INTEGERS: ELECTRONIC JOURNAL OF COMBINATORIAL NUMBER THEORY 6 (2006), #A33

TRIVIAL SELMER GROUPS AND EVEN PARTITIONS OF A GRAPH

Morgan V. Brown [1]
Department of Mathematics, Duke University, Durham, NC 27708, USA

Neil J. Calkin [2]
Department Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

Kevin James [3]
Department Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

Adam J. King [4]
Department Mathematical Sciences, University of California - Los Angeles, Los Angeles, CA 90095, USA

Shannon Lockard [5]
Department Mathematical Sciences, Clemson University, Clemson, SC 29634, USA

Robert C Rhoades [6]
Department Mathematics, University of Wisconsin–Madison, Madison, WI 53706, USA

Received: 3/23/06, Revised: 8/30/06, Accepted: 10/6/06, Published: 11/2/06

Abstract

Feng and Xiong give necessary and sufficient conditions to determine when the elliptic curve $E_n : y^2 = x^3 - n^2x$ has trivial 2-Selmer groups in terms of certain graphs $G(n)$ determined by the prime factorization of n. These conditions involve understanding when this graph has no *even* partitions of its vertex set; such a graph is called *odd*. Our main theorems give the probability that a random graph on k vertices is odd, and the probability that a random undirected graph on k vertices has a certain number of even partitions. We relate these probabilities to the problem of determining how many square-free integers yield 2-Selmer groups of a given size and the problem of counting congruent numbers.

[1]Partially supported by NSF grant DMS:0244001.
[2]Partially supported by NSF grant DMS:0244001
[3]Partially supported by NSF grant DMS:0244001
[4]Partially supported by NSF grant DMS:0244001
[5]Partially supported by NSF grant DMS:0244001
[6]Partially supported by NSF grant DMS:0244001 and an NSF graduate fellowship

1. Introduction

A square-free integer n is said to be congruent provided that it is the area of a rational right triangle. The determination of which n are congruent is an old problem studied by many mathematicians (see [K]). It is well known (see [K, sections 1.1 and 1.2]) that n is congruent if and only if the rank of the the elliptic curve

$$E_n : y^2 = x^3 - n^2x$$

is positive.

The rank of an elliptic curve can be a difficult property to study, so we study a more tractable invariant, namely the sizes of the 2-Selmer groups. In particular we study the 2-Selmer groups of the congruent number curves E_n. Let $S = \{\infty\} \cup \{p \text{ prime} : p|2n\}$ and M be the subgroup of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ generated by -1 and all the prime factors of $2n$. For each $d \in M$, we define the curves

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

Then the Selmer groups S_n and S'_n arising from a 2-isogeny of E_n and its dual are defined by

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

where $C_d(\mathbb{Q}_v) \neq \emptyset$ means the curve C_d has nontrivial solutions $(w, t, z) \neq (0, 0, 0)$ in $\mathbb{Q}_v$.

The sizes of these Selmer groups can give information about the rank of E_n as well as information useful in verifying the Birch and Swinnerton-Dyer conjecture. It is clear from the definition that $\{1\} \subset S_n$ and $\{\pm 1, \pm n\} \subset S'_n$. It is well known ([S]) that when $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$, the rank of E_n is zero. In particular, in this case n is a non-congruent number. Furthermore, under these assumptions on S_n and S'_n it is possible to deduce that the Tate-Shafarevic group of E_n has odd order. The significance of this is that for such E_n, verifying the celebrated Birch and Swinnerton-Dyer conjecture becomes a matter of showing a certain special value of the L-function associated to E_n is odd. For more about this the interested reader should see [R1, R2]. This analysis shows why it is useful to understand when the Selmer groups are as small as possible.

The focus of this paper is the problem of counting how many $n < X$, for large X, have Selmer groups a given size. This question was the focus of Heath-Brown's two papers [HB1, HB2]. He gave the following answer to this question.

Theorem 1.1 (Heath-Brown, [HB2] Theorem 2) *Let* $2^{2+s(n)} = |S_n| \cdot |S'_n|$, $\lambda = \prod_{n\geq 1}(1+2^{-n})^{-1} = \prod_{j\geq 1}(1-2^{-2j+1}) = 0.4194\ldots$, *and*

$$d_r = \lambda \frac{2^r}{\prod_{1\leq j\leq r}(2^j - 1)}.$$

Then if $h \equiv 1, 3 \pmod 8$ *and* r *is even, or* $h \equiv 5, 7 \pmod 8$ *and* r *is odd, we have*

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

where $S(X, h)$ *is the set of all square-free integers less than* X *which are congruent to* h *modulo 8.*

Heath-Brown remarks in [HB2] that the convergence in this theorem is very slow. He also remarks that one should consider the rate of convergence to the limiting distribution as depending on the number of prime factors of the number rather than the size of the numbers. For this reason we study the refined problem of determining an asymptotic for the size of

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

where $S(X, h, k)$ is the set of all square-free integers less than X congruent to h modulo 8 which have exactly k prime factors. We will focus on the case where $h = 3$ and $r = 0$.

Our approach begins with a theorem of Feng and Xiong [FX], who give necessary and sufficient conditions for the Selmer groups associated to E_n to have this trivial form. In order to characterize the n for which $E_n : y^2 = x^3 - n^2x$ has trivial 2-Selmer groups, Feng and Xiong [FX] introduce the idea of an even partition of a graph.

Definition 1.2 *Suppose that* G *is a graph with vertex set* V *and edge set* E*. A* partition *of* G *is a pair* (S, T) *of sets 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.) A partition* (S, T) *is* even *provided that all* $v \in S$ *have an even number of edges directed from* v *to vertices in* T *and all* $v \in T$ *have an even number of edges directed from* v *to vertices in* S*.*

In particular, the partition $(G, \emptyset)$ is always an even partition. We call this the trivial (even) partition.

Definition 1.3 *A graph* G *is called* even *provided that it admits a nontrivial even partition. A graph* G *is said to be* odd *provided that it only admits the trivial even partition.*

For example, note that all disconnected graphs are even. Likewise K_4, the complete graph on 4 vertices, is an even graph. To see this, note that the partition $(\{v_1, v_2\}, \{v_3, v_4\})$ is even since each vertex has two neighbors in the other set. In fact, K_{2n} is an even graph for all n. It is easy to see that K_{2n+1} is an odd graph for all $n \geq 1$. Indeed, if (S, T) is a nontrivial partition of $V(K_{2n+1})$, either S or T (say S) contains an odd number of vertices. Then all $v \in T$ have an odd number of neighbors in S, so that (S, T) is not even. Thus K_{2n+1} is an odd graph. Furthermore, 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 $E(C_{2n}) = \{\overline{v_1v_2}, \ldots, \overline{v_{2n}v_1}\}$, and

let $S = \{v_1, v_3, \dots, v_{2n-1}\}$ and $T = \{v_2, v_4, \dots, v_{2n}\}$. 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.

Before stating the first of the main theorems of [FX], we will need to define the graphs considered in that paper. For a square-free odd integer $n = p_1 \dots p_t$, define the directed graph $G(n)$ by

$$V(G(n)) = \{p_1, \dots, p_t\} \text{ and } E(G(n)) = \left\{\overrightarrow{p_i p_j} : \left(\frac{p_i}{p_j}\right) = -1, 1 \le i \ne j \le t\right\}.$$

Theorem 1.4 (Feng-Xiong, [FX] Theorem 2.4) *Suppose that $n \equiv \pm 3 \pmod 8$. Then $S_n = \{1\}$ and $S'_n = \{\pm 1, \pm n\}$ if and only if the following three conditions are satisfied:*

1. $n \equiv 3 \pmod 8$
2. $n = p_1 \dots p_t$, $p_1 \equiv 3 \pmod 4$ *and* $p_j \equiv 1 \pmod 4$ *for* $(2 \le j \le t)$.
3. $G(n)$ *is an odd graph.*

For any n that satisfies the first two conditions, by quadratic reciprocity $G(n)$ can be viewed as an undirected graph. Furthermore, by Dirichlet's theorem on primes in arithmetic progressions and induction on the number of prime factors of n, we see that for any undirected graph G there exist infinitely many n such that $G(n) = G$.

Given that there are infinitely many n such that each undirected graph G appears as $G(n)$, one might hope that selecting n at random would result in selecting a random graph $G(n)$. To make this more precise, fix an integer k, and let $n_1, n_2, n_3, \dots$ be the square-free integers with k prime factors that satisfy the first two conditions of Theorem 1.4. We might hope that if we look at the corresponding sequence of graphs $G(n_1), G(n_2), \dots$, the undirected graphs on k vertices will appear in the sequence with equal proportion. If this is true the proportion of $n_j \in \{n_1, n_2, \dots\}$ that have trivial Selmer groups S_n and S'_n should be the same as the probability that a random undirected graph on k vertices is odd.

In Section 4, we compute the probability that a random undirected graph on k vertices is odd, denoted $q(k)$. We show

$$q(k) = \prod_{j=1}^{s} \left(1 - 2^{-2j+1}\right), \tag{1.1}$$

where $s = \lfloor \frac{k}{2} \rfloor$ is the greatest integer less than or equal to $k/2$. This yields

$$|\{n \in S(X, 3, k) : s(n) = 0\}| \sim q(k) S_k(X),$$

where

$$S_k(X) := \{n < X : n \equiv 3 \pmod 8 \text{ and } n = p_1 p_2 \cdots p_k \text{ where } p_1 \equiv 3, p_j \equiv 1 \pmod 4, j \ne 1\}. \tag{1.2}$$

Although we only give the details for computing an asymptotic for the size of $\{n \in S(X,3,k) : s(n) = 0\}$, the approach given here can be generalized to computing asymptotics for the size of the sets

$$\{n \in S(X,h,k) : s(n) = r\}$$
$$\{n \in S(X,h,k) : |S_n| = 2^r\}$$
$$\{n \in S(X,h,k) : |S_n'| = 2^r\},$$

where h, k, and r are arbitrary. To do so, one would begin with additional work of Feng and Xiong and more recent work of James and Faulkner. Feng and Xiong [FX] give theorems like Theorem 1.4 for the cases when $n \equiv \pm 1 \pmod 8$ and for the case when n is even. Furthermore, recent work of Faulkner and James [FJ] has greatly generalized the work of Feng and Xiong. For each n, Faulkner and James use the prime factorization of n to define a graph associated to n. Then they describe how to compute the size of S_n and S_n' by counting the number of even partitions of a graph depending on n which is defined similarly to $G(n)$.

As a result of their work and the results presented in Sections 3 and 4, for any fixed k, h, s, and s', it is possible to conjecture the proportion of n congruent to h modulo 8 with k prime factors that have $|S_n| = 2^s$ and the proportion of such n with $|S_n'| = 2^{s'}$.

In general, for some set of square-free positive integers $S(X,h,k) = \{n_1, n_2, \dots\}$, we may determine the set of graphs that appear among $G(n_1), G(n_2), \dots$, where $G(n)$ is the appropriately defined graph. Once the structure of these graphs is understood, using Theorems 3.10 and 4.16, or slight variations of them, we can determine the probability that a graph selected at random from this set will have r even partitions. Using the results of Faulkner and James we can then conjecture the proportion of integers in $\{n_1, n_2, \dots\}$ that have Selmer group with size r. To prove the conjecture it is enough to establish the fact that the graphs in the set are independent. In all cases, this should follow from the fact that as we run over all primes p_i and p_j the values of the Legendre symbol $\left(\frac{p_i}{p_j}\right)$ are independent.

Though the motivation for studying even partitions of a graph was its connection to the congruent number problem, the results may be of independent interest. In Section 2 we will give some preliminary results about matrix representations of graphs and how to compute the number of odd partitions of a graph via that representation. One result from this section is that the number of even partitions is a power of two. With this result in hand, in Section 3 we obtain the following theorem:

Theorem 1.5 *If a directed graph on k vertices is chosen at random where the probability of each such graph being selected is equal, then the probability that our graph has 2^j even partitions is given by*

$$\frac{1}{2^{k(k-1)}} \frac{2^{(k-1)^2}(2^k-1)\prod_{i=j+1}^{k-1}\left[1-(1/2)^i\right]^2}{2^{j^2}(2^{j+1}-1)\prod_{i=1}^{k-1-j}\left[1-(1/2)^i\right]}.$$

Answering the same question for the set of undirected graphs is harder. We do that in Section 4 with the following theorem:

Theorem 1.6 *Let $q(k,n)$ be the probability that a graph on k vertices has 2^n even partitions with $0 \leq n \leq k-1$. Then*

$$q(k,n) = d(k-1,n) \cdot 2^{\left[\binom{k-n}{2}-\binom{k}{2}\right]} \prod_{j=1}^{s} \left(1 - \left(\frac{1}{2}\right)^{2j-1}\right),$$

where $s = \lfloor \frac{k-n}{2} \rfloor$, and

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

Finally in Section 5 we relate these results back to the number theoretic results about the congruent number curves by giving numerical evidence to support the claims discussed in this introduction.

2. Matrix Representations

The adjacency matrix $A(G)$ of a graph G is defined by $A(G) = (a_{ij})_{1 \leq i,j \leq k}$, where $a_{ij} = 1$ if $\overrightarrow{v_i v_j} \in E(G)$ and $a_{ij} = 0$ otherwise. It will be more convenient to work with the Laplace matrix of G. Let $d_i = \sum_{j=1}^{k} a_{ij}$ (the out degree of vertex v_i $(1 \leq i \leq k)$). The Laplace matrix of G is defined by $L(G) = diag(d_1, \cdots, d_k) - A(G)$. We will consider $L(G)$ as a matrix over $\mathbb{F}_2$. The following proposition 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 $\vec{v}(S) = (g_j)_{1 \leq j \leq k}$ by $g_j = 1$ if $v_j \notin S$ and $g_j = 0$ if $v_j \in S$.

Proposition 2.7 *The partition (S,T) of $V(G)$ is even if and only if $L(G)\vec{v}(S) = \vec{0}$.*

Proof. Suppose that $b = L(G)\vec{v}(S) \in \mathbb{F}_2^k$ and $b = (b_1, \ldots, b_n)$. Then we have

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

If $v_j \notin S$, then $g_j = 1$ and we have $b_j = \sum_{i=1}^{k}(g_i+1)a_{ji}$. Since $(g_i+1)a_{ji} = 1$ 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 neighbors 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. □

Notice, the matrix $L(G)$ is constructed so that the sum of its columns is 0. This fact in combination with the previous result 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.

The following theorem which appears as Lemma 2.2 in [FX] is an immediate corollary of Proposition 2.7.

Corollary 2.8 *Let $G = (V, E)$ be a directed graph, $k = |V|$ and $r = rank_{\mathbb{F}_2} L(G)$. Then the total number of even partitions of V is 2^{k-r-1}. In particular, 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. By Corollary 2.8, counting graphs on k vertices with 2^m even partitions is equivalent to counting the matrices $L(G)$ which 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 directed graphs on k vertices with 2^m even partitions for all k and m. In Section 4 we consider the case of undirected graphs.

3. Directed Graphs

If G is a directed graph on k vertices then the matrix $L(G)$ is $k \times k$. By the definition of $L(G)$ we see that the sum of its first $k-1$ columns is equal to the k-th column. As a result, the rank of $L(G)$ is the same as the rank of the $k \times (k-1)$ matrix formed by removing the k-th column from $L(G)$. Using this operation there is a 1-1 correspondence between the $k \times (k-1)$ matrices of rank $k-j$ $(1 \le j \le k)$ and the directed graphs with 2^{k-j} even partitions. Thus it suffices to enumerate the $k \times (k-1)$ matrices over $\mathbb{F}_2$ with given rank. This problem has been considered in [BM1] and [GR]. For completeness, we provide a simple proof of the theorem that counts the number of such matrices of rank $k-1$. We then give a second theorem which treats the general problem. For each theorem we state the result in both the language of graph theory and that of matrices over $\mathbb{F}_2$.

We begin by counting the number of $k \times (k-1)$ matrices over $\mathbb{F}_2$ with rank $k-1$.

Theorem 3.9 *The number of directed odd graphs G on k vertices is $\prod_{j=0}^{k-2}(2^k - 2^j)$. This is also the number of $k \times k$ matrices over $\mathbb{F}_2$ that have rank $k-1$ and the sum of the first $(k-1)$ columns is the k^{th} column.*

Proof. Counting the $k \times k$ matrices over $\mathbb{F}_2$ which have rank $k-1$ and the sum of the first $(k-1)$ columns is the k^{th} column is simply the number of ways of selecting $k-1$ independent vectors over $(\mathbb{F}_2)^k$. Once we have selected the first $k-1$ columns of the matrix the final column is determined since it is the sum of the previous $k-1$ columns. Now an ordered set of one linearly independent vector is just a single nonzero vector, of which there are $2^k - 1$ of length k over $\mathbb{F}_2$. Now, assume that there are

$$\prod_{j=0}^{m-1}(2^k - 2^j)$$

ordered sets of m linearly independent vectors of length k. To extend this ordered set to an ordered set of $m+1$ linearly independent vectors, we must append a vector which is not in the span of the first m vectors. Since every vector in this span has the form $\sum_{j=0}^{m} c_j v_j$, where $c_j \in \mathbb{F}_2$, and each choice of c_j's corresponds to a unique vector in the span, there are 2^m vectors in the span. Thus there are $2^k - 2^m$ vectors which are independent with the first m, and therefore there are $2^k - 2^m$ choices for the $(m+1)$st vector. Thus there are

$$\prod_{j=0}^{m}(2^k - 2^j)$$

ordered sets of $m+1$ linearly independent vectors. The following is therefore true by induction: There are exactly

$$\prod_{j=0}^{k-2}(2^k - 2^j)$$

linearly independent ordered sets of $k-1$ vectors of length k. □

It remains to find the number of graphs on k vertices that have 2^j even partitions where $j > 0$. Theorem 1.1 from [BM1] gives the number of $(n+\Delta) \times n$ matrices over $\mathbb{F}_2$ that have a given rank for all n and $\Delta \geq 0$. We now give this result in terms of graphs.

Theorem 3.10 *Suppose that $0 \leq j \leq k-1$. Let $J(k,j)$ denote the number of directed graphs G on k vertices that have 2^j even partitions. Then $J(k,j)$ is also the number of $k \times (k-1)$ matrices over $\mathbb{F}_2$ that have rank $k-1-j$ and*

$$J(k,j) = \frac{2^{(k-1)^2}(2^k - 1)\prod_{i=j+1}^{k-1}\left[1 - (1/2)^i\right]^2}{2^{j^2}(2^{j+1} - 1)\prod_{i=1}^{k-1-j}\left[1 - (1/2)^i\right]}.$$

Taking $j = 0$ in Theorem 3.10, we see that the number of odd graphs on k vertices is given by

$$\begin{aligned} 2^{(k-1)^2}(2^k-1)\prod_{i=1}^{k-1}\left[1-(1/2)^i\right] &= (2^k-1)\prod_{i=1}^{k-1}\left[2^{k-1}-2^{k-1-i}\right] \\ &= \frac{1}{2^{k-1}}\prod_{i=0}^{k-1}\left[2^k-2^i\right] \end{aligned}$$

which is consistent with Theorem 3.9.

We easily obtain the proof of Theorem 1.5.

Proof. (of Theorem 1.5) We note that the total number of directed graphs on k vertices is $2^{k(k-1)}$ and invoke Theorem 3.10. □

4. Undirected Graphs

As mentioned after the statement of Theorem 1.4 we will be interested in determining the number of odd undirected graphs. Counting the number of odd undirected graphs is a bit more difficult to handle than was the case for directed graphs. We will again proceed by counting the number of graphs G on k vertices for which the matrix $L(G)$ has rank $k-1$. To do this we require the following lemma.

Lemma 4.11 *Let G be an undirected graph on k vertices. Let $L(G)$ be defined as before. Define $L^*(G) = (l_{ij})_{1\le i,j\le k-1}$. Then* $\mathrm{rk}(L(G)) = \mathrm{rk}(L^*(G))$.

Proof. We recall from the definition of $L(G)$ that the k-th column is just the sum of the first $k-1$ columns. Since, for undirected graphs, $L(G)$ is symmetric, we also have that the k-th row of $L(G)$ is the sum of the first $k-1$ rows. By performing a sequence of elementary row operations, we can replace the k-th row of $L(G)$ by the sum of all rows. This will have the effect of replacing the k-th row of $L(G)$ by a zero row. (Recall that we are considering $L(G)$ to be a matrix over $\mathbb{F}_2$.) We can then perform a sequence of elementary column operations to replace the k-th column of $L(G)$ by the sum of all columns. This will have the effect of zeroing the k-th column of our matrix. Since none of these operations change the rank of our matrix, the resulting matrix will have the same rank as $L(G)$. However, the resulting matrix has only zeros in its k-th row and column and has $(1,1)$-minor equal to $L^*(G)$. Thus the rank of this matrix is the same as that of $L^*(G)$. □

We note that the * operator gives a 1-1 correspondence between the set of all $L(G)$ as G varies over all undirected graphs on k vertices and the set of $(k-1)\times(k-1)$ symmetric matrices. To see this, note that if we are given any $(k-1)\times(k-1)$ symmetric matrix

$A = (a_{ij})_{1\le i,j\le(k-1)}$, we can 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_* is a symmetric $k \times k$ matrix whose k-th column is equal to the sum of its first $k-1$ columns. Thus there is an undirected graph G on k vertices such that $L(G) = A_*$. Also, $(A_*)^* = A$ and $(L(G)^*)_* = L(G)$.

So to count undirected graphs on k vertices with a given number of even partitions, it suffices to count symmetric $(k-1) \times (k-1)$ matrices with a given rank. Brent and McKay [BM2] determined the number of $n \times n$ symmetric matrices over $\mathbb{F}_2$ with rank n. We extend their results to count the number of matrices with prescribed rank. Throughout the section we give the results in terms of 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 $k \times k$ invertible symmetric matrices. The next two lemmas will allow us to give a recursive formula for the probability that such a symmetric matrix is invertible.

Lemma 4.12 *Suppose $A = (a_{ij})_{1\le i,j\le k}$ is a symmetric $k\times k$ matrix over $\mathbb{F}_2$ and that $a_{11} = 1$. Additionally, let $\Lambda = (\lambda_{ij})_{1\le i,j\le k}$ 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 $B = (b_{ij})_{1\le i,j\le(k-1)}$ is a symmetric $(k-1) \times (k-1)$ matrix. Furthermore, if A is random then so is B.

Proof. Multiplying out, we see that $\Lambda^T A \Lambda$ 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 that B is symmetric. It also follows from this formula that if the first row and column of A are held fixed, then the the lower right $(k-1) \times (k-1)$ submatrix of A completely determines B. Thus, if A is chosen uniformly from the set of all symmetric matrices then so will B be. □

Lemma 4.13 *Suppose $A = (a_{ij})_{1\le i,j\le k}$ is a symmetric $k \times k$ matrix over $\mathbb{F}_2$, $a_{11} = 0$ and $a_{12} = 1$. Additionally, let $\Gamma = (\gamma_{ij})_{1\le i,j\le k}$ 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 $C = (c_{ij})_{1\le i,j\le (k-2)}$ 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 above, the formula implies that if the first row and column of A are held fixed, then the the lower right $(k-2) \times (k-2)$ submatrix of A completely determines C. Thus if A is chosen uniformly from the set of all symmetric matrices, then so will C be. □

The following theorem now gives us a recursion for the probability that a graph on $k+1$ vertices is odd.

Theorem 4.14 *Let $p(k)$ be the probability that a random $k \times k$ symmetric matrix over $\mathbb{F}_2$ is invertible. Then*

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

for $k \ge 2$. We define $p(0) = 1$, and we have $p(1) = 1/2$.

This recursion gives

$$\begin{aligned} p(2n) &= p(2n-1) \\ p(2n-1) &= \left(1 - \left(\frac{1}{2}\right)^{2n-1}\right)p(2n-2) \end{aligned} \tag{4.4}$$

for all $n \ge 1$.

Proof. We begin by deriving (4.3). Let A be a random symmetric $k \times k$ matrix with $k \geq 2$. We derive the recursion by calculating the probability that A is invertible in each of the two cases $a_{11} = 1$ and $a_{11} = 0$. Since these cases are equally likely, we then average their respective conditional probabilities to find $p(k)$.

First suppose $a_{11} = 1$. With the notation of Lemma 4.12 and using the fact $\det(\Lambda) = \det(\Lambda^T) = 1$, we see that $\det(A) = \det(\Lambda^T A \Lambda) = \det(B)$. 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 $p(k-1)$.

Next suppose that $a_{11} = 0$. If $a_{1j} = 0$ for all j, then $\det(A) = 0$, and A is not invertible. Suppose that there exists at least one $j \neq 1$ such that $a_{1j} \neq 0$. This happens with probability $\left(1 - \left(\frac{1}{2}\right)^{k-1}\right)$. 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 4.13 and using the fact $\det(\Gamma) = \det(\Gamma^T) = 1$, we see that $\det(A) = \det(\Gamma^T A \Gamma) = \det(C)$. 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 $\left(1 - \left(\frac{1}{2}\right)^{k-1}\right) p(k-2)$. Averaging these two probabilities gives (4.3).

We will now prove (4.4) by using (4.3) 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 (4.3) we have

$$\begin{aligned} p(2n+1) =& \frac{1}{2}\left(p(2n) + \left(1 - \left(\frac{1}{2}\right)^{2n}\right) p(2n-1)\right) \\ =& \frac{1}{2}\left(1 + \left(1 - \left(\frac{1}{2}\right)^{2n}\right)\right) p(2n) = \left(1 - \left(\frac{1}{2}\right)^{2n+1}\right) p(2n), \end{aligned} \tag{4.5}$$

as desired.

Now using (4.5) 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.

Corollary 4.15 *Let G be an undirected graph on k vertices. The probability that G is odd is*

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

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 4.14 we see that $q(k) = p(k-1)$. Also, using the second set of recursions in Theorem 4.14, 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

Using the same kinds of ideas that we used to derive the number of odd graphs 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 Corollary 2.8 and Lemma 4.11, to reduce the problem to finding how many graphs on k vertices have $k - n - 1 = \mathrm{rk}(L(G)) = \mathrm{rk}(L^*(G))$. 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 $\mathbb{F}_2$. Then in the previous section we showed that

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

where $s = \lfloor \frac{k+1}{2} \rfloor$.

Now, using this result and the following theorem, we can calculate $I(k, r)$ explicitly.

Theorem 4.16 *In the notation above, $I(n, n-j) = d(n, j) I(n-j, n-j)$, where $d(n, j)$ is the number of j dimensional subspaces of $\mathbb{F}_2^n$ 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. As usual, let $e_i = (\underbrace{0,\ldots,0}_{i-1 \text{ times}},1,0,\ldots,0)^T \in \mathbb{F}_2^n$ and $E = \text{span}\,\{e_1,\ldots,e_j\}$. Then we will show that there are $I(n-j,n-j)$ matrices A of size $n\times n$ with rank $n-j$ and $\text{Null}(A) = E$.

To see this we begin by noting that Ae_m is the m^{th} column of the matrix A. Therefore, if A is a symmetric matrix with $Ae_m = \vec{0}$ then the m^{th} 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 all 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 $\hat{A} = (a_{ij})_{(j+1)\le i,j\le n}$ has linearly independent column vectors, that is, if and only if $\hat{A}$ 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$\}$. We will show that there is a 1-1 map from $\mathcal{S}$ onto $\mathcal{E}$, so that these sets have the same size.

We will demonstrate the 1-1 onto map as follows. There exist $k_1,\ldots,k_{n-j}$ such that $\{v_1,\ldots,v_j,\, e_{k_1},\ldots,e_{k_{n-j}}\}$ is a basis for $\mathbb{F}_2^n$. Let B be the change of basis matrix such that $e_s \mapsto v_s$ for $1\le s\le j$ and $e_{j+t}\mapsto e_{k_t}$ for $1\le t\le(n-j)$.

Define the map $\phi:\mathcal{S}\to\mathcal{E}$ by $\phi(A) = B^TAB$. Since B is invertible, so is B^T. Thus, $B^TABv = \vec{0}$ 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 $B^TABv = \vec{0}$ if and only if $v\in E$. Therefore, the map is well-defined onto the spaces indicated. Furthermore, ϕ is 1-1 and onto, since B and B^T are both invertible.

Additionally if A, a symmetric $n\times n$ matrix over $\mathbb{F}_2$, has rank $n-j$ then it has a null space of dimension j. That is $\text{Null}(A) = S$ for some j dimensional subspace S. There are $d(n,j)$ such choices for S. So this step 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 $\prod_{i=0}^{j-1}(2^n-2^i)$ ways to choose j linearly independent vectors from $\mathbb{F}_2^n$. Also, for any subspace of $\mathbb{F}_2^n$ of dimension j there are $\prod_{i=0}^{j-1}(2^j-2^i)$ different bases for that subspace. Hence, the total number of subspaces of $\mathbb{F}_2^n$ of dimension j is $\prod_{i=0}^{j-1}\frac{2^n-2^i}{2^j-2^i}$. □

Proof of Theorem 1.6. We note that the number of undirected graphs on k vertices with 2^n

even partitions is given by

$$\begin{aligned} I(k-1,k-1-n) &= d(k-1,n)\cdot I(k-1-n,k-1-n) \\ &= d(k-1,n)\cdot 2^{\binom{k-n}{2}}\prod_{j=1}^{s}\left(1-\left(\frac{1}{2}\right)^{2j-1}\right), \end{aligned}$$

where $s=\lfloor\frac{k-n}{2}\rfloor$. Theorem 1.6 follows immediately.

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 undirected graphs on k vertices with m distinct even partitions.

$k\backslash m$	1	2	4	8
1	1			
2	1	1		
3	4	3	1	
4	28	28	7	1

5. The Random Model for E_n

In our discussion after Theorem 1.4, we explained that for each graph $G(n)$ with $n\equiv\pm 3 \pmod 8$, if n satisfies the first two conditions of the theorem, then $G(n)$ is an undirected graph. In the previous section we computed the probability that an undirected graph on k vertices is odd. We would like to think of the graph $G(n)$ as being a random graph, and hence be able to deduce the probability that the elliptic curve E_n has trivial Selmer groups.

Theorem 1.4 shows that for each $n=p_1\cdots p_k\equiv 3 \pmod 8$, the fact that $s(n)=0$ depends only on the congruence classes of each p_j modulo 8 and the values of $\left(\frac{p_i}{p_j}\right)$. Thus if these are independent as we vary over all possible sets of primes, then we may deduce that the random model is the appropriate one. More precisely we are led to the following notation. Let $S_k(X)$, be defined as in equation (1.2), so $S_k(X)$ is the set of all $n\equiv\pm 3 \pmod 8$ with $n<X$ such that n also satisfies the first two conditions of Theorem 1.4. Let

$$G(S_k(X))=(G(n):n\in S_k(X))\,,$$

where this list contains each graph with multiplicity. That is, the set $G(S_3(X))$ may contain more than one copy of any particular graph.

In fact, as mentioned earlier each undirected graph on k vertices will appear infinitely often as $X\to\infty$. Thus for large enough X, $G(S_k(X))$ must contain more than one copy of any particular graph. We would like to be able to conclude that as $X\to\infty$ each of the $2^{k(k-1)/2}$ undirected graphs appears equally often in the set $G(S_k(X))$.

For $k = 2, 3, 4$ we have $q(k) = 1/2, 1/2, 7/16 = .4375$, respectively. Thus, if the random model is correct, we would expect the proportion of $n \in S_k(X)$ such that $G(n)$ is odd to approach $q(k)$. We tested this conjecture computationally for $k = 2, 3, 4$. The results are presented in Figures 1, 2 and 3 below. Although these computations are not extensive enough to be conclusive, they do seem to suggest that the conjecture is true for $k = 2$ and that it possibly holds for $k = 3, 4$ as well.

X	Number with $G(n)$ odd	$\lvert S_2(X)\rvert$	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 1: generated from products of two primes not greater than X.

X	Number with $G(n)$ odd	$\lvert S_3(X)\rvert$	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 2: products of three primes not greater than X.

X	Number with $G(n)$ odd	$\lvert S_4(X)\rvert$	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 3: products of four primes not greater than X.

One possible approach to showing that each graph appears with equal probability as $X \to \infty$ would be to show that each edge $\overline{p_i p_j}$ appears with probability 1/2. We expect this probability to be about $\frac{1}{2}$, since the existence of an edge between the vertices corresponding to the primes p_i and p_j is entirely dependent on whether $(\frac{p_i}{p_j})$ is 1 or -1. Furthermore, each

possibility occurs for half of the congruence classes modulo p_j. Actually, since we are putting an extra restriction on p_i, it is necessary to look at which congruence class p_i falls in modulo $8p_j$. This distinction makes no real difference, since each of the two possible values for $(\frac{p_i}{p_j})$ still occurs for exactly half of the allowed congruence classes modulo $8p_j$.

Dirichlet's theorem says that there are infinitely many primes in any arithmetic progression $\{8p + a\}_{k\in\mathbb{N}}$ for each a that is relatively prime to $8p$ and there are the same density of primes in the set $\{8p + a\}$ 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 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.

Acknowledgments

This research took place during the 2004 REU at Clemson University. The authors are thankful for useful discussions with Bryan Faulkner; sixth author is also thankful for useful discussions with Pamela Gorkin and Jeremy Rouse. We are grateful to the referee for making several helpful corrections and very useful suggestions that greatly improved this paper.

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.

[FJ] B. Faulkner and K. James *A graphical approach to computing Selmer groups of congruent number curves*, (preprint).

[FX] K. Feng and M. Xiong, *On elliptic curves $y^2 = x^3 - n^2x$ with rank zero*, *J. Number Theory*, **109** (2004), no. 1, 1 - 26.

[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.

[HB1] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, *Invent. Math.* **111** (1993), no.1, 171-195.

[HB2] D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem. II.* Invent. Math. 118 (1994), no. 2, 331–370

[K] N. Koblitz, *Introduction to elliptic curves and modular forms*, Springer-Verlag, 1984.

[JO] K. James and K. Ono, *Selmer groups of quadratic twists of elliptic curves.* Math. Ann. 314 (1999), no. 1, 1-17.

[R1] K. Rubin, *Tate-Shafarevich group and L-functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527 - 560.

[R2] K. Rubin, *The main conjecture for imaginary quadratic fields*, Invent. Math. **103** (1991), 25 - 68.

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

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