J. Ramanujan Math. Soc. **29**, No.1 (2014) 75–92

Partitions of graphs and Selmer groups of elliptic curves of Neumann-Setzer type

Tomasz Jędrzejak[1] and Małgorzata Wieczorek[2]

University of Szczecin, Institute of Mathematics, Wielkopolska 15, 70-451 Szczecin, Poland
e-mail: tjedrzejak@gmail.com; wieczorek@wmf.univ.szczecin.pl

Communicated by: R. Sujatha

Received: November 16, 2013

Abstract. We consider the elliptic curves $E^u : y^2 = x^3 + ux^2 - 16x$ and their quadratic twists E_n^u by a squarefree integer n, where $u^2 + 64 = p_1 \dots p_l$, (p_i are primes). When $l \le 2$, $n \equiv 1 \pmod 4$ and all prime divisors of n are congruent to 3 modulo 4 we give a complete description of sizes of Selmer groups of E_n^u in terms of number of even partitions of some graphs. If n is even or $l > 2$, we give some conditions for twists of rank zero. We deduce also that E_n^u has rank zero for a positive proportion of squarefree integers n with a fixed number of prime divisors.

2000 *Mathematics Subject Classification.* 11G05, 14H52, 11R42, 94C15.

1. Introduction

Let p be a prime $\neq 2, 3, 17$. Then there is an elliptic curve of conductor p defined over $\mathbb{Q}$ with a rational 2-division point if and only if $p = u^2 + 64$ for some integer u. If p is of the form $u^2 + 64$, there are, up to isomorphism, just two such curves (connected by a 2-isogeny): $y^2 = x^3 + ux^2 - 16x$ and $y^2 = x^3 - 2ux^2 + px$, where the sign of u is chosen so that $u \equiv 1 \pmod 4$. There are the so-called *Neumann-Setzer elliptic curves*, studied in [15], [16].

Dąbrowski [2] studied quadratic twists by primes of generalized Neumann-Setzer curves $E^u : y^2 = x^3 + ux^2 - 16x$, where $u^2 + 64$ is a prime or a product of two primes. By a famous result of Iwaniec [12], there are infinitely many integers u such that $u^2 + 64$ is the product of at most two primes.

In this article we study quadratic twists E_n^u of E^u by square-free integers n. We extend the ideas of Feng and others ([4], [5], [6], [7]) to calculate the Selmer groups of E_n^u using graph theory. They consider the elliptic curves $y^2 = x^3 - n^2x$ associated with congruent numbers and are especially interested in rank zero curves (i.e., when n is a non-congruent number). Goto [10] consider the curves $y^2 = x(x+3n)(x-n)$ and uses similar method for description of non $\pi/3$-congruent numbers. In [9] he also considers elliptic curves connected with other θ-congruent numbers. Li and Qiu [14] used graph theory to calculate the Selmer groups of quadratic twists of $E_{\varepsilon p,\varepsilon q} : y^2 = x(x+\varepsilon p)(x+\varepsilon q)$ where $\varepsilon = \pm 1$ and p, q are odd primes satisfying $q - p = 2^m$ $(m \geq 1)$. Note that in [3] the second author considers quadratic twists of the family $y^2 = x(x+p)(x-2^m)$ without using graphs. It seems that the articles cited above are the only ones where the authors use graph theory to calculate Selmer groups.

The case when the quadratic twists of some elliptic curve have rank zero is particularly interesting. This is because it is believed [8] that a positive proportion of quadratic twists have rank zero. There have been numerous papers treating this problem. Most of them focus on the nonvanishing of the L-functions but there is also another approach via the descent method. For example, Yu [18] proved that a positive proportion of quadratic twists of elliptic curves with 2-torsion $(\mathbb{Z}/2\mathbb{Z})^2$ have rank 0. Dąbrowski [2] proved that for any positive integer k there are k pairwise non-isogenous curves $E_1, \ldots, E_k$ such that rank $(E_i^{(p)}(\mathbb{Q})) = 0$ $(1 \leq i \leq k)$ for a positive proportion of primes p. The first author showed in [13] that quadratic twists of the Fermat elliptic curve $E_2 : x^3 + y^3 = 2$ (note that $E_2[2](\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$) have rank zero for a positive proportion of squarefree integers with a fixed number of prime divisors. He also investigated rank zero cubic twists of this curve and proved a similar result.

In this paper we give a complete description of sizes of Selmer groups of E_n^u in terms of numbers of even partitions of some graphs when $u^2 + 64 = p$ or p_1p_2, and $n = \pm q_1 \ldots q_k \equiv 1 (\mathrm{mod}\ 4)$ with all primes $q_i \equiv 3 (\mathrm{mod}\ 4)$ (Theorems 1 and 2). We also give conditions (in terms of the values of Legende's symbols) to rank $(E_n^u(\mathbb{Q}))$ equals 0 or (conjecturally) 1 (Corollaries 1, 3, 4 and 6). As a consequence, we deduce that E_n^u has rank zero for a positive proportion of squarefree integers n with a fixed number of prime divisors (Propositions 2 and 4). When n is even, we (avoid using graphs) only focus on rank zero twists and show similar density result (Propositions 5 and 6, and Corollary 8). Similarly, when $u^2 + 64 = p_1 \ldots p_l$ with $l > 2$, we will give conditions for rank zero twists without using graph theory (Proposition 7).

2. Preliminaries

2.1 2-descent method

The 2-descent method is described in Silverman book [17, Chap. 10, Section 4]. In this paper we consider a special case for the quadratic twists E_n^u of E^u. Note that $E_n^u : y^2 = x^3 + unx^2 - 16n^2x$ where $u^2 + 64 = p_1 \dots p_l$ and $n = \pm q_1 \dots q_k$ or $n = \pm 2 \cdot q_1 \dots q_k$ (n squarefree integer) and $u \equiv 1 (\mathrm{mod}\ 4)$. We will assume furthermore that $\gcd(u, n) = 1$ and $\gcd(u^2 + 64, n) = 1$. The curve E_n^u has bad reduction at primes dividing $n(u^2 + 64)$. Moreover, the reduction at 2 is good if and only if $n \equiv 1 (\mathrm{mod}\ 4)$. Let S denote the finite set consisting of ∞ and primes of bad reduction of E_n^u, and let M denote the subgroup of $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $S \backslash \{\infty\}$ and -1, i.e.

$$S = \{\infty, 2^\epsilon, p_1, \dots, p_l, q_1, \dots, q_k\}$$

$$M = \langle -1, 2^\epsilon, p_1, \dots, p_l, q_1, \dots, q_k \rangle \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2,$$

where $\epsilon = 0$ for $n \equiv 1 (\mathrm{mod}\ 4)$ and $\epsilon = 1$ for $n \equiv 2, 3 (\mathrm{mod}\ 4)$.

There exists an isogeny ϕ of degree 2 from E_n^u to $E_n'^u : y^2 = x^3 - 2unx^2 + n^2(u^2 + 64)x$. Let S_n^ϕ and $S_n^{\phi'}$ denote the Selmer groups corresponding to ϕ and its dual, respectively. Then we can identify the Selmer groups S_n^ϕ and $S_n^{\phi'}$ with some subgroups of M as follows:

$$S_n^\phi = \{d \in M : C_d(\mathbb{Q}_v) \neq \emptyset \quad \text{for all} \quad v \in S\},$$

$$S_n^{\phi'} = \{d \in M : C_d'(\mathbb{Q}_v) \neq \emptyset \quad \text{for all} \quad v \in S\},$$

where

$$C_d : dy^2 = d^2 - 2dunx^2 + n^2(u^2 + 64)x^4,$$

$$C_d' : dy^2 = d^2 + 4dunx^2 - (16n)^2x^4.$$

We define

$$rs(E_n^u/\mathbb{Q}) := \dim_{\mathbb{F}_2} S_n^\phi + \dim_{\mathbb{F}_2} S_n^{\phi'} - 2.$$

The number $rs(E_n^u/\mathbb{Q})$ we call the Selmer rank of $E_n^u/\mathbb{Q}$. Clearly, $\mathrm{rank}\,(E_n^u/\mathbb{Q}) \leq rs(E_n^u/\mathbb{Q})$.

Lemma 1. *Under the above assumptions we have*

1) $C_d(\mathbb{R}) \neq \emptyset \Longleftrightarrow d > 0$;

1′) $C_d'(\mathbb{R}) \neq \emptyset$;

2) $C_d(\mathbb{Q}_{p_j}) \neq \emptyset$;

2′) $C_d'(\mathbb{Q}_{p_j}) = \emptyset \Longleftrightarrow \left(\frac{d}{p_j}\right) \neq 1$;

3) $\left(q_i \equiv 3 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = -1\right) \Longrightarrow (C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow q_i \mid d)$;

3′) $\left(q_i \equiv 3 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = -1\right) \Longrightarrow (C'_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow q_i \mid d)$;

4) $\left(q_i \equiv 3 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1\right) \Longrightarrow \left(C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\frac{d}{q_i}\right) \neq 1\right)$;

4′) $\left(q_i \equiv 3 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1\right) \Longrightarrow C'_d(\mathbb{Q}_{q_i}) \neq \emptyset$;

5) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = -1\right) \Longrightarrow C_d(\mathbb{Q}_{q_i}) \neq \emptyset$;

5′) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = -1\right) \Longrightarrow \left(C'_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\frac{d}{q_i}\right) \neq 1\right)$;

6) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1 \textit{ and } \left(\frac{n/q_i(u+8\sqrt{-1})}{q_i}\right) = 1\right)$
$\Longrightarrow \left(C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\left(\frac{d}{q_i}\right) \neq 1 \textit{ and } \left(q_i \nmid d \textit{ or } \left(\frac{d/q_i}{q_i}\right) \neq 1\right)\right)\right)$;

6′) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1 \textit{ and } \left(\frac{n/q_i(u+8\sqrt{-1})}{q_i}\right) = 1\right)$
$\Longrightarrow \left(C'_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\left(\frac{d}{q_i}\right) \neq 1 \textit{ and } \left(q_i \nmid d \textit{ or } \left(\frac{d/q_i}{q_i}\right) \neq 1\right)\right)\right)$;

7) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1 \textit{ and } \left(\frac{n/q_i(u+8\sqrt{-1})}{q_i}\right) = -1\right)$
$\Longrightarrow \left(C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\left(\frac{d}{q_i}\right) \neq 1 \textit{ and } \left(q_i \nmid d \textit{ or } \left(\frac{d/q_i}{q_i}\right) \neq -1\right)\right)\right)$;

7′) $\left(q_i \equiv 1 (\mathrm{mod}\ 4) \textit{ and } \left(\frac{u^2+64}{q_i}\right) = 1 \textit{ and } \left(\frac{n/q_i(u+8\sqrt{-1})}{q_i}\right) = -1\right)$
$\Longrightarrow \left(C'_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\left(\frac{d}{q_i}\right) \neq 1 \textit{ and } \left(q_i \nmid d \textit{ or } \left(\frac{d/q_i}{q_i}\right) \neq -1\right)\right)\right)$;

8) $nu \equiv 1 (\mathrm{mod}\ 4) \Longrightarrow (C_d(\mathbb{Q}_2) = \emptyset \Longleftrightarrow d \not\equiv 5 (\mathrm{mod}\ 8))$;

8′) $nu \equiv 1 (\mathrm{mod}\ 4) \Longrightarrow (C'_d(\mathbb{Q}_2) = \emptyset \Longleftrightarrow d \not\equiv 5, 7 (\mathrm{mod}\ 8))$;

9) $nu \equiv 3 (\mathrm{mod}\ 4) \Longrightarrow C_d(\mathbb{Q}_2) \neq \emptyset$;

9′) $nu \equiv 3 (\mathrm{mod}\ 4) \Longrightarrow (C_d(\mathbb{Q}_2) = \emptyset \Longleftrightarrow d \not\equiv 1 (\mathrm{mod}\ 8))$;

10) $nu \equiv 2 (\mathrm{mod}\ 16) \Longrightarrow \big(C_d(\mathbb{Q}_2) = \emptyset$
$\Longleftrightarrow \left(2 \nmid d \textit{ or } \frac{d}{2} \not\equiv 1 (\mathrm{mod}\ 8)\right) \textit{ and } d \not\equiv 1 (\mathrm{mod}\ 8)\big)$;

10′) $nu \equiv 2 (\mathrm{mod}\ 16) \Longrightarrow \big(C'_d(\mathbb{Q}_2) = \emptyset$
$\Longleftrightarrow \left(2 \nmid d \textit{ or } \frac{d}{2} \not\equiv 1, 7 (\mathrm{mod}\ 8)\right) \textit{ and } d \not\equiv 1, 7 (\mathrm{mod}\ 8)\big)$;

11) $nu \equiv 10 (\mathrm{mod}\ 16) \Longrightarrow \big(C_d(\mathbb{Q}_2) = \emptyset$
$\Longleftrightarrow \left(2 \nmid d \textit{ or } \frac{d}{2} \not\equiv 5 (\mathrm{mod}\ 8)\right) \textit{ and } d \not\equiv 1 (\mathrm{mod}\ 8)\big)$;

11′) $nu \equiv 10 (\mathrm{mod}\ 16) \Longrightarrow \big(C'_d(\mathbb{Q}_2) = \emptyset$
$\Longleftrightarrow \left(2 \nmid d \textit{ or } \frac{d}{2} \not\equiv 3, 5 (\mathrm{mod}\ 8)\right) \textit{ and } d \not\equiv 1, 7 (\mathrm{mod}\ 8)\big)$;

12) $nu \equiv 6 (\mathrm{mod}\ 8) \Longrightarrow (C_d(\mathbb{Q}_2) = \emptyset \Longleftrightarrow d \not\equiv 1 (\mathrm{mod}\ 8))$;

12′) $nu \equiv 6 (\mathrm{mod}\ 8) \Longrightarrow C'_d(\mathbb{Q}_2) \neq \emptyset$.

Proof. Follows from Goto thesis [9, Prop. 7.1, 7.3, 7.5, 7.7.]. □

2.2 Graphs and their partitions

This subsection contains necessary terminology of graph theory. Let G be a simple nondirected graph with vertex set $V(G) = \{v_1, \dots, v_t\}$ and edge set $E(G)$.

Definition 1. *A* partition *of a vertex set V is a pair $\{V_1, V_2\}$ such that $V_1 \cup V_2 = V$ and $V_1 \cap V_2 = \emptyset$. The partition $\{\emptyset, V\}$ is called* trivial.

Definition 2. *For $v \in V_1$ we denote by $\#\{v \to V_2\}$ the number of vertices in V_1 adjacent to v. A partition $\{V_1, V_2\}$ of V is called* odd, *if there exists $v \in V_1$ such that $\#\{v \to V_2\}$ is odd or there exists $v \in V_2$ such that $\#\{v \to V_1\}$ is odd. Otherwise, a partition $\{V_1, V_2\}$ is called* even.

Note that trivial partitions are even.

Definition 3. *We say that a graph G is* odd *if any nontrivial partition is odd, otherwise, we call G an* even *graph. We say that a graph G is* semi-odd *if there exists only one nontrivial even partition.*

3. Main results and their proofs

In this section we assume that $u^2 + 64 = p$ or $p_1 p_2$ with $u \equiv 1 (\mathrm{mod}\ 4)$. We will consider both cases separately. We will study the quadratic twists of $E^u : y^2 = x^3 + ux^2 - 16x$ by integers $n \equiv 1 (\mathrm{mod}\ 4)$. We will give a full description of the size of the corresponding Selmer groups in terms of numbers of even paritItions of some graphs.

3.1 The case $u^2 + 64 = p$

Suppose that $u^2 + 64 = p$ and $n = \pm q_1 \dots q_k \equiv 1 (\mathrm{mod}\ 4)$, where, for all $1 \le i \le k$, primes $q_i \equiv 3 (\mathrm{mod}\ 4)$ and $\gcd(q_i, up) = 1$. Note that necessarily $p \equiv 1 (\mathrm{mod}\ 8)$.

Definition 4. *We define the nondirected graph $G_1(n)$ as follows. The vertex set $V(G_1(n)) := \{p, q_1, \dots, q_k\}$ and the edge set $E(G_1(n)) := \{\overline{pq_i} : \left(\frac{p}{q_i}\right) = -1, i = 1, \dots, k\}$.*

Proposition 1. *Under the above assumptions we have*

i) $S_n^{\phi} = \langle p \rangle$, $\langle -1 \rangle \subset S_n^{\phi'}$,

ii) *if $\{V_1, V_2\}$ is a nontrivial even partition of $G_1(n)$, then $\prod_{q \in V_j} q \in S_n^{\phi'}$, where $p \notin V_j$ ($j = 1$ or 2),*

iii) *if* $q_{i_1}\dots q_{i_s} \in S_n^{\phi'}$ $(1 \le s \le k)$, *then* $\{\{q_{i_1},\dots,q_{i_s}\}, V(G_1(n))\setminus \{q_{i_1},\dots,q_{i_s}\}\}$ *is nontrivial even partition,*

iv) $|S_n^{\phi'}| = 2\times$ *number of even partitions of the graph* $G_1(n)$.

Proof.

i) By Lemma 1, we have $S_n^{\phi} \subset \langle p, q_1, \dots, q_k\rangle$ and $S_n^{\phi'} \subset \langle -1, q_1, \dots, q_k\rangle$ (note that in this case E_n^u has good reduction at 2). Moreover, if q_i divides d then $C_d(\mathbb{Q}_{q_i}) = \emptyset$ $(i = 1,\dots,k)$. Hence $S_n^{\phi} \subset \langle p\rangle$. Again, by Lemma 1, we get $C_d(\mathbb{Q}_p) \ne \emptyset$, $C_d(\mathbb{R}) \ne \emptyset$ and $C_d(\mathbb{Q}_{q_i}) \ne \emptyset$ for $1 \le i \le k$. Therefore $S_n^{\phi} = \langle p\rangle$. Also by Lemma 1, we obtain $C'_{-1}(K) \ne \emptyset$ for $K = \mathbb{Q}_v$ where $v = p, q_1, \dots, q_k$ and ∞. Hence $-1 \in S_n^{\phi'}$.

ii) Let $\{V_1, V_2\}$ be a nontrivial even partition of $G_1(n)$. Without loss of generality we may assume that $V_1 = \{q_1,\dots,q_s\}$ and $V_2 = \{p, q_{s+1},\dots,q_k\}$ for some $1 \le s \le k$. Let r denote the product $\prod_{q\in V_1} q$. We will show that $\left(\frac{p}{q}\right) = 1$ for all $q \in V_1$. Suppose, on the contrary, that (without loss of generality) $\left(\frac{p}{q_1}\right) = -1$. Then the number of edges $\#\{q_1 \to V_2\}$ equals 1, which contradicts the parity of partition $\{V_1, V_2\}$. Hence by Lemma 1, $C'_r(\mathbb{Q}_v) \ne \emptyset$ for $v = p, q_1, \dots, q_k$ and ∞. Consequently $r \in S_n^{\phi'}$.

iii) Without loss of generality we assume that $r := q_1 \dots q_s \in S_n^{\phi'}$. Let $V_1 := \{q_1,\dots,q_s\}$ and $V_2 := \{p, q_{s+1},\dots,q_k\}$. We explain, that $\{V_1, V_2\}$ is even partition of $G_1(n)$. Let $q \in V_1$. Then we have $\#\{q \to V_2\} = \#\{q \to p\} = 0$ if $\left(\frac{p}{q}\right) = 1$ and $\#\{q \to V_2\} = \#\{q \to p\} = 1$ if $\left(\frac{p}{q}\right) = -1$. But if $\left(\frac{p}{q}\right) = -1$ then by Lemma 1, $C'_r(\mathbb{Q}_q) = \emptyset$ because $q \mid r$, contrary to the assumption. Hence the number $\#\{q \to V_2\}$ is even. Now, let v be any element of V_2. If $v \ne p$ then of course $\#\{v \to V_1\} = 0$. We have shown above that $\left(\frac{p}{q}\right) = 1$ for all $q \in V_1$, hence also $\#\{p \to V_1\} = 0$, and the assertion iii) follows.

iv) By parts ii) and iii) there is one-to-one correspondence between even partitions of $G_1(n)$ and positive elements in $S_n^{\phi'}$ (note that trivial partition corresponds to $1 \in S_n^{\phi'}$). Since $-1 \in S_n^{\phi'}$, we have $g \in S_n^{\phi'}$ if and only if $-g \in S_n^{\phi'}$. And we are done.

□

Theorem 1. *Under the above assumptions,* $2^{rs(E_n^u/\mathbb{Q})}$ *equals the number of even partitions of the graph* $G_1(n)$. *In particular,* $\operatorname{rank}(E_n^u/\mathbb{Q}) = rs(E_n^u/\mathbb{Q}) = 0$ *if and only if* $G_1(n)$ *is odd. Moreover,* $rs(E_n^u/\mathbb{Q})$ *is maximal (equals* k*) if and only if* $E(G_1(n)) = \emptyset$.

Proof. Let 2^e denote the number of even partitions of the graph $G_1(n)$ (this number is indeed a power of 2, see for example [7, p. 5, Lemma 2.2]). By Proposition 1, we get

$$2^{rs(E_n^u/\mathbb{Q})} = 2^{\dim_{\mathbb{F}_2} S_n^{\phi} + \dim_{\mathbb{F}_2} S_n^{\phi'} - 2} = 2^{1+(e+1)-2} = 2^e.$$

Hence $rs(E_n^u/\mathbb{Q}) = 0$ if and only if $2^e = 1$, i.e. by definition, that $G_1(n)$ is odd. Similarly, $E(G_1(n)) = \emptyset$ if and only if any partition of $G_1(n)$ is even, that is $2^e = 2^{\#V(G_1(n))-1} = 2^k$, and the assertion follows. □

Corollary 1. *Assume that* $n = \pm q_1 \dots q_k \equiv 1 \pmod 4$, *where primes* $q_i \equiv 3 \pmod 4$, $\left(\frac{q_i}{p}\right) = -1$ *and* $q_i \nmid u$ *for all* $1 \le i \le k$. *Then* $\operatorname{rank}(E_n^u/\mathbb{Q}) = 0$.

Proof. It is enough to show that the graph $G_1(n)$ is odd. Suppose, by contradiction, that $\{V_1, V_2\}$ is even nontrivial partition of it. Let (without loss of generality) $p \in V_2$ and let q be some element of V_1. Then $\#\{q \to V_2\} = \#\{q \to p\}$ is even, which contradicts to $\left(\frac{p}{q}\right) = -1$. Using Theorem 1 yields the assertion. □

Corollary 2. *Assume that* $n = \pm q_1 \dots q_k \equiv 1 \pmod 4$, *where primes* $q_i \equiv 3 \pmod 4$, $q_i \nmid u$ *for all* $1 \le i \le k$, *and* $\exists_{i_0} \left(\frac{q_{i_0}}{p}\right) = 1$, *and* $\forall_{i \neq i_0} \left(\frac{q_i}{p}\right) = -1$. *Then* $rs(E_n^u/\mathbb{Q}) = 1$.

Proof. We will show that the graph $G_1(n)$ is semi-odd, i.e. it has only one nontrivial even partition. Assume without loss of generality that $i_0 = 1$. First, we show that the partition $\{V_1, V_2\}$, where $V_1 = \{q_1\}$ and $V_2 = \{p, q_2, \dots, q_k\}$, is even. Indeed, $\#\{q_1 \to V_2\} = \#\{q_1 \to p\} = 0$ because $\left(\frac{q_1}{p}\right) = 1$. Similarly, for any $v \in V_2$ we have $\#\{v \to V_1\} = \#\{v \to q_1\} = 0$. Now, we show that there are no other nontrivial even partition of $G_1(n)$. Suppose that the partition $\{V_1', V_2'\} \neq \{V_1, V_2\}$ is nontrivial. Without loss of generality let $q_1 \in V_1'$. We need to consider two cases: $p \in V_1'$ or $p \in V_2'$. In the first case, for $q \in V_2'$ we have $\#\{q \to V_1'\} = \#\{q \to p\} = 1$ because $\left(\frac{q}{p}\right) = -1$. Hence $\{V_1', V_2'\}$ is odd. In the second case, for $q \in V_1' \setminus \{q_1\}$ we get $\#\{q \to V_2'\} = \#\{q \to p\} = 1$. Thus again $\{V_1', V_2'\}$ is odd. Now, by Theorem 1, we obtain $2^{rs(E_n^u/\mathbb{Q})} = 2$, and we are done. □

Lemma 2. *Under the assumptions from Corollary 2, the global root number* $W(E_n^u)$ *of the L-function associated to* E_n^u *is equal to* -1.

Proof. It is well known (for example see [1]) that for any elliptic curve E over $\mathbb{Q}$ its global root number $W(E)$ is equal to $\prod_{l \le \infty} W_l(E)$ where the product is taken over all primes l and ∞, and $W_l := W_l(E) = \pm 1$ is the local root number. Moreover, $W_\infty = -1$, and if E has a good reduction at l then $W_l(E) = 1$. If E has bad reduction at l then W_l depends on the reduction type (see [1]). In our case we have $W(E_n^u) = W(E_n'^u) = -W_p\prod_{1\leq i\leq k} W_{q_i}$. The curve $E_n'^u$ has potential good reduction at q_i (i.e. additive reduction and $\mathrm{ord}_{q_i}(j_{E_n'^u}) \geq 0$). Hence $W_{q_i} = \left(\frac{-1}{q_i}\right) = -1$ if $q_i > 3$. If $3|n$ then from [11, Table 2], we get $W_3 = -1$. Hence always $\prod_{1\leq i\leq k} W_{q_i} = (-1)^k$. At the prime $p = u^2 + 64$, the curve $E_n'^u$ has multiplicative reduction. We must decide whether this reduction is split or nonsplit. To this aim we consider $a_p = p + 1 - \#E_n'^u(\mathbb{F}_p)$. Note that $E_n'^u$ over $\mathbb{F}_p$ has the equation $y^2 = x^3 - 2unx^2$. Therefore $E_n'^u(\mathbb{F}_p)$ contains points ∞, $(0,0)$ and $(2un, 0)$. Substituting $z := (y/x)^2$, we get $z^2 = x - 2un$. This equation has $p-3$ solutions in $\mathbb{F}_p\backslash\{0, 2un\}$ if $\left(\frac{-2un}{p}\right) = 1$, and $p-1$ solutions if $\left(\frac{-2un}{p}\right) = -1$. Note that $\left(\frac{-2un}{p}\right) = \left(\frac{\sqrt{-1}}{p}\right)\left(\frac{n}{p}\right) = (-1)^{k-1}$, because $p \equiv 1 (\mathrm{mod}\ 8)$. Since $E_n'^u$ has nonsplit multiplicative reduction (i.e. $a_p = -1$) if and only if $(-1)^{k-1} = -1$, we obtain $W_p = (-1)^k$. Hence $W(E_n^u) = -(-1)^k(-1)^k = -1$, and we are done. □

Corollary 3. *Assume the Parity Conjecture. Then under the assumptions from Corollary 2, we have* $\mathrm{rank}\,(E_n^u/\mathbb{Q}) = 1$.

Proof. By Corollary 2, $\mathrm{rank}\,(E_n^u/\mathbb{Q}) \leq 1$ and by Lemma 2, the global root number of the associated L-function is equal to -1. Therefore (under the Parity Conjecture) the rank is odd and we are done. □

For a positive integer k, let A_k^1 denote the set of odd squarefree (positive if k is even and negative if k is odd) integers n such that $\gcd(n, u) = \gcd(n, u^2 + 64) = 1$, and with exactly k prime factors.

Proposition 2. *The set* $\{n \in A_k^1 : \mathrm{rank}\,(E_n^u(\mathbb{Q})) = 0\}$ *has positive density in* A_k^1 *for all k. In particular, for infinitely many odd squarefree integers the quadratic twists of the curve* $y^2 = x^3 + ux^2 - 16x$ *(*$u^2 + 64$ *is prime) have rank 0.*

Proof. Let B_k denote the set of integers satisfying the assumptions from Corollary 1. Then $B_k \subset A_k^1$ and by this Corollary, $\mathrm{rank}\,(E_n^u(\mathbb{Q})) = 0$ for $n \in B_k$. By the Dirichlet Prime Number Theorem, the set B_k has positive density in A_k^1, and we are done. □

3.2 The case $u^2 + 64 = p_1p_2$

Now suppose that $u^2 + 64 = p_1p_2$ and $n = \pm q_1 \cdots q_k \equiv 1 (\mathrm{mod}\ 4)$, where primes $q_i \equiv 3 (\mathrm{mod}\ 4)$ for all $1 \leq i \leq k$. Note that necessarily $p_1p_2 \equiv 1 (\mathrm{mod}\ 8)$ and $p_1 \equiv p_2 \equiv 1 (\mathrm{mod}\ 4)$.

Definition 5. *We define the nondirected graph $G_2(n)$ as follows. The vertex set $V(G_2(n)) := \{p_1, p_2, q_1, \dots, q_k\}$ and the edge set $E(G_2(n)) := \{\overline{p_j q_i} : \left(\frac{p_j}{q_i}\right) = -1, i = 1, \dots, k, j = 1, 2\}$.*

Proposition 3. *Under the above assumptions we have*

i) $\langle p_1 p_2\rangle \subset S_n^{\phi} \subset \langle p_1, p_2\rangle$, $\langle -1\rangle \subset S_n^{\phi'}$,
ii) $S_n^{\phi} = \langle p_1, p_2\rangle$ *if and only if there exists an even partition* $\{V_1, V_2\}$ *of* $G_2(n)$ *such that* $p_1 \in V_1$ *and* $p_2 \in V_2$ *(or vice versa)*
iii) *if* $\{V_1, V_2\}$ *is an even partition of* $G_2(n)$ *such that* $p_1, p_2 \in V_1$ *or* $p_1, p_2 \in V_2$, *then* $\prod_{q\in V_j} q \in S_n^{\phi'}$, *where* p_1 *and* $p_2 \notin V_j$ *(*$j = 1$ *or* 2*),*
iv) *if* $q_{i_1} \cdots q_{i_s} \in S_n^{\phi'} (1 \le s \le k)$, *then* $\{\{q_{i_1}, \dots, q_{i_s}\}, V(G_2(n))\setminus \{q_{i_1}, \dots, q_{i_s}\}\}$ *is even partition (and clearly, satisfies property from iii),*
v) $|S_n^{\phi'}| = 2\times$ *number of even partitions* $\{V_1, V_2\}$ *of the graph* $G_2(n)$, *such that both* $p_1, p_2 \in V_1$ *or both* $p_1, p_2 \in V_2$.

Proof.

i) By Lemma 1, we have $S_n^{\phi} \subset \langle p_1, p_2, q_1, \dots, q_k\rangle$ and $S_n^{\phi'} \subset \langle -1, q_1, \dots, q_k\rangle$. Also by Lemma 1, we get $C_{p_1p_2}(\mathbb{Q}_v) \neq \emptyset$ for $v = p_1, p_2, q_1, \dots, q_k$ and ∞. Thus $p_1p_2 \in S_n^{\phi}$. On the other hand, $C_d(\mathbb{Q}_{q_i}) = \emptyset$ if q_i divides d. Hence $\langle p_1 p_2\rangle \subset S_n^{\phi} \subset \langle p_1, p_2\rangle$. Similarly, by Lemma 1, $C'_{-1}(\mathbb{Q}_v) \neq \emptyset$ for $v = p_1, p_2, q_1, \dots, q_k$ and ∞, and the assertion follows.

ii) Assume that $p_1, p_2 \in S_n^{\phi}$. Then, in particular, $C_{p_j}(\mathbb{Q}_{q_i}) \neq \emptyset$ for all $i = 1, \dots, k$ and $j = 1, 2$. Hence by Lemma 1, for any prime divisor q of n we have either $\left(\frac{p_1p_2}{q}\right) = -1$ or $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = 1$. We define the partition $\{V_1, V_2\}$ of $G_2(n)$ as follows: $V_1 := \{p_1\} \cup \left\{q : \left(\frac{p_2}{q}\right) = 1\right\}$ and $V_2 := \{p_2\} \cup \left\{q \notin V_1 : \left(\frac{p_1}{q}\right) = 1\right\}$. We claim that $\{V_1, V_2\}$ is an even partition. Indeed, simply $\#\{p_1 \to V_2\} = \#\left\{q \in V_2 : \left(\frac{p_1}{q}\right) = -1\right\} = 0$ and similarly $\#\{p_2 \to V_1\} = 0$. Let $q \in V_1$ and $q' \in V_2$. Then $\#\{q \to V_2\} = \#\{q \to p_2\} = 0$ and $\#\{q' \to V_1\} = \#\{q' \to p_1\} = 0$. Conversely, assume that we have an even partition $\{V_1, V_2\}$ of $G_2(n)$ such that $p_1 \in V_1$ and $p_2 \in V_2$. By part i), it suffices to prove that $p_1 \in S_n^{\phi}$. By Lemma 1, we just have $C_{p_1}(\mathbb{Q}_v) \neq \emptyset$ for $v = p_1, p_2$ and ∞. Let q' be any element of V_2. The number $\#\{q' \to V_1\} = \#\{q' \to p_1\}$ is even, hence equals 0, i.e. $\left(\frac{p_1}{q'}\right) = 1$. Similarly, $\#\{q \to V_2\} = 0$, that is $\left(\frac{p_2}{q}\right) = 1$ for any $q \in V_1$. Now take $i \in \{1, \dots, k\}$. If $\left(\frac{p_1p_2}{q_i}\right) = -1$, then by Lemma 1, $C_{p_1}(\mathbb{Q}_{q_i}) \neq \emptyset$ just because $q_i \nmid p_1$. If $\left(\frac{p_1p_2}{q_i}\right) = 1$ then by above, $\left(\frac{p_1}{q_i}\right) = 1$ (if $q_i \in V_2$) or $\left(\frac{p_2}{q_i}\right) = 1$ (if $q_i \in V_1$). Therefore $\left(\frac{p_1}{q_i}\right) = \left(\frac{p_2}{q_i}\right) = 1$, and by Lemma 1, $C_{p_1}(\mathbb{Q}_{q_i}) \neq \emptyset$ so $p_1 \in S_n^{\phi}$.

iii) Without loss of generality assume that $V_1 = \{q_1, \dots, q_s\}$ and $V_2 = \{p_1, p_2, q_{s+1}, \dots, q_k\}$ for some $s \in \{1, \dots, k\}$. Let $r := q_1, \dots, q_s$. Clearly, $C_r'(\mathbb{Q}_{q_i}) \neq \emptyset$ for $i = s+1, \dots, k$. Now let $i \leq s$. By assumption, the number $\#\{q_i \to V_2\} = \#\{q_i \to \{p_1, p_2\}\}$ is even (i.e. equals 0 or 2). Hence $\left(\frac{p_1 p_2}{q_i}\right) = 1$, and consequently by Lemma 1, we get $C_r'(\mathbb{Q}_{q_i}) \neq \emptyset$. Let $j = 1$ or 2. Since the number $\#\{p_j \to V_1\} = \#\{q \in V_1 : \left(\frac{q}{p_j}\right) = -1\}$ is even, $\left(\frac{r}{p_j}\right) = 1$ and by Lemma 1, $C_r'(\mathbb{Q}_{p_j}) \neq \emptyset$. Clearly, $C_r'(\mathbb{R}) \neq \emptyset$ thus $r \in S_n^{\phi'}$.

iv) Without loss of generality, we assume that $r := q_1, \dots, q_s \in S_n^{\phi'}$. Let $V_1 := \{q_1, \dots, q_s\}$ and $V_2 := \{p_1, p_2, q_{s+1}, \dots, q_k\}$. We prove by definition, that $\{V_1, V_2\}$ is an even partition of $G_2(n)$. By assumption, we have $C_r'(\mathbb{Q}_v) \neq \emptyset$ for $v = p_1, p_2, q_1, \dots, q_k$ and ∞. Hence in particular, by Lemma 1, we get $\left(\frac{p_1 p_2}{q_i}\right) = 1$ for $i \leq s$ and $\left(\frac{r}{p_j}\right) = 1$ for $j = 1, 2$. Now let $q \in V_1$. By above, we obtain that $\#\{q \to V_2\} = \#\{q_i \to \{p_1, p_2\}\} = 0$ if $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = 1$ and $\#\{q \to V_2\} = \#\{q_i \to \{p_1, p_2\}\} = 2$ if $\left(\frac{p_1}{q}\right) = \left(\frac{p_2}{q}\right) = -1$, and the number $\#\{p_j \to V_1\} = \#\left\{q \in V_1 : \left(\frac{q}{p_j}\right) = -1\right\}$ is even too, because $1 = \left(\frac{r}{p_j}\right) = \prod_{q \in V_1} \left(\frac{q}{p_j}\right) = (-1)^{\#\left\{q \in V_1 : \left(\frac{q}{p_j}\right) = -1\right\}}$. Clearly, $\#\{q' \to V_1\} = 0$ for any $q' \in V_2$, and the assertion follows.

v) By parts iii) and iv) there is one-to-one correspondence between even partitions of $G_2(n)$ such that both vertices p_1 and p_2 are in the same set and positive elements in $S_n^{\phi'}$ (note that trivial partition has such property and corresponds to $1 \in S_n^{\phi'}$). Since $-1 \in S_n^{\phi'}$, we have $g \in S_n^{\phi'}$ if and only if $-g \in S_n^{\phi'}$. And we are done. □

Lemma 3. *Suppose that a graph G has vertex set $V = \{v_1, v_2, v_3, \dots, v_t\}$. Then the number of even partitions $\{V_1, V_2\}$ of the graph G such that either both $v_1, v_2 \in V_1$ or both $v_1, v_2 \in V_2$ is equal to $\alpha \times$number of even partitions $\{V_1, V_2\}$ of the graph G, where $\alpha = 1$ or $\frac{1}{2}$.*

Proof. Follows from [5, p. 122–123, Lemmas 5.3 and 5.4] (note that we consider non-ordered partitions). □

Theorem 2. *Under the above assumptions, $2^{rs(E_n^u/\mathbb{Q})}$ equals the number of even partitions of the graph $G_2(n)$. In particular,* $\operatorname{rank}(E_n^u/\mathbb{Q}) = rs(E_n^u/\mathbb{Q}) = 0$ *if and only if $G_2(n)$ is odd. Moreover $rs(E_n^u/\mathbb{Q})$ is maximal (equals $k+1$) if and only if $E(G_2(n)) = \emptyset$.*

Proof. Let 2^e denote the number of even partitions of the graph $G_2(n)$ and let 2^f denote the number of even partitions of the graph $G_2(n)$ such that both vertices p_1 and p_2 are in the same set. By Proposition 3 and Lemma 3, we get $2^{rs(E_n^u/\mathbb{Q})} = 2^{\dim_{\mathbb{F}_2} S_n^{\phi}+\dim_{\mathbb{F}_2} S_n^{\phi'}-2} = 2^{2+(f+1)-2}$ if $f < e$ and $2^{rs(E_n^u/\mathbb{Q})} = 2^{\dim_{\mathbb{F}_2} S_n^{\phi}+\dim_{\mathbb{F}_2} S_n^{\phi'}-2} = 2^{1+(f+1)-2}$ if $f = e$. In both cases $2^{rs(E_n^u/\mathbb{Q})} = 2^e$. Then $rs(E_n^u/\mathbb{Q}) = 0$ if and only if $2^e = 1$, i.e. by definition, that $G_2(n)$ is odd. Similarly, $E(G_2(n)) = \emptyset$ if and only if any partition of $G_2(n)$ is even, that is $2^e = 2^{\#V(G_2(n))-1} = 2^{k+1}$, and the assertion follows. □

Corollary 4. *Assume that* $n = \pm q_1 \dots q_k \equiv 1 (\mathrm{mod}\ 4)$, *where primes* $q_i \equiv 3(\mathrm{mod}\ 4)$, $\left(\frac{q_i}{p_1}\right) = -1$ *and* $q_i \nmid u$ *for all* $1 \le i \le k$. *Moreover, assume that* $\exists_{i_0}\left(\frac{q_{i_0}}{p_2}\right) = -1$ *and* $\forall_{i \neq i_0}\left(\frac{q_i}{p}\right) = 1$. *Then* $\operatorname{rank}(E_n^u/\mathbb{Q}) = 0$.

Proof. We claim that in this case the graph $G_2(n)$ is odd. Suppose, by contradiction, that $\{V_1, V_2\}$ is even nontrivial partition of it. Let (without loss of generality) $p_1 \in V_2$ and let q_i be some element of V_1. Then $\#\{q_i \to V_2\} = \#\{q_i \to p_1\}$ is even, which contradicts to $\left(\frac{p_1}{q_i}\right) = -1$. If no such q_i exists, i.e. $V_1 = \{p_2\}$, then the number $\#\{q_{i_0} \to V_1\} = \#\{q_i \to p_2\}$ is even, contrary to $\left(\frac{q_{i_0}}{p_2}\right) = -1$. Using Theorem 2 yields the assertion. □

Corollary 5. *Assume that* $n = \pm q_1 \dots q_k \equiv 1(\mathrm{mod}\ 4)$, *where primes* $q_i \equiv 3(\mathrm{mod}\ 4)$, $q_i \nmid u$ *for all* $1 \le i \le k$ *and* $\forall_i \left(\frac{q_i}{p_2}\right) = -\left(\frac{q_i}{p_1}\right) = 1$ *(or vice versa). Then* $rs(E_n^u/\mathbb{Q}) = 1$.

Proof. We show that the graph $G_2(n)$ is semi-odd, i.e. has only one nontrivial even partition. First, we show that the partition $\{V_1, V_2\}$, where $V_1 = \{p_2\}$ and $V_2 = \{p_1, q_1, q_2, \dots, q_k\}$ is even. Indeed, $\#\{q_i \to V_1\} = \#\{q_1 \to p_2\} = 0$ because $\left(\frac{q_i}{p_2}\right) = 1$. Clearly, $\#\{p_1 \to V_1\} = 0$ and $\#\{p_2 \to V_2\} = \#\left\{q_i : \left(\frac{q_i}{p_2}\right) = -1\right\} = 0$. Now, we show that there are no other nontrivial even partition of $G_2(n)$. Suppose that the partition $\{V_1', V_2'\} \neq \{V_1, V_2\}$ is nontrivial. Without loss of generality let $p_2 \in V_1'$ but now $V_1' \neq \{p_2\}$. We need to consider two cases: $p_1 \in V_1'$ or $p_1 \in V_2'$. In the first case, for $q \in V_2'$ we have $\#\{q \to V_1'\} = \#\{q \to p_1\} = 1$ because $\left(\frac{q}{p}\right) = -1$. Hence $\{V_1', V_2'\}$ is odd. In the second case, there exists some $q_i \in V_1'$. Then we get $\#\{q_i \to V_2'\} = \#\{q_i \to p_1\} = 1$. Thus again $\{V_1', V_2'\}$ is odd. Now, by Theorem 2, we obtain $2^{rs(E_n^u/\mathbb{Q})} = 2$ and we are done. □

Lemma 4. *Under the assumptions from Corollary 5, the global root number* $W(E_n^u)$ *of the L-function associated to* E_n^u *is equal to* -1.

Proof. The proof is very similar to the proof of Lemma 2. Now we have $W(E_n^u) = W(E_n'^u) = -W_{p_1} W_{p_2} \prod_{1 \le i \le k} W_{q_i}$. The curve $E_n'^u$ has potential good reduction at q_i, hence $W_{q_i} = -1$ (the sign of W_3 follows from [11, Table 2]). At the primes p_1 and p_2 the curve $E_n^{\prime u}$ has multiplicative reduction. Moreover, this reduction at p_i is nonsplit if and only if $\left(\frac{-2un}{p_i}\right) = -1$, and hence $W_{p_i} = -\left(\frac{-2un}{p_i}\right) = -\left(\frac{2un}{p_i}\right)$. Since $p_1 \equiv p_2 \equiv 1, 5 \pmod 8$, we get $\left(\frac{2u}{p_1}\right) = \left(\frac{2u}{p_2}\right)$, and consequently $W(E_n^u) = -(-1)^k(-1)^k = -1$. This finishes the proof. □

Corollary 6. *Assume the Parity Conjecture. Then under the assumptions from Corollary 5, we have* rank $(E_n^u/\mathbb{Q}) = 1$.

Proof. By Corollary 5, rank $(E_n^u/\mathbb{Q}) \leq 1$ and by Lemma 4, the global root number of the associated L-function is equal to -1. Therefore (under the Parity Conjecture) this rank is odd, and we are done. □

Proposition 4. *The set $\{n \in A_k^1 : rank\,(E_n^u(\mathbb{Q})) = 0\}$ has positive density in A_k^1 for all k. In particular, for infinitely many odd squarefree integers the quadratic twists of the curve $y^2 = x^3 + ux^2 - 16x$ ($u^2 + 64$ is a product of two primes) have rank 0.*

Proof. Let C_k denote the set of integers satisfying the assumptions from Corollary 4. Then $C_k \subset A_k^1$ and by this Corollary, rank $(E_n^u(\mathbb{Q})) = 0$ for $n \in B_k$. By the Dirichlet Prime Number Theorem, the set C_k has positive density in A_k^1, and the assertion follows. □

4. Related results

In this section we consider quadratic twists of E^u by an even n. We focus on rank zero twists only.

Proposition 5. *Assume that $u^2 + 64 = p$ and $u \equiv 1 \pmod 4$. Let $n = \pm 2q_1 \dots q_k$, where primes $q_i \equiv 3 \pmod 4$ for all $1 \leq i \leq k$ and let $\frac{n}{2} \equiv 1 \pmod 4$, $\frac{n}{2} \not\equiv u \pmod 8$. If $\left(\frac{p}{q_i}\right) = -1$ for all $1 \leq i \leq k$, then $S_n^{\phi} = \langle p \rangle$ and $S_n^{\phi'} = \langle -1 \rangle$.*

Proof. By Lemma 1, we have $S_n^{\phi} \subset \langle 2, p, q_1, \dots, q_k \rangle$ and $S_n^{\phi'} \subset \langle -1, 2, q_1, \dots, q_k \rangle$. From the implication 3 from Lemma 1, we get $S_n^{\phi} \subset \langle 2, p \rangle$. Since $\frac{n}{2} \not\equiv u \pmod 8$ (by assumption) and $p \equiv 1 \pmod 8$, using condition 11 from Lemma 1, we obtain $2, 2p \notin S_n^{\phi}$. Hence $S_n^{\phi} = \langle p \rangle$.

Consider now the group $S_n^{\phi'}$. Since for all $1 \leq i \leq k$ Legendre's symbol $\left(\frac{q_i}{p}\right) = -1$, then the condition 3' from Lemma 1 leads to the inclusion $S_n^{\phi'} \subset \langle -1, 2 \rangle$. Additionally, using condition $11'$ from Lemma 1, we obtain $\pm 2 \notin S_n^{\phi}$. Finally, we get $S_n^{\phi'} = \langle -1 \rangle$. □

Proposition 6. *Assume that* $u^2 + 64 = p_1p_2$ *and* $u \equiv 1 \pmod 4$. *Let* $n = \pm 2q_1 \dots q_k$, *where primes* $q_i \equiv 3 \pmod 4$ *for all* $1 \le i \le k$ *and let* $\frac{n}{2} \equiv 1 \pmod 4$.

1) *If* $\frac{n}{2} \not\equiv u \pmod 8$, $p_1 \equiv p_2 \equiv 5 \pmod 8$, *and for certain* $1 \le i_0 \le k$ *we have* $q_{i_0} \equiv 3 \pmod 8$ *and* $\left(\frac{p_1}{q_{i_0}}\right) = \left(\frac{p_2}{q_{i_0}}\right) = 1$ *or* $q_{i_0} \equiv 7 \pmod 8$ *and* $\left(\frac{p_1}{q_{i_0}}\right) = \left(\frac{p_2}{q_{i_0}}\right) = -1$, *and for all* $1 \le i \ne i_0 \le k$ *we have* $\left(\frac{p_1p_2}{q_i}\right) = -1$, *then* $S_n^{\phi} = \langle p_1p_2\rangle$ *and* $S_n^{\phi'} = \langle -1\rangle$.
2) *If* $\frac{n}{2} \not\equiv u \pmod 8$, $p_1 \equiv p_2 \equiv 1 \pmod 8$, *and for certain* $1 \le i_0 \le k$ *we have* $\left(\frac{p_1}{q_{i_0}}\right) = \left(\frac{p_2}{q_{i_0}}\right) = -1$, *and for all* $1 \le i \ne i_0 \le k$ *we have* $\left(\frac{p_1p_2}{q_i}\right) = -1$, *then* $S_n^{\phi} = \langle p_1p_2\rangle$ *and* $S_n^{\phi'} = \langle -1\rangle$.
3) *If* $\frac{n}{2} \equiv u \pmod 8$, $p_1 \equiv p_2 \equiv 5 \pmod 8$, *and for certain* $1 \le i_0 \le k$ *we have* $q_{i_0} \equiv 3 \pmod 8$ *and* $\left(\frac{p_1p_2}{q_{i_0}}\right) = 1$, *and for all* $1 \le i \ne i_0 \le k$ *we have* $\left(\frac{p_1p_2}{q_i}\right) = -1$, *then* $S_n^{\phi} = \langle p_1p_2\rangle$ *and* $S_n^{\phi'} = \langle -1\rangle$.

Proof. By Lemma 1, we have $S_n^{\phi} \subset \langle 2, p_1, p_2\rangle$ and $S_n^{\phi'} \subset \langle -1, 2, q_1, q_2, \dots, q_k\rangle$. Without loss of generality assume that $i_0 = 1$. Let $\left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_1}\right) = -1$, then using condition 4 of this Lemma, we obtain $p_1, p_2 \notin S_n^{\phi}$. Next, if $q_1 \equiv 3 \pmod 8$, then $\left(\frac{2}{q_1}\right) = -1$ and $C_2(\mathbb{Q}_{q_1}) = C_{2p_1p_2}(\mathbb{Q}_{q_1}) = \emptyset$. Consequently $S_n^{\phi} \subset \langle 2p_1, 2p_2\rangle$. However, if $q_1 \equiv 7 \pmod 8$, then $\left(\frac{2}{q_1}\right) = 1$ and $C_{2p_1}(\mathbb{Q}_{q_1}) = C_{2p_2}(\mathbb{Q}_{q_1}) = \emptyset$ and consequently $S_n^{\phi} \subset \langle 2, p_1p_2\rangle$.

Let $\frac{n}{2} \not\equiv u \pmod 8$. Then, using condition 11 from Lemma 1, we get $C_2(\mathbb{Q}_2) = C_{2p_1p_2}(\mathbb{Q}_2) = \emptyset$. Additionally, if $p_1 \equiv p_2 \equiv 1 \pmod 8$, then we have $C_{2p_1}(\mathbb{Q}_2) = C_{2p_2}(\mathbb{Q}_2) = \emptyset$, which means that $2p_1, 2p_2 \notin S_n^{\phi}$.

Thus we obtain: if $\frac{n}{2} \equiv u \pmod 8$, $q_1 \equiv 3 \pmod 8$, $p_1 \equiv p_2 \equiv 5 \pmod 8$ or $\frac{n}{2} \not\equiv u \pmod 8$, $q_1 \equiv 7 \pmod 8$, $p_1 \equiv p_2 \equiv 5 \pmod 8$ or $\frac{n}{2} \not\equiv u \pmod 8$, $q_1 \equiv 3 \pmod 4$, $p_1 \equiv p_2 \equiv 1 \pmod 8$, then $S_n^{\phi} = \langle p_1p_2\rangle$.

Consider now the group $S_n^{\phi'}$. Let $\left(\frac{p_1p_2}{q_i}\right) = -1$ for all $2 \le i \le k$. Since $\left(\frac{u^2+64}{q_i}\right) = -1 \Longrightarrow (C_d(\mathbb{Q}_{q_i}) = \emptyset \iff q_i \mid d)$, we get $S_n^{\phi'} \subset \langle -1, 2, q_1\rangle$. If $\frac{n}{2} \not\equiv u \pmod 8$, then $\pm 2 \notin S_n^{\phi'}$, because $C'_{\pm 2}(\mathbb{Q}_2) = \emptyset$. Additionally, if $q_1 \equiv 3 \pmod 8$, then $\pm q_1 \notin S_n^{\phi'}$ ($C'_{\pm q_1}(\mathbb{Q}_2) = \emptyset$) and if $q_1 \equiv 7 \pmod 8$, then $\pm 2q_1 \notin S_n^{\phi'}$ ($C'_{\pm 2q_1}(\mathbb{Q}_2) = \emptyset$). Hence if $q_1 \equiv 3 \pmod 8$, then $S_n^{\phi'} \subset \langle -1, 2q_1\rangle$ and if $q_1 \equiv 7 \pmod 8$, then $S_n^{\phi'} \subset \langle -1, q_1\rangle$.

By assumptions we have:

1) $p_1 \equiv p_2 \equiv 5 \pmod 8, q_1 \equiv 3 \pmod 8, \left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_1}\right) = 1,$
2) $p_1 \equiv p_2 \equiv 5 \pmod 8, q_1 \equiv 7 \pmod 8, \left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_1}\right) = -1,$
3) $p_1 \equiv p_2 \equiv 1 \pmod 8, q_1 \equiv 3 \pmod 4, \left(\frac{p_1}{q_1}\right) = \left(\frac{p_2}{q_1}\right) = -1,$

when $\frac{n}{2} \not\equiv u \pmod 8$. In the first case $\left(\frac{2}{p_1}\right) = \left(\frac{-2}{p_1}\right) = -1$ and $\left(\frac{2q_1}{p_1}\right) = \left(\frac{-2q_1}{p_1}\right) = -1$, hence $C'_{\pm 2}(\mathbb{Q}_{p_1}) = C'_{\pm 2q_1}(\mathbb{Q}_{p_1}) = \emptyset$, which means that $S_n^{\phi'} = \langle -1 \rangle$. In the second case, since $\left(\frac{q_1}{p_1}\right) = \left(\frac{-q_1}{p_1}\right) = -1$, then $S_n^{\phi'} = \langle -1 \rangle$ too. In the third case $\left(\frac{2}{p_1}\right) = \left(\frac{-2}{p_1}\right) = 1$, consequently $\left(\frac{2q_1}{p_1}\right) = \left(\frac{-2q_1}{p_1}\right) = -1$ and $S_n^{\phi'} = \langle -1 \rangle$. If $\frac{n}{2} \equiv u \pmod 8$ and $q_1 \equiv 3 \pmod 8$, then $C'_{\pm q_1}(\mathbb{Q}_2) = C'_{\pm 2q_1}(\mathbb{Q}_2) = \emptyset$ and $S_n^{\phi'} \subset \langle -1, 2 \rangle$. Because in the case $\frac{n}{2} \equiv u \pmod 8$ we assume, that $p_1 \equiv p_2 \equiv 5 \pmod 8$, then $\left(\frac{2}{p_1}\right) = \left(\frac{-2}{p_1}\right) = -1$, so $C'_{\pm 2}(\mathbb{Q}_{p_1}) = \emptyset$ and $S_n^{\phi'} = \langle -1 \rangle$. □

Corollary 7. *Under the assumptions from Proposition 5 or Proposition 6, we have* $\operatorname{rank}(E_n^u/\mathbb{Q}) = 0$.

For a positive integer k, let A_k^2 denote the set of even squarefree (positive if k is even and negative if k is odd) integers such that $\gcd(n, u) = \gcd(n, u^2 + 64) = 1$, and with exactly k prime factors.

Corollary 8. *The set* $\{n \in A_k^2 : \operatorname{rank}(E_n^u(\mathbb{Q})) = 0\}$ *has positive density in* A_k^2 *for all* k. *In particular, for infinitely many even squarefree integers the quadratic twists of the curve* $y^2 = x^3 + ux^2 - 16x$ *(*$u^2 + 64$ *is a prime or a product of two primes) have rank 0.*

Proof. Similar to the proof of Propositions 2 and 4. □

5. Generalizations

In this section we consider more general curves $E^u : y^2 = x^3 + ux^2 - 16x$, with $u^2 + 64 = p_1 \dots p_l$, where l is a positive integer and p_i are primes. We focus on rank zero twists E_n^u only.

Proposition 7. *Suppose that* $u^2 + 64 = p_1 \dots p_l$, $l \geq 2$ *and* $n = \pm q_1 \dots q_k \equiv 1 \pmod 4$, $k \geq l - 1$, *where (for all* $1 \leq i \leq k$*) primes* $q_i \equiv 3 \pmod 4$ *and* $q_i \nmid u$. *Let* $\forall_{1 \leq i \leq k} \left(\frac{p_1}{q_i}\right) = -1$, $\exists_{1 \leq i_1 \leq k} \left(\frac{p_2}{q_{i_1}}\right) = -1$, $\forall_{i \neq i_1, 1 \leq i \leq k} \left(\frac{p_2}{q_i}\right) = 1$, $\exists_{i_2 \neq i_1, 1 \leq i_2 \leq k} \left(\frac{p_3}{q_{i_2}}\right) = -1$, $\forall_{i \neq i_2, 1 \leq i \leq k} \left(\frac{p_3}{q_i}\right) = 1, \dots,$ $\exists_{i_{l-1} \neq i_1, i_2, \dots, i_{l-2}, 1 \leq i_{l-1} \leq k} \left(\frac{p_l}{q_{i_{l-1}}}\right) = -1$, $\forall_{i \neq i_{l-1}, 1 \leq i \leq k} \left(\frac{p_l}{q_i}\right) = 1$. *Then* $S_n^{\phi} = \langle p_1 \dots p_l \rangle$, $S_n^{\phi'} = \langle -1 \rangle$.

Proof. The table below consists of the values of Legendre's symbol $\left(\frac{p_j}{q_i}\right)$, $1 \le i \le k$, $1 \le j \le l$, under assumption, which may be taken without loss of generality, that $i_1 = 1, i_2 = 2, \ldots, i_{l-1} = l-1$.

	p_1	p_2	p_3	$\ldots$	p_{l-1}	p_l
q_1	-1	-1	1	$\ldots$	1	1
q_2	-1	1	-1	$\ldots$	1	1
q_3	-1	1	1	$\ldots$	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
q_{l-2}	-1	1	1	$\ldots$	-1	1
q_{l-1}	-1	1	1	$\ldots$	1	-1
q_l	-1	1	1	$\ldots$	1	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
q_k	-1	1	1	$\ldots$	1	1

In order to calculate the Selmer groups we apply Lemma 1. The starting point is the condition

$$S_n^{\phi}, S_n^{\phi'} \subset \langle -1, p_1, p_2, \ldots, p_l, q_1, q_2, \ldots, q_k \rangle.$$

From the equivalence $2'$ from Lemma 1, we first get $S_n^{\phi'} \subset \langle -1, q_1, q_2, \ldots, q_k \rangle$. Note (using the same equivalence over $\mathbb{Q}_{p_1}$), that no product of odd number of factors q_i, either multiplied by -1 or not, belongs to $S_n^{\phi'}$. Next, over $\mathbb{Q}_{p_j}$, where $2 \le j \le l$, no product of even number of factors q_i, including q_{j-1}, either multiplied by -1 or not, belongs to $S_n^{\phi'}$. The remaining products of numbers q_i (that is the products where q_i, $i \in \{1, \ldots, l-1\}$ do not appear) are excluded from the group $S_n^{\phi'}$, applying $\left(\frac{u^2+64}{q_i}\right) = -1 \Longrightarrow (C_d'(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow q_i \mid d)$. So are the same products multiplied by -1. Finally, we get $S_n^{\phi'} = \langle -1 \rangle$.

Consider now the group S_n^{ϕ}. The condition $C_d(\mathbb{R}) \neq \emptyset \Longrightarrow d > 0$ leads to the inclusion $S_n^{\phi} \subset \langle p_1, p_2, \ldots, p_l, q_1, q_2, \ldots, q_k \rangle$. Next, from the implication $\left(\frac{u^2+64}{q_i}\right) = -1 \Longrightarrow (C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow q_i \mid d)$, taking $i = l, l+1, \ldots, k$, we conclude that $S_n^{\phi} \subset \langle p_1, p_2, \ldots, p_l, q_1, q_2, \ldots, q_{l-1} \rangle$. For $i = 1, \ldots, l-1$ we get $\left(\frac{u^2+64}{q_i}\right) = 1$, so $C_d(\mathbb{Q}_{q_i}) = \emptyset \Longleftrightarrow \left(\frac{d}{q_i}\right) \neq 1$. Obviously, no product M of primes q_i $(1 \le i \le l-1)$ belongs to S_n^{ϕ}, as it is enough to observe that $\left(\frac{M}{q_{i_0}}\right) = 0$ if $q_{i_0} \mid M$, which gives $C_M(\mathbb{Q}_{i_0}) = \emptyset$. The table also shows that no product N of numbers p_j, $1 \le j \le l$, such that $p_1p_2 \nmid N$ and ($p_1 \mid N$ or $p_2 \mid N$), belongs to S_n^{ϕ} (in particular $p_1, p_2 \notin S_n^{\phi}$), as $\left(\frac{N}{q_1}\right) = -1$. In turn, the products of numbers p_j, such that $p_1p_3 \nmid N$

and ($p_1 \mid N$ or $p_3 \mid N$) (in particular, such that $p_1 p_2 \mid N$ and $p_3 \nmid N$) do not belong to S_n^{ϕ}, as $\left(\frac{N}{q_2}\right) = -1$, etc., finally, S_n^{ϕ} does not contain such products N of numbers p_j, $1 \le j \le l$, that $p_1 p_l \nmid N$ and ($p_1 \mid N$ or $p_l \mid N$), as $\left(\frac{N}{q_{l-1}}\right) = -1$. This way we obtain $S_n^{\phi} \subset \langle p_1 p_2 \cdots p_l \rangle$. □

Corollary 9. *Under the assumptions from Proposition 7, we have* **rank** $(E_n^u/\mathbb{Q}) = 0$.

Now we show that in some cases the assumption $k \ge l - 1$ in the Proposition 7 is necessary but in some cases is not.

Proposition 8. *Let* $u^2 + 64 = p_1 p_2 p_3$ *where* $p_1 \equiv p_2 \equiv p_3 \equiv 1 \pmod 8$. *Let* $n = \pm q$ *or* $\pm 2q$, *where* q *is an odd prime. Then* $rs(E_n^u/\mathbb{Q}) \ge 1$.

Proof. By Lemma 1, we have $S_n^{\phi} \subset \langle 2, p_1, p_2, p_3, q \rangle$ and $S_n^{\phi'} \subset \langle -1, 2, q \rangle$. Moreover, $C_d(\mathbb{R}) \ne \emptyset \Leftrightarrow d > 0$ and $C'_d(\mathbb{R}) \ne \emptyset$ for all d. We have to consider many (not necessary disjoint) cases according to residue classes of q modulo 8, values of Legendre symbol $\left(\frac{q}{p_i}\right)$, and residue classes of n modulo 4.

Case 1. $n \equiv 1 \pmod 4$. Then the reduction of E_n^u is good at 2, hence $S_n^{\phi} \subset \langle p_1, p_2, p_3, q \rangle$ and $S_n^{\phi'} \subset \langle -1, q \rangle$. By Lemma 1, $C_d(\mathbb{Q}_{p_i}) \ne \emptyset$ for all d and $i = 1, 2, 3$. Again by Lemma 1, $C'_{-1}(\mathbb{Q}_{p_i}) \ne \emptyset$ ($i = 1, 2, 3$), and if $\left(\frac{q}{p_i}\right) = 1$ for $i = 1, 2, 3$ then $C'_d(\mathbb{Q}_{p_i}) \ne \emptyset$ for $d = \pm q$ but if $\left(\frac{q}{p_i}\right) = -1$ for some $i \in \{1, 2, 3\}$ then $\pm q \notin S_n^{\phi'}$. Now it remains to consider C_d and C'_d over $\mathbb{Q}_q$.

Case 1.1. $q \equiv 3 \pmod 4$. If $\left(\frac{p_1 p_2 p_3}{q}\right) = -1$ then $C_d(\mathbb{Q}_q) \ne \emptyset$ and $C'_d(\mathbb{Q}_q) \ne \emptyset$ for all d not dividing by q. Thus $\langle p_1, p_2, p_3 \rangle \subset S_n^{\phi}$ and $\langle -1 \rangle \subset S_n^{\phi'}$, and consequently $rs(E_n^u/\mathbb{Q}) \ge 2$. If $\left(\frac{p_1 p_2 p_3}{q}\right) = 1$ then $C'_d(\mathbb{Q}_q) \ne \emptyset$ for all d and $C_d(\mathbb{Q}_q) \ne \emptyset$ if $\left(\frac{d}{q}\right) = 1$. Therefore $\langle p_1 p_2 p_3, p_i \rangle \subset S_n^{\phi}$ for some i, and $\langle -1 \rangle \subset S_n^{\phi'}$. Hence $rs(E_n^u/\mathbb{Q}) \ge 1$.

Case 1.2. $q \equiv 1 \pmod 4$. If $\left(\frac{p_1 p_2 p_3}{q}\right) = -1$ then by Lemma 1, $C_d(\mathbb{Q}_q) \ne \emptyset$ for all d and $C'_d(\mathbb{Q}_q) \ne \emptyset$ if and only if $\left(\frac{d}{q}\right) = 1$. Thus $\langle p_1, p_2, p_3, q \rangle \subset S_n^{\phi}$ and $\langle -1 \rangle \subset S_n^{\phi'}$, so $rs(E_n^u/\mathbb{Q}) \ge 3$. Assume that $\left(\frac{p_1 p_2 p_3}{q}\right) = 1$. Then $C'_{-1}(\mathbb{Q}_q) \ne \emptyset$, hence $\langle -1 \rangle \subset S_n^{\phi'}$. For at least one $i \in \{1, 2, 3\}$ we have $\left(\frac{p_i}{q}\right) = 1$. Thus, by Lemma 1, we get $\langle p_i, p_1 p_2 p_3 \rangle \subset S_n^{\phi}$, and $rs(E_n^u/\mathbb{Q}) \ge 1$.

Case 2. $n \equiv 3 \pmod 4$. Then E_n^u has bad reduction at 2. Besides $\mathbb{Q}_{p_i}$ and $\mathbb{Q}_q$ we have also to consider C_d and C'_d over $\mathbb{Q}_2$. Considerations over $\mathbb{Q}_{p_i}$ and $\mathbb{Q}_q$ are similar (almost the same) to that above. Thus we only regard the field $\mathbb{Q}_2$.

Note that $un \equiv 3 \pmod 4$. Therefore, by Lemma 1, we obtain, $C'_d(\mathbb{Q}_q) \neq \emptyset$ for all d and $C_d(\mathbb{Q}_q) \neq \emptyset$ if and only if $d \equiv 1 \pmod 8$. Consequently, the Selmer groups S_n^{ϕ} and $S_n^{\phi'}$ in this case are greater than or equal to the groups S_n^{ϕ} and $S_n^{\phi'}$ in case 1, and $rs(E_n^u/\mathbb{Q}) \geq 1$.

Case 3. $n \equiv 2 \pmod 4$. Then E_n^u has bad reduction at 2, too. Now, existence of $\mathbb{Q}_2$-rational point on C_d and C'_d depends on residue class $un \pmod{16}$ (see Lemma 1) but in all cases $C_d(\mathbb{Q}_2) \neq \emptyset$ for $d \in \langle p_1, p_2, p_3 \rangle$ and $C'_{-1}(\mathbb{Q}_2) \neq \emptyset$. Thus, the group S_n^{ϕ} in case 3 is greater than or equal to S_n^{ϕ} in case 1, and $S_n^{\phi'} \supset \langle -1 \rangle$. Consequently $rs(E_n^u/\mathbb{Q}) \geq 1$ and the assertion follows. □

Proposition 9. *Let $u^2 + 64 = p_1p_2p_3$, where $p_1 \equiv 1 \pmod 8$ and $p_2 \equiv p_3 \equiv 5 \pmod 8$. Let $n = q$ where $q \equiv 3 \pmod 4$ is a prime such that $\left(\frac{q}{p_1}\right) = \left(\frac{q}{p_2}\right) = -\left(\frac{q}{p_3}\right) = -1$, and $q \nmid u$. Then $S_n^{\phi} = \langle p_1p_2p_3 \rangle$ and $S_n^{\phi'} = \langle -1 \rangle$. In particular, $rs(E_n^u/\mathbb{Q}) = 0$.*

Proof. Since $n \equiv 3 \pmod 4$, the curve E_n^u has bad reduction at 2, and so $S_n^{\phi} \subset \langle 2, p_1, p_2, p_3, q \rangle$ and $S_n^{\phi'} \subset \langle -1, 2, q \rangle$. Moreover, $\left(\frac{\pm 2}{p_2}\right) = -1$, $\left(\frac{\pm 2q}{p_3}\right) = -1$ and $\left(\frac{\pm q}{p_2}\right) = -1$, hence by Lemma 1, $S_n^{\phi'} \subset \langle -1 \rangle$ and $C'_{-1}(\mathbb{Q}_{p_i}) \neq \emptyset$ for $i = 1, 2, 3$. Since $un \equiv 3 \pmod 4$, by Lemma 1, we obtain $C'_d(\mathbb{Q}_2) \neq \emptyset$ and $C_d(\mathbb{Q}_2) \neq \emptyset$ if and only if $d \equiv 1 \pmod 8$. Thus $S_n^{\phi} \subset \langle p_1, p_2, p_3 \rangle$ and $p_2, p_3, p_1p_2, p_1p_3 \notin S_n^{\phi}$. Now it remains to consider C_d and C'_d over $\mathbb{Q}_q$. Since $\left(\frac{p_1p_2p_3}{q}\right) = 1$, we get $C'_d(\mathbb{Q}_q) \neq \emptyset$ for all d and $C_d(\mathbb{Q}_q) \neq \emptyset$ if and only if $\left(\frac{d}{q}\right) = 1$. Thus $C_d(\mathbb{Q}_q) = \emptyset$ for $d = p_1, p_2p_3$ and $C_d(\mathbb{Q}_q) \neq \emptyset$ for $d = p_1p_2p_3$. Hence $S_n^{\phi} = \langle p_1p_2p_3 \rangle$ and $S_n^{\phi'} = \langle -1 \rangle$, and we are done. □

Acknowledgement

We would like to thank Andrzej Dąbrowski for suggesting the problem and helpful conversations.

References

[1] I. Connell, Calculating root numbers of elliptic curves over $\mathbb{Q}$, *Manuscripta Math.*, **82** (1994) 93–104.

[2] A. Dąbrowski, On the proportion of rank 0 twists of elliptic curves, *C. R. Math. Acad. Sci.*, Paris **346** (2008) no. 9–10, 483–486.

[3] A. Dąbrowski and M. Wieczorek, On the equation $y^2 = x(x - 2^m)(x + q - 2^m)$, *J. Number Theory*, **124** (2007), 364–379.

[4] B. Faulkner, Estimates related to the arithmetic of elliptic curves, Ph.D. Dissertation, Clemson Univerity (2007).
[5] B. Faulkner and K. James, A graphical approach to computing Selmer groups of congruent number curves, *Ramanujan J.*, **14** (2007) 107–129.
[6] K. Feng, Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture, *Acta Arith.*, **75** (1996) 71–83.
[7] K. Feng and M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero, *J. Number Theory*, **109** (2004) 1–26.
[8] D. Goldfeld, Conjectures on elliptic curves over quadratic fields, *Springer Lecture Notes*, Springer, Berlin, **751** (1979) 108–118.
[9] T. Goto, A study on the Selmer groups of the elliptic curves with a rational 2-torsion, *Doctoral Thesis*, Kyushu University (2002).
[10] T. Goto, Odd graphs and Selmer groups of certain elliptic curves, *Algebra and Computation*, **6** (2005).
[11] E. Halberstadt, Signes locaux des courbes elliptiques en 2 et 3, *C. R. Acad. Sci.*, Paris **326**, (1998) 1047–1052.
[12] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.*, **47** (1978), 171–188.
[13] T. Jędrzejak, On twists of the Fermat cubic $x^3 + y^3 = 2$, *Int. J. Number Theory*, **10**, No. 1 (2014), 55–72.
[14] F. Li and D. Qiu, A graphical method to calculate Selmer groups of several families of non-CM elliptic curves, arXiv:0912.5072v1 (preprint 2009).
[15] O. Neumann, Elliptische Kurven mit vorgeschriebenen Reduktionsverhalten. I, *Math. Nachr.* **49** (1971) 107–123.
[16] B. Setzer, Elliptic curves of prime conductor, *J. London Math. Soc.*, **10** (1975) 367–378.
[17] J. Silverman, The Arthmetic of elliptic curves, *Grad. Texts in Math.*, Springer, **106** (1986).
[18] G. Yu, On the quadratic twists of a family of elliptic curves, *Mathematika*, **52** (2005), no. 1–2, 139–154.