} \Big)^4 \Big(\sum_{n \leq 2C} \frac{2^{-\omega(n)}}{n} \Big) \\
&\ll X(\log X)^{-1/2} (\log 2C)^{\frac{1}{4} \cdot 4} (\log 2C)^{\frac{1}{2}} \ll X(\log X)^{-\frac{1}{2} + \kappa \frac{3}{2}}.
\end{aligned}$$

Let $\sum''$ indicate the condition that $A_4, A_5 \le C$ and at least one of A_0, A_1, A_2, A_3 is less than C. Then

$$\begin{aligned}\sum_{\boldsymbol{A}}{}'' |S(\boldsymbol{A})| &\le \sum_{D_0D_1D_2D_3D_4D_5\le X} 4^{-\omega(D_0)}\dots 4^{-\omega(D_3)}2^{-\omega(D_4)}2^{-\omega(D_5)}\\ &= \sum_{mn\le X} 4^{-\omega(m)}2^{-\omega(n)}\Big(\sum_{D_0D_1D_2D_3=m}1\Big)\Big(\sum_{D_4D_5=n}1\Big)\\ &\le \sum_{n\le(2C)^2}1\sum_{m\le X/n}4^{-\omega(m)}\sum_{D_0D_1D_2D_3=m}1.\end{aligned}$$

Write

$$m_1=\prod_{D_i<2C}D_i,\quad m_2=\prod_{D_i\ge 2C}D_i,$$

so that $m_1\le(2C)^4$. One has

$$\begin{aligned}\sum_{\boldsymbol{A}}{}'' |S(\boldsymbol{A})| &\ll \sum_{n\le(2C)^2}1\sum_{m_1\le(2C)^4}\sum_{m_2\le\frac{X}{m_1n}}\Big(\frac{3}{4}\Big)^{\omega(m_2)}\\ &\ll \sum_{n\le(2C)^2}1\sum_{m_1\le(2C)^4}\frac{X}{m_1n}(\log X)^{-1/4}\\ &\ll X(\log X)^{-1/4}(\log 2C)^2\ll X(\log X)^{-\frac14+2\kappa}.\end{aligned}$$

We summarize our results as follows.

Lemma 12. *Choosing $\kappa=\frac{1}{40}$, we have*

$$\sum_{\boldsymbol{A}}|S(\boldsymbol{A})|\ll X(\log X)^{-1/5},$$

where the sum over $\boldsymbol{A}$ is for all sets in which either $A_0, A_1, A_2, A_3\le C$ and at least one of $A_4, A_5\le C$, or $A_4, A_5\le C$ and at least one of $A_0, A_1, A_2, A_3\le C$, or there are linked variables D_i and D_j with $D_i\ge C$ and $D_j>1$.

4.1.4. The remaining cases. The cases where the sums $S(\boldsymbol{A})$ are not handled by Lemma 12 are as follows.

(1) $A_4, A_5\ge C\Longrightarrow D_0=D_1=D_2=D_3=1$.

(2) $A_4\ge C, A_5<C\Longrightarrow D_0=D_2=D_5=1$, A_1 or $A_3\ge C$.

(3) $A_4<C, A_5>C\Longrightarrow D_1=D_3=D_4=1$, A_0 or $A_2\ge C$.

(4) $A_4, A_5\le C\Longrightarrow A_0, A_1, A_2, A_3\ge C$ and $D_4=D_5=1$.

Case (1). With $D_0 = D_1 = D_2 = D_3 = 1$ the function $g(\boldsymbol{D})$ reduces to $2^{-\omega(D_4)}2^{-\omega(D_5)}$. The sum is

$$\sum_{D_4,D_5} 2^{-\omega(D_4)}2^{-\omega(D_5)},$$

where D_4, D_5 are subject to the conditions

$$D_4, D_5 > C, \quad n = D_4D_5 \equiv h \pmod 8, \quad n \text{ square-free}, \ n \le X.$$

We can remove the condition $D_4, D_5 > C$ with an error

$$\le 2 \sum_{D_4 \le C} 2^{-\omega(D_4)} \sum_{D_5 \le \frac{X}{D_4}} 2^{-\omega(D_5)} \ll X(\log X)^{-1/2} \sum_{D_4 \le C} \frac{2^{-\omega(D_4)}}{D_4}$$
$$\ll X(\log X)^{-\frac{1}{2}+\frac{1}{2}\kappa} \ll X(\log X)^{-1/5}.$$

Since $n = D_4D_5$ is square-free it factors as D_4D_5 in exactly $2^{\omega(n)}$ different ways. We therefore obtain

$$\sum_{n \in S(X,h)} 1 + O(X(\log X)^{-1/5}) = \#S(X,h) + O(X(\log X)^{-1/5}).$$

Case (2). With $D_0 = D_2 = D_5 = 1$ the function $g(\boldsymbol{D})$ reduces to

$$f(\boldsymbol{D}) = 4^{-\omega(D_1D_3)}2^{-\omega(D_4)} \left(\frac{-1}{D_1}\right)\left(\frac{D_4}{D_1}\right)\left(\frac{D_1}{D_4}\right)\left(\frac{D_4}{D_3}\right)\left(\frac{D_3}{D_4}\right),$$

and the conditions for $\boldsymbol{A}$ are $A_4 \ge C$ and at least one of $A_1, A_3 \ge C$. We separate it into two cases.

(i) If $A_1 \le C$, we have

$$S(\boldsymbol{A}) \le \sum_{D_1,D_3,D_4} 4^{-\omega(D_1)}4^{-\omega(D_3)}2^{-\omega(D_4)} \le \sum_{D_1<2C} 4^{-\omega(D_1)} \sum_{D_3,D_4} 4^{-\omega(D_3)}2^{-\omega(D_4)}$$
$$= \sum_{D_1<2C} 4^{-\omega(D_1)} \sum_{n \le \frac{X}{D_1}} \sum_{r=0}^{\omega(n)} \binom{\omega(n)}{r} \left(\frac{1}{4}\right)^r \left(\frac{1}{2}\right)^{\omega(n)-r}$$
$$= \sum_{D_1<2C} 4^{-\omega(D_1)} \sum_{n \le \frac{X}{D_1}} \left(\frac{3}{4}\right)^{\omega(n)} \ll X(\log X)^{-1/4} \sum_{D_1<2C} \frac{4^{-\omega(D_1)}}{D_1}$$
$$\ll X(\log X)^{-1/5}.$$

A similar estimate holds true if $A_3 \le C$.

(ii) Suppose $A_1, A_3, A_4 \geq C$. We write the sums as

$$S(\boldsymbol{A}) = \sum_{\boldsymbol{D}} f(\boldsymbol{D}),$$

where the variables $\boldsymbol{D} = (D_1, D_3, D_4)$ are subject to the conditions

$$D_i \in [A_i, 2A_i)\ (i = 1, 3, 4), \quad n = D_1 D_3 D_4 \leq X, \quad n \equiv h \pmod 8,\ n \text{ square-free.}$$

Now we write

$$\begin{aligned} S(\boldsymbol{A}) &= \sum_{\boldsymbol{D}} \frac{1}{4} \sum_{\psi \pmod 8} \psi(D_1 D_3 D_4)\overline{\psi(h)} f(\boldsymbol{D}) \\ &= \frac{1}{4} \sum_{\psi \pmod 8} \overline{\psi(h)} \sum_{\boldsymbol{D}} \psi(D_1 D_3 D_4) f(\boldsymbol{D}) = \frac{1}{4} \sum_{\psi \pmod 8} \overline{\psi(h)} S(\boldsymbol{A}, \psi), \end{aligned}$$

and we have

$$\begin{aligned} S(\boldsymbol{A}, \psi) &= \sum_{\boldsymbol{D}} \psi(D_1 D_3 D_4) f(\boldsymbol{D}) \\ &\leq \sum_{D_4} \Big| \sum_{D_1, D_3} 4^{-\omega(D_1)} 4^{-\omega(D_3)} \left(\frac{-1}{D_1}\right) \psi(D_1)\chi(D_1)\psi(D_3)\chi(D_3) \Big|. \end{aligned}$$

Here the character χ depends on D_4 and is defined as

$$\chi(n) = \left(\frac{D_4}{n}\right)\left(\frac{n}{D_4}\right)$$

for any $n \in \mathbb{Z}$. We may proceed by applying the following lemma.

Lemma 13 (Lemma 10, [20]). *Let $X > 0$ and $M, N \geq C > 0$ be given. Then for an arbitrary positive integer r, any odd integer h, and any distinct characters χ_1, $\chi_2 \pmod 8$, we have*

$$\sum_{m,n} \mu^2(m)\mu^2(n) 4^{-\omega(m)-\omega(n)} \chi_1(m)\chi_2(n) \ll X\tau(r) \exp\big(-c\sqrt{\log C}\big) \log X,$$

for some positive absolute constant c, where the sum runs over coprime m, n satisfying the conditions

$$M < m \leq 2M, \quad N < n \leq 2N, \quad mn \leq X,\ mn \equiv h \pmod 8,\ \gcd(mn, r) = 1.$$

It follows that the sums $S(\boldsymbol{A}, \psi)$ and also $S(\boldsymbol{A})$ in question are all $O\left(X(\log X)^{-7}\right)$, since the constant κ in Lemma 11 may be taken sufficiently large. The total contribution of these sums is therefore $O(X(\log X)^{-1})$.

Case (3). With $D_1 = D_3 = D_4 = 1$ the function $g(\boldsymbol{D})$ reduces to

$$4^{-\omega(D_0D_2)}2^{-\omega(D_5)}\left(\frac{-1}{D_2}\right),$$

and the conditions for $\boldsymbol{A}$ are $A_5 \geq C$ and at least one of $A_0, A_2 \geq C$. If one of $A_0, A_2 \leq C$, following the argument in (i) of Case (2) one finds that the total contribution is $O(X(\log X)^{-1/5})$, while if $A_0, A_2, A_4 \geq C$, similar to (ii) of Case (2), the total contribution is $O(X(\log X)^{-1})$.

Case (4). With $D_4 = D_5 = 1$ the function $g(\boldsymbol{D})$ reduces to

$$4^{-\omega(D_0)-\omega(D_1)-\omega(D_2)-\omega(D_3)}\left(\frac{-1}{D_1D_2}\right),$$

and the conditions for $\boldsymbol{A}$ are $A_0, A_1, A_2, A_3 \geq C$. One has in this case

$$\begin{aligned} S(\boldsymbol{A}) &= \sum_{D_0,D_1,D_2,D_3} 4^{-\omega(D_0)-\omega(D_1)-\omega(D_2)-\omega(D_3)}\left(\frac{-1}{D_1D_2}\right) \\ &= \sum_{m,n} 2^{-\omega(m)-\omega(n)}\left(\frac{-1}{m}\right). \end{aligned}$$

By the same argument as in (ii) of Case (2) one finds that the total contribution is $O(X(\log X)^{-1})$.

We conclude that for $h = 3$ or 5, one has

$$\sum_{n\in S(X,h)} 2^{s(n,\phi_1)} = \#S(X,h) + O\big(X(\log X)^{-1/5}\big)$$

as $X \to \infty$.

4.2. The case $n \equiv \pm 1 \pmod 8$. Let $h = 1$ or 7 and $n \in S(X,h)$. Expanding the product in the formula for $2^{s(n,\phi_1)}$ one obtains that

$$2^{s(n,\phi_1)} = \sum_{\boldsymbol{D}} g(\boldsymbol{D}) + \sum_{\boldsymbol{D}} h(\boldsymbol{D}),$$

where $g(\boldsymbol{D})$ is the same function appearing in the case $n \equiv \pm 3 \pmod 8$ and

$$\begin{aligned} h(\boldsymbol{D}) = 4^{-\omega(D_0D_1D_2D_3)}&2^{-\omega(D_4D_5)} \\ &\times \left(\frac{-1}{D_1D_2}\right)\left(\frac{2}{D_1D_3D_4}\right)\left(\frac{D_4}{D_1}\right)\left(\frac{D_1}{D_4}\right) \\ &\times \left(\frac{D_4}{D_3}\right)\left(\frac{D_3}{D_4}\right)\left(\frac{D_5}{D_1}\right)\left(\frac{D_5}{D_3}\right)\left(\frac{D_0}{D_4}\right)\left(\frac{D_2}{D_4}\right). \end{aligned}$$

Here the vector $\boldsymbol{D} = (D_0, D_1, D_2, D_3, D_4, D_5)$ is subject to the condition that $n = D_0D_1D_2D_3D_4D_5$. Our goal is to estimate

$$\sum_{n\in S(X,h)} 2^{s(n,\phi_1)} = \sum_{n\in S(X,h)} \sum_{\boldsymbol{D}} g(\boldsymbol{D}) + \sum_{n\in S(X,h)} \sum_{\boldsymbol{D}} h(\boldsymbol{D}).$$

While the first term from the previous computation is

$$\sum_{n\in S(X,h)} \sum_{\boldsymbol{D}} g(\boldsymbol{D}) = \#S(X,h) + O\big(X(\log X)^{-1/5}\big),$$

we need to estimate the second term by the same idea. We sum over the six variables D_i, subject to the conditions that each D_i is square-free, that they are coprime in pairs, and that their product n satisfies

$$n \le X, \quad n \equiv h \pmod 8.$$

We divide the range of each variable D_i into intervals $[A_i, 2A_i)$, where A_i runs over powers of 2. There are $O(\log^6 X)$ many non-empty subsums, which we write as $S'(\boldsymbol{A})$, where $\boldsymbol{A} = (A_0, A_1, A_2, A_3, A_4, A_5)$. We assume the condition

$$1 \le \prod_{i=1}^{5} A_i \ll X.$$

We see that $(D_1, D_5), (D_3, D_5), (D_0, D_4)$ and (D_2, D_4) are all the pairs of linked variables in the function $h(\boldsymbol{D})$. Following the proof for the case $n \equiv \pm 3 \pmod 8$, one sees that Lemma 12 holds true for the sum $S'(\boldsymbol{A})$. The remaining cases are

(1) $A_4, A_5 \ge C \Longrightarrow D_0 = D_1 = D_2 = D_3 = 1$,

(2) $A_4 \ge C, A_5 < C \Longrightarrow D_0 = D_2 = D_5 = 1$, A_1 or $A_3 \ge C$,

(3) $A_4 < C, A_5 > C \Longrightarrow D_1 = D_3 = D_4 = 1$, A_0 or $A_2 \ge C$,

(4) $A_4, A_5 \le C \Longrightarrow A_0, A_1, A_2, A_3 \ge C$ and $D_4 = D_5 = 1$.

In Case (1), the function $g(\boldsymbol{D})$ reduces to $2^{-\omega(D_4)}2^{-\omega(D_5)}\big(\frac{2}{D_4}\big)$; in Case (2), the function $g(\boldsymbol{D})$ reduces to $4^{-\omega(D_1D_3)}2^{-\omega(D_4)}\big(\frac{-1}{D_1}\big)\big(\frac{2}{D_1D_3D_4}\big)\big(\frac{D_4}{D_1}\big)\big(\frac{D_1}{D_4}\big)\big(\frac{D_4}{D_3}\big)\big(\frac{D_3}{D_4}\big)$; in Case (3), $g(\boldsymbol{D})$ reduces to $4^{-\omega(D_0D_2)}2^{-\omega(D_5)}\big(\frac{-1}{D_2}\big)$; and lastly in Case (4), $g(\boldsymbol{D})$ reduces to $4^{-\omega(D_0)-\omega(D_1)-\omega(D_2)-\omega(D_3)}\big(\frac{-1}{D_1D_2}\big)\big(\frac{2}{D_1D_3}\big)$. All these four cases are similar to the Case (2) for $n \equiv \pm 3 \pmod 8$ and we can apply Lemma 13 to obtain enough cancellation. So we have

$$\sum_{n\in S(X,h)} \sum_{\boldsymbol{D}} h(\boldsymbol{D}) = O\big(X(\log X)^{-1/5}\big).$$

In conclusion one has for $h = 1, 3, 5$ or 7,

$$\sum_{n\in S(X,h)} 2^{s(n,\phi_1)} = \#S(X,h) + O\big(X(\log X)^{-1/5}\big)$$

as $X \to \infty$.

4.3. The Selmer groups $\mathbf{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ for $i = 2, 3$. Let $h = 1, 3, 5$ or 7. For any $n \in S(X,h)$, when $i = 2$, one has from Lemma 4

$$2^{s(n,\phi_2)} \le \sum_{n=dd'} \prod_{p\mid d} \frac{1}{4}\left(\left(\frac{2}{p}\right)+1\right)\left(\left(\frac{d'}{p}\right)+1\right) \prod_{p\mid d'} \frac{1}{2}\left(\left(\frac{d}{p}\right)+1\right),$$

where one has equality "=" when $n \equiv 3 \pmod 4$ and inequality "$\le$" when $n \equiv 1 \pmod 4$. Denoting the right-hand side by $S_2(n)$ and expanding the product one has

$$S_2(n) = \sum_{n=D_0D_1D_2D_3D_4D_5} 4^{-\omega(D_0D_1D_2D_3)}2^{-\omega(D_4D_5)}\left(\frac{2}{D_1D_2}\right)\left(\frac{D_4}{D_1}\right)\left(\frac{D_1}{D_4}\right) \times \left(\frac{D_4}{D_3}\right)\left(\frac{D_3}{D_4}\right)\left(\frac{D_5}{D_1}\right)\left(\frac{D_5}{D_3}\right)\left(\frac{D_0}{D_4}\right)\left(\frac{D_2}{D_4}\right).$$

When $i = 3$, from Lemma 6 we have

$$2^{s(n,\phi_3)} \le \sum_{n=dd'} \prod_{p\mid d} \frac{1}{4}\left(\left(\frac{2}{p}\right)+1\right)\left(\left(\frac{-d'}{p}\right)+1\right) \prod_{p\mid d'} \frac{1}{2}\left(\left(\frac{d}{p}\right)+1\right),$$

where one has equality "=" when $n \equiv 1 \pmod 4$ and inequality "$\le$" when $n \equiv 3 \pmod 4$. Denoting the right-hand side by $S_3(n)$ and expanding the corresponding product one has

$$S_3(n) = \sum_{n=D_0D_1D_2D_3D_4D_5} 4^{-\omega(D_0D_1D_2D_3)}2^{-\omega(D_4D_5)}\left(\frac{-1}{D_1D_3}\right)\left(\frac{2}{D_1D_2}\right)\left(\frac{D_4}{D_1}\right)\left(\frac{D_1}{D_4}\right) \times \left(\frac{D_4}{D_3}\right)\left(\frac{D_3}{D_4}\right)\left(\frac{D_5}{D_1}\right)\left(\frac{D_5}{D_3}\right)\left(\frac{D_0}{D_4}\right)\left(\frac{D_2}{D_4}\right).$$

Notice that both sums

$$\sum_{n\in S(X,h)} S_2(n) \quad \text{and} \quad \sum_{n\in S(X,h)} S_3(n)$$

are very similar to the sums treated before for the case $n \equiv \pm 3 \pmod 8$ for the Selmer group $\mathrm{Sel}^{(\phi_1)}(E_n/\mathbb{Q})$. When we sum over the six variables D_i, subject to the

same conditions, Lemma 12 holds true for both sums $S_2(n)$ and $S_3(n)$, and similarly we also have the same four remaining cases (1), (2), (3) and (4). A little thought gives that only the first case contributes to the main term, which is $\#S(X,h)$, and altogether the errors are of size $O\left(X(\log X)^{-1/5}\right)$. Since $s(n,\phi_2), s(n,\phi_3) \geq 0$, we obtain the same asymptotic formula for the Selmer groups $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$ for $i = 2,3$. We conclude this section with the following result.

Theorem 6. *Let $h = 1,3,5$ or 7. For $i \in \{1,2,3\}$, one has*

$$\sum_{n\in S(X,h)} 2^{s(n,\phi_i)} = \#S(X,h) + O\big(X(\log X)^{-1/5}\big)$$

as $X \to \infty$.

5. Proof of Theorem 1

5.1. For $\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q})$. Fix $i \in \{1,2,3\}$. For any integer $r \geq 0$, let

$$a_r = \#\{n \in S(X,h) : s(n,\phi_i) = r\}.$$

Then

$$\sum_{r\geq 0} a_r = \#S(X,h).$$

Theorem 6 yields

$$\sum_{r\geq 0} 2^r a_r = \#S(X,h) + O\big(X(\log X)^{-1/5}\big),$$

hence

$$\sum_{r\geq 1} 2^{r-1} a_r \leq \sum_{r\geq 1} (2^r - 1) a_r = O\big(X(\log X)^{-1/5}\big),$$

and

$$a_r = O\big(X(\log X)^{-1/5} 2^{-r}\big), \quad r \geq 1.$$

Therefore for any positive integer k,

$$\sum_{n\in S(X,h)} s(n,\phi_i)^k = \sum_{r\geq 1} r^k \cdot a_r = O_k\big(X(\log X)^{-1/5}\big). \tag{6}$$

Notice $\#S(X,h) \gg X$, this shows that $s(n,\phi_i) = 0$ for almost all $n \in S(X,h)$, and for any positive integer k,

$$\lim_{X\to\infty} \frac{1}{\#S(X,h)} \sum_{n\in S(X,h)} s(n,\phi_i)^k = 0.$$

This completes the first part of the proof of Theorem 1.

5.2. For $\mathbf{Sel}^{(\hat{\phi_i})}(E_{i,n}/\mathbb{Q})$. For coprime integers a, q, we define the additive function $\omega_{a,q}$ as

$$\omega_{a,q}(n) = \sum_{\substack{p|n \\ p\equiv a \pmod q}} 1,$$

for any $n \in \mathbb{N}$. By Theorem 3, if $n \equiv \pm 3 \pmod 8$, then

$$s(n, \hat{\phi}_1) = s(n, \phi_1) - 1 + s,$$

and if $n \equiv \pm 1 \pmod 8$,

$$s(n, \hat{\phi}_1) = s(n, \phi_1) - 2 + s,$$

where $s = \omega_{3,8}(n) + \omega_{7,8}(n)$. Similar results hold for ϕ_2 and ϕ_3 by Theorems 4 and 5. Therefore for any square-free integer n one has

$$s(n, \hat{\phi}_i) = s(n, \phi_i) + h_i(n) + c_{i,n}, \quad i \in \{1, 2, 3\}, \tag{7}$$

with the functions $h_1 = \omega_{3,8} + \omega_{7,8}$, $h_2 = h_3 = \omega_{3,8} + \omega_{5,8}$, and the constants $c_{1,n} = -1$ if $n \equiv \pm 3 \pmod 8$ and -2 if $n \equiv \pm 1 \pmod 8$, $c_{2,n} = 0$ if $n \equiv 1 \pmod 4$ and -1 if $n \equiv 3 \pmod 4$, and finally $c_{3,n} = -2$ if $n \equiv 1 \pmod 4$ and -1 if $n \equiv 3 \pmod 4$. Since $s(n, \phi_i) = 0$ for almost all $n \in S(X, h)$, one has

$$s(n, \hat{\phi}_i) = h_i(n) + c_{i,n},$$

for almost all $n \in S(X, h)$. It is enough to show Gaussian distribution for the functions $h_i(n)$ with the conditions $n \in S(X, h)$ for $h = 1, 3, 5$ or 7 and $X \to \infty$.

We contend ourselves to applying the following generalization of Erdös–Kac Theorem obtained by Ru-Yu Liu ([31]). For completeness we reproduce the statement here. Let S be an infinite subset of $\mathbb{N}$. For $X \in \mathbb{R}$, $X > 1$, define

$$S(X) = \{n \le X : n \in S\}.$$

We assume that S satisfies the cardinality condition

$$\left|S(X^{1/2})\right| = o\left(|S(X)|\right), \tag{8}$$

where $|S(X)|$ is the cardinality of $S(X)$. Let $f : S \to \mathbb{N}$ be a map. For each prime l, write

$$\frac{1}{|S(X)|}\#\{n \in S(X) \colon f(n) \text{ is divisible by } l\} = \lambda_l(X) + e_l(X),$$

and for any u-tuples of distinct primes $(l_1, l_2, \ldots, l_u)$, write

$$\frac{1}{|S(X)|}\#\{n \in S(X) : f(n) \text{ is divisible by } l_1 l_2 \ldots l_u\} = \prod_{i=1}^{u} \lambda_{l_i}(X) + e_{l_1 l_2 \ldots l_u}(X).$$

We will use abbreviated notations λ_l, e_l and $e_{l_1 l_2 \dots l_u}$ below.

Suppose there exist absolute constants β and c with $0 < \beta \leq 1$ and $c > 0$, and a function $Y = Y(X) < X^\beta$ such that the following conditions hold:

(i) For each $n \in S(X)$, the number of distinct prime divisors l of $f(n)$ with $l > X^\beta$ is bounded uniformly.

(ii) $\sum_{Y<l\leq X^\beta} \lambda_l = o((\log\log X)^{1/2})$, where the sum is over primes l.

(iii) $\sum_{Y<l\leq X^\beta} |e_l| = o((\log\log X)^{1/2})$.

(iv) $\sum_{l\leq Y} \lambda_l = c\log\log X + o((\log\log X)^{1/2})$.

(v) $\sum_{l\leq Y} \lambda_l^2 = o((\log\log X)^{1/2})$.

(vi) For $r \in \mathbb{N}$, let $u = 1, 2, \dots, r$. We have

$$\sum{}'' |e_{l_1 \dots l_u}| = o((\log\log X)^{-r/2}),$$

where $\sum''$ extends over all u-tuples of distinct primes $(l_1, l_2, \dots, l_u)$ with $l_i \leq Y$.

(Notice that the condition (4) in Liu's paper [31] is actually $c = 1$. However there is no essential difference by introducing the constant $c > 0$ here.)

Theorem 7 (Theorem 3, [31]). *Let S be an infinite subset of $\mathbb{N}$ satisfying condition* (8) *and $f : S \to \mathbb{N}$. Suppose there exist absolute constants β, c with $0 < \beta \leq 1$, $c > 0$ and $Y = y(X) < X^\beta$ such that the conditions* (i)–(vi) *hold. Then for $\gamma \in \mathbb{R}$, we have*

$$\lim_{X\to\infty} \frac{1}{|S(X)|} \# \left\{ n \in S(X) : \frac{\omega(f(n)) - c\log\log n}{\sqrt{c\log\log n}} \leq \gamma \right\} = G(\gamma).$$

Let

$$S = \{n \in \mathbb{N} : n \text{ square-free and } n \equiv h \pmod 8\}.$$

Define the map $f : S \to \mathbb{N}$ as

$$f(n) = \prod_{\substack{p|n \\ p\equiv 3 \bmod 4}} p,$$

for any $n \in \mathbb{N}$. Then

$$h_1(n) = \omega(f(n)), \quad n \in \mathbb{N}.$$

It is easy to verify by Merten's estimate and the estimates proved in Appendix below that S and f satisfy all the conditions listed in Theorem 7 with constant $c = \frac{1}{2}$. Therefore for $n \in S(X, h)$, $h = 1, 3, 5, 7$ and $X \to \infty$, $h_1(n)$, as well as $s(n, \hat{\phi}_1)$ satisfies the Gaussian distribution, with mean and variance $\frac{1}{2}\log\log n$. This result also holds true for the values $h_2(n)$ and $h_3(n)$. This proves the second part of Theorem 1. Now Theorem 1 is completely proved.

6. On Ш($E_n/\mathbb{Q}$)[ϕ_i] and Ш($E_{i,n}/\mathbb{Q}$)[$\hat{\phi}_i$]

For $h = 1, 3, 5$ or 7 and $i = 1, 2$ or 3, $n \in S(X, h)$, denote

$$\#Ш(E_n/\mathbb{Q})[\phi_i] = 2^{t(n,\phi_i)},\ \ \#Ш(E_{i,n}/\mathbb{Q})[\hat{\phi}_i] = 2^{t(n,\hat{\phi}_i)},\ \ \#Ш(E_n/\mathbb{Q})[2] = 2^{t(n)},$$

and as in previous sections

$$\#\mathrm{Sel}^{(\phi_i)}(E_n/\mathbb{Q}) = 2^{s(n,\phi_i)},\ \ \#\mathrm{Sel}^{(\hat{\phi}_i)}(E_{i,n}/\mathbb{Q}) = 2^{s(n,\hat{\phi}_i)},\ \ \#\mathrm{Sel}^{(2)}(E_n/\mathbb{Q}) = 2^{s(n)}.$$

From the commutative diagrams in the introduction one has the formula

$$t(n, \hat{\phi}_i) = s(n, \phi_i) + s(n, \hat{\phi}_i) - s(n) + t(n) - t(n, \phi_i)$$

and the inequalities

$$0 \le t(n, \phi_i) \le s(n, \phi_i), \quad 0 \le t(n, \hat{\phi}_i) \le s(n, \hat{\phi}_i), \quad 0 \le t(n) \le s(n).$$

Since $s(n, \phi_i) = 0$ for almost all $n \in S(X, h)$, one has that $t(n, \phi_i) = 0$ for almost all $n \in S(X, h)$. Moreover by the asymptotic formula (6) one has

$$\sum_{n \in S(X,h)} t(n, \phi_i)^k = O_k\big(X(\log X)^{-1/5}\big),$$

for any fixed positive integer k. This proves the first part of Theorem 2.

Next, for any fixed positive integer k, we will prove in the Appendix that

$$\sum_{n \in S(X,h)} s(n, \hat{\phi}_i)^k = \#S(X, h) \left(\frac{\log\log X}{2}\right)^k + O_k\big(X\,(\log\log X)^{k-1}\big) \tag{9}$$

as $X \to \infty$. Noticing that

$$s(n, \hat{\phi}_i) - s(n) \le t(n, \hat{\phi}_i) \le s(n, \hat{\phi}_i),$$

one has

$$\sum_{n \in S(X,h)} \big(s(n, \hat{\phi}_i) - s(n)\big)^k \le \sum_{n \in S(X,h)} t(n, \hat{\phi}_i)^k \le \sum_{n \in S(X,h)} s(n, \hat{\phi}_i)^k.$$

The magnitude of the right-hand side is known from (9), and the left-hand side is

$$\sum_{n \in S(X,h)} s(n, \hat{\phi}_i)^k + O_k\Big(\max_{0 \le r \le k-1} \Big\{ \sum_{n \in S(X,h)} s(n, \hat{\phi}_i)^r s(n)^{k-r} \Big\}\Big).$$

For any r with $0 \le r \le k-1$, one obtains that

$$\begin{aligned}\sum_{n\in S(X,h)} s(n,\hat{\phi}_i)^r s(n)^{k-r} &\le \Big(\sum_{n\in S(X,h)} s(n,\hat{\phi}_i)^{2r}\Big)^{1/2}\Big(\sum_{n\in S(X,h)} s(n)^{2(k-r)}\Big)^{1/2}\\ &\le \Big(\sum_{n\in S(X,h)} s(n,\hat{\phi}_i)^{2r}\Big)^{1/2}\Big(\sum_{n\in S(X,h)} 2^{2(k-r)s(n)}\Big)^{1/2}\\ &\ll_k \big(X(\log\log X)^{2r}\big)^{1/2}(X)^{1/2} \le X(\log\log X)^{k-1},\end{aligned}$$

by using (9) again and the formula (2) obtained by Heath-Brown. Therefore

$$\sum_{n\in S(X,h)} t(n,\hat{\phi}_i)^k = \#S(X,h)\left(\frac{\log\log X}{2}\right)^k + O_k\big(X\,(\log\log X)^{k-1}\big),$$

which completes the proof of Theorem 2.

Appendix

To establish formula (9), we first prove the case $k = 1$, which is essentially the following lemma.

Lemma 14. *For any $h \in \{1,3,5,7\}$ and two coprime integers $a, q > 0$, one has*

$$\sum_{n\in S(X,h)} \omega_{a,q}(n) = \#S(X,h)\left(\frac{\log\log X}{\phi(q)}\right) + O(X)$$

as $X \to \infty$, where ϕ is Euler's totient function.

Proof. First we write

$$\sum_{n\in S(X,h)} \omega_{a,q}(n) = \sum_{\substack{n\le X\\ n\equiv h \pmod 8}} \mu^2(n)\omega_{a,q}(n).$$

Removing the condition $n \equiv h \pmod 8$ by inserting the factor

$$\frac{1}{4}\sum_{\psi \pmod 8} \psi(n)\overline{\psi(h)},$$

and interchanging the summation one has

$$\sum_{n\in S(X,h)} \omega_{a,q}(n) = \frac{1}{4}\sum_{\psi \pmod 8} \overline{\psi(h)} \sum_{n\le X} \mu^2(n)\omega_{a,q}(n)\psi(n).$$

For the character $\psi \pmod 8$, denote

$$S(\psi, X) = \sum_{n \le X} \mu^2(n)\omega_{a,q}(n)\psi(n).$$

If $\psi \neq 1$, one has

$$\begin{aligned} S(\psi, X) &= \sum_{n \le X} \mu^2(n)\psi(n) \sum_{\substack{p \mid n \\ p \equiv a \pmod q}} 1 = \sum_{\substack{p \le X \\ p \equiv a \pmod q}} \sum_{p \mid n, n \le X} \mu^2(n)\psi(n) \\ &= \sum_{\substack{p \le X \\ p \equiv a \pmod q}} \psi(p) \sum_{\substack{m \le X/p \\ \gcd(m,p)=1}} \mu^2(m)\psi(m). \end{aligned}$$

By Lemma 10, one has

$$\sum_{\substack{m \le X/p \\ \gcd(m,p)=1}} \mu^2(m)\psi(m) \ll \frac{X}{p} \exp\big(-\eta\sqrt{\log(X/p)}\big).$$

Since

$$\begin{aligned} \sum_{p \le \sqrt{X}} \frac{1}{p \exp\big(\eta\sqrt{\log(X/p)}\big)} &\le \exp\big(-\eta\sqrt{(\log X)/2}\big) \sum_{p \le \sqrt{X}} p^{-1} \\ &\ll \exp\big(-\eta\sqrt{\log X}\big) \log\log X \ll 1, \end{aligned}$$

and

$$\sum_{\sqrt{X} < p \le X} \frac{1}{p \exp\big(\eta\sqrt{\log(X/p)}\big)} \le \sum_{\sqrt{X} < p \le X} p^{-1} \ll 1,$$

one has

$$S(\psi, X) \ll X.$$

When $\psi = 1$, one has

$$S(1, X) = \sum_{\substack{n \le X \\ \gcd(n,2)=1}} \mu^2(n) \sum_{\substack{p \mid n \\ p \equiv a \pmod q}} 1 = \sum_{\substack{p \le X \\ p \equiv a \pmod q}} \sum_{\substack{m \le X/p \\ \gcd(m,2p)=1}} \mu^2(m).$$

For any integer $r > 0$, denote

$$A(r, X) = \sum_{\substack{n \le X \\ \gcd(n,r)=1}} \mu^2(n).$$

We define the multiplicative function g by the convolution $g = \mu^2 * \mu$. One sees that $\mu^2 = 1 * g$ and at any prime p,

$$g(p^m) = \begin{cases} 0 & \text{if } m = 1, \\ -1 & \text{if } m = 2, \\ 0 & \text{if } m \geq 3. \end{cases}$$

$$\begin{aligned} A(r, X) &= \sum_{\substack{n \leq X \\ \gcd(n,r)=1}} \sum_{d|n} g(d) = \sum_{\substack{d \leq X \\ \gcd(d,r)=1}} g(d) \sum_{\substack{m \leq X/d \\ \gcd(m,r)=1}} 1 \\ &= \sum_{\substack{n \leq \sqrt{X} \\ \gcd(n,r)=1}} \mu(n) \sum_{\substack{m \leq X/n^2 \\ \gcd(m,r)=1}} 1. \end{aligned}$$

Since

$$\sum_{\substack{m \leq X \\ \gcd(m,r)=1}} 1 = \sum_{d|r} \mu(d) \cdot \left[\frac{X}{d}\right] = \sum_{d|r} \mu(d) \cdot \left(\frac{X}{d} + O(1)\right) = \frac{\phi(r)X}{r} + O(\tau(r)),$$

where ϕ is Euler's totient function, we have

$$\begin{aligned} A(r, X) &= \sum_{\substack{n \leq \sqrt{X} \\ \gcd(n,r)=1}} \mu(n) \left(\frac{\phi(r)X}{rn^2} + O(\tau(r))\right) \\ &= \frac{\phi(r)X}{r} \sum_{\substack{n \leq \sqrt{X} \\ \gcd(n,r)=1}} \frac{\mu(n)}{n^2} + O\big(\sqrt{X}\tau(r)\big). \end{aligned}$$

It is easy to see that

$$\sum_{\substack{n \leq \sqrt{X} \\ \gcd(n,r)=1}} \frac{\mu(n)}{n^2} = \frac{6}{\pi^2} \prod_{p|r} (1 - p^{-2})^{-1} + O(X^{-1/2}).$$

Hence

$$\begin{aligned} A(r, X) &= \frac{\phi(r)X}{r} \left(\frac{6}{\pi^2} \prod_{p|r} (1 - p^{-2})^{-1} + O(X^{-1/2})\right) + O\big(\sqrt{X}\tau(r)\big) \\ &= \frac{6X}{\pi^2} \prod_{p|r} (1 + p^{-1})^{-1} + O\big(\sqrt{X}\tau(r)\big). \end{aligned}$$

Now we have

$$\begin{aligned} S(1,X) &= \sum_{\substack{p\le X\\ p\equiv a \pmod q}} A(2p, X/p) \\ &= \sum_{\substack{p\le X\\ p\equiv a \pmod q}} \left(\frac{6X}{\pi^2 p}(1+2^{-1})^{-1}(1+p^{-1})^{-1} + O\Big(\sqrt{\tfrac{X}{p}}\,\tau(2p)\Big)\right) \\ &= \frac{4X}{\pi^2} \sum_{\substack{p\le X\\ p\equiv a \pmod q}} \frac{1}{p+1} + O\Big(X^{1/2}\sum_{p\le X} p^{-1/2}\Big). \end{aligned}$$

Since

$$\sum_{\substack{p\le X\\ p\equiv a \pmod q}} \frac{1}{p+1} = \sum_{\substack{p\le X\\ p\equiv a \pmod q}} \frac{1}{p} + O(1) = \frac{\log\log X}{\phi(q)} + O(1)$$

by Merten's estimate, and

$$\sum_{p\le X} p^{-1/2} \le \Big(\sum_{p\le X} 1\Big)^{1/2}\cdot\Big(\sum_{p\le X} p^{-1}\Big)^{1/2} \ll \left(\frac{X}{\log X}\right)^{1/2} (\log\log X)^{1/2},$$

one obtains that

$$\begin{aligned} S(1,X) &= \frac{4X}{\pi^2}\left(\frac{\log\log X}{\phi(q)} + O(1)\right) + O\left(X\left(\frac{\log\log X}{\log X}\right)^{1/2}\right) \\ &= \frac{4}{\pi^2\phi(q)}\, X\log\log X + O(X). \end{aligned}$$

Finally, using the estimates for $S(1,X)$ and $S(\psi,X)$ for $\psi \ne 1$ one concludes that

$$\begin{aligned} \sum_{n\in S(X,h)} \omega_{a,q}(n) &= \frac{1}{4}\Big(S(1,X) + \sum_{\substack{\psi \pmod 8\\ \psi\ne 1}} \overline{\psi(h)} S(\psi,X)\Big) \\ &= \frac{X\log\log X}{\pi^2\phi(q)} + O(X). \end{aligned}$$

Since

$$\begin{aligned}\#S(X,h) &= \sum_{\substack{n\le X\\ n\equiv h \pmod 8}} \mu^2(n) = \frac{1}{4}\sum_{\psi \pmod 8} \overline{\psi(h)} \sum_{n\le X} \mu^2(n)\psi(n)\\ &= \frac{1}{4}\sum_{\substack{n\le X\\ \gcd(n,2)=1}} \mu^2(n) + \frac{1}{4}\sum_{\substack{\psi \pmod 8\\ \psi\neq 1}} \overline{\psi(h)} \sum_{n\le X} \mu^2(n)\psi(n)\\ &= \frac{1}{4}\left(\frac{6}{\pi^2}X\frac{1}{1+2^{-1}} + O(X^{1/2})\right) + O\big(X\exp\big(-\eta\sqrt{\log X}\big)\big)\\ &= \frac{X}{\pi^2} + O\big(X\exp\big(-\eta\sqrt{\log X}\big)\big),\end{aligned}$$

one immediately has

$$\sum_{n\in S(X,h)} \omega_{a,q}(n) = \#S(X,h)\left(\frac{\log\log X}{\phi(q)}\right) + O(X).$$

This completes the proof of Lemma 14. □

Noticing that $\phi(8) = 4$, one has

$$\sum_{n\in S(X,h)} \omega_{a,8}(n) = \#S(X,h)\left(\frac{\log\log X}{4}\right) + O(X).$$

for any $a = 1, 3, 5, 7$. Since $s(n, \hat{\phi}_i)$ is a sum of two distinct functions $w_{a,8}$ plus a bounded constant, this establishes formula (9) for the case $k = 1$. We remark that in verifying the six conditions in the generalized Erdös–Kac Theorem we also need the above estimates.

Lemma 15. *Let the function $f : \mathbb{N} \to \mathbb{N}$ be defined as*

$$f = h_i = \begin{cases} \omega_{3,8} + \omega_{7,8} & \text{for } i = 1,\\ \omega_{3,8} + \omega_{5,8} & \text{for } i = 2, 3.\end{cases}$$

Then for any positive integer k and $h = 1, 3, 5, 7$, one has

$$\sum_{n\in S(X,h)} f(n)^k = \#S(X,h)\left(\frac{\log\log X}{2}\right)^k + O_k\big(X\,(\log\log X)^{k-1}\big)$$

as $X \to \infty$.

Proof. For $k = 1$, this is established in Lemma 14. For $k \geq 2$, we recall the following high-power analogues of the Turán–Kubilius inequalities (see [12] or [22]),

$$\frac{1}{X}\sum_{n\leq X}|f(n)-A(X)|^k \ll B(X)^k + \sum_{p^m\leq X}\frac{|f(p^m)|^k}{p^m},$$

where

$$A(X) = B^2(X) = \sum_{p^m\leq X}\frac{f(p^m)}{p^m} = \frac{\log\log X}{2} + O(1),$$

by Merten's estimate. For $k \geq 2$ one has

$$\begin{aligned}\sum_{n\leq X}\left|f(n)-\frac{\log\log X}{2}\right|^k &\ll_k \sum_{n\leq X}|f(n)-A(X)|^k + \sum_{n\leq X}\left|A(X)-\frac{\log\log X}{2}\right|^k\\ &\ll_k XB(X)^k + X \ll_k X(\log\log X)^{k/2}.\end{aligned}$$

Therefore

$$\begin{aligned}&\sum_{n\in S(X,h)} f(n)^k\\ &= \sum_{n\in S(X,h)}\left(f(n)-\frac{\log\log X}{2}+\frac{\log\log X}{2}\right)^k\\ &= \left(\frac{\log\log X}{2}\right)^k \#S(X,h) + k\left(\frac{\log\log X}{2}\right)^{k-1}\sum_{n\in S(X,h)}\left(f(n)-\frac{\log\log X}{2}\right)\\ &\quad + O_k\left(\max_{0\leq r\leq k-2}\left\{(\log\log X)^r\sum_{n\in S(X,h)}\left|f(n)-\frac{\log\log X}{2}\right|^{k-r}\right\}\right).\end{aligned}$$

The second term is

$$O_k\big(X(\log\log X)^{k-1}\big)$$

by Lemma 14, while for any $0 \leq r \leq k-2$, one has

$$\begin{aligned}(\log\log X)^r\sum_{n\in S(X,h)}\left|f(n)-\frac{\log\log X}{2}\right|^{k-r} &\ll_k (\log\log X)^r\, X\,(\log\log X)^{(k-r)/2}\\ &\leq X\,(\log\log X)^{k-1}.\end{aligned}$$

Putting these two error terms together we complete the proof of Lemma 15.

Noticing that

$$\sum_{n\in S(X,h)} s(n,\hat{\phi}_i)^k = \sum_{n\in S(X,h)}\big(f(n)+s(n,\phi)+c_{i,n}\big)^k,$$

$|c_{i,n}| \leq 3$ and recalling the asymptotic formula (6), one obtains the asymptotic formula (9), as $X \to \infty$. □

References

[1] N. Aoki, On the 2-Selmer groups of elliptic curves arising from the congruent number problems. *Comment. Math. Univ. St. Paul.* **48** (1999), 77–101. Zbl 0934.11030 MR 1684768

[2] N. Aoki, On the Tate-Shafarevich group of semistable elliptic curves with a rational 3-torsion. *Acta Arith.* **112** (3) (2004), 209–227. Zbl 1083.11035 MR 2046181

[3] D. Atake, On elliptic curves with large Tate-Shafarevich groups. *J. Number Theory.* **87** (2001), 282–300. Zbl 1014.11039 MR 1824149

[4] R. Alter, T. B. Curtz, K. K. Kubota, Remarks and results on congruent numbers. In *Proc. Third Southeastern Conf. on Combinatorics*, Graph Theory and Computing 1972, 27–35. Zbl 0326.10014 MR 0349554

[5] R. Alter, The congruent number problem. *Amer. Math. Monthly* **87** (1980), 43–45. Zbl 0422.10009 MR 1539253

[6] R. Bölling, Die Ordnung der Schafarewitsch-Tate-Gruppe kann beliebig groß werden. *Math. Nachr.* **67** (1975), 157–179. Zbl 0314.14008 MR 0384812

[7] J. W. S. Cassels, Arithmetic on curves of genus 1. VI. The Tate-Shafarevich group can be arbitrarily large. *J. Reine Angew. Math.* **214** (1963), 65–70. Zbl 0236.14012 MR 0162800

[8] J. Chahal, Congruent numbers and elliptic curves. *Amer. Math. Monthly* **113** (4) (2006), 308–317. Zbl 1099.11030 MR 2211757

[9] C. Delaunay, Heuristics on Tate-Shafarevitch groups of elliptic curves defined over $\mathbb{Q}$. *Experiment. Math.* **10** (2) (2001), 191-–196. Zbl 1045.11038 MR 1837670

[10] C. Delaunay, Moments of the orders of Tate-Shafarevich groups. *Int. J. Number Theory* **1** (2) (2005), 243–264. Zbl 1082.11042 MR 2173383

[11] N. Elkies, Curves $Dy^2 = x^3 - x$ of odd analytic rank. In *Algorithmic number theory* (Sydney, 2002), Lecture Notes in Comput. Sci. 2369, Springer-Verlag, Berlin 2002, 244–251. Zbl 1058.11034 MR 2041088

[12] P. D. T. A. Elliott, High-power analogues of the Turán-Kubilius inequality, and an application to number theory. *Canad. J. Math.* **32** (4) (1980), 893–907. Zbl MR 0590654

[13] K. Feng, Non-congruent numbers, odd graph and BSD conjecture on $y^2 = x^3 - n^2x$. *Acta. Arith.* **75** (1996), 71–83. Zbl 0838.11039 MR 1379391

[14] K. Feng and M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero. *J. Number Theory* **109** (1) (2004), 1–26. Zbl 1076.11036 MR 2098473

[15] K. Feng, Y. Xue, New series of odd non-congruent numbers. *Sci. China Ser. A* **49** (11) (2006), 1642–1654.. Zbl 1118.11029 MR 2288221

[16] Genocchi, Sur l'impossibilité de quelques égalités doubles. *C. R. Acad. Sci. Paris* **78** (1874), 423–436. JFM 06.0112.03

[17] D. Goldfeld, D. Lieman, Effective bounds on the size of the Tate-Shafarevich group. *Math. Res. Lett.* **3** (3) (1996), 309–318. Zbl 0869.11053 MR 1397680

[18] D. Goldfeld, L. Szpiro, Bounds for the order of the Tate-Shafarevich group. *Compositio Math.* **97** (1–2) (1995), 71–87. Zbl 0860.11032 MR 1355118

[19] J. M. Harris, J. L. Hirst, M. J. Mossinghoff, *Combinatorics and graph theory.* Undergrad. Texts Math., Springer-Verlag, New York 2000. Zbl 0949.05001 MR 1770510

[20] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, I. *Invent. Math.* **111** (1993), 171–195. Zbl 0808.11041 MR 1193603

[21] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, II. *Invent. Math.* **118** (1994), 331–370. Zbl 0815.11032 MR 1292115

[22] A. Hildebrand, Sur les moments d'une fonction additive. *Ann. Inst. Fourier Grenoble* **33** (3) (1983), 1–22. Zbl 0486.10043 MR 0723945

[23] B. Iskra, Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. *Proc. Japan Acad. Ser. A* **72** (1996), 168–169. Zbl 0877.11014 MR 1420609

[24] R. Kloosterman, The p-part of the Tate-Shafarevich groups of elliptic curves can be arbitrarily large. *J. Théor. Nombres Bordeaux* **17** (3) (2005), 787–800. Zbl 05016588 MR 2212126

[25] N. Koblitz, *Introduction to elliptic curves and modular forms.* Grad. Texts in Math. 97, 2nd ed., Springer-Verlag, New York 1993. Zbl 0804.11039 MR 1216136

[26] K. Kramer, A family of semistable elliptic curves with large Tate-Shafarevitch groups. *Proc. Amer. Math. Soc.* **89** (1983), 379–386. Zbl 0567.14018 MR 0715850

[27] J. Langrange, *Nombres congruents et courbes elliptiques*. Sémin. Delange-Pisot-Poitou, 1974/75, Fasc. 1, Exposé 16. Zbl 0328.10013 MR 0398973

[28] F. Lemmermeyer, On Tate-Shafarevich groups of some elliptic curves. In *Algebraic number theory and Diophantine analysis* (Graz, 1998), Walter de Gruyter, Berlin 2000, 277–291. Zbl 0973.11061 MR 1770467

[29] F. Lemmermeyer, Some families of non-congruent numbers. *Acta. Arith.* **110** (2003), 15–36. Zbl 1047.11055 MR 2007541

[30] F. Lemmermeyer, R. Mollin, On Tate-Shafarevich groups of $y^2 = x(x^2 - k^2)$. *Acta Math. Univ. Comenian.* (*N.S.*) **72** (2003), no. 1, 73–80. Zbl 1097.11012 MR 2020580

[31] Y.-R. Liu, Prime analogues of the Erdös-Kac theorem for elliptic curves. *J. Number Theory* **119** (2) (2006), 155–170. Zbl 1120.11042 MR 2250042

[32] F. R. Nemenzo, All congruent numbers less than 40000. *Proc. Japan Acad. Ser. A* **74** (1998), 29–31. Zbl 0922.11023 MR 1617754

[33] K. Ono, Tate-Shafarevich groups of the congruent number elliptic curves. *Acta Arith.* **81** (3) (1997), 247–252. Zbl 0886.11038 MR 1460580

[34] N. Rogers, Rank computations for the congruent number elliptic curves. *Experiment. Math.* **9** (4) (2000), 591–594. Zbl 1050.11061 MR 1806294

[35] P. Serf, Congruent numbers and elliptic curves. In *Computational Number Theory* (Debrecen, 1989), Walter de Gruyter, Berlin 1991, 227–238. Zbl 0736.11017 MR 1151867

[36] J. H. Silverman, *The arithmetic of elliptic curves.* Grad. Texts in Math. 106, Springer-Verlag, 1986. Zbl 0585.14026 MR 0817210

[37] N. M. Stephens, Congruence properties of congruent numbers. *Bull. London Math. Soc.* **7** (1975), 182–184. Zbl 0304.10011 MR 0379355

[38] J. B. Tunnell, A classical diophantine problem and modular forms of weight 3/2. *Invent. Math.* **72** (1983), 323–334. Zbl 0515.10013 MR 0700775

[39] G. Yu, Rank 0 quadratic twists of a family of elliptic curves. *Compositio Math.* **135** (3) (2003), 331–356. Zbl 1090.11038 MR 1956817

[40] G. Yu, Average size of 2-Selmer groups of a family of elliptic curves. I. *Trans. Amer. Math. Soc.* **358** (4) (2006), 1563–1584. Zbl 1113.11034 MR 2186986

[41] G. Yu Average size of 2-Selmer groups of elliptic curves. II. *Acta. Arith.* **117** (1) (2005), 1–33. Zbl 02169956 MR 2110501

[42] C. Zhao, A criterion for elliptic curves with lowest 2-power in L(1). *Math. Proc. Cambridge Philos. Soc.* **121** (1997), 385–400. Zbl 1042.11038 MR 1434649

[43] C. Zhao, A criterion for elliptic curves with lowest 2-power in L(1) II. *Acta. Math. Sinica* (*English series*) **21** (2005), 961–976. Zbl 1122.11041 MR 2176306

Received January 25, 2007

Maosheng Xiong, Department of Mathematics, Eberly College of Science, Pennsylvania State University, University Park, State College, PA 16802, U.S.A.

E-mail: xiong@math.psu.edu

Alexandru Zaharescu, Department of Mathematics, University of Illinois at Urbana-Champaign, 273 Altgeld Hall, MC-382, 1409 W. Green Street, Urbana, Illinois 61801-2975, U.S.A.

E-mail: zaharesc@math.uiuc.edu