# A GRAPHICAL APPROACH TO COMPUTING SELMER GROUPS OF CONGRUENT NUMBER CURVES.

BRYAN FAULKNER AND KEVIN JAMES

Abstract. Let $E_n : y^2 = x^3 - n^2 x$ denote the family of congruent number elliptic curves. In [1], Feng and Xiong equate the nontriviality of the Selmer groups associated with $E_n$ to the presence of certain types of partitions of graphs associated with the prime factorization of $n$. In this paper, we extend the ideas of Feng and Xiong in order to compute the Selmer groups of $E_n$.

## 1. Introduction

Throughout this paper $n$ will represent a positive square free integer greater than one. We will denote by $E_n : y^2 = x^3 - n^2 x$, the family of congruent number curves. If $n = p_1 \cdots p_s$, then let

$$M =< -1, 2, p_1, \ldots, p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$$

We define (see [1], [6, Ch. 10 §4] for more details) Selmer groups $S_n$ and $S'_n$ by

$$\begin{aligned} S_n &= \{d \in M \mid \ C_d(\mathbb{Q}_p) \neq \emptyset \ \forall p|2n, \ C_d(\mathbb{Q}_\infty) \neq \emptyset\}, \\ S'_n &= \{d \in M \mid \ C'_d(\mathbb{Q}_p) \neq \emptyset \ \forall p|2n, \ C'_d(\mathbb{Q}_\infty) \neq \emptyset\}, \end{aligned}$$

where the equations $C_d$ and $C'_d$, in variables $(w, t, z)$ are given by

$$C_d : \ dw^2 = t^4 + (2n/d)^2 z^4, \quad C'_d : \ dw^2 = t^4 - (n/d)^2 z^4.$$

We should note that $(0, 0, 0)$ is always a solution to $C_d(C'_d)$. So, when we write $C_d(\mathbb{Q}_p) \neq \emptyset$ $(C'_d(\mathbb{Q}_p) \neq \emptyset)$, we mean there exists nontrivial solutions.

There has been much interest in understanding these groups (see [2, 3, 4, 5] and references there in). In a recent paper of Feng and Xiong ([1]), graph theory is used to describe conditions such that $S_n$ and $S'_n$ are trivial, which in turn implies that the rank of $E_n$ is zero. In this paper we use graph theoretic concepts similar to those introduced in [1] to compute $S_n$ and $S'_n$.

In order to understand $S_n$ and $S'_n$, we must determine for which $d \in M$ the equations $C_d$ and $C'_d$ have solutions over $\mathbb{Q}_p$ for all $p|2n$. For odd primes $p$, we search for solutions over $\mathbb{F}_p$ and then invoke Hensel's Lemma to lift solutions in $\mathbb{F}_p$ to solutions in $\mathbb{Q}_p$. The application of Hensel's lemma in the 2-adic case is a bit more difficult. However, in all but one case, it is sufficient to consider $C_d$ and $C'_d$ modulo $2^3$ as solutions here will lift to solutions in $\mathbb{Q}_2$.

Following Feng and Xiong we make the following definitions.

*Date*: January 13, 2006.

**Definition 1.1.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$. Define a graph, $G(n)$, by defining the vetex set to be $V(G(n)) = \{p_1, \ldots, p_t, q_1, \ldots q_l\}$ and the edge set as*

$$\begin{aligned} E(G(n)) &= \{\overline{p_i p_j} : \left(\frac{p_i}{p_j}\right) = -1 \text{ for } 1 \leq i \leq t \text{ and } 1 \leq j \leq t\} \\ &\cup \{\overline{p_i q_j} : \left(\frac{p_i}{q_j}\right) = -1 \text{ for } 1 \leq i \leq t \text{ and } 1 \leq j \leq l\} \end{aligned}$$

A partition of a vertex set $V$ is an ordered pair $(V_1, V_2)$ such that $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = V$. The trivial partitions are $(\emptyset, V)$ and $(V, \emptyset)$. We will be interested in the partitions of $V$ which are even in the following sense.

**Definition 1.2.** *Let $G = (V, E)$ be a directed graph. A partition $(V_1, V_2)$ of $V$ is even provided that for any vertex, $p \in V_1$ ($V_2$), $\#\{p \to V_2\ (V_1)\}$ is even. In this case, we shall write $(V_1, V_2) \vdash_e V$.*

Notice that the trivial partitions are even. We will also be interested in partitions of $V$ which are *quasi-even* in the following sense.

**Definition 1.3.** *A partition $(V_1, V_2)$ of $V$ is quasi-even provided that for any vertex, $p \in V_1$ ($V_2$)*

$$\#\{p \to V_2(V_1)\} \equiv \begin{cases} 0 \pmod 2, & \text{if } \left(\frac{2}{p}\right) = 1 \\ 1 \pmod 2, & \text{if } \left(\frac{2}{p}\right) = -1. \end{cases}$$

*In this case, we shall write $(V_1, V_2) \vdash_{qe} V$.*

In this paper, we prove that the number of even and quasi-even partitions of $G(n)$ predict the size of the Selmer group $S_n$. We also prove that the number of even partitions of similiar graphs predict the size of the Selmer group, $S'_n$. It will be clear from our proofs that the even and quasi-even partitions of these graphs correspond in a natural way to elements of $S_n$ and $S'_n$.

**Theorem 1.1.** *Let $p_1, \ldots, p_t, q_1, \ldots, q_l$ be the odd prime factors of $n$, where $p_i \equiv 1 \pmod 4$ for $0 \leq i \leq t$ and $q_j \equiv 3 \pmod 4$ for $0 \leq j \leq l$ (t,l not both zero).*

(1) *If $n \equiv \pm 3 \pmod 8$ or $n \equiv 0 \pmod 2$, then*
$$|S_n| = \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\}$$
(2) *If $n \equiv \pm 1 \pmod 8$ and $\exists\, p | n$, $p \equiv \pm 3 \pmod 8$, then*
$$\begin{aligned} |S_n| = &\ \#\ \{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\} + \\ &\ \#\ \{(V_1, V_2) \vdash_{qe} V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\} \end{aligned}$$
(3) *If $p_i \equiv 1 \pmod 8$ for all $0 \leq i \leq t$ and $q_j \equiv 7 \pmod 8$ for all $0 \leq j \leq l$, then*
$$|S_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_j \notin V_1;\ 0 \leq j \leq l\}$$

In order to compute $S'_n$, we require three additional tools.

**Definition 1.4.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 3 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \le i \le t$ and $0 \le j \le l$. Define a graph, $g(n)$, by defining the vetex set to be $V(g(n)) = \{p_1, \dots p_t, q_1, \dots q_l\}$ and the edge set as*

$$\begin{aligned} E(g(n)) &= \{\overline{p_i p_j} \ : \ \left(\frac{p_i}{p_j}\right) = -1 \textit{ for } 1 \le i \le t \textit{ and } 0 \le j \le t\} \\ &\cup \ \{\overrightarrow{p_i q_j} \ : \ \left(\frac{p_i}{q_j}\right) = -1 \textit{ for } 0 \le i \le t \textit{ and } 0 \le j \le l\} \end{aligned}$$

**Definition 1.5.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \le i \le t$ and $0 \le j \le l$. Define a graph, $G(-n)$, by defining the vetex set to be $V(G(-n)) = \{-1, p_1, \dots p_t, q_1, \dots q_l\}$ and the edge set as*

$$\begin{aligned} E(G(-n)) &= \{\overline{p_i p_j} \ : \ \left(\frac{p_i}{p_j}\right) = -1 \textit{ for } 0 \le i \le t \textit{ and } 0 \le j \le t\} \\ &\cup \ \{\overrightarrow{p_i q_j} \ : \ \left(\frac{p_i}{q_j}\right) = -1 \textit{ for } 0 \le i \le t \textit{ and } 0 \le j \le l\} \\ &\cup \ \{\overrightarrow{-1 r} \ : \ r \in V(G(-n)) \quad \textit{and} \quad r \equiv \pm 3 \pmod 8\} \end{aligned}$$

**Definition 1.6.** *Let $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \le i \le t$ and $0 \le j \le l$. Define a graph $G'(n)$ in the following way.*

$$\begin{aligned} V(G'(n)) &= \{2, p_1, \dots p_t, q_1, \dots q_l\} \\ E(G'(n)) &= \{\overline{p_i p_j} \mid \left(\frac{p_j}{p_i}\right) = -1 \ \ 0 \le i \ne j \le t\} \\ &\cup \ \{\overrightarrow{p_i q_j} \ \mid \left(\frac{p_i}{q_j}\right) = -1 \ \ 0 \le i \le t, 0 \le j \le l\} \\ &\cup \ \{\overrightarrow{p_i 2} \ \mid \left(\frac{2}{p_i}\right) = -1 \ \ 0 \le i \le t\} \end{aligned}$$

Then we have the following theorem.

**Theorem 1.2.** *Let $n$ be a positive square free integer greater than one.*

(1) *If $n \equiv \pm 3 \pmod 8$, then*
$$|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e g(n)\}$$
(2) *If $n \equiv \pm 1 \pmod 8$, then*
$$|S'_n| = \#\{(V_1, V_2) \vdash_e G(-n)\}$$
(3) *If $n \equiv 0 \pmod 2$, then*
$$|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e G'(n)\}$$

The organization of the rest of this paper is as follows. In section 2, we state several lemmas which allow us to characterize for which $d$, $C_d$ and $C'_d$ have nontrivial solutions in $\mathbb{Q}_p$. In sections 3 and 4, we prove Theorems 1.1 and 1.2. In section 5 we review some concepts of graph theory related to counting even partitions and give corollaries of the two theorems which are more amenable to computation. Finally, in section 6 we give an example and a remark concerning the generators of these groups.

## 2. $C_d(\mathbb{Q}_p)$ AND $C'_d(\mathbb{Q}_p)$

In this section we wish to characterize, in terms of $n$ and $d$, when $C_d$ and $C'_d$ have solutions over $\mathbb{Q}_p$, for $p|2n$, and over $\mathbb{Q}_\infty$. We first recall the following lemmas from [1].

**Lemma 2.1.** *(Feng and Xiong* [1, lemma 3.1]*) Let $p$ be an odd prime, $n$ an odd positive integer with odd prime divisors $\{p_1, \ldots, p_s\}$, and $d \in M =< -1, 2, p_1, \ldots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(1) $C_d(\mathbb{Q}_\infty) = \emptyset \iff d < 0$
(2) *For* $p|d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = 1.$
(3) *For* $p|2n/d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1$
(4) $d \equiv 1 \pmod 4 \implies C_d(\mathbb{Q}_2) \neq \emptyset$
(5) $n \equiv \pm 3 \pmod 8$ *and* $2|d \implies C_d(\mathbb{Q}_2) = \emptyset$
(6) $n \equiv \pm 1 \pmod 8$ *and* $d = 2d'|2n$ *and* $d' \equiv 1 \pmod 4 \implies C_d(\mathbb{Q}_2) \neq \emptyset$

**Lemma 2.2.** *(Feng and Xiong* [1, lemma 3.2]*) Let $p$ be an odd prime, $n$ an odd positive integer with odd prime divisors $\{p_1, \ldots p_s\}$, and $d \in M =< -1, 2, p_1, \ldots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(1) *For* $p|d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ *or* $\left(\frac{n/d}{p}\right) = 1.$
(2) *For* $p|n/d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ *or* $\left(\frac{d}{p}\right) = 1.$
(3) *If* $d \equiv 1 \pmod 2$, *then* $C'_d(\mathbb{Q}_2) \neq \emptyset \iff d \equiv \pm 1 \pmod 8$ *or* $n/d \equiv \pm 1 \pmod 8$
(4) *If* $d \equiv 0 \pmod 2$ *then* $C'_d(\mathbb{Q}_2) = \emptyset.$

We introduce two additional lemmas to handle the cases when $n$ is even.

**Lemma 2.3.** *Let $p$ be an odd prime, $n$ an even positive integer with odd prime divisors $\{p_1, \ldots p_s\}$, and $d \in M =< -1, 2, p_1, \ldots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(1) $C_d(\mathbb{Q}_\infty) = \emptyset \iff d < 0.$
(2) $d \equiv 0 \pmod 2 \implies C_d(\mathbb{Q}_2) = \emptyset$
(3) *For* $p|d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{n/d}{p}\right) = 1$ *and* $\left(\frac{-1}{p}\right) = 1.$
(4) *For* $p|n/d$, $C_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{d}{p}\right) = 1.$
(5) $d \equiv 1 \pmod 8 \implies C_d(\mathbb{Q}_2) \neq \emptyset$
(6) $d \equiv 5 \pmod 8 \implies C_d(\mathbb{Q}_2) = \emptyset$

*Proof.*
For the proofs of (1) and (2) see [1, lemma 5.1].
(3) ($\Leftarrow$) See [1, lemma 3.1].
(3) ($\Rightarrow$) Suppose $(w, t, z) \in C_d(\mathbb{Q}_p)$. Since $p|d$ we have,

$$-1 \equiv (2n/d)^2 z^4 t^{-4} \pmod p$$

so that $\left(\frac{-1}{p}\right) = 1$. Let $\alpha \in \mathbb{F}_p$ be such that $\alpha^2 \equiv -1 \pmod p$.
Then we have

$$\alpha^2 (2n/d)^{-2} \equiv \left(z^2/t^2\right)^2 \pmod p$$

$$\Rightarrow \quad 1 = \left(\frac{\pm\alpha\,(2n/d)^{-1}}{p}\right) = \left(\frac{\alpha\,(2n/d)^{-1}}{p}\right) \quad \text{since} \quad \left(\frac{-1}{p}\right) = 1$$

Consider two cases. First, suppose $p \equiv 1 \pmod 8$. Then

$$\left(\frac{\alpha}{p}\right) = 1 \Rightarrow \left(\frac{2n/d}{p}\right) = 1 \Rightarrow \left(\frac{n/d}{p}\right) = 1$$

Second, suppose $p \equiv 5 \pmod 8$. We must have $\left(\frac{\alpha}{p}\right) = -1$. Therefore, we have

$$\left(\frac{2}{p}\right) = -1, \quad \left(\frac{\alpha 2^{-1}}{p}\right) = 1, \quad \text{and} \quad \left(\frac{\alpha\,(2n/d)^{-1}}{p}\right) = 1 \quad \text{which implies} \quad \left(\frac{n/d}{p}\right) = 1$$

(4) ($\Rightarrow$) This is clear.
(4) ($\Leftarrow$) Suppose $\left(\frac{d}{p}\right) = 1$. Then there exists an $\alpha \in \mathbb{F}_p$ such that $\alpha^2 \equiv d\ (mod\ p)$. We have,

$$\begin{aligned} dw^2 \equiv t^4\ (mod\ p) \quad &\Leftrightarrow \quad \alpha^2 w^2 \equiv t^4\ (mod\ p) \\ &\Leftrightarrow \quad (\alpha w)^2 \equiv t^4\ (mod\ p) \end{aligned}$$

Hence, $(w_0, t_0, z_0) = (\alpha^{-1}, 1, 0) \in C_d(\mathbb{F}_p)$. Using Hensel's lemma we may lift this solution to a solution in $\mathbb{Q}_p$ (see the argument for (5) below for example).
(5) For $d \equiv 1 \pmod 8$, let $(w_0, t_0, z_0) = (1, 1, 0)$. This is a solution to $C_d \pmod 8$ and we may lift this solution using Hensel's lemma. More explicitly, consider a solution $(w_0, t_0, z_0)$ to $C_d(mod\ 2^k)$ for $k \geq 3$ with $w_0$ odd. This is also a solution to $C_d(mod\ 2^{k-1})$. Let

$$\begin{aligned} w_1 &= w_0 + 2^{k-1} m \\ t_1 &= t_0 + 2^{k-1} s \\ z_1 &= z_0 + 2^{k-1} l \end{aligned}$$

for some integers $m, s$, and $l$. Write, $t_0^4 + \left(\frac{2n}{d}\right)^2 z_0^4 - dw_0^2 = 2^k N$ for some integer $N$. Substituting, we have

$$\begin{aligned} &(t_0 + 2^{k-1}s)^4 + \left(\frac{2n}{d}\right)^2 (z_0 + 2^{k-1}l)^4 - d(w_0 + 2^{k-1}m)^2 \equiv 0 \quad (mod\ 2^{k+1}) \\ \Leftrightarrow \quad & 2^k N - 2^k d w_0 m \equiv 0 \quad (mod\ 2^{k+1}) \\ \Leftrightarrow \quad & N \equiv w_0 m \quad (mod\ 2) \end{aligned}$$

Since $w_0$ is odd, let $m \equiv N w_0^{-1} (mod\ 2)$. Thus, $C_d(\mathbb{Q}_2) \neq \emptyset$.
(6) Suppose $(w', t', z')$ is a solution to $C_d$ over $\mathbb{Q}_2$. Then $(w', t', z')$ is a solution to $C_d \pmod 8$. This gives, $d(w')^2 \equiv (t')^4 \pmod 8$. Therefore, $2|t'$ and $4|w'$. Thus, $(T = t'/2, W = w'/4, z')$ is a solution to

$$\overline{C_d} : dw^2 = t^4 + (m/d)^2 z^4$$

where $m = n/2$. Thus, if $C_d$ has solutions in $\mathbb{Q}_2$ then so does $\overline{C_d}$. We claim that $\overline{C_d}$ has no nontrivial solutions. To see this assume that $(0, 0, 0) \neq (w_0, t_0, z_0) \in \overline{C_d}(\mathbb{Q}_2)$. Note that if

$w_0, t_0, z_0$ are all even then $4|w_0$, so we may divide $w_0$ by 4 and $t_0, z_0$ by 2 and obtain a new solution to $\overline{C_d}$. Thus, we may assume that at least one of $w_0, t_0, z_0$ is odd. However, we note that all solutions to $\overline{C_d} \pmod 8$ have $w, t, z$ all even. Thus, there are no solutions to $\overline{C_d}$ in $\mathbb{Q}_2$. Therefore, there are no solutions to $C_d$ in $\mathbb{Q}_2$ when $d \equiv 5 \pmod 8$.

□

**Lemma 2.4.** *Let $p$ be an odd prime, $n$ an even positive integer with odd prime divisors $\{p_1, \ldots p_s\}$, and $d \in M =< -1, 2, p_1, \ldots p_s > \subseteq \mathbb{Q}^*/(\mathbb{Q}^*)^2$.*

(1) $d \equiv 1 \pmod 2 \implies C'_d(\mathbb{Q}_2) \neq \emptyset$
(2) $d \equiv 0 \pmod 2 \implies C'_d(\mathbb{Q}_2) \neq \emptyset$
(3) *For $p|d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{n/d}{p}\right) = 1$*
(4) *For $p|n/d$, $C'_d(\mathbb{Q}_p) \neq \emptyset \iff \left(\frac{-1}{p}\right) = -1$ or $\left(\frac{d}{p}\right) = 1$*

*Proof.*
For the proofs of (1),(3), and (4) see [1, lemma 5.2].
(2) If $(n/d)^2 \equiv 9 \pmod{16}$, let $(w_0, t_0, z_0) = (2, 1, 1)$. If $(n/d)^2 \equiv 1 \pmod{16}$, let $(w_0, t_0, z_0) = (4, 1, 1)$. These are solutions to $C'_d \pmod{16}$ and we may lift these solutions using Hensel's lemma. More explicitly, consider a solution $(w_0, t_0, z_0)$ to $C'_d(mod\ 2^k)$ for $k \geq 4$ and with $t_0$ odd. $(w_0, t_0, z_0)$ is also a solution to $C'_d(mod\ 2^{k-1})$. Let

$$\begin{aligned} w_1 &= w_0 + 2^{k-1}m \\ t_1 &= t_0 + 2^{k-2}s \\ z_1 &= z_0 + 2^{k-1}l \end{aligned}$$

for some integers $m, s$, and $l$. Write, $t_0^4 - \left(\frac{n}{d}\right)^2 z_0^4 - dw_0^2 = 2^k N$ for some integer $N$. Substituting, we have

$$\begin{aligned} & (t_0 + 2^{k-2}s)^4 + \left(\frac{n}{d}\right)^2 (z_0 + 2^{k-1}l)^4 - d(w_0 + 2^{k-1}m)^2 \equiv 0 \quad (mod\ 2^{k+1}) \\ \Leftrightarrow \quad & 2^k N - 2^k t_0^3 s \equiv 0 \quad (mod\ 2^{k+1}) \\ \Leftrightarrow \quad & N \equiv t_0^3 s \quad (mod\ 2) \end{aligned}$$

Since $t_0$ is odd take $s \equiv N t_0^{-3} (mod\ 2)$. Thus, $C_d(\mathbb{Q}_2) \neq \emptyset$.

□

## 3. Proof of Theorem 1.1

We first establish a correspondence between odd positive elements of $S_n$ with even partitions of $G(n)$.

**Lemma 3.1.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \leq i \leq t$ and $0 \leq j \leq l$ (t,l not both zero). For every even partition, $(V_1, V_2)$ of $V(G(n))$ such that $V_1$ contains no prime factors which are 3 modulo 4 we have $d$ in $S_n$, where*

$$d = \prod_{p \in V_1} p$$

*Proof.* If $t = 0$, $S_n\{1\}$. Suppose $(V_1, V_2)$ is an arbitrary nontrivial even partition of $V(G(n))$ with $V_1$ containing no prime factors which are 3 modulo 4. Let

$$V_1 = \{p_1, \ldots, p_s\} \text{ for some s, } 1 \leq s \leq t$$

then

$$V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$$

Consider $d = p_1 \cdots p_s$. Notice here that $\left(\frac{-1}{p_i}\right) = 1$, thus one of the conditions of lemma 2.1 (2) is satisfied. For any $1 \leq i \leq s$, we have

$$\begin{aligned}
\left(\frac{n/d}{p_i}\right) &= \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\
&= (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\
&= 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is even}
\end{aligned}$$

Therefore, $C_d(\mathbb{Q}_{p_i}) \neq \emptyset$ for $1 \leq i \leq s$ by lemma 2.1 (2).

Also, for $r \in V_2$

$$\begin{aligned}
\left(\frac{d}{r}\right) &= \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\
&= (1)^{\#\{p \in V_1 : \overline{pr} \notin E(G(n))\}} \times (-1)^{\#\{p \in V_1 : \overline{pr} \in E(G(n))\}} \\
&= 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is even}
\end{aligned}$$

Therefore, $C_d(\mathbb{Q}_r) \neq \emptyset$ for $r \in V_2$ by lemma 2.1 (3). There is a point on $C_d$ over $\mathbb{Q}_2$ by lemma 2.1 (4), since $d \equiv 1 \pmod 4$. Therefore, $d \in S_n$.

□

**Remark 3.1.** *Suppose $n$ is squarefree, and $d|n$. If $q \equiv 3 \pmod 4$ and $q|d$ then by lemma 2.1 (2) $d \notin S_n$. That is, a necessary condition for a number to be in $S_n$ is that the number have no prime factors which are 3 modulo 4.*

The next lemma shows that for any odd element, $d$, of the Selmer group, $S_n$, there exists an even partition, $(V_1, V_2)$ of $V(G(n))$, with $V_1$ corresponding to $d$ as in lemma 3.1.

**Lemma 3.2.** *Let $n$ be as in lemma 3.1. Suppose $d$ is odd and $d \in S_n$, by the above remark we may assume $d = p_1 \cdots p_s \in S_n$ for some $s$, $1 \leq s \leq t$, then, letting $V_1 = \{p_1, \ldots p_s\}$ and $V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$, $(V_1, V_2)$ is an even partition of $V(G(n))$.*

*Proof.* Suppose $d = p_1 \cdots p_s$ is a member of $S_n$. By definition,

$$C_d(\mathbb{Q}_p) \neq \emptyset \ \ \forall p|2n \text{ and } C_d(\mathbb{Q}_\infty) \neq \emptyset$$

Using lemma 2.1 (1) we have $d > 0$. From lemma 2.1 (2), for $p|d$, $\left(\frac{n/d}{p}\right) = 1$. Therefore, for $1 \leq i \leq s$

$$\begin{aligned}
1 = \left(\frac{n/d}{p_i}\right) &= \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\
&= (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\
\Rightarrow & \quad \#\{p_i \to V_2\} \quad \text{is even}
\end{aligned}$$

Similarly, Lemma 2.1 (3) gives $\left(\frac{d}{r}\right) = 1$ for $r|2n/d$. So that, for $1 \leq i \leq s$ and $r \in V_2$,

$$\begin{aligned} 1 = \left(\frac{d}{r}\right) &= \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &\Rightarrow \#\{r \to V_1\} \quad \text{is even} \end{aligned}$$

Thus, $(V_1, V_2)$ is an even partition of $V(G(n))$.

$\square$

Now, we will establish a correspondence between the even positive elements of $S_n$ with quasi-even partitions of $G(n)$.

**Lemma 3.3.** *Let* $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ *with* $p_i \equiv 1 \pmod 4$ *and* $q_j \equiv 3 \pmod 4$ *for* $0 \leq i \leq t$ *and* $0 \leq j \leq l$ *(t,l not both zero). For every quasi-even partition,* $(V_1, V_2)$ *of* $V(G(n))$ *such that* $V_1$ *contains no prime factors which are 3 modulo 4 we have* $2d$ *in* $S_n$*, where*

$$d = \prod_{p \in V_1} p$$

*Proof.* Suppose $(V_1, V_2)$ is an arbitrary nontrivial quasi-even partition of $V(G(n))$ with $V_1$ containing no prime factors which are 3 modulo 4. Let

$$V_1 = \{p_1, \ldots, p_s\} \ \text{ for some s, } \ 1 \leq s \leq t$$

then

$$V_2 = \{p_{s+1}, \ldots p_t, q_1, \ldots q_l\}$$

Let $d = p_1 p_2 \cdots p_s$. Consider $2d$. Notice here that $\left(\frac{-1}{p_i}\right) = 1$, thus one of the conditions of lemma 2.1 (2) is satisfied. Suppose $p_i \equiv 1 \pmod 8$. Then

$$\begin{aligned} \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right) \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (1) \times (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &= 1 \times 1 \times 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is quasi-even} \end{aligned}$$

Suppose $p_i \equiv 5 \pmod 8$. Then

$$\begin{aligned} \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right) \prod_{r \in V_2} \left(\frac{r}{p_i}\right) \\ &= (-1) \times (1)^{\#\{r \in V_2 : \overline{p_i r} \notin E(G(n))\}} \times (-1)^{\#\{r \in V_2 : \overline{p_i r} \in E(G(n))\}} \\ &= -1 \times 1 \times -1 = 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is quasi-even} \end{aligned}$$

Therefore, $C_{2d}(\mathbb{Q}_{p_i}) \neq \emptyset$ for $1 \leq i \leq s$ by lemma 2.1 (2).

Also, for $r \in V_2$. If $r \equiv \pm 1 \pmod 8$, then

$$\begin{aligned} \left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right) \prod_{i=1}^{s} \left(\frac{p_i}{r}\right) \\ &= (1) \times (1)^{\#\{p \in V_1 : \overline{pr} \notin E(G(n))\}} \times (-1)^{\#\{p \in V_1 : \overline{pr} \in E(G(n))\}} \\ &= 1 \times 1 \times 1 = 1 \quad \text{since} \quad (V_1, V_2) \quad \text{is quasi-even} \end{aligned}$$

If $r \equiv \pm 3 \pmod 8$, then

$$\begin{aligned}\left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right)\prod_{i=1}^{s}\left(\frac{p_i}{r}\right)\\ &= (-1)\times(1)^{\#\{p\in V_1:\overline{pr}\notin E(G(n))\}}\times(-1)^{\#\{p\in V_1:\overline{pr}\in E(G(n))\}}\\ &= -1\times 1\times -1 = 1 \quad \text{since} \quad (V_1,V_2) \quad \text{is quasi-even}\end{aligned}$$

Therefore, $C_{2d}(\mathbb{Q}_r) \neq \emptyset$ for $r \in V_2$ by lemma 2.1 (3). Note also that $C_{2d}(\mathbb{Q}_2) \neq \emptyset$ by lemma 2.1 (6), since $d \equiv 1 \pmod 4$. Therefore, $2d \in S_n$.

□

**Lemma 3.4.** *Let $n$ be as in lemma 3.3. Suppose $d$ is odd and $2d \in S_n$, by remark 3.1 we may assume $2d = 2\cdot p_1\cdots p_s \in S_n$ for some $s$, $1 \leq s \leq t$. Then, letting $V_1 = \{p_1,\dots p_s\}$ and $V_2 = \{p_{s+1},\dots p_t, q_1\dots q_l\}$, $(V_1,V_2)$ is a quasi-even partition of $V(G(n))$.*

*Proof.* Suppose $2d = 2\cdot p_1\cdots p_s$ is a member of $S_n$. By definition,

$$C_{2d}(\mathbb{Q}_p) \neq \emptyset \ \ \forall p|2n \text{ and } C_{2d}(\mathbb{Q}_\infty) \neq \emptyset$$

Using lemma 2.1 (1) we have $2d > 0$. From lemma 2.1 (2), for $p|d$, $\left(\frac{n/2d}{p}\right) = 1$. Therefore, for $1 \leq i \leq s$. If $p_i \equiv 1 \pmod 8$, then

$$\begin{aligned}1 = \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right)\prod_{r\in V_2}\left(\frac{r}{p_i}\right)\\ &= (1)\times(1)^{\#\{r\in V_2:\overline{p_ir}\notin E(G(n))\}}\times(-1)^{\#\{r\in V_2:\overline{p_ir}\in E(G(n))\}}\\ &\Rightarrow \quad \#\{p_i \to V_2\} \quad \text{is even}\end{aligned}$$

If $p_i \equiv 5 \pmod 8$, then

$$\begin{aligned}1 = \left(\frac{n/2d}{p_i}\right) &= \left(\frac{2}{p_i}\right)\prod_{r\in V_2}\left(\frac{r}{p_i}\right)\\ &= (-1)\times(1)^{\#\{r\in V_2:\overline{p_ir}\notin E(G(n))\}}\times(-1)^{\#\{r\in V_2:\overline{p_ir}\in E(G(n))\}}\\ &\Rightarrow \quad \#\{p_i \to V_2\} \quad \text{is odd}\end{aligned}$$

Similarly, Lemma 2.1 (3) gives $\left(\frac{2d}{r}\right) = 1$ for $r|2n/d$. So that, for $1 \leq i \leq s$ and $r \in V_2$,
If $r \equiv \pm 1 \pmod 8$, then

$$\begin{aligned}1 = \left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right)\prod_{i=1}^{s}\left(\frac{p_i}{r}\right)\\ &\Rightarrow \ \#\{r \to V_1\} \quad \text{is even}\end{aligned}$$

If $r \equiv \pm 3 \pmod 8$, then

$$\begin{aligned}1 = \left(\frac{2d}{r}\right) &= \left(\frac{2}{r}\right)\prod_{i=1}^{s}\left(\frac{p_i}{r}\right)\\ &\Rightarrow \ \#\{r \to V_1\} \quad \text{is odd}\end{aligned}$$

Thus, $(V_1,V_2)$ is a quasi-even partition of $V(G(n))$.

□

Thus far it has been shown, if $n$ is an odd, squarefree, positive integer and $(V_1, V_2)$ is an even partition of $V(G(n))$ such that $V_1$ contains no prime factors which are 3 modulo 4, then $d = \prod_{p \in V_1} p \in S_n$. Moreover, suppose $d$ is odd and $d \in S_n$, then it has been shown that $d$ corresponds to such an even partition of $V(G(n))$. It has also been shown that even elements of $S_n$ are in one to one correspondence with quasi-even partitions of $G(n)$.

**Remark 3.2.** *By lemma 2.1 (3), $S_n$ contains the element 2 if $\left(\frac{2}{p}\right) = 1$ for all $p|n$.*

*Proof of Theorem 1.1* (1) By remark 3.1, we need only consider partititions $(V_1, V_2)$ of $V(G(n))$ for which $V_1$ contains no primes which are congruent to 3 modulo 4 in order to determine the elements of $S_n$. By lemmas 3.1 and 3.2, the odd positive elements of $S_n$ are in one to one correspondence with the even partitions $(V_1, V_2)$ of $G(n)$ for which $V_1$ contains no primes which are congruent to 3 modulo 4. Therefore, the first set appearing in formula one counts the odd positive elements of $S_n$. By lemmas 3.3 and 3.4, the even positive elements of $S_n$ are in one to one correspondence with the quasi-even partitions $(V_1, V_2)$ of $G(n)$ for which $V_1$ contains no primes which are congruent to 3 modulo 4. Therefore, the second set appearing in the formula counts the even positive elements of $S_n$. By lemma 2.1 (1) $S_n$ contains no negative elements.

□

*Proof of Theorem 1.1* (2) If $n \equiv \pm 3 \pmod 8$ or $n \equiv 0 \pmod 2$, then using lemma 2.1 (5) or lemma 2.3 (2), we see $S_n$ contains no even elements. So, preceding as in the proof of (1) yields the result.

□

*Proof of Theorem 1.1* (3) Suppose $n$ contains no prime factors which are $\pm 3$ modulo 8. By remark 3.2, $2 \in S_n$. Therefore, $2d \in S_n$ if and only if $d \in S_n$. To see this, note that if $2, 2d \in S_n$ then $2 \cdot 2d \equiv d \pmod{(\mathbb{Q}^*)^2} \in S_n$. By lemma 2.3 (2), $S_n$ contains no negative elements. Thus, $|S_n|$ is twice the number of odd positive elements which we count as in (1).

□

## 4. Proof of Theorem 1.2

For $S'_n$ we consider three cases: $n \equiv \pm 3 \pmod 8$, $n \equiv \pm 1 \pmod 8$, and $n$ even.

**Lemma 4.1.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 3 \pmod 8$ with $p_i \equiv 1 \pmod 4$ and $q_j \equiv 3 \pmod 4$ for $0 \le i \le t$ and $0 \le j \le l$ (t,l not both zero). Suppose that the partition $(V_1, V_2)$ of $V(g(n))$ is even. Then $d$, $n/d \in S'_n$ where $d = \prod_{p \in V_1} p$ and $n/d = \prod_{p \in V_2} p$.*

*Proof.* Since $n \equiv \pm 3 \pmod 8$, $n$ has an odd number of prime factors which are $\pm 3$ modulo 8. Suppose that $(V_1, V_2)$ is an even partition of $V(g(n))$. Then either $V_1$ or $V_2$ contains an even number of primes which are congruent to $\pm 3$ modulo 8. Without loss of generality, we will assume that $V_1$ contains an even number of primes which are congruent to $\pm 3$ modulo 8. Let $d = \prod_{p \in V_1} p$. We must show that $C'_d(\mathbb{Q}_p) \neq \emptyset$ for $p|2n$.
First, consider the case $p = 2$. We have, $d \equiv \pm 1 \pmod 8$ and lemma 2.2 (3) gives that $C'_d(\mathbb{Q}_2) \neq \emptyset$. We note that for $q|n$, $q \equiv 3 \pmod 4$ $C'_d(\mathbb{Q}_q) \neq \emptyset$, by lemma 2.2 (1) and (2).

Second, consider the case $p|d$. If $p \equiv 1 \pmod 4$ then since $\#\{p \to V_2\} \equiv 0 \pmod 2$ we have

$$\begin{aligned} \left(\frac{n/d}{p}\right) &= \prod_{r \in V_2} \left(\frac{r}{p}\right) \\ &= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} = 1 \end{aligned}$$

For $p|n/d$. If $p \equiv 1 \pmod 4$ then since $\#\{p \to V_1\} \equiv 0 \pmod 2$, we have

$$\begin{aligned} \left(\frac{d}{p}\right) &= \prod_{r \in V_1} \left(\frac{r}{p}\right) \\ &= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} = 1 \end{aligned}$$

Hence, by lemma 2.2 (1) and (2), $d \in S'_n$. A similiar argument shows that $n/d \in S'_n$.

□

**Lemma 4.2.** *Let $n$ be as in lemma 4.1. Suppose $d = p_1 \cdots p_s \cdot q_1 \cdots q_r \in S'_n$ for $0 \le s \le t$ and $0 \le r \le l$. Let $V_1 = \{p_1, \ldots, p_s, q_1, \ldots q_r\}$ and $V_2 = \{p_{s+1}, \ldots p_t, q_{r+1}, \ldots q_l\}$. Then $(V_1, V_2)$ is an even partition of $V(g(n))$.*

*Proof.* By definition, $d \in S'_n$ if

$$C'_d(\mathbb{Q}_p) \neq \emptyset \quad \forall p|2n \text{ and } C'_d(\mathbb{Q}_\infty) \neq \emptyset$$

Since $n \equiv \pm 3 \pmod 8$ one of $d$ or $n/d \equiv \pm 1 \pmod 8$. Without loss of generality, suppose $d \equiv \pm 1 \pmod 8$, then by lemma 2.2 (3), $C'_d(\mathbb{Q}_2) \neq \emptyset$. From lemma 2.2 (1), for $p|d$, if $p \equiv 1 \pmod 4$ and $C'_d(\mathbb{Q}_p) \neq \emptyset$, then $\left(\frac{n/d}{p}\right) = 1$. Thus we have,

$$\begin{aligned} 1 = \left(\frac{n/d}{p}\right) &= \prod_{q \in V_2} \left(\frac{q}{p}\right) \qquad p \in V_1 \\ &= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(g(n))\}} \\ &\Rightarrow \#\{p \to V_2\} \quad \text{is even for} \quad p \in V_1, p \equiv 1 \pmod 4 \end{aligned}$$

Also, Lemma 2.2 (2) gives $\left(\frac{d}{p}\right) = 1$ for $p|n/d$, if $p \equiv 1 \pmod 4$. Then we have,

$$\begin{aligned} 1 = \left(\frac{d}{p}\right) &= (1)^{\#\{r \in V_1 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_1 : \overrightarrow{pr} \in E(g(n))\}} \\ &\Rightarrow \#\{p \to V_1\} \equiv 0 \pmod 2 \text{ for } p \in V_2,\ p \equiv 1 \pmod 4 \end{aligned}$$

Since there are no edges beginning at $q_1, \ldots q_l$, $(V_1, V_2)$ is an even partition of $V(g(n))$.

□

*Proof of Theorem 1.2 (1).* Let $n$ be as in lemma 4.1. By lemma 4.1 we have for *any* even partition of $g(n)$, say $(V_1, V_2)$,

$$\prod_{p \in V_1} p \in S'_n \quad \text{and} \quad \prod_{p \in V_2} p \in S'_n$$

So, by lemma 4.2, odd positive $d \in S'_n$ are in one to one correspondence with even partitions of $V(g(n))$. By lemma 2.2, there are no even elements in $S'_n$. Also, $-1 \in S'_n$, so that $d \in S'_n$ if and only if $-d \in S'_n$. Therefore, $|S'_n| = 2 \cdot \#\{(V_1, V_2) \vdash_e g(n)\}$.

$\square$

**Lemma 4.3.** *Let* $n = p_1 \cdots p_t \cdot q_1 \cdots q_l \equiv \pm 1 \pmod 8$ *with* $p_i \equiv 1 \pmod 4$ *and* $q_j \equiv 3 \pmod 4$ *for* $0 \le i \le t$ *and* $0 \le j \le l$ *(t,l not both zero). If* $(V_1, V_2)$ *is an even partition of* $V(G(-n))$ *then* $\prod_{p \in V_1} p \in S'_n$ *and* $\prod_{p \in V_2} p \in S'_n$*, where* $p$ *is prime or* $-1$.

*Proof.* Suppose we have an even partition, $(V_1, V_2)$, of $V(G(-n))$. Notice that $-1$ is necessarily in one of $V_1$ or $V_2$ so that both $V_1$ and $V_2$ have an even number of primes (counting -1 as a prime) which are $\pm 3 \pmod 8$. This gives $\mathbb{Q}_2$ solutions on $C'_d$ by lemma 2.2 (3), if $d = \prod_{p \in V_1} p$ or $d = \prod_{p \in V_2} p$. We may proceed just as in lemma 4.1 to finish the proof.

$\square$

**Lemma 4.4.** *Let* $n$ *be as in lemma 4.3. If* $d \in S'_n$ *and* $V_1$ *is the set of prime divisors of* $d$ *along with* $-1$*, if* $d < 0$*, then* $(V_1, V_2)$ *is an even partition of* $V(G(-n))$*. Where* $V_2 = V(G(-n)) - V_1$.

*Proof.* Suppose $d \in S'_n$. Let $V_1$ be the set of prime divisors of $d$ along with $-1$, if $d < 0$. Let $V_2$ be the set of prime divisors of $n/d$ along with $-1$, if $d > 0$. Since $d \in S'_n$, $C'_d(\mathbb{Q}_2) \neq \emptyset$. Thus, $d \equiv \pm 1 \pmod 8$ or $n/d \equiv \pm 1 \pmod 8$, by lemma 2.2. Thus, $V_1$ and $V_2$ contain an even number of primes (counting -1 as a prime) which are $\pm 3$ modulo 8, since $n \equiv \pm 1 \pmod 8$. Therefore, $\#\{-1 \to W\} \equiv 0 \pmod 2$, where $W = V_1$ or $V_2$ is the set not containing $-1$. If $p \equiv 1 \pmod 4$ and $p|d$, then Lemma 2.2 (2) gives $\left(\frac{n/d}{p}\right) = 1$. Thus,

$$\begin{aligned} 1 = \left(\frac{n/d}{p}\right) &= \prod_{r \in V_2} \left(\frac{r}{p}\right) \\ &= (1)^{\#\{r \in V_2 : \overrightarrow{pr} \notin E(G(-n))\}} \times (-1)^{\#\{r \in V_2 : \overrightarrow{pr} \in E(G(-n))\}} \\ &\Rightarrow \#\{p \to V_2\} \equiv 0 \pmod 2 \end{aligned}$$

If $p \equiv 1 \pmod 4$ and $p|n/d$, then Lemma 2.2 (2) gives $\left(\frac{d}{p}\right) = 1$. Thus,

$$\begin{aligned} 1 = \left(\frac{d}{p}\right) &= (1)^{\#\{r \in V_1 : \overrightarrow{pr} \notin E(g(n))\}} \times (-1)^{\#\{r \in V_1 : \overrightarrow{pr} \in E(g(n))\}} \\ &\Rightarrow \#\{p \to V_1\} \equiv 0 \pmod 2 \text{ for } p \in V_2,\ p \equiv 1 \pmod 4 \end{aligned}$$

Since there are no edges beginning at $q_1, \ldots q_l$, $(V_1, V_2)$ is an even partition of $V(G(-n))$.

$\square$

*Proof of Theorem 1.2 (2).* Even partitions of $V(G(-n))$ are in one to one correspondence with the odd elements of $S'_n$, by lemma 4.3 and lemma 4.4. By lemma 2.2 (4) there are no even elements.

$\square$

**Lemma 4.5.** *Let* $n = 2 \cdot p_1 \cdots p_t \cdot q_1 \cdots q_l$ *with* $p_i \equiv 1 \pmod 4$ *and* $q_j \equiv 3 \pmod 4$ *for* $0 \le i \le t$ *and* $0 \le j \le l$ *(t,l not both zero). Suppose that the partition* $(V_1, V_2)$ *of* $V(G'(n))$ *is even. Then* $d$, $n/d \in S'_n$ *where* $d = \prod_{p \in V_1} p$ *and* $n/d = \prod_{p \in V_2} p$.

*Proof.* The proof of this result is identical to the proof of lemma 4.1.

□

**Lemma 4.6.** *Let $n$ be as in lemma 4.5. If $d \in S'_n$ and $V_1$ is the set of prime divisors of $d$ (along with 2, if $d \equiv 0 \pmod 2$), then $(V_1, V_2)$ is an even partition of $V(G'(n))$. Where $V_2 = V(G'(n)) - V_1$.*

*Proof.* The proof of this result is identical to the proof of lemma 4.2.

□

*Proof of Theorem 1.2 (3).* The previous two lemmas give a one to one correspondence between even partitions of $V(G'(n))$ and positive elements of $S'_n$. Since $-1$ is necessarily in $S'_n$, we multiply the number of even partitions of $V(G'(n))$ by 2.

□

## 5. Graph Theory and Linear Algebra

**Definition 5.1.** *Let $G$ be a graph, with vertex set*

$$V(G) = \{v_1, \dots v_s\}$$

*and edge set, $E(G)$. The adjacency matrix of $G$ is defined by*

$$A(G) = (a_{ij})_{1 \le i,j \le s}$$

*where*

$$a_{ij} = \begin{cases} 1 & \textit{if } \overrightarrow{v_i v_j} \in E(G) \ (1 \le i \ne j \le s) \\ 0 & \textit{otherwise} \end{cases}$$

Let

$$d_i = \sum_{j=1}^{s} a_{ij} \quad \text{(out degree of vertex } v_i \quad (1 \le i \le s))$$

**Definition 5.2.** *The Laplace matrix of $G$ is defined by*

$$L(G) = diag(d_1, \cdots, d_s) - A(G)$$

In [1], Feng and Xiong showed,

**Lemma 5.1.** *(Feng and Xiong* [1, lemma 2.2]*) The number of even partitions of $V(G)$ is $2^{s-R}$, where $R = \mathrm{rank}_{\mathbb{F}_2} NS(L(G))$.*

**Lemma 5.2.** *Suppose a graph $G$ has vertex set, $V(G) = \{q_1, \dots q_s, p_{s+1}, \dots p_t\}$. Futhermore, suppose that $L(G) \in \mathbb{F}_2^{t \times t}$ is given by*

$$\begin{array}{c} \\ q_1 \\ q_2 \\ \vdots \\ q_s \\ p_{s+1} \\ \vdots \\ p_t \end{array} \begin{array}{c} \begin{array}{ccccccc} q_1 & q_2 & \dots & q_s & p_{s+1} & \dots & p_t \end{array} \\ \begin{pmatrix} * & * & \dots & * & * & \dots & * \\ * & * & \dots & * & * & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ * & * & \dots & * & * & \dots & * \\ * & * & \dots & * & * & \dots & * \\ \vdots & \vdots & \dots & \vdots & \vdots & \dots & \vdots \\ * & * & \dots & * & * & \dots & * \end{pmatrix} \end{array}$$

*and let $l_k$ denote the $k-th$ column of $L(G)$, then*

$$\#\{(V_1,V_2)\vdash_e V(G)|q_i\notin V_1, 0\leq i\leq s\}=2^{(t-s)-R}$$

*where*

$$R=\mathrm{rank}_{\mathbb{F}_2}[l_{s+1}|l_{s+2}|\cdots|l_t]$$

*Proof.* We wish to count even partitions, $(V_1,V_2)$, such that $q_i\notin V_1$ for $0\leq i\leq s$. Define $v(V_1)=[g_1\dots g_s\ g_{s+1}\dots g_t]^T$, by

$$g_k=\begin{cases}1 & \text{if } q_k\in V_1\ 1\leq k\leq s\\ 0 & \text{if } q_k\notin V_1\ 1\leq k\leq s\\ 1 & \text{if } p_k\in V_1\ s+1\leq k\leq t\\ 0 & \text{if } p_k\notin V_1\ s+1\leq k\leq t\end{cases}$$

Following Feng and Xiong we see, $(V_1,V_2)\vdash_e V(G)$ if and only if $v(V_1)\in NS(L(G))$. Write $L(G)=[L_1\ L_2]$ where $L_1$ [resp. $L_2$] represents the columns corresponding to $q_j$ for $1\leq j\leq s$ [resp. $p_i$ for $s+1\leq i\leq t$]. Let $v(V_1)=\begin{bmatrix}v_1(V_1)\\ v_2(V_1)\end{bmatrix}$, where $v_1(V_1)$ [resp. $v_2(V_1)$] corresponds to $q_j$ for $1\leq j\leq s$ [resp. $p_i$ for $s+1\leq i\leq t$]. We may then write

$$\begin{aligned}L(G)v(V_1) &= [L_1\ L_2]\begin{bmatrix}v_1(V_1)\\ v_2(V_1)\end{bmatrix}\\ &= \sum_{k=1}^{t} g_k\cdot l_k\\ &= \sum_{k=1}^{s} 0\cdot l_k+\sum_{k=s+1}^{t} g_k\cdot l_k = L_2v_2(V_1)\end{aligned}$$

So $L(G)\cdot v(V_1)=0\Leftrightarrow v_2(V_1)\in NS(L_2)$.
For similiar reasons, we have

**Lemma 5.3.** *Let $\{p_1\cdots p_t\cdot q_1\cdots q_l\}$ be the odd prime factors of $n$ with $p_i\equiv 1 \pmod 4$ and $q_j\equiv 3 \pmod 4$ for $0\leq i\leq t$ and $0\leq j\leq l$. Let $r_k$ be the prime dividing $n$ corresponding to the $k^{th}$ row of $L(G(n))$. We construct $b\in\mathbb{F}_2^{t+l}$ in the following way.*

$$b(k)=\begin{cases}0 & \textit{if } r_k\equiv\pm 1 \pmod 8\\ 1 & \textit{if } r_k\equiv\pm 3 \pmod 8\end{cases}$$

*If $L(G(n))x=b$ is solvable, then $x$ corresponds to a quasi-even partition of $V(G(n))$ and solutions to $L(G(n))x=b$ and $L(G(n))x=0$ are in one to one correspondence. Hence, if $L(G(n))x=b$ is solvable, then*

$$\#\{(V_1,V_2)\vdash_{qe} V(G(n))|q_j\notin V_1, 0\leq j\leq l\}=2^{t-R}$$

*where*

$$R=\mathrm{rank}_{\mathbb{F}_2}[l_1|l_2|\cdots|l_t]$$

*On the other hand, if $L(G(n))x=b$ is not solvable, then there are no quasi-even partitions of $V(G(n))$.*

With the above lemmas we may now compute the selmer groups, $S_n$ and $S'_n$, using linear algebra. The following corollaries follow from theorems 1.1 and 1.2.

**Corollary 5.1.** *Let $n > 1$ be squarefree and let $L(G(n))$, $R$, and $b$ be as above. Then,*

(1) *If $n \equiv \pm 3 \pmod 8$ or $n \equiv 0 \pmod 2$, then*

$$|S_n| = 2^{t-R}$$

(2) *If $n \equiv \pm 1 \pmod 8$ and $\exists\, p|n$, $p \equiv \pm 3 \pmod 8$, then*

$$|S_n| = \begin{cases} 2^{t-R+1} & \text{if } L(G(n))x = b \text{ is solvable} \\ 2^{t-R} & \text{otherwise} \end{cases}$$

(3) *If $p_i \equiv 1 \pmod 8$ for all $0 \le i \le t$ and $q_j \equiv 7 \pmod 8$ for all $0 \le j \le l$, then*

$$|S_n| = 2^{t-R}$$

**Corollary 5.2.** *Let $n = p_1 \cdots p_t \cdot q_1 \cdots q_l$, as before. Then,*

(1) *If $n \equiv \pm 3 \pmod 8$, then*

$$|S'_n| = 2^{t+l-\mathrm{rank}_{\mathbb{F}_2}\mathrm{L(g(n))}+1}$$

(2) *If $n \equiv \pm 1 \pmod 8$, then*

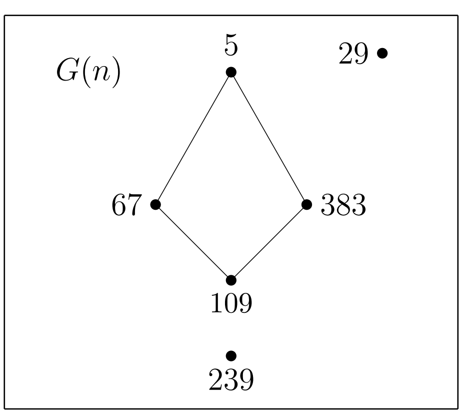
$$|S'_n| = 2^{t+l-\mathrm{rank}_{\mathbb{F}_2}\mathrm{L(G(-n))}}$$

(3) *If $n \equiv 0 \pmod 2$, then*

$$|S'_n| = 2^{t+l-\mathrm{rank}_{\mathbb{F}_2}\mathrm{L(G'(n))}+1}$$

## 6. An Example

Let $n = 67 \cdot 383 \cdot 239 \cdot 5 \cdot 29 \cdot 109$ and notice $n \equiv (3)(7)(7)(5)(5)(5) \equiv 7 \pmod 8$. By lemma 2.1 $S_n$ contains only odd positive elements. Thus, by theorem 1.1 the elements of $S_n$ are in one to one correspondence with the even partitions, $(V_1, V_2)$ of $G(n)$ for which $V_1$ contains no primes which are 3 modulo 4. Such even partitions of $G(n)$ are given below.




$(\{29\}, \{5, 109, 67, 383, 239\})$
$(\{5, 109\}, \{29, 67, 383, 239\})$
$(\{5, 29, 109\}, \{67, 383, 239\})$
$(\emptyset, \{5, 29, 109, 67, 383, 239\})$

$$L(G(n)) = \begin{array}{c|cccccc} & 67 & 383 & 239 & 5 & 29 & 109 \\ \hline 67 & 0 & 0 & 0 & 1 & 0 & 1 \\ 383 & 0 & 0 & 0 & 1 & 0 & 1 \\ 239 & 0 & 0 & 0 & 0 & 0 & 0 \\ 5 & 1 & 1 & 0 & 0 & 0 & 0 \\ 29 & 0 & 0 & 0 & 0 & 0 & 0 \\ 109 & 1 & 1 & 0 & 0 & 0 & 0 \end{array}$$

Here $\dim(NS([\ l_4 \mid l_5 \mid l_6\ ])) = 2$, so that

$$\begin{aligned} |S_n| &= \#\{(V_1, V_2) \vdash_e V(G(n)) \mid q_i \notin V_1,\ 1 \le i \le s\} \\ &= 2^2 \end{aligned}$$

Notice that a basis for $NS([\ l_4 \mid l_5 \mid l_6\ ])$ is

$$\left\{ \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\}$$

Let $v_1 = [1, 0, 1]^t$ and $v_2 = [0, 1, 0]^t$ and define

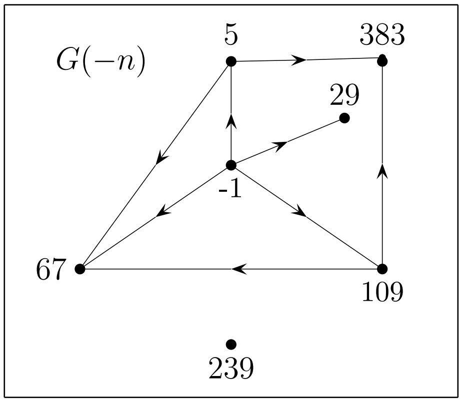
$$n(v_i) = \prod_{j=1}^{3} p_j^{v_i[j]}$$

where $p_1 = 5$, $p_2 = 29$, and $p_3 = 109$. Then $n(v_1) = 5^1 \times 29^0 \times 109^1$ and $n(v_2) = 5^0 \times 29^1 \times 109^0$. Finally, observe that

$$S_n = < n(v_1), n(v_2) > .$$

Thus, our basis for $NS([\ l_4 \mid l_5 \mid l_6\ ])$ corresponds in a natural way to generators of $S_n$.

By lemma 2.2 $S'_n$ contains only odd elements. Thus, by theorem 1.2 the elements of $S'_n$ are in one to one correspondence with the even partitions, $(V_1, V_2)$ of $G(-n)$. The graph, $G(-n)$ is given below.




$$L(G(-n)) = \begin{array}{c} \\ 67 \\ 383 \\ 239 \\ 5 \\ 29 \\ 109 \\ -1 \end{array} \begin{array}{c} \begin{array}{ccccccc} 67 & 383 & 239 & 5 & 29 & 109 & -1 \end{array} \\ \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Here $\dim(NS(L(G(-n)))) = 5$, so that

$$\begin{aligned} |S'_n| &= \#\{(V_1, V_2) \vdash_e V(G(-n))\} \\ &= 2^5 \end{aligned}$$

Notice that a basis for $NS(L(G(-n)))$ is

$$\left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \right\}$$

Let

$$\begin{aligned} v_1 &= [1,1,0,1,0,0,0]^t \\ v_2 &= [1,1,0,0,1,0,0]^t \\ v_3 &= [1,1,0,0,0,1,0]^t \\ v_4 &= [0,0,0,0,0,0,1]^t \\ v_5 &= [0,0,1,0,0,0,0]^t. \end{aligned}$$

Define

$$n(v_i) = \prod_{j=1}^{7} p_j^{v_i[j]}$$

where $p_1 = 67$, $p_2 = 383$, $p_3 = 239$, $p_4 = 5$, $p_5 = 29$, $p_6 = 109$, and $p_7 = -1$. Then

$$\begin{aligned} n(v_1) &= 67^1 \times 383^1 \times 239^0 \times 5^1 \times 29^0 \times 109^0 \times -1^0 \\ n(v_2) &= 67^1 \times 383^1 \times 239^0 \times 5^0 \times 29^1 \times 109^0 \times -1^0 \\ n(v_3) &= 67^1 \times 383^1 \times 239^0 \times 5^0 \times 29^0 \times 109^1 \times -1^0 \\ n(v_4) &= 67^0 \times 383^0 \times 239^0 \times 5^0 \times 29^0 \times 109^0 \times -1^1 \\ n(v_5) &= 67^0 \times 383^0 \times 239^1 \times 5^0 \times 29^0 \times 109^0 \times -1^0 \end{aligned}$$

Finally, observe that

$$S'_n =< n(v_1), \dots n(v_5) > .$$

Thus, our basis for $NS(L(G(-n))$ corresponds in a natural way to generators of $S'_n$.

## References


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

[2] Heath-Brown, D. R., The size of Selmer groups for the congruent number problem. Invent. Math. 111 (1993), no. 1, 171–195.

[3] Heath-Brown, D. R., The size of Selmer groups for the congruent number problem. II. Invent. Math. 118 (1994), no. 2, 331–370

[4] James, Kevin; Ono, Ken, Selmer groups of quadratic twists of elliptic curves. Math. Ann. 314 (1999), no. 1, 1–17.

[5] Yu, Gang, Average size of 2-Selmer groups of elliptic curves, II, Acta Arith. 117 (2005), no. 1, 1-33

[6] J. Silverman *The Arithmetic of elliptic curves*, Grad. Texts in Math. 106, Springer, 1986



Department of Mathematical Sciences, Clemson University BOX 340975 Clemson, SC 29634-0975, USA

Department of Mathematical Sciences, Clemson University BOX 340975 Clemson, SC 29634-0975, USA

*E-mail address*: blfaulk@clemson.edu

*E-mail address*: kevja@clemson.edu

*URL*: <http://www.math.clemson.edu/~kevja/>