TRIVIAL SELMER GROUPS AND EVEN PARTITIONS OF A GRAPH

ABSTRACT. For a square-free number $n = p_1 p_2 \dots p_k$ Feng and Xiong in [FX] give a way to construct a corresponding graph on k-vertices and then give necessary and sufficient conditions on these graphs for the integers n to determine when the elliptic curve $E_n : y^2 = x^3 - n^2 x$ has trivial 2-Selmer groups. These conditions involve understanding when a graph is *even*. In this note we give a substantial understanding when graphs are even. Our main results count the number of square-free n less than X such that the 2-Selmer groups are trivial ($S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$).

1. INTRODUCTION

Let n be a square free integer then n is a congruent number if it is the area of a rational right triangle. For example, 6 is a congruent number since it is the area of the right triangle with side lengths 3, 4, and 5. Also, 3 is a congruent number since 3 is the area of the right triangle with side lengths 3/2, 4/2, and 5/2. Determining what n are congruent numbers is an old problem studied by many mathematicians. In [K] it is shown that n is a noncongruent number if and only if the rank of the group $E_n(Q)$ of rational points on the elliptic curve $E_n : y^2 = x^3 - n^2 x$ is zero. Furthermore, it is known that if the 2-Selmer groups are $S_n = Sel_2(E_n(Q)) = \{1\}$ and $S'_n = Sel_2(E'_n(Q)) = \{\pm 1, \pm n\}$ then the rank of the curve E_n is zero. Hence n is a noncongruent number if the 2-Selmer groups are trivial. Feng and Xiong give in graph theory language necessary and sufficient conditions for the 2-Selmer groups of E_n to have this form.

To solve the problem of when the elliptic curves $E_n : y^2 = x^3 - n^2 x$ have trivial Selmer groups Feng and Xiong in [FX] introduce the idea of an even partition of a graph. If G is a graph on k vertices with edge set E and vertex set V, then a partition of G is a pair of sets S and T such that $S \cap T = \emptyset$ and $S \cup T = V$. (Furthermore, we consider the partitions (S, T) and (T, S) to be the same partition.) Additionally, we say that a vertex v is a neighbor of w if $\overrightarrow{wv} \in E(G)$. A partition (S, T) is *even* if all $v \in S$ have an even number of neighbors in T and all $v \in T$ have an even number of neighbors in S. For example, the partition $(G, \emptyset)$ is always an even partition. We call this the trivial partition. The graph G is called *even* if there is a nontrivial even partition of its vertices and it is it odd if there is only the trivial even partition of its vertices.

1.1. **Some Examples.** There are many examples of odd and even graphs. It is easy to see that if G is a disconnected graph then the partition of the vertices into seperate disconnected components is an even partition. Therefore, all disconnected graphs are even. On the other hand, there exist many connected graphs that are also even. For example, the complete graph on 4 vertices, K_4, is an even graph. Consider the partition $(\{v_1, v_2\}, \{v_3, v_4\})$. This partition is even since each vertex has two neighbors in the other set. In fact, K_{2n} is an even graph for all n. The partition $(\{v_1, v_2\}, \{v_3, \dots, v_{2n}\})$ is an even partition of K_{2n}.

Date: December 6, 2004.

On the other hand K_{2n+1} is an odd graph for all $n \geq 1$. Let (S,T) be an arbitrary nontrivial partition of $V(K_{2n+1})$. Then one of S or T must have an odd number of vertices in it. Without loss of generality suppose S has an odd number of vertices in it. Then all $v \in T$ have an odd number of neighbors in S. Hence all no nontrivial partitions of K_{2n+1} are even. So K_{2n+1} is an odd graph.

Additionally all undirected cycles on an even number of vertices are even. Let C_{2n} be a cycle on $2n$ vertices $v_1, \ldots, v_{2n}$ with $E(C_{2n}) = \{\overline{v_1v_2}, \ldots, \overline{v_{2n}v_1}\}$. Let $S = \{v_1, v_3, \ldots, v_{2n-1}\}$ and $T = \{v_2, v_4, \ldots, v_{2n}\}$. Then every vertex in S is adjacent to exactly two vertices in T and every vertex in T is adjacent to exactly two vertices in S.

In section 2 we discuss the results of Feng and Xiong. Once we understand what kinds of graphs come up in their paper we begin our discussion of how many graphs are even and when they are even how many even partitions they have. In section 4 we treat the very general cases of directed graphs. We compute the probability, assuming each graph appears with equal probability, that a graph on k vertices is odd. Furthermore, for any m we count how many graphs on k vertices have exactly m even partitions.

While calculating the probability that a graph on k vertices is odd we assume that each graph appears equally often. In section **??** we will prove that this is indeed what happens for graphs that are derived from the congruent number curves. Finally we count the number of square free integers $n \equiv a(\mod 8)$ less than X such that $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$. These results are presented section 6.

2. Congruent numbers and Selmer Groups

The next three theorems appear as Theorem 2.4, 2.5 and 2.6 in [FX]. We list them here because the derived graphs that appear in each of the theorems will be the focus of this paper.

Before we can state the theorems we will need to define a construction of a graph. For a square-free integer $n = p_1 \ldots p_t$ define the directed graph $G(n)$ by

$$V(G(n)) = \{p_1, \ldots, p_t\} \quad \text{and} \quad E(G(n)) = \{\overrightarrow{p_ip_j} : \left(\frac{p_i}{p_j}\right) = -1, 1 \leq i \neq j \leq t\}.$$

Theorem 2.1. *Suppose that $n \equiv \pm 3(\mod 8)$. Then $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$ if and only if the following three conditions are satisfied:*
(i) $n \equiv 3(\mod 8)$
(ii) $n = p_1 \ldots p_t$, $p_1 \equiv 3(\mod 4)$ and $p_j \equiv 1(\mod 4)$ $(2 \leq j \leq t)$.
(iii) $G(n)$ is an odd graph.

Assuming the first two conditions, we see that at most one of the prime factors of n is 3 modulo 4. Thus using the law of quadratic reciprocity, $G(n)$ must be a non-directed graph. Additionally by using the Dirichlet theorem on primes in an arithmetic progression and induction on the number of primes, we can see that for any undirected graph G there exist infinitely many n such that $G(n) = G$. We later show that not only does each graph on k vertices appear infinitely often, but each graph appears with equal probability. More precisely, if we consider all graphs derived from $n < X$, $n \equiv 3(\mod 4)$, and n has k prime factors then as X tends to infinity each of the 2^k graphs on k vertices occurs equally often as the others.

In section 4 we give the probability that a graph on k vertices is an odd graph. In section 6 we apply this result to count the $n \equiv 3(\mod 8)$ that give trivial Selmer groups.

For the case $n \equiv \pm 1(\mod 4)$ Feng and Xiong define a second graph $G(-n)$. Let $n = p_1 \dots p_t q_1 \dots q_s$ where $p_j \equiv 1(\mod 4)$ and $q_j \equiv 3(\mod 4)$. The graph $G(-n)$ is defined by

$$\begin{aligned} V(G(-n)) =& \{p_1, \dots, p_t, q_1, \dots, q_s\} \\ E(G(-n)) =& \{\overline{p_i p_j} : \left(\frac{p_j}{p_i}\right) = -1, 1 \le i \ne j \le t\} \\ & \cup \{\overrightarrow{p_i q_j} : \left(\frac{q_j}{p_i}\right) = -1, 1 \le i \le t, 1 \le j \le s\} \\ & \cup \{\overrightarrow{(-1) r} : r \in \{p_1, \dots, p_t, q_1, \dots, q_s\}, r \equiv \pm 3(\mod 8)\} \end{aligned}$$

Theorem 2.2. *Suppose that $n \equiv \pm 1(\mod 8)$. Then $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$ if and only if the following three conditions are satisfied:*
(i) $n \equiv 1(\mod 8)$
(ii) n has one of the following decompositions:

$$n = p_1 \dots p_r P_1 \dots P_s Q_1 Q_2; \tag{2.1}$$

$$n = p_1 \dots p_r P_1 \dots P_t q_1 q_2; \tag{2.2}$$

$$n = p_1 \dots p_r P_1 \dots P_l Q_1 q_1; \tag{2.3}$$

where $p_i \equiv 1, P_j \equiv 5, Q_i \equiv 3, q_j \equiv 7(\mod 8)$ and

$$r \ge 0, \ \ 2|s \ge 0 \ \ 2|t \ge 2 \ \ 2 \nmid l \ge 1.$$

(iii) $G(-n)$ has only one non-trivial even partition, namely $\{-1\}$ and $V \setminus \{-1\}$.

Again in the case of the each of the decomposition listed in the theorem we can use Dirichlet's theorem on primes in an arithmetic progression to show that each of the allowable graphs appear infinitely often. This is done by first characterizing what the graphs for each decomposition must look like and then using Dirichlet's theorem showing that each of those graphs must appear infinitely often.

In section 4 we show that every graph that can appear, appears equally likely. In section 6 we give the number of n such that $G(-n)$ has exactly one non-trivial partition. Thus we give the number of $n \equiv \pm 1(\mod 8)$ that have trivial 2-Selmer groups.

The final case to consider is when $2||n$. In this case we define a third graph $G'(n)$. Let $n = 2p_1 \dots p_t q_1 \dots q_s$ where $p_j \equiv 1(\mod 4)$ and $q_j \equiv 3(\mod 4)$. The graph $G'(n)$ is defined by

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

It is worth noting that $\left(\frac{2}{p_i}\right) = -1$ if and only if $p_i \equiv 5(\mod 8)$.

We now have the final of the three main theorems given in [FX]

Theorem 2.3. *Suppose that $2||n$ and n has the decomposition given above. Then $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$ if and only if the graph $G'(n)$ is odd. Furthermore, if $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$ then $s = 0$ and there exists at least one i such that $p_i \equiv 5(\mod 8)$.*

Due to the second part of the theorem we only consider n such that $n = 2p_1 \dots p_t$ where each $p_j \equiv 1(\mod 4)$. In section 4 we show that each graph appears equally likely. In section 6 for a fixed t we count the number of n such that E_n has trivial Selmer group.

3. Matrix Representations

In this section we determine the probability that a random graph is odd. To determine whether or not a graph is even and also to count the number of odd graphs on n vertices it will be useful to represent the graphs in terms of a matrix. The adjacency matrix is defined by $A(G) = (a_{ij})_{1\le i,j\le k}$, where $a_{ij} = 1$ if $\overrightarrow{v_iv_j} \in E(G)$ and $a_{ij} = 0$ otherwise. For us it will be more convenient to work with the Laplace matrix of G. The Laplace matrix is defined by $L(G) = (l_{ij})_{1\le i,j\le k}$, where $l_{ij} = a_{ij}$ if $i \neq j$ and $l_{jj} = 1$ if v_j has an odd number of neighbors and $l_{jj} = 0$ if v_j has an even number of neighbors. We could have also defined $l_{jj} \equiv \sum_{n=1}^{k} a_{jn} \equiv \sum_{n\neq j} l_{jn} \pmod 2$.

It is worth noting that when the graph is undirected the matrices $A(G)$ and $L(G)$ are symmetric.

The following Theorem allows us to use this matrix representation to tell whether or not a partition is an even partition. Let (S, T) be a partition. Then we define the vector $\vec{v}(S) = (g_j)_{1\le j\le k}$ by $g_j = 1$ if $v_j \notin S$ and $g_j = 0$ if $v_j \in S$.

Theorem 3.1. *The partition (S, T) of $V(G)$ is even if and only if $L(G)\vec{v}(S) = \vec{0}$.*

Proof. Say $b = L(G)\vec{v}(S) \in \mathbb{Z}_2^k$ and $b = (b_1, \dots, b_n)$. Then we have

$$\begin{aligned} b_j &= \sum_{i=1}^{k} g_i l_{ji} \\ &= l_{jj}g_j + \sum_{i=1}^{k} g_i a_{ji} \\ &= g_j \sum_{i=1}^{k} a_{ji} + \sum_{i=1}^{k} g_i a_{ji} \\ &= \sum_{i=1}^{k} (g_i + g_j) a_{ji}. \end{aligned}$$

If $v_j \notin S$, then $g_j = 1$ and we have $b_j = \sum_{i=1}^{k} (g_i + 1)a_{ji}$. Since $(g_j + 1)a_{ji} = 1$ if and only if $v_i \in S$ and $\overrightarrow{v_jv_i} \in E$, $\sum_{i=1}^{k} (g_i + 1)a_{ji}$ counts the number of neighbors of v_j in S. So b_j, which is either 0 or 1, is 0 if and only if v_j has an even number of vertices in S.

Similarly, if $v_j \in S$, then $g_j = 0$ and we have $b_j = \sum_{i=1}^{k} g_i a_{ji}$. But, $\sum_{i=1}^{k} g_i a_{ji}$ counts the number of edges from v_j to T, since $g_i a_{ji} = 1$ if and only if $v_i \in T$ and $\overrightarrow{v_jv_i} \in E$. So b_j, is 0 if and only if there are an even number of edges from v_j to T.

Since $L(G)\vec{v}(S) = \vec{0}$ if and only if $b_j = 0$ for each j, $L(G)\vec{v}(S) = \vec{0}$ if and only if S is an even partition. □

Notice, the matrix $L(G)$ is constructed so that the sum of its rows is 0. This fact in combination with Theorem 3.1 gives us a proof that the trivial partition $(G, \emptyset)$ is always even. Furthermore, the rank of $L(G)$ is at most $k-1$, since the vector $(1, 1, \cdots, 1)$ is in the nullspace.

With this condition we now have the following theorem which appears as Lemma 2.2 in [FX]. We prove this theorem for completeness.

Theorem 3.2. *Let $G = (V, E)$ be a directed graph, $k = |V|$ and $r = rank_{\mathbb{Z}_2} L(G)$. Then the total number of even partitions of V is 2^{k-r-1}. Particularly, G is an odd graph if and only if $r = k-1$.*

In particular, we see that the number of even partitions must be a power of 2.

Recall that we counted the partitions (S, T) and (T, S) as being the same partition, thus we obtain 2^{k-r-1} in the previous theorem. Had we counted these partitions as distinct we would obtain 2^{k-r} partitions.

Proof. Since we consider (S, T) and (T, S) to be the same partition there is a 2-to-1 correspondence between the vectors in Z_2^k and the partitions of $V(G)$. Namely, the two vectors $(g_1, \ldots, g_k)$ and $(g_1 + 1, \ldots, g_k + 1)$ correspond to the partition (S, T), where $S = \{v_j : g_j = 0,\ 1 \leq j \leq k\}$.

Therefore by Theorem 3.1 the number of even partitions is $\frac{1}{2}\#\{\vec{v} \in Z_2^k : L(G)\vec{v} = 0\} = \frac{1}{2}2^{k-r} = 2^{k-r-1}$, as desired. □

As a result of Theorem 3.2, if we want to know how many graphs on k vertices have 2^m even partitions it is enough to determine how many such $L(G)$ have rank $k-m-1$. In particular, to determine the number of odd graphs on k vertices it is enough to determine the number of $L(G)$ that have rank $k-1$.

In the next section, we determine the number of graphs on k vertices with 2^m partitions for all k and m. In the next section we determine the number of such graphs for undirected graphs.

4. Undirected Graphs

We will look at the matrix $L(G)$ and discuss when it has rank $k-1$. To do this calculation we will use the following Lemma to reduce the problem to a different problem.

Lemma 4.1. *Let G be an undirected graph on k vertices. Let $L(G)$ be defined as above. Then $L(G)$ will have rank r if and only if the matrix $L^*(G) = (l_{ij})_{1 \leq i,j \leq k-1}$ has rank r.*

Proof. Let the columns of $L(G)$ be $c_1, \ldots, c_k$. It is clear that c_k is a linear combination of $c_1, \ldots, c_{k-1}$ since by definition all of the rows of the matrix $L(G)$ sum to 0. Say that $c_j = (c_{j,1}, \ldots, c_{j,k})$ and let $w_j = \big(c_{j,1}, \ldots, c_{j,(k-1)}\big)$. So $w_1, \ldots, w_{(k-1)}$ are the column vectors of L^*. We set $w_{j,i} = c_{j,i}$.

We show that for any set $\{m_1, \ldots, m_j\} \subset \{1, \cdots, k-1\}$, $\{w_{m_1}, \ldots, w_{m_j}\}$ is a linearly independent set if and only if $\{c_{m_1}, \ldots, c_{m_j}\}$ is a linearly independent set. This condition guarantees that $L(G)$ has rank r if and only if L^* has rank r.

It remains to show that $\{w_{m_1}, \ldots, w_{m_j}\}$ is linearly independent if and only if $\{c_{m_1}, \ldots, c_{m_j}\}$ is linearly independent. We show a slightly stronger result, namely, $\sum_{i=1}^{j} a_i w_{m_i} = \vec{0}$ if and only if $\sum_{i=1}^{j} a_i c_{m_i} = \vec{0}$, for some $a_k \in \mathbb{Z}_2$.

The converse direction is clearly true since each w_{m_i} is c_{m_i} with the last slot in the vector left out. Now, suppose that $\sum_{i=1}^{j} a_i w_{m_i} = \vec{0}$. Then $\sum_{i=1}^{j} a_i w_{m_i,s} = 0$ for each $s \in \{1, \ldots, k-1\}$. Using the fact that $c_{m_i,s} = w_{m_i,s}$ for $s \in \{1, \ldots, k-1\}$ we obtain $\sum_{i=1}^{j} a_i c_{m_i,s} = 0$ for $s \in \{1, \ldots, k-1\}$. It remains to show that $\sum_{i=1}^{j} a_i c_{m_i,k} = 0$. However using the fact that the matrix is symmetric and that the sum of first $(k-1)$ columns is the k^{th} column we have,

$$\begin{aligned}\sum_{i=1}^{j} a_i c_{m_i,k} &= \sum_{i=1}^{j} a_i \sum_{x=1}^{k-1} c_{m_i,x} \\ &= \sum_{i=1}^{j} \sum_{x=1}^{k-1} a_i c_{m_i,x} \\ &= \sum_{x=1}^{k-1} \sum_{i=1}^{j} a_i c_{m_i,x} = \sum_{x=1}^{k-1} 0 = 0,\end{aligned}$$

as desired. This proves that $\sum_{i=1}^{j} a_i c_{m_i} = \vec{0}$, completing the proof of this theorem. □

If we demonstrate a 1-1 correspondence between the symmetric $(k-1) \times (k-1)$ matrices and the undirected graphs on k vertices, then to count the number of graphs with 2^n even partitions it is enough to count the number of symmetric $(k-1) \times (k-1)$ matrices with rank $k-n-1$. We show there is a 1-1 correspondence between all $(k-1) \times (k-1)$ symmetric matrices and the set of all $L(G)$ when $|V(G)| = k$.

Suppose you have a $(k-1) \times (k-1)$ symmetric matrix $A = (a_{ij})_{1 \le i,j \le (k-1)}$. Define $a_{ik} = a_{ki} = \sum_{j=1}^{k-1} a_{ij}$ and $a_{kk} = \sum_{j=1}^{k-1} a_{kj}$ and let $A^* = (a_{ij})_{1 \le i,j \le k}$. Then $A^* = L(G)$ for some undirected graph G with k vertices since the sum of its rows is 0 and it is by definition symmetric. This process gives a function from the set of $(k-1) \times (k-1)$ symmetric matrices to the set of all undirected graphs on k vertices.

This function is clearly 1-1. Let G be a graph on k vertices. Then $L(G)$ is a symmetric $k \times k$ matrix. Deleting the last column and row of $L(G)$ gives a symmetric $(k-1) \times (k-1)$ matrix. Call this matrix A. Then it is easy to see that performing the above operation on A gives $L(G)$ back. Therefore, we have a 1-1 correspondence between $(k-1) \times (k-1)$ symmetric matrices and undirected graphs on k vertices.

So to count undirected graphs with a given number of even partitions we need to count symmetric matrices with a given rank. The case of counting the number of $n \times n$ symmetric matrices with rank n has been treated before. Brent and McKay in [BM2] determine the number of $n \times n$ symmetric matrices over $\mathbb{Z}_2$ with rank n. We give an argument similar to count these matrices. We then extend their results to count the number of matrices with any rank. Throughout the section we give the results in terms of the graph theory as well as in terms of matrices.

4.1. **Number of Odd Graphs on k Vertices.** We begin by counting the number of odd graphs on $k+1$ vertices. To do this we will count the number of invertible symmetric matrices. The next two lemmas will allow us to give a recursive formula for the probability that a $k \times k$ symmetric matrix is invertible.

Lemma 4.2. *Suppose $A = (a_{ij})_{1\leq i,j\leq k}$ is a symmetric $k\times k$ matrix over $\mathbb{Z}_2$ and that $a_{11} = 1$. Additionally, let $k \times k$ matrix $\Lambda = (\lambda_{ij})_{1\leq i,j\leq k}$ with*

$$\lambda_{ij} = \begin{cases} 1 & \text{if } i = j \\ a_{1j} & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then

$$\Lambda^T A\Lambda = \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & b_{11} & b_{12} & \dots & b_{1(k-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & b_{(k-1)1} & b_{(k-1)2} & \cdots & b_{(k-1)(k-1)} \end{pmatrix}$$

where the matrix $B = (b_{ij})_{1\leq i,j\leq (k-1)}$ is a symmetric $(k-1)\times(k-1)$ matrix. Furthermore, if A is random then so is B.

Proof. By doing the multiplication we see that $\Lambda A\Lambda^T$ has the desired form. Furthermore, $b_{ij} = a_{1(i+1)}a_{1(j+1)} + a_{(i+1)(j+1)}$. Thus $b_{ij} = b_{ji}$. So B is symmetric. Furthermore, if A is a random matrix, then matrix B is random. □

Lemma 4.3. *Suppose $A = (a_{ij})_{1\leq i,j\leq k}$ is a symmetric $k \times k$ matrix over $\mathbb{Z}_2$, $a_{11} = 0$ and $a_{12} = 1$. Additionally, let $k \times k$ matrix $\Gamma = (\gamma_{ij})_{1\leq i,j\leq k}$ with*

$$\gamma_{ij} = \begin{cases} 1 & \text{if } i = j \\ a_{1j} & \text{if } i = 2 \\ a_{2j} + a_{22}a_{1j} & \text{if } i = 1 \\ 0 & \text{otherwise} \end{cases}.$$

Then

$$\Gamma^T A\Gamma = \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 1 & a_{22} & 0 & \dots 0 & \\ 0 & 0 & c_{11} & \dots & c_{1(k-2)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & c_{(k-2)1} & \cdots & c_{(k-2)(k-2)} \end{pmatrix}$$

where the matrix $C = (c_{ij})_{1\leq i,j\leq (k-2)}$ is a symmetric $(k-2)\times(k-2)$ matrix. Furthermore, if A is random then so is C.

Proof. The proof is similar to the proof of the previous Lemma. Doing the multiplication we see that the matrix has the desired form and that $c_{ij} = a_{1(i+2)}a_{2(j+2)} + a_{1(j+2)}a_{2(i+2)} + a_{22}a_{1(i+2)}a_{1(j+2)} + a_{(i+2)(j+2)}$. So C is a symmetric matrix. As in the previous Lemma C will be random if A is random. □

The following theorem now gives us a recursion for the probability that a graph on k vertices is odd.

Theorem 4.4. *Let $p(k)$ be the probability that a random $k\times k$ symmetric matrix over $\mathbb{Z}_2$ is invertible. Then*

$$p(k) = \frac{1}{2}\left(p(k-1) + \left(1 - \left(\frac{1}{2}\right)^{k-1}\right)p(k-2)\right) \tag{4.1}$$

for $n \geq 2$. We define $p(0) = 1$ and we have $p(1) = 1/2$.

This recursion gives

$$\begin{aligned} p(2n) =& p(2n-1) \\ p(2n-1) =& \left(1 - \left(\frac{1}{2}\right)^{2n-1}\right) p(2n-2) \end{aligned}$$

for all $n \geq 1$.

Proof. We begin by deriving equation (4.1). Let A be a random symmetric $k \times k$ matrix with $k \geq 2$. Throughout the proof we use the fact that A is invertible if and only if $det(A) \neq 0$. We derive the recursion by considering the two cases when $a_{11} = 1$ and when $a_{11} = 0$.

First suppose $a_{11} = 1$ this happens with probability $1/2$. With the notation of Lemma 4.2 and using the fact that $det(\Lambda) = det(\Lambda^T) = 1$, we see that $det(A) = det(\Lambda)det(A)det(\Lambda^T) = det(\Lambda A \Lambda^T) = det(B)$. Since A was random B is a random symmetric $(k-1) \times (k-1)$ matrix. Hence, if $a_{11} = 1$ then the probability that A is invertible is $\frac{1}{2}p(k-1)$.

Next suppose that $a_{11} = 0$. If $a_{1j} = 0$ for all j, then $det(A) = 0$. So, A is not invertible. Suppose that there exists at least one $j \neq 1$ such that $a_{1j} \neq 0$. This happens with probability $\frac{1}{2}\left(1 - \left(\frac{1}{2}\right)^{k-1}\right)$. Switching the j^{th} column with the 2^{nd} column and switching the j^{th} row with the 2^{nd} row keeps A a symmetric matrix. Furthermore, whether or not the determinant is 0 is not changed. Thus we may assume without loss of generality that $a_{12} = 1$.

With the notation of Lemma 4.3 and using the fact $det(\Gamma) = det(\Gamma^T) = 1$, we see that $det(A) = det(\Gamma)det(A)det(\Gamma^T) = det(\Gamma A \Gamma^T) = det(C)$. Since A was random C is a random symmetric $(k-2) \times (k-2)$ matrix. Hence, if $a_{11} = 0$ then the probability that A is invertible is $\frac{1}{2}\left(1 - \left(\frac{1}{2}\right)^{k-1}\right) p(k-2)$.

Summing the two probabilities gives equation (4.1).

We will now prove the set of equations by using this recursion and induction. Suppose for some n that

$$\begin{aligned} p(2n) =& p(2n-1) \\ p(2n-1) =& \left(1 - \left(\frac{1}{2}\right)^{2n-1}\right) p(2n-2). \end{aligned}$$

This is easily verified for small n. Then by equation (4.1) we have

$$p(2n+1) = \frac{1}{2}\left(p(2n) + \left(1 - \left(\frac{1}{2}\right)^{2n}\right) p(2n-1)\right) \tag{4.2}$$

$$= \frac{1}{2}\left(1 + (1 - \left(\frac{1}{2}\right)^{2n}\right) p(2n) = \left(1 - \left(\frac{1}{2}\right)^{2n+1}\right) p(2n), \tag{4.3}$$

as desired.

Now using equation (4.2) we have

$$\begin{aligned} p(2n+2) =& \frac{1}{2}\left(p(2n+1) + \left(1 - \left(\frac{1}{2}\right)^{2n+1}\right) p(2n)\right) \\ =& \frac{1}{2}\left(p(2n+1) + p(2n+1)\right) \\ =& p(2n+1). \end{aligned}$$

This completes the proof. □

The following theorem is an immediate consequence of the previous theorem and the discussion at the opening of this section.

Theorem 4.5. *Let G be an undirected graph on k vertices. The probability that G is odd is*

$$q(k) = \prod_{j=1}^{s}\left(1 - \left(\frac{1}{2}\right)^{2s-1}\right)$$

where $s = \lfloor \frac{k}{2} \rfloor$.

Hence there are $2^{\binom{k}{2}} q(k)$ odd graphs on k vertices.

Proof. From the discussion above and in the notation of Theorem 4.4 we see that $q(k) = p(k-1)$. Also, using the second set of recursions in Theorem 4.4, it is easy to deduce that $p(k-1) = \prod_{j=1}^{s}\left(1 - \left(\frac{1}{2}\right)^{2j-1}\right)$ where $s = \lfloor \frac{k}{2} \rfloor$.

□

4.2. **Number of Even Partitions of a Graph.** Generalizing the ideas that we used to derive the number of odd graph on k vertices we can determine the number of graphs on k vertices that have 2^n even partitions, for any n. Again, we can use Theorems 3.2, to reduce the problem to finding how many graphs on k vertices have $L^*(G)$ with rank $k-1-n$. In the above discussion we found the number of graphs with 2^0 distinct even partitions and hence the number of $L(G)$ with rank $k-1$.

Let $I(k,r)$ be the number of $k \times k$ symmetric matrices of rank r over $\mathbb{Z}_2$. Then in the previous section we showed that

$$I(k,k) = 2^{\binom{k}{2}} \prod_{j=1}^{s}\left(1 - \left(\frac{1}{2}\right)^{2j-1}\right)$$

where $s = \lfloor \frac{k}{2} \rfloor$.

The next proposition is a well known result about symmetric matrices. We use it to prove a Lemma that we will need in the proof of the general theorem.

Proposition 4.6. *An $n \times n$ matrix M is symmetric if and only if $v^T M = (Mv)^T$ for all vectors v.*

Lemma 4.7. *Let A be a symmetric $n \times n$ matrix and let B be an $n \times n$ matrix. Then $B^T A B$ is a symmetric matrix.*

Proof. To prove this we will show that for all $\vec{v} \in Z_2^n$, $v^T B^T A B = (B^T A B v)^T$. If we establish this, then the result follows from Proposition 4.6.

It is well known that $v^T B^T = (Bv)^T$. Using this twice and Proposition 4.6 we have

$$v^T B^T AB = (Bv)^T AB = (ABv)^T (B^T)^T = (B^T ABv)^T,$$

as desired. □

Theorem 4.8.

$$I(n, n-j) = d(n, j) I(n-j, n-j),$$

where $d(n, j)$ is the number of j dimensional subspaces of $\mathbb{Z}_2^n$ and

$$d(n, j) = \prod_{i=0}^{j-1} \frac{2^n - 2^i}{2^j - 2^i}.$$

Proof. We will prove this theorem in three steps.

Step 1. Let $E = \text{span } \{e_1, \ldots, e_j\}$. Then there are $I(n-j, n-j)$ rank $n-j$ $n \times n$ matrices that take exactly S to zero.

To see this we begin by noting that Me_m is the mth column of the matrix M. Therefore, if A is a symmetric matrix with $Ae_m = \vec{0}$ then the mth column and row of A must be zero. Furthermore, A has rank $n-j$ if and only if $n-j$ of the column vectors are independent.

Let A be a symmetric $k \times k$ matrix with rank $n-j$ that takes E to zero. Since the first j columns of A are zero, if A has rank $n-j$ we must have that the final $n-j$ column vectors of A are linearly independent. Since the first j rows of A are also the zero, A will send $e_1, \ldots, e_j$ to $\vec{0}$ and have rank $n-j$ if and only if the symmetric $(n-j) \times (n-j)$ submatrix $A^* = (a_{ij})_{(j+1) \leq i,j \leq n}$ has linearly independent column vectors. That is if and only if A^* is invertible.

Therefore, there are $I(n-j, n-j)$ symmetric $n \times n$ matrices of rank $n-j$ that send $e_1, \ldots, e_j$ to $\vec{0}$.

Step 2. Let S be any j dimensional subspace with basis $\{v_1, \cdots, v_j\}$. Also let $\mathcal{S} = \{$ all $n \times n$ symmetric matrices of rank $n-j$ that take S to zero$\}$ and let $\mathcal{E} = \{$ all $n \times n$ symmetric matrices of rank $n-j$ that take E to zero$\}$. I will show that there is a 1-1 onto map from $\mathcal{S}$ to $\mathcal{E}$, thus these sets have the same size. The result follows, since the subspace S was arbitrarily chosen and there are $I(n-j, n-j)$ elements in $\mathcal{E}$.

It remains to demonstrate the 1-1 onto map. There exists $k_1, \ldots, k_{n-j}$ such that $\{v_1, \ldots, v_j, e_{k_1}, \ldots, e_{k_{n-j}}\}$ is a basis for $\mathbb{Z}_2^n$. Let B be the change of basis matrix such that $e_s \mapsto v_s$ for $1 \leq s \leq j$ and $e_{j+t} \mapsto e_{k_t}$ for $1 \leq t \leq (n-j)$.

Define the map $\phi : \mathcal{S} \to \mathcal{E}$ by $\phi(A) = B^T AB$. Since B is invertible so is B^T. Thus, $B^T ABv = \vec{0}$ if and only if $ABv = \vec{0}$. But $ABv = \vec{0}$ if and only if $Bv \in S$. Since B is the change of basis matrix from $\{e_1, \ldots, e_j\}$ and $\{v_1, \ldots, v_j\}$ we have $B^T ABv = \vec{0}$ if and only if $v \in E$. Therefore, the map is well defined onto the spaces indicated.

Furthermore, ϕ is 1-1, since B and B^T are both invertible. To show that ϕ is onto let $X \in \mathcal{E}$ be arbitrary and $Y = (B^T)^{-1} X B^{-1}$. Since $\phi(Y) = B^T Y B = B^T (B^T)^{-1} X B^{-1} B = X$, it is enough to show that $Y \in \mathcal{S}$. Since B^T is invertible $Yv = \vec{0}$ if and only if $XB^{-1}v = \vec{0}$. Furthermore, since $X \in \mathcal{E}$, $XB^{-1}v = \vec{0}$ if and only if $B^{-1}v \in E$. But B^{-1} is the change of basis matrix from $\{v_1, \ldots, v_j\}$ to $\{e_1, \ldots, e_j\}$, thus $Yv = \vec{0}$ if and only if $v \in S$. So $Y \in \mathcal{S}$.

This completes the proof that $I(n, n-j) = d(n, j)I(n-j, n-j)$. The final step in the proof is to compute $d(n, j)$.

Step 3. There are $\prod_{k=0}^{j-1}(2^n - 2^k)$ ways to choose j linearly independent vectors from $\mathbb{Z}_2^n$. Furthermore, for any subspace of $\mathbb{Z}_2^n$ of dimension j there are $\prod_{k=0}^{j-1}(2^j - 2^k)$ different bases for that subspace. Hence the total number of subspaces of $\mathbb{Z}_2^n$ of dimension j is $\prod_{k=0}^{j-1} \frac{2^n - 2^k}{2^j - 2^k}$. □

The following table gives the values for the number of even partitions of a graph for some small graphs. Each entry gives the number of graphs on k vertices with m distinct even partitions

k/m	1	2	4	8	16
0	0				
1	1				
2	1	1			
3	4	3	1		
4	28	28	7	1	

5. Probability Each Graph Appears

Now that we have determined how many graphs on a specified number of vertices are odd, we will try to relate this information back to the original number theory. Let

$$S_{3,k}(X) = \{n < X : n \equiv 3(\mod 8) \text{ and } n = p_1 \dots p_k \text{ where } p_1 \equiv 3, p_j \equiv 1(\mod 4),\ j \neq 1\}.$$

Furthermore, let $G(S_{3,k})(X) = \{G(n) : n \in S_{3,k}(X)$. Recall that in the discussion following Theorem **??** we showed that every graph on k vertices appears infinitely often in $G(S_{3,k})(\infty)$. In this section we wish to show that every graph in $G(S_{3,k})(X)$ for X sufficiently large appears with equal probability. Similarly define

$$\begin{aligned}
S_{1,k}(X, 1) =& \{n < X : n \equiv 1(\mod 8) \text{ and } n \text{ has decomposition 1 from Theorem 2.2}\},\\
S_{2,k}(X, 2) =& \{n < X : n \equiv 1(\mod 8) \text{ and } n\text{has decomposition 2 from Theorem 2.2}\},\\
S_{1,k}(X, 3) =& \{n < X : n \equiv 1(\mod 8) \text{ and } n\text{has decomposition 3 from Theorem 2.2}\},\\
S_{2,k}(X) =& \{n < X : n = 2p_1 \dots p_k \text{ and } p_j \equiv 1(\mod 4)\}.
\end{aligned}$$

Define $G(T)$ where T is one of the above sets in a similar way. Again in each of these other cases we want to show that each graph in the set appears equally often for sufficiently large X. If we establish this then we will have shown that the probability that an E_n for n chosen from $S_{3,k}(X)$, where X is large, has trivial 2-Selmer groups is the same as the probability that a graph on k vertices is odd.

Since the work is tedious we only work this result out for $G(S_{3,k}(X))$. Specifically, we want to know the probability that an edge exists between two given vertices. We expect this probability to be about $\frac{1}{2}$, since the existence of an edge between the vertices corresponding to the primes p and q is entirely dependent on whether $(\frac{q}{p})$ is 1 or -1. Note that each possibility occurs for half of the congruence classes (mod p). Actually, since we are putting an extra restriction on q, it is necessary to look at which congruence class q falls in (mod $8p$). This

distinction makes no real difference, since each of the two possible values for $(\frac{q}{p})$ still occurs for exactly half of the allowed congruence classes modulo $8p$.

Dirichlet's theorem says that there are infinitely many primes in any arithmetic progression $\{8kp+a\}_{k\in\mathbb{N}}$ for each a that is relatively prime to $8p$ and there are the same density of primes in the set $\{8kp+a\}$ for each a. Since $(\frac{a}{p})$ is 1 for half of the allowable a's relatively prime to $8p$, it is reasonable to suspect that the probability that each edge on $G(n)$ for some n with k prime factors appears with probability $1/2$. Furthermore, if each edge appears with probability $1/2$, then each graph appears equally likely.

We would like to know whether each graph does indeed show up with the same frequency as every other. If each graph does indeed show up with the same frequency as every other graph then we would expect that the probability that any E_n, where n has k prime factors, has trivial Selmer groups is $q(k)$ where q is defined in Theorem **??**. In other words we know the proportion of $n = p_1p_2\cdots p_k$ with $p_1 \equiv 3(\mathrm{mod}\,4)$, $p_i \equiv 1(\mathrm{mod}\,4)$ for $2 \leq i \leq k$, and $n \equiv 3(\mathrm{mod}\,8)$, that correspond to E_n with trivial Selmer groups.

We have done many calculations to verify that this is indeed true. In particular we know that $q(2) = 1/2$, so we would expect that when $k = 2$ we would have $1/2$ of the n less than X give E_n with trivial Selmer groups. Figure 1 shows how when $k = 2$, the proportion of even graphs in $S_{3,2}(X)$ approaches 0.5 as we increase X. Since half of all random graphs on two vertices are even, this is exactly the result we should be getting if each graph in $S_{3,2}(X)$ appears with equal proportion.

X	Proportion
10^6	0.495612
10^7	0.497637
10^8	0.499127
10^9	0.499626
10^{10}	0.499808
10^{11}	0.499902

FIGURE 1. Proportion of even graphs generated from products of two primes not greater than N.

In the case $k = 3$, again since the probability that a random graph on 3 vertices is even is $1/2$ we expect the proportion of $n < X$ with 3 prime factors that give trivial Selmer groups to be 0.5. This time the convergence is significantly slower, however our data verifies this expectation.

The proportion of random graphs on four vertices that have even partitions is $q(4) = 9/16 = 0.5625$. Encouragingly, as we let X grow, the proportion of even graphs generated from products of four primes tends to 0.5625. Curiously, this convergence is nearly as quick as in the three prime case.

All of this data supports the reasoning that each graph each graph on $S_{3,k}(X)$ appears with equal probability. In the next section we will prove this result. We do not give the proofs for the other cases because they are very detailed, however their proofs are similar.

5.1. **Each Edge Appears With Probability** $1/2$**.** .

We now give a sketch proof to establish the result that each graph in $G(S_{3,k}(X))$ appears

N	Proportion
10^6	0.430035
10^7	0.447058
10^8	0.459316
10^9	0.466598
10^{10}	0.471562
10^{11}	0.475111

FIGURE 2. Proportion of even graphs generated from products of three primes not greater than X.

N	Proportion
10^6	0.482466
10^7	0.502105
10^8	0.517575
10^9	0.526370
10^{10}	0.532565
10^{11}	0.536957
10^{12}	0.540226

FIGURE 3. Proportion of even graphs generated from products of four primes not greater than N.

with equal probability as X tends to infinity. We establish this result by first fixing k. We note that by Dirichlet's theorem on primes in an arithmetic progression every undirected graph on k vertices appears in $G(S_{3,k}(X))$. Finally we argue that each edge between the k vertices appears with probability $1/2$ as X tends to infinity, therefore, each graph appears with equal probability as X tends to infinity.

Conjecture 5.1. *Let k be an integer. Let $n \in S_{3,k}(X)$. $G(n)$ is an undirected graph on the k vertices $p_1, \ldots, p_k$. As X tends to infinity the probability that the edge $\overline{p_j p_i} \in V(G(n))$ tends to $1/2$.*

Given the following reasonable conjecture we will make an inductive argument to prove Conjecture 5.1.

Conjecture 5.2. *There exists $\epsilon = \epsilon(k)$ such that for any product of k distinct primes $p_1 \ldots p_k < X^\epsilon$ and for all primes p_{k+1} such that $p_1 \ldots p_k p_{k+1} < X$ the proportion of p_{k+1} with $\left(\frac{p_{k+1}}{p_j}\right) = 1$ tends to $1/2$ as X increases to infinity.*

Dirichlet's theorem states that the sum of the reciprocals of the primes in a particular congruence class diverges. Mertens was able to refine the theorem to say that

$$\sum_{\substack{p \leq X \\ p \equiv a(\mod q)}} \frac{1}{p} = \frac{1}{\phi(q)} \log\log X + A(q,a) + O[(\log X)^{-1}]$$

[DAV]

This means, roughly, that given sufficiently large X, equal amounts of primes appear in each congruence class ($\mod q$).

However, now it is necessary to ensure that q is small compared to X. Consider the case when we are looking at square free integers less than X with $k+1$ prime factors. Since we need the last prime factor to be able to take on a wide range of values compared to the size of the first k factors, we want the first k prime factors to be small.

Let $p_1, p_2, \dots p_{k+1}$ be the prime factors of $x \leq X$, with $p_1 < p_2 < \ldots < p_{k+1}$. Consider the sum

$$\sum_{\substack{p_1 p_2 \dots p_{k+1} < X \\ p_1 < p_2 < \dots p_k}} 1$$

This sum counts the number of square free integers less than X with $k+1$ prime factors. We want most of this sum to consist of terms where $p_1 p_2 \dots p_k < X^{\varepsilon}$, for a given small $\varepsilon > 0$.

In other words given ε, for sufficiently large X we want

$$\sum_{\substack{p_1 p_2 \dots p_{k+1} < X \\ p_1 < p_2 < \dots p_k \\ X^{\varepsilon} < p_1 p_2 \dots p_k < X^{\frac{k}{k+1}}}} 1 = o\left(\sum_{\substack{p_1 p_2 \dots p_{k+1} < X \\ p_1 < p_2 < \dots p_k \\ p_1 p_2 \dots p_k < X^{\varepsilon}}} 1 \right).$$

Soon, we will prove a theorem regarding this expression, but we first need a few lemmas.

Lemma 5.3.

$$\sum_{p_1 < p_2 \dots < p_k < x} \frac{1}{p_1 p_2 \dots p_k} = \frac{1}{k!} (\log \log x)^k + O((\log \log x)^{k-1})$$

Proof. Consider this expression:

$$k! \sum_{p_1 < p_2 \dots < p_k < x} \frac{1}{p_1 p_2 \dots p_k} < \left(\sum_{p<x} \frac{1}{p} \right)^k < k! \sum_{p_1 < p_2 \dots < p_k < x} \frac{1}{p_1 p_2 \dots p_k} + \binom{k}{2} \left(\sum_{p<x} \frac{1}{p} \right)^{k-2} \left(2 \sum_{p<x} \frac{1}{p^2} \right)$$

The left side is less than the middle because it does not count the terms where some of the primes are equal. The right side is greater than the middle because it counts all the terms, overcounting those where the same prime appears more than twice or multiple primes appear at least twice.

We already know from Mertens that

$$\sum_{p<x} \frac{1}{p} = \log \log x + A + O[(\log x)^{-1}]$$

[DAV] So we already have the answer for $k = 1$. Now consider when $k \geq 2$. If we raise both sides to the kth power, we get a similar type of sum. We would like to separate the terms which have all distinct prime factors on the bottom from those which do not. Note that

$$\sum_{p<x} \frac{1}{p^2} < \zeta(2) = \frac{\pi^2}{6}.$$

$$\left(\sum_{p<x} \frac{1}{p} \right)^{k-2} = O((\log \log x)^{k-2})$$

So,

$$k! \sum_{p_1<p_2\ldots<p_k<x} \frac{1}{p_1p_2\ldots p_k} < \left(\sum_{p<x} \frac{1}{p}\right)^k \leq k! \sum_{p_1<p_2\ldots<p_k<x} \frac{1}{p_1p_2\ldots p_k} + O((\log\log x)^{k-2})$$

Plugging in $\sum_{p<x} \frac{1}{p} = \log\log x + A + O[(\log x)^{-1}]$ gives

$$\sum_{p_1<p_2\ldots<p_k<x} \frac{1}{p_1p_2\ldots p_k} = \frac{1}{k!}(\log\log x + A + O[(\log x)^{-1}])^k + O((\log\log x)^{k-2})$$

Finally, applying the binomial theorem gives

$$\sum_{p_1<p_2\ldots<p_k<x} \frac{1}{p_1p_2\ldots p_k} = \frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1})$$

□

Lemma 5.4.

$$\sum_{p_1<p_2<\ldots p_k<x^{\frac{1}{k}}} \frac{1}{p_1p_2\ldots p_k} = \frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1})$$

Proof.

$$\sum_{p_1<p_2<\ldots p_k<x^{\frac{1}{k}}} \frac{1}{p_1p_2\ldots p_k} < \sum_{p_1p_2\ldots p_k<x} \frac{1}{p_1p_2\ldots p_k} < \sum_{p_1<p_2<\ldots p_k<x} \frac{1}{p_1p_2\ldots p_k}$$

The expression on the left is $\frac{1}{k!}(\log\log(x^{\frac{1}{k}}))^k + O((\log\log(x^{\frac{1}{k}}))^{k-1})$, by 5.3. Likewise, the expression on the right is $\frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1})$, also by 5.3.

Now, if we note that $\log\log(x^{\frac{1}{k}}) = \log\log x - \log k$, so that by the binomial theorem $(\log\log(x^{\frac{1}{k}}))^k = (\log\log x)^k + O((\log\log x)^{k-1})$, we have that

$$\frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1}) < \sum_{p_1p_2\ldots p_k<x} \frac{1}{p_1p_2\ldots p_k} < \frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1})$$

So,

$$\sum_{p_1<p_2<\ldots p_k<x^{\frac{1}{k}}} \frac{1}{p_1p_2\ldots p_k} = \frac{1}{k!}(\log\log x)^k + O((\log\log x)^{k-1})$$

□

Theorem 5.5. *If $p_1 < p_2 < \ldots < p_k$, then for a given integer $k > 0$ and real $\varepsilon > 0$ there exist $B_2 > B_1 > 0$ such that*

$$B_1\frac{X}{k!\log X}(\log\log X)^k + O\left(\frac{X}{\log X}(\log\log X)^{k-1}\right) < \sum_{\substack{p_1p_2\ldots p_k<X^\varepsilon \\ p_1<p_2<\ldots<p_{k+1} \\ p_1p_2\ldots p_{k+1}<X}} 1$$

$$< B_2\frac{X}{k!\log X}(\log\log X)^k + O\left(\frac{X}{\log X}(\log\log X)^{k-1}\right)$$

Also,

$$\sum_{\substack{X^{\varepsilon}<p_1p_2\ldots p_k<X^{\frac{k}{k+1}}\\ p_1<p_2<\ldots<p_{k+1}\\ p_1p_2\ldots p_{k+1}<X}} 1 = O\left(\frac{X}{\log X}(\log\log X)^{k-1}\right)$$

Proof. We want to place an upper and lower bound on the sum

$$\sum_{\substack{p_1p_2\ldots p_k<X^{\varepsilon}\\ p_1<p_2<\ldots<p_{k+1}\\ p_1p_2\ldots p_{k+1}<X}} 1.$$

The upper bound in the following line comes from the fact that every square-free integer less than X with $k+1$ prime factors is the product of a square-free integer less than $X^{\frac{k}{k+1}}$ with k prime factors and another prime. It is an upper bound because some of the numbers are counted twice this way.

(5.1)

$$\sum_{p_1p_2\ldots p_k<X^{\varepsilon}} \pi\left(\frac{X}{p_1p_2\ldots p_k}\right) > \sum_{\substack{p_1p_2\ldots p_k<X^{\varepsilon}\\ p_1<p_2<\ldots<p_{k+1}\\ p_1p_2\ldots p_{k+1}<X}} 1 > \left(\sum_{p_1<p_2<\ldots<p_k<X^{\frac{\varepsilon}{k}}} \pi\left(\frac{X}{p_1p_2\ldots p_k}\right)\right) - k\begin{pmatrix}\pi(X^{\frac{\varepsilon}{k+1}})\\ k+1\end{pmatrix}$$

The lower bound counts the number of square-free integers which are the products of k primes all less than $X^{\frac{\varepsilon}{k+1}}$. This is a subset of the numbers we sum over in the middle term. The second term on the lower bound, $k\begin{pmatrix}\pi(X^{\frac{\varepsilon}{k+1}})\\ k+1\end{pmatrix}$ eliminates all the possible over counting, since we can over count up to k times for any set of $k+1$ primes all less than $X^{\frac{\varepsilon}{k+1}}$.

A similar line of reasoning gives

$$\sum_{\substack{X^{\varepsilon}<p_1p_2\ldots p_k<X^{\frac{k}{k+1}}\\ p_1<p_2<\ldots<p_{k+1}\\ p_1p_2\ldots p_{k+1}<X}} 1 < \sum_{X^{\varepsilon}<p_1p_1\ldots p_k<X^{\frac{k}{k+1}}} \pi\left(\frac{X}{p_1p_2\ldots p_k}\right)$$

Now, we need only find an appropriate approximation for $\pi(x)$ and then apply the lemmas. Tchebychev has shown that $0.92\ldots\frac{x}{\log x} < \pi(x) < 1.105\ldots\frac{x}{\log x}$, for all sufficiently large x. [DAV] Thus,

$$(0.92\ldots)\sum_{X^{\alpha}<p_1p_2\ldots p_k<X^{\beta}} \frac{X}{p_1p_2\ldots p_k(\log X-\log(p_1p_2\ldots p_k))}$$

$$< \sum_{X^{\alpha}<p_1p_2\ldots p_k<X^{\beta}} \pi\left(\frac{X}{p_1p_2\ldots p_k}\right)$$

$$< (1.105\ldots)\sum_{X^{\alpha}<p_1p_2\ldots p_k<X^{\beta}} \frac{X}{p_1p_2\ldots p_k(\log X-\log(p_1p_2\ldots p_k))}$$

Now, since $X^\alpha < p_1p_2\dots p_k < X^\beta$, $\alpha \log X < \log(p_1p_2\dots p_k) < \beta \log X$. So, if we let $B_1 = (0.92\dots)^{\frac{1}{1-\beta}}$ and $B_2 = (1.105\dots)^{\frac{1}{1-\alpha}}$, we have that

$$B_1 \sum_{X^\alpha < p_1p_2\dots p_k < X^\beta} \frac{X}{p_1p_2\dots p_k(\log X)} < \sum_{X^\alpha < p_1p_2\dots p_k < X^\beta} \pi\left(\frac{X}{p_1p_2\dots p_k}\right) \tag{5.2}$$

$$< B_2 \sum_{X^\alpha < p_1p_2\dots p_k < X^\beta} \frac{X}{p_1p_2\dots p_k(\log X))}$$

Plugging in $\alpha = 0$ and substituting back into 5.1 gives

$$B_2 \sum_{p_1p_2\dots p_k < X^\varepsilon} \frac{X}{p_1p_2\dots p_k(\log X)} > \sum_{\substack{p_1p_2\dots p_k < X^\varepsilon \\ p_1<p_2<\dots<p_{k+1} \\ p_1p_2\dots p_{k+1} < X}} 1$$

$$> B_1 \left(\sum_{p_1<p_2<\dots<p_k<X^{\frac{\varepsilon}{k}}} \frac{X}{p_1p_2\dots p_k(\log X)} \right) - k \begin{pmatrix} \pi(X^{\frac{\varepsilon}{k+1}}) \\ k+1 \end{pmatrix}$$

Applying 5.3 to the right and 5.4 to the left, this evaluates to

$$B_2 \frac{X}{k! \log X}((\log\log x)^k + O((\log\log x)^{k-1})) > \sum_{\substack{p_1p_2\dots p_k < X^\varepsilon \\ p_1<p_2<\dots<p_{k+1} \\ p_1p_2\dots p_{k+1} < X}} 1$$

$$> B_1 \frac{X}{k! \log X}((\log\log x)^k + O((\log\log x)^{k-1})) - k \begin{pmatrix} \pi(X^{\frac{\varepsilon}{k+1}}) \\ k+1 \end{pmatrix}.$$

But what is $k \begin{pmatrix} \pi(X^{\frac{\varepsilon}{k+1}}) \\ k+1 \end{pmatrix}$? We can approximate this term by saying

$$k \begin{pmatrix} \pi(X^{\frac{\varepsilon}{k+1}}) \\ k+1 \end{pmatrix} = O\left(k \frac{(\pi(X^{\frac{\varepsilon}{k+1}}))^{k+1}}{(k+1)!} \right)$$

$$= O\left(k \frac{(\frac{X^{\frac{\varepsilon}{k+1}}}{\log X^{\frac{\varepsilon}{k+1}}})^{k+1}}{(k+1)!} \right) = O((\frac{X}{\log X})^\varepsilon)$$

This falls into the error term we already have, so we get the first statement of our theorem:

$$B_1 \frac{X}{k! \log X}(\log\log X)^k + O\left(\frac{X}{\log X}(\log\log X)^{k-1} \right) < \sum_{\substack{p_1p_2\dots p_k < X^\varepsilon \\ p_1<p_2<\dots<p_{k+1} \\ p_1p_2\dots p_{k+1} < X}} 1$$

$$< B_2 \frac{X}{k! \log X}(\log\log X)^k + O\left(\frac{X}{\log X}(\log\log X)^{k-1} \right)$$

Note that while our result is not very precise, the main term agrees with the established result of Sathe in [SAT], which was reproved by Selberg in [SEL].

Denote by $\pi_\nu(x)$ the number of square-free integers having ν prime factors. Put $\nu = k \log\log x$. Let $k < e$. Then

$$\pi_\nu(x) = (1+o(1))f(k)\frac{x}{\log x}\frac{(\log\,\log x)^{\nu-1}}{(\nu-1)!}$$

where (p runs through all primes)

$$f(k) = \frac{1}{\Gamma(k+1)}\left[\prod_p \left(1-\frac{1}{p}\right)e^{1/p}\right]^k \prod_p \left(1+\frac{k}{p}e^{-k/p}\right).$$

Now for the second half of our theorem:

$$\sum_{X^\alpha < p_1p_2\ldots p_k < X^\beta} \frac{X}{p_1p_2\ldots p_k(\log X)} = \sum_{p_1p_2\ldots p_k < X^\beta} \frac{X}{p_1p_2\ldots p_k(\log X)} - \sum_{p_1p_2\ldots p_k < X^\alpha} \frac{X}{p_1p_2\ldots p_k(\log X)}$$

$$= \frac{X}{\log X}\left[(\log\log X)^k + O((\log\log X)^{k-1}) - (\log\log X)^k + O((\log\log X)^{k-1})\right]$$

$$= O\left(\left(\frac{X}{\log X}\log\log X\right)^{k-1}\right)$$

by 5.1.

Again, plugging back into 5.2 gives the second statement of the theorem:

$$\sum_{\substack{X^\varepsilon < p_1p_2\ldots p_k < X^{\frac{k}{k+1}} \\ p_1<p_2<\ldots<p_{k+1} \\ p_1p_2\ldots p_{k+1}<X}} 1 < \sum_{X^\varepsilon < p_1p_2\ldots p_k < X^{\frac{k}{k+1}}} \pi\left(\frac{X}{p_1p_2\ldots p_k}\right) = O\left(\frac{X}{\log X}(\log\log X)^{k-1}\right)$$

$$\sum_{\substack{X^\varepsilon < p_1p_2\ldots p_k < X^{\frac{k}{k+1}} \\ p_1<p_2<\ldots<p_{k+1} \\ p_1p_2\ldots p_{k+1}<X}} 1 = O\left(\frac{X}{\log X}(\log\log X)^{k-1}\right)$$

□

Conjecture 5.6. *There exists an $\varepsilon > 0$ such that $\lim_{X\to\infty} max\{|\frac{1}{\phi(q)} - \frac{\pi_{q,a}(X)}{\pi(X)}|, q < X^\varepsilon, (a,q) = 0\} = 0$.*

If this conjecture is true, we can argue inductively that asymptotically, every possible graph on k vertices is equally likely:

Our base case is the fact that there is only one graph on one vertex, so all graphs on one vertex have equal probability. Assume that each possible graph becomes equally distributed among all square-free integers less than y with k prime factors as $y \to \infty$.

Now, consider what happens when we add a $k+1$th prime factor, with the restriction that $p_1p_2\ldots p_{k+1} < y^{\frac{1}{\varepsilon}}$. Our theorem 5.5 shows that this encompasses all but a negligible number of square-free integers with $k+1$ prime factors less than $y^{\frac{1}{\varepsilon}}$, for sufficiently large y.

By hypothesis, all edges among the first k prime factors occur with probability close to $\frac{1}{2}$. The remaining k edges are determined by what congruence classes the $k+1$th prime falls into mod the other primes. By the Chinese Remainder Theorem, this is equivalent to asking which congruence class it belongs to mod $p_1p_2\ldots p_k$. Now, we can apply our conjecture 5.6

to say that as $y \to \infty$, the edges from the subgraph of k points to the $k+1$th point occur in every possible way with equal probability. Combining this with the inductive hypothesis, we get that as $y \to \infty$, every possible graph for numbers less than $y^{\frac{1}{\varepsilon}}$with $k+1$ distinct prime factors becomes equally likely.

Thus, by induction, as $X \to \infty$, the probability that a square-free number less than X will have a specific graph is the same as the probability of choosing the graph randomly by picking edges with probability $\frac{1}{2}$.

Again, we must reiterate that this result depends on our conjecture 5.6 or something similar to give bounds on how soon primes start to appear uniformly across the possible congruence classes for a given modulus.

6. Application to graphs for E_n

Now that we have established that each graph on k vertices appears equally likely in each of the cases discussed above we can apply graph theory results to the graphs that appear in [FX].

6.1. **The case** $n \equiv 3(\mod 8)$**.** Throughout this section we assume that $n \equiv 3(\mod 8)$. From Theorem 2.1 we know that if $n = p_1 \dots p_t$, $p_1 \equiv 3(\mod 4)$ and $p_j \equiv 1(\mod 4)$ $(2 \leq j \leq t)$, then E_n has trivial Selmer Groups if and only if $G(n)$ is odd.

As a result, for any $n \equiv 3(\mod 8)$ with the factorization given above (and k prime factors) the probability that E_n has trivial Selmer groups is the same as the probability that a graph on t vertices is odd. This probability is $\prod_{j=1}^{s}\left(1-\left(\frac{1}{2}\right)^{2s-1}\right)$ where $s = \lfloor \frac{k}{2} \rfloor$.

The following theorem was first established by Sathe in [SAT] and then reproved by Selberg in [SEL].

Theorem 6.1. *Denote by $\pi_\nu(x)$ the number of square-free integers having ν prime factors. Put $\nu = k \log\log x$. Let $k < e$. Then*

$$\pi_\nu(x) = (1+o(1))f(k)\frac{x}{\log x}\frac{(\log\log x)^{\nu-1}}{(\nu-1)!}$$

where (p runs through all primes)

$$f(k) = \frac{1}{\Gamma(k+1)}\left[\prod_p \left(1-\frac{1}{p}\right)e^{1/p}\right]^k \prod_p \left(1+\frac{k}{p}e^{-k/p}\right).$$

We now give an easily deduced corollary.

Corollary 6.2. *In the notation of the previous theorem,*

$$\pi_k(X) = (1+o(1))f\left(\frac{k}{\log\log(X)}\right)\frac{X}{\log X}\frac{(\log\log X)^{k-1}}{(k-1)!}$$

for X such that $\frac{k}{\log\log(X)} < e$.

In 6.1 fixing ν and letting x go to infinity we see that $f(k)$ converges to 1, the result follows. Now define $\pi_k^*(X)$ to be the number of square-free integers less than X with exactly k prime factors none of which are 2. The number of square free integers less than X with 2 as a factor is less than then number of square free integers less than $X/2$ with exactly $k-1$ prime

factors. But from Corollary 6.2 we know that this number is close to $\frac{X/2}{\log X/2}\frac{(\log\log(X/2))^{k-2}}{(k-2)!}$. This is much smaller than $\frac{X}{\log(X)}\frac{\log\log(X)^{k-1}}{(k-1)!}$. This reasoning gives the following theorem.

Theorem 6.3. *In the notation above,*

$$\pi_k^*(X) = (1+o(1))\,\frac{X}{\log(X)}\frac{\log\log(X)^{k-1}}{(k-1)!}$$

In our main theorems the n that we cared about had a specific prime factorization. The following discussion leads us to be able to count the numbers with this prime factorization. Let $\pi_k^*(X;a_1,\ldots,a_k)$ be the number of square free integers $n = p_1\ldots p_k$ less than X such that $p_j \equiv a_j(\mod 8)$ and each $a_j \equiv 1,3,5$ or $7(\mod 8)$. Notice that there are $\binom{k+3}{3}$ distinct k-tuples. (We consider tuples with the same numbers of $a_j \equiv 1,3,5$,and 7 to be the same. For example, the 2-tuples $(3,5)$ and $(5,3)$ are the same.) Also,

$$\pi_k^*(X) = \sum_{(a_1,\ldots,a_k)} \pi_k^*(X;a_1,\ldots,a_k),$$

where the sum is over all such k-tuples. It is reasonable to assume that for large enough X each of the the terms in the sum contribute the same amount to the value of $\pi_k^*(X)$. We state this in the next theorem.

Theorem 6.4. *In the notation above,*

$$\pi_k^*(X;a_1,\ldots,p_k) = (1+o(1))\,\frac{X}{\log(X)}\frac{\log\log(X)^{k-1}}{\binom{k+3}{3}(k-1)!}$$

Now to count the number of $n \in S_{3,k}(X)$ it is enough to count the number of allowable decompositions for $n = p_1\ldots p_k$. Recall n must have the decomposition $n = p_1\ldots p_t \equiv 3(\mod 8)$, where exactly one of the $p_j \equiv 3(\mod 4)$ and for all $i \neq j$ $p_i \equiv 1(\mod 4)$. Suppose we have $n = rq_1\ldots q_tQ_1\ldots Q_t$ where $s+t+1 = k$, $r \equiv 3,7(\mod 8)$, $q_i \equiv 1(\mod 8)$, and $Q_i \equiv 5(\mod 8)$. If $2|s$ then we must have $r \equiv 3$, There are $\lceil \frac{k}{2} \rceil$ possible $k-tuples$ when $2|s$. If $2 \nmid s$, then $r \equiv 7$. There are $\lfloor \frac{k}{2} \rfloor$ possible tuples when on of the primes is 7 modulo 8.

Putting these two results together we see that there are k possible tuples that give the desired decomposition.

Using this result and applying the result discussed in section **??** gives the following counting theorem.

Theorem 6.5. *Let $N_{3,k}(X)$ be the number of square-free integers n with exactly k prime factors, $n \equiv 3(mod\ 8)$, and $n < X$ such that $S_n = \{1\}$ and $S_n'\{\pm 1, \pm n\}$. Then for large X*

$$N_{3,k}(X) \approx f\left(\frac{k}{\log\log(X)}\right) q(k)\frac{k}{\binom{k+3}{3}}\frac{X}{\log(X)}\frac{\log\log(X)^{k-1}}{(k-1)!}, \tag{6.1}$$

where $q(k)$ is the probability that a random undirected graph on k vertices is odd.

Recall from Theorem 4.5

$$q(k) = \prod_{j=1}^{s}\left(1-\left(\frac{1}{2}\right)^{2s-1}\right)$$

where $s = \lfloor \frac{k}{2} \rfloor$.

For example when $k = 2$ this gives $N_{3,2}(X) \approx \frac{1}{16}\frac{X\log\log X}{\log X}$.

6.1.1. *Data.* The following calculations verify our counting theorems.

X	Number with $G(n)$ odd	$\lvert S_{3,2}(X)\rvert$	Proportion
10^6	21207	42045	0.504388
10^7	195391	388944	0.502363
10^8	1806154	3606013	0.500873
10^9	16815798	33606444	0.500374
10^{10}	157413227	314705475	0.500192
10^{11}	1480332478	2960087660	0.500098

FIGURE 4. generated from products of two primes not greater than N.

X	Number with $G(n)$ odd	$\lvert S_{3,3}(X)\rvert$	Proportion
10^6	11291	19810	0.569965
10^7	118637	214556	0.552942
10^8	1211721	2241087	0.540685
10^9	12215739	22901580	0.533402
10^{10}	122070712	231002932	0.528438
10^{11}	1213147587	2311247337	0.524889
10^12	12012228025	23002085447	0.522223

FIGURE 5. products of three primes not greater than X.

X	Number with $G(n)$ odd	$\lvert S_{3,4}(X)\rvert$	Proportion
10^6	1402	2709	0.517534
10^7	19864	39896	0.497895
10^8	248032	514136	0.482425
10^9	2906818	6137321	0.473630
10^{10}	32641358	69830762	0.467435
10^{11}	356306278	769488112	0.463043
10^12	3813142242	8293523085	0.459774

FIGURE 6. products of four primes not greater than X.

6.2. **The case** $n \equiv 1(\mod 8)$**.** Let $q_1^*(k)$ be the probability that a graph on k vertices with the form that appears when $n \equiv 1(\mod 8)$ has the form appears in the first decomposition. Then $q_1^*(k) = \frac{1}{2}q(k,k) + \frac{1}{4}q(k,k-1)$.

Now, we know already how often a random graph with k vertices meets the condition for non-congruence of a number $n \equiv 3(\mod 8)$ with $n = p_1p_2...p_t, p_1 \equiv 3(\mod 4)$ and $p_i \equiv 1(\mod 4)$ for $2 \leq i < t$ Specifically, the number of graphs is $I(k-1,k-1)$.

The question remains for the other cases: How many graphs on k vertices meet the condition for non-congruence for $n \equiv 1(\mod 8)$ or for $2 \mid n$?

Let us consider the $k \times k$ Laplace matrix L for the graphs $G(S_{1,k}(X,1))$. For the congruence condition to hold, L must have rank $k-2$ Now consider the rows of L corresponding to the factors q_1 and q_2. By the definition of the graph, these rows will contain only zeros. Thus we

can remove them from the matrix without changing the rank. Likewise we can remove the column corresponding to -1 (since it is all zeros) and one other column (since the columns sum to zero. Now we are left with a $k-2$ by $k-2$ matrix, which we will call L', the upper left $k-3$ by $k-3$ block of which is symmetric. Call this block S. Also, let T be L' with the bottom row removed. We wish to know how often the rank of S is $k-2$. We will consider three cases:

1) S is singular. In this case, some unique linear combination of the columns of S will form the last column of T If this combination, applied to the first $k-3$ columns of L' gives the last column, $r(L') = k-3$, otherwise $r(L) = k-2$. However, this is contingent only on whether the bottom right element of L' matches the application of the linear combination to the last elements of the first $k-3$ columns of L'. This will happen half the time, so this case contributes $\frac{1}{2}I(k-3, k-3)$ graphs that fulfill the condition.

2) S has rank $k-4$ Here, for L' to be singular, it is necessary for the last column of T to lie outside the space spanned by the columns of S. This happens half the time, since the columns of S span a space of rank $k-4$, which has half as many members (in F_2) as a space of rank $k-3$. Now, it is possible to switch the last column of T with another column so that the first $k-3$ rows have rank $k-3$. But this is just the situation we had in case 1, so in a further half of these cases L' will have rank $k-3$. Thus, this case contributes $\frac{1}{4}I(k-3, k-4)$ graphs that fulfill the condition.

3) S has rank $\leq k-5$. Here, no choice of the other entries of L' will make it singular.

Thus, the total number of graphs on k vertices meeting the condition for non-congruence for $n \equiv 1(\mod 8)$ is

$$\frac{1}{2}I(k-3, k-3) + \frac{1}{4}I(k-3, k-4) = \frac{3}{4}I(k-3, k-3)$$

6.3. **The case** $2||n$**.** Finally, what happens when $2 \mid n$?

Again, let us consider graphs on k vertices. Feng and Xiong state later in the paper [**?**] that all odd prime factors must be of the form $p \equiv 1(\mod 4)$ for the graph $G'(n)$ to have rank $k-1$. Thus, we will assume this condition is also met. If we consider the Laplace matrix L of the graph $G'(n)$ we will notice that the row corresponding to 2 is all zeros, so it gives nothing to the rank. Likewise, the column corresponding to 2 is the sum of all the other columns, so it will not contribute to the rank either. Thus, $G'(n)$ is odd only if the upper left $k-1$ by $k-1$ block of L is singular. This block is symmetric, so the number of graphs on k vertices meeting the above conditions is $I(k-1, k-1)$.

References

[BM1] R. P. Brent and B. D. McKay, *Determinants of and rank of random matrices over $\mathbb{Z}_m$, Discrete Math.*, **66** (1987) 35 - 49.

[BM2] R. P. Brent and B. D. McKay, *On determinants of random symmetric matrices over $\mathbb{Z}_m$, ARS Combinatoria*, **26A** (1988) 57 - 64.

[DAV] Davenport, Harold. *Multiplicative Number Theory*, Third Edition (Revised by Hugh L. Montgomery), Springer, New York, 1994.

[FX] K. Feng and M. Xiong, *On Elliptic Curves $y^2 = x^3 - n^2x$ with Rank Zero*, .

[GR] J. Goldman and G.-C. Rota, *On the foundations of combinatorial theory IV: Finite vector spaces and Eulerian generating functions*, *Stud. Appl. Math.* 49(3) (1970) 239 - 258.

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

[K] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer-Verlag, 1984.

[SAT] L. G. Sathe, *On a problem of Hardy on the distribution of intgers having a given number of prime factors I*, *J. Indian Math. Soc.*. **17** (1953) 63-82.
[SEL] A. Selberg, *Note on a paper by L. G. Sathe*, *J. Indian Math. Soc.*. **18** (1954) 83-87.