Ilija S. Vrećica

Joint distribution for the Selmer ranks of the congruent number curves

Czechoslovak Mathematical Journal, Vol. 70 (2020), No. 1, 105–119

Persistent URL: http://dml.cz/dmlcz/148044

Czechoslovak Mathematical Journal, 70 (145) (2020), 105–119

JOINT DISTRIBUTION FOR THE SELMER RANKS OF THE CONGRUENT NUMBER CURVES

Ilija S. Vrećica, Belgrade

Received April 4, 2018. Published online September 23, 2019.

Abstract. We determine the distribution over square-free integers n of the pair $(\dim_{\mathbb{F}_2}\operatorname{Sel}^{\Phi}(E_n/\mathbb{Q}), \dim_{\mathbb{F}_2}\operatorname{Sel}^{\widehat{\Phi}}(E'_n/\mathbb{Q}))$, where E_n is a curve in the congruent number curve family, $E'_n\colon y^2 = x^3 + 4n^2x$ is the image of isogeny $\Phi\colon E_n \to E'_n$, $\Phi(x,y) = (y^2/x^2, y(n^2-x^2)/x^2)$, and $\widehat{\Phi}$ is the isogeny dual to Φ.

Keywords: elliptic curve; congruent number problem; Selmer group

MSC 2010: 11G05, 14H52, 11N45

1. Introduction

The elliptic curve E, described by the equation

$$E\colon\ y^2 = x^3 - x,$$

along with the family of its quadratic twists

$$E_n\colon\ y^2 = x^3 - n^2x$$

(where n is an integer), is interesting, because the square-free integer n is a congruent number if and only if the rank $r(n)$ of E_n over $\mathbb{Q}$ is nonzero (see [8]). However, it is difficult to determine the rank of an elliptic curve.

Instead of considering $r(n)$, we may consider the Selmer group associated to isogenies on this curve. Let $\mathcal{M}_2$ be the multiplication by 2 map, let

$$\Phi\colon\ E_n \to E'_n$$

Supported by the Ministry for Science and Technology of Serbia, Grant 174034.

DOI: 10.21136/CMJ.2019.0171-18

be the degree 2 map whose codomain is

$$E'_n\colon\ y^2 = x^3 + 4n^2x$$

defined by

$$\Phi(x,y) = \Big(\frac{y^2}{x^2}, \frac{y(n^2-x^2)}{x^2}\Big),$$

and $\widehat{\Phi}$ its dual isogeny (that is $\Phi \circ \widehat{\Phi} = \mathcal{M}_2$). Let us denote by $\mathrm{Sel}^{\mathcal{M}_2}(E_n)$, $\mathrm{Sel}^{\Phi}(E_n)$ and $\mathrm{Sel}^{\widehat{\Phi}}(E_n)$ the 2-Selmer groups for these isogenies.

From [10] we see that for an odd square-free integer $n = p_1, \dots, p_t$ (where p_i are prime factors), we may identify

$$\mathrm{Sel}^{\Phi}\Big(\frac{E_n}{\mathbb{Q}}\Big) \cong \{d \in M\colon\ C_{1,d}(\mathbb{Q}_v) \neq \emptyset \quad \text{for all } v \in S\},$$
$$\mathrm{Sel}^{\widehat{\Phi}}\Big(\frac{E'_n}{\mathbb{Q}}\Big) \cong \{d \in M\colon\ C'_{1,d}(\mathbb{Q}_v) \neq \emptyset \quad \text{for all } v \in S\},$$

where M is a subgroup of the multiplicative group $\mathbb{Q}^*/(\mathbb{Q}^*)^2$ generated by $-1, 2$, $p_1, \dots, p_t$, $S = \{\infty, 2, p_1, \dots, p_t\}$, and for each $d \in M$, sets $C_{1,d}$ and $C'_{1,d}$ are the homogeneous spaces corresponding to isogenies Φ and $\widehat{\Phi}$. The problem of finding $|\mathrm{Sel}^{\Phi}(E_n/\mathbb{Q})|$ and $|\mathrm{Sel}^{\widehat{\Phi}}(E'_n/\mathbb{Q})|$ is equivalent to determining how many homogeneous spaces $C_{1,d}$ and $C'_{1,d}$, respectively, have nontrivial solutions over certain local fields.

Then, a graph $G_1(n) = (V_1, E_1)$ was constructed in [10] such that $d = p_1, \dots, p_r$ was in $\mathrm{Sel}^{\Phi}(E_n/\mathbb{Q})$ (where $V_1 = \{p_1, \dots, p_t\}$) if and only if the partition

$$\{p_1, \dots, p_r\} \cup \{p_{r+1}, \dots, p_t\}$$

was even (as defined in Definition 2.2). Thus, $\mathrm{Sel}^{\Phi}(E_n/\mathbb{Q})$ has cardinality equal to the number of these partitions of graph $G_1(n)$. Similarly, a graph $G_2(n)$ can be constructed such that $\mathrm{Sel}^{\widehat{\Phi}}(E'_n/\mathbb{Q})$ has cardinality equal to the number of even partitions of $G_2(n)$.

Remark 1.1. Cardinalities of these Selmer groups can thus be expressed as $2^{2+s(n)}$, $2^{s^{\Phi}(n)}$ and $2^{2+s^{\widehat{\Phi}}(n)}$ (as seen in [10]).

An important inequality related to our problem is

$$r(n) \leqslant s(n),$$

which gives a little information as to how likely it is that n is a congruent number. This method has been applied many times (for instance, [2], [3], [4], [5], [6], [10], etc.).

Another approach is to use the fact that $r(n) \leqslant s^{\Phi}(n) + s^{\widehat{\Phi}}(n)$. Since $s^{\Phi}(n)$ and $s^{\widehat{\Phi}}(n)$ are related to the problem of congruent numbers in this way, it is natural to study their joint distribution $(s^{\Phi}(n), s^{\widehat{\Phi}}(n))$.

Rhoades determined the probability that a square-free integer n with m prime factors has $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (0,0)$ in [9]. He utilized a form of representing elements of Selmer groups by even partitions of certain graphs similar to [10]. If $n \equiv \pm 3 \pmod 8$, then $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (0,0)$ if and only if the following three conditions are satisfied:

(1) $n \equiv 3 \pmod 8$,

(2) $n = p_1, \dots, p_m \equiv 3 \pmod 4$, where $p_1 \equiv 3 \pmod 4$ and $p_j \equiv 1 \pmod 4$ for $2 \leqslant j \leqslant m$,

(3) $G(n)$ is an odd graph,

where $G(n)$ is constructed as in Proposition 2.3. First, the density of integers satisfying necessary congruence conditions was calculated, and then amongst those integers the density of integers such that $G_1(n)$ was an odd graph was determined.

In [7], Kane and Klagsbrun determine the distribution of $\dim_{\mathbb{F}_2} \operatorname{Sel}^{\Phi}(E_n/\mathbb{Q})$ when $\dim_{\mathbb{F}_2} \operatorname{Sel}^{\Phi}(E_n/\mathbb{Q}) - \dim_{\mathbb{F}_2} \operatorname{Sel}^{\widehat{\Phi}}(E'_n/\mathbb{Q}) = u$ for a fixed integer u, where E_n are the quadratic twists of E (where E is an elliptic curve with $E(\mathbb{Q})[\mathcal{M}_2] \cong \mathbb{Z}/2\mathbb{Z}$ that has no cyclic 4-isogeny defined over $\mathbb{Q}(E[\mathcal{M}_2])$, and n ranges over square-free integers such that $|d| \leqslant X$), and Φ and $\widehat{\Phi}$ are dual, degree two isogenies on E.

Heath-Brown has found the number of square-free integers $n \leqslant X$ such that $s(n) = r$ in [5] and [6], where r is an integer. Heath-Brown remarked in [6], page 336 that the problem of determining the density of integers n such that $s(n) = r$ should be regarded also for integers with a fixed number of prime factors.

In this paper we calculate the joint distribution for $(s^{\Phi}(n), s^{\widehat{\Phi}}(n))$ over odd, square-free integers n as in [7], with the added condition that the integers n have a fixed number of prime factors. This is why we use the description of the Selmer groups from [10]. Then, in Section 3, we will give the distribution in the case when $n \equiv \pm 3 \pmod 8$ (Theorem 1.2), and in Section 4 when $n \equiv \pm 1 \pmod 8$ (Theorem 1.3).

Theorem 1.2. *For $m \in \mathbb{N}$, p and q nonnegative integers, and $X > 0$ a real number, let $\alpha(X; p, q, m)$ be the probability that a square-free integer $n \leqslant X$ congruent to $\pm 3 \pmod 8$, with m prime factors has $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (p, q)$. When $X \to \infty$, we have:*

(1) *If $q \geqslant p + 1$, we have*

$$\alpha(X; p, q, m) = \sum_{\substack{t_1+t_2=m-q+p-1 \\ s_1+s_2=q-p+1 \\ t_2+s_1 \equiv 1 \pmod 2}} (1+o(1)) \frac{m!}{t_1!\, t_2!\, s_1!\, s_2!} \frac{1}{4^m} \sum_{k=0}^{m-q-1} \operatorname{sym}(m-q+p-1, k) \times E_{m-q+p-1-k, q-p}(m-q-1-k),$$

where sym *is as in Definition* 2.11, *and* E *is as in Proposition* 2.9.

(2) *If* $q = p$, *we have*

$$\alpha(X; q, q, m) = \sum_{\substack{t_1+t_2=m-1\\ s_1+s_2=1\\ t_2+s_1\equiv 1 \pmod 2}} (1+o(1))\frac{m!}{4^m t_1!\, t_2!}\operatorname{sym}(m-1, m-1-q).$$

(3) *If* $p = q + 1$, *we have*

$$\alpha(X; q+1, q, m) = \sum_{\substack{t_1+t_2=m\\ t_2\equiv 1 \pmod 2}} (1+o(1))\frac{m!}{4^m t_1!\, t_2!}\operatorname{par}(m, q),$$

where $\operatorname{par}(m, q)$ *is as in Proposition* 2.4.

(4) *If* $q < p - 1$, $q > m + p - 1$ *or* $m < q + 1$, *then*

$$\alpha(X; p, q, m) = 0.$$

Theorem 1.3. *For* $m \in \mathbb{N}$, p *and* q *nonnegative integers, and* $X > 0$ *a real number, let* $\beta(X; p, q, m)$ *be the probability that a square-free integer* $n \leqslant X$ *congruent to* $\pm 1 \pmod 8$, *with* m *prime factors has* $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (p, q)$. *When* $X \to \infty$, *we have:*

(1) *If* $q \geqslant p$, *we have*

$$\begin{aligned}\beta(X; p, q, m) = &\sum_{\substack{t_1+t_2=m-q+p-2\\ t_2\neq 0\\ s_1+s_2=q-p+2\\ t_2+s_1\equiv 0 \pmod 2}} (1+o(1))\frac{m!}{t_1!\, t_2!\, s_1!\, s_2!}\frac{1}{4^m}\\ &\times\Bigg\{\sum_{k=0}^{m-q-2}\operatorname{sym}(m-q+p-2, k)E_{m-q+p-2-k,q-p}(m-q-2-k)2^{-q}\\ &\quad+\sum_{k=0}^{m-q-3}\operatorname{sym}(m-q+p-2, k)E_{m-q+p-2-k,q-p}\\ &\qquad\qquad\times(m-q-k-3)(1-2^{-q})\Bigg\}\\ &+\sum_{\substack{s_1+s_2=q-p+2\\ s_1\neq 0\\ s_1\equiv 0 \pmod 2}} (1+o(1))\frac{m!}{(m-q+p-2)!\, s_1!\, s_2!}\frac{1}{4^m}\\ &\times\sum_{k=0}^{m-q-2}\operatorname{sym}(m-q+p-2, k)E_{m-q+p-1-k,q-p}(m-q-k-2)\end{aligned}$$

$$+ (1+o(1))\frac{m!}{(m-q+p-2)!\,(q-p+2)!}\frac{1}{4^m}$$
$$\times \sum_{k=0}^{m-q-1} \operatorname{sym}(m-q+p-2,k)E_{m-q+p-k-2,q-p+1}(m-q-k-1).$$

(2) *If* $q = p-1$, *then*

$$\beta(X;q+1,q,m) = \sum_{\substack{t_1+t_2=m-1\\ t_2\neq 0\\ s_1+s_2=1\\ t_2+s_1\equiv 0 \pmod 2}} (1+o(1))\frac{m!}{t_1!\,t_2!}\frac{1}{4^m}(\operatorname{sym}(m-2,m-q-2)2^{-q}$$
$$+\operatorname{sym}(m-2,m-q-3)(1-2^{-q}))$$
$$+(1+o(1))\frac{m}{4^m}\operatorname{sym}(m-1,m-q-1).$$

(3) *If* $q = p-2$, *then*

$$\beta(X;q+2,q,m) = \sum_{\substack{t_1+t_2=m\\ t_2\neq 0\\ t_2\equiv 0 \pmod 2}} (1+o(1))\frac{m!}{t_1!\,t_2!}\frac{1}{4^m}(\operatorname{sym}(m-2,m-q-2)2^{-q}$$
$$+\operatorname{sym}(m-2,m-q-3)(1-2^{-q}))+(1+o(1))\frac{1}{4^m}\operatorname{par}(m,q).$$

(4) *If* $q < p-2$, $q > m-p+2$ *or* $m < q+1$, *then*

$$\beta(X;p,q,m) = 0.$$

2. Preliminaries

In this section we provide the tools necessary for our work.

Definition 2.1. For a directed graph $G = (V,E)$ (where $V = \{v_1,\dots,v_n\}$), we denote by $A(G) = [a_{ij}]$ its adjacency matrix, where for $i \neq j$, we have $a_{ij} = 1$ if $\overrightarrow{v_iv_j} \in E$, and $a_{ij} = 0$ if $\overrightarrow{v_iv_j} \notin E$, and for $i = j$ we have $a_{ii} = 0$. The degree of a vertex $v_i \in V$ is $d_i = \sum_{j=1}^{n} a_{ij}$.

The Laplace matrix of the graph G is the matrix $M(G) = A(G)+\operatorname{diag}(d_1,\dots,d_n)$.

Definition 2.2. If $G = (V,E)$ is a graph, a partition of G is a pair (S,T) of subsets of V such that $S \cap T = \emptyset$ and $S \cup T = V$. A partition (S,T) is even if all $v \in S$ have an even number of edges directed from v to T and all $v \in T$ have an even number of edges directed from v to S. A graph G is odd if it only has two trivial even partitions.

Proposition 2.3 ([10], Theorem 3). *Let $n = p_1 \dots p_t q_1 \dots q_s$ be an odd, square-free integer, p_i odd prime factors of n congruent to* 1 (mod 4), *and q_j odd prime factors congruent to* 3 (mod 4).

(1) *If $n \equiv \pm 3 \pmod 8$, let $G_1(n) = (V_1, E_1)$ be the graph*

$$\begin{aligned}
V_1 &= \{p_1, \dots, p_t, q_1, \dots q_s\},\\
E_1 &= \Big\{\overline{p_i p_j}\colon \Big(\frac{p_j}{p_i}\Big) = -1,\ 1 \leqslant i \neq j \leqslant t\Big\}\\
&\quad \cup \Big\{\overrightarrow{p_i q_r}\colon \Big(\frac{q_r}{p_i}\Big) = -1,\ 1 \leqslant i \leqslant t, 1 \leqslant r \leqslant s\Big\}.
\end{aligned}$$

If $M_1(n)$ is the Laplace matrix of $G_1(n)$, then $s^{\Phi}(n) = t - \mathrm{rank}_{\mathbb{F}_2} M_1(n)$ and $s^{\widehat{\Phi}}(n) = s - 1 + t - \mathrm{rank}_{\mathbb{F}_2} M_1(n)$, where $s^{\Phi}(n)$ and $s^{\widehat{\Phi}}(n)$ are as in Remark 1.1.

(2) *If $n \equiv \pm 1 \pmod 8$, let $G_2(n) = (V_2, E_2)$ be the graph*

$$\begin{aligned}
V_2 &= \{p_1, \dots, p_t, q_1, \dots q_s, -1\},\\
E_2 &= \Big\{\overline{p_i p_j}\colon \Big(\frac{p_j}{p_i}\Big) = -1,\ 1 \leqslant i \neq j \leqslant t\Big\}\\
&\quad \cup \Big\{\overrightarrow{p_i q_r}\colon \Big(\frac{q_r}{p_i}\Big) = -1,\ 1 \leqslant i \leqslant t, 1 \leqslant r \leqslant s\Big\}\\
&\quad \cup \Big\{\overrightarrow{(-1)p}\colon\ p \equiv \pm 3 \pmod 8, p \in V_2\Big\}.
\end{aligned}$$

If $M_2(n)$ is the Laplace matrix of $G_2(n)$, then $s^{\Phi}(n) = t + 1 - \mathrm{rank}_{\mathbb{F}_2} M_2(n)$ and $s^{\widehat{\Phi}}(n) = s - 1 + t - \mathrm{rank}_{\mathbb{F}_2} M_2(n)$.

We will need the next lemmas at the very end of Section 3.

Lemma 2.4 ([9], Theorem 2.7). *Denote the probability that an undirected graph on t vertices has 2^{e+1} even partitions by $\mathrm{par}(t, e)$ for $0 \leqslant e \leqslant t - 1$. Then*

$$\mathrm{par}(t, e) = 2^{\binom{t-e}{2} - \binom{t}{2}} d(t-1, e) \prod_{j=1}^{\lfloor t-e/2 \rfloor} \Big(1 - \Big(\frac{1}{2}\Big)^{2j-1}\Big),$$

where $d(m, j) = \prod\limits_{i=0}^{j-1} (2^m - 2^i)/(2^j - 2^i)$, and $d(m, 0) = 1$.

Lemma 2.5 ([9], Lemma 2.6). *Let G be an undirected graph on t vertices, and denote by ϱ the rank of its Laplace matrix. Then the number of even partitions of graph G is $2^{t-\varrho}$.*

Remark 2.6. Since we will be working over the finite field $\mathbb{F}_2$, we also have the following property for Laplace matrices: any column can be represented as the sum of all the others. This will be useful, as removing the last column will not change the rank of the matrix.

The following proposition tells us what is the density of integers with prime factors that satisfy certain congruence conditions.

Proposition 2.7 ([9], Theorem 3.1). *Let k and m be fixed positive integers with $m > 1$, X a positive real number, $0 \leqslant a_1, \ldots, a_{\varphi(m)} \leqslant k$ integers such that $a_1 + \ldots + a_{\varphi(m)} = k$, and $\pi_k(X; m; a_1, \ldots, a_{\varphi(m)})$ the number of square-free integers $n \leqslant X$ with k prime factors with exactly a_j prime factors congruent to r_j modulo m, where $1 = r_1 < \ldots < r_{\varphi(m)} < m$ are the $\varphi(m)$ standard representatives for $(\mathbb{Z}/m\mathbb{Z})^\times$.*

(1) *When $m = 4$, $t = a_1$, $s = a_2$ and $X \to \infty$, we have*

$$\pi_k(X; 4; t, s) = (1 + o(1)) \frac{k!}{t!\, s!} \frac{1}{2^k (k-1)!} \frac{X (\log\log X)^{k-1}}{\log X}.$$

(2) *When $m = 8$, $t_1 = a_1$, $s_1 = a_2$, $t_2 = a_3$, $s_2 = a_4$, and $X \to \infty$, we have*

$$\pi_k(X; 8; t_1, t_2, s_1, s_2) = (1 + o(1)) \frac{k!}{t_1!\, s_1!\, t_2!\, s_2!} \frac{1}{4^k (k-1)!} \frac{X (\log\log X)^{k-1}}{\log X}.$$

The next proposition tells us that if we wish to add further conditions on the Legendre symbols between prime factors, then the distribution of integers satisfying them will be uniform.

Proposition 2.8 ([9], Theorem 4.1). *Let $k > 1$ be a positive integer. Fix $\varepsilon_{ij} \in \{-1, 1\}$ and $\delta_j \in \{1, 3, 5, 7\}$ for $1 \leqslant j \leqslant k$ and $1 \leqslant i < j \leqslant k$. Let $C_k(X, \delta)$ be the set of k-tuples $(p_1, \ldots, p_k)$ of primes with $2 < p_1 < \ldots < p_k \leqslant X$, $p_1 \ldots p_k \leqslant X$, $p_j \equiv \delta_j \pmod 8$. Then the number of elements of $C_k(X, \delta)$ with $(p_i/p_j) = \varepsilon_{ij}$ for $i < j$ is*

$$2^{-\binom{k}{2}} (1 + o(1)) |C_k(X, \delta)|,$$

when $X \to \infty$.

Denote by $E_{t,s}(\varrho)$ the probability that a $t \times s$ matrix over $\mathbb{F}_2$ has rank ϱ. A simple application of [1], Theorem 1.1 gives us this proposition:

Proposition 2.9 ([1], Theorem 1.1). *Let $t, s, \varrho \geqslant 0$ be integers, $\Pi_n(q) = (1 - q)(1 - q^2) \ldots (1 - q^n)$, $\Pi_0(q) = 1$, and let*

$$\begin{bmatrix} n \\ k \end{bmatrix} (q) = \frac{\Pi_n(q)}{\Pi_k(q) \Pi_{n-k}(q)}$$

be the Gaussian coefficients. Then we have

(1) *If* $s = 0$, $t = 0$, *or* $\varrho > \min\{t, s\}$, *then*

$$E_{t,s}(\varrho) = 0.$$

(2) *If* $t \geqslant s$, *then*

$$E_{t,s}(\varrho) = 2^{(-s+\varrho)(t-\varrho)} \begin{bmatrix} s \\ s-\varrho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_t(\frac{1}{2})}{\Pi_{t-\varrho}(\frac{1}{2})}.$$

(3) *If* $s \geqslant t$, *then*

$$E_{t,s}(\varrho) = 2^{(-t+\varrho)(s-\varrho)} \begin{bmatrix} t \\ t-\varrho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_s(\frac{1}{2})}{\Pi_{s-\varrho}(\frac{1}{2})}.$$

(4) *In the case of a random* $t \times (t+s)$ *matrix over* $\mathbb{F}_2$, *we have*

$$E_{t,t+s}(\varrho) = 2^{(\varrho-t)(t-\varrho+s)} \begin{bmatrix} t \\ t-\varrho \end{bmatrix} \left(\frac{1}{2}\right) \frac{\Pi_{t+s}(\frac{1}{2})}{\Pi_{t-\varrho+s}(\frac{1}{2})}.$$

And finally, we have the probability that a random $n \times n$ symmetric matrix has rank r over the field $\mathbb{F}_2$:

Proposition 2.10. *The number of symmetric* $n \times n$ *matrices of rank* r *over the field* $\mathbb{F}_2$ *is*

$$\begin{bmatrix} n \\ n-r \end{bmatrix}(2) \cdot \prod_{j=1}^{\lceil r/2 \rceil} \left(1 - \left(\frac{1}{2}\right)^{2j-1}\right) 2^{r(r+1)/2}.$$

We have been unable to give an adequate reference to this claim, but we will give a sketch for the proof:

First one shows that if $e_1, \dots, e_r$ are the first r canonical base vectors for $\mathbb{F}_2^n$, then the number of symmetric matrices over $\mathbb{F}_2$ with dimension $n \times n$ and rank $n-r$ which sends $e_1, \dots, e_r$ to 0 is equal to the number of invertible matrices over $\mathbb{F}_2$ with dimension $(n-r) \times (n-r)$, which can be seen (through recursion) to be $2^{(n-r+1)(n-r)/2} \prod_{j=1}^{\lceil n-r/2 \rceil} (1 - (\frac{1}{2})^{2j-1})$.

Next, one proves that the number of matrices with rank $n-r$ which send $e_1, \dots, e_r$ to 0 is equal to the number of matrices with rank $n-r$ which send any set of linearly independent vectors $v_1, \dots, v_r$ to 0.

Finally, one notes that the number of matrices over $\mathbb{F}_2$ of rank $n-r$ and dimension $n \times n$ can be written as a product of the number of r dimensional subspaces of $\mathbb{F}_2^n$ (which can be seen to be equal to the Gaussian coefficient $\begin{bmatrix} n \\ r \end{bmatrix}$) and the number of invertible symmetric matrices over $\mathbb{F}_2$ with dimension $(n-r) \times (n-r)$.

It will be useful to introduce:

Definition 2.11. The probability that a symmetric matrix of dimension $n \times n$ over the field $\mathbb{F}_2$ has rank r is

$$\operatorname{sym}(n,r) = \begin{bmatrix} n \\ n-r \end{bmatrix}(2) \cdot \prod_{j=1}^{\lceil r/2 \rceil} \Big(1 - \Big(\frac{1}{2}\Big)^{2j-1}\Big) 2^{r(r+1)/2 - n(n+1)/2}.$$

3. Proof of Theorem 1.2

Let n be an integer congruent to $\pm 3 \pmod 8$, let $G_1(n)$ be the graph from Proposition 2.3, and let $M_1(n)$ be its Laplace matrix. In order to have $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (p,q)$, we need to have $s^{\Phi}(n) = t - \operatorname{rank}_{\mathbb{F}_2} M_1(n) = p$ and $s^{\widehat{\Phi}}(n) = s - 1 + t - \operatorname{rank}_{\mathbb{F}_2} M_1(n) = q$. Thus we have $s = q - p + 1$, $t = m - s = m - q + p - 1$ and $\operatorname{rank}_{\mathbb{F}_2} M_1(n) = t - p = m - q - 1$. Therefore, the problem is reduced to finding the probabilities that $s = q - p + 1$, $t = m - q + p - 1$, and the probability that the matrix $M_1(n)$ will have rank $\varrho = m - q - 1$.

Remark 3.1. If we look at Proposition 2.3, the above conditions correspond to integers congruent to $\pm 3 \pmod 8$. However, these conditions will be different for integers congruent to $\pm 1 \pmod 8$, which is why we have to separate these cases.

If we look at vertices p_i in the graph described in Proposition 2.3, all edges going between them are undirected, all edges between p_i and q_j are directed towards q_j, there are no edges going from q_j. So, the Laplace matrix $M_1(n)$ of dimension $(t+s) \times (t+s)$ has the form

$$M_1(n) = \left[\begin{array}{c|c} A & B \\ \hline 0 & 0 \end{array}\right],$$

where A is a symmetric matrix of dimension $t \times t$, and B is a matrix of dimension $t \times s$. This matrix has uniformly and independently distributed entries in $\mathbb{F}_2$, up to quadratic reciprocity (Theorem 2.8). So, what we are interested in is the probability that a matrix of the form $[A|B]$ has a certain rank. By Remark 2.6 the last column is the sum of all the others, so we may remove it, and the rank will remain the same.

Lemma 3.2. *The probability that a matrix over $\mathbb{F}_2$ of the form $[AB]$ (with dimension $t \times (t+s)$, and A being a symmetric matrix with dimension $t \times t$) has a given rank ϱ is*

$$\sum_{k=0}^{\varrho} (\operatorname{sym}(t,k) E_{t-k,s}(\varrho - k)).$$

Proof. Let A have rank k. Then we can use elementary row and column operations to transform A into A^0 (canonical matrix for A), which turns $[AB]$ into

$$\left[\begin{array}{c|c|c} E_{k\times k} & 0_{k\times(t-k)} & \multirow{2}{*}{$B'_{t\times s}$} \\ \hline 0_{(t-k)\times k} & 0_{(t-k)\times(t-k)} & \end{array}\right],$$

where E is the identity matrix, and 0 is the zero matrix. We observe that entries in B being independent and uniformly distributed in $\mathbb{F}_2$ will not change after using these elementary row operations. We can then use elementary column operations to make every coefficient in B' that is in the same row as a 1 in A^0 into zero, which gives us

$$\left[\begin{array}{c|c|c} E_{k\times k} & 0_{k\times(t-k)} & 0_{k\times s} \\ \hline 0_{(t-k)\times k} & 0_{(t-k)\times(t-k)} & B''_{(t-k)\times s} \end{array}\right].$$

Therefore, the matrix $[AB]$ having rank ϱ is the same as A having rank k, and B'' having rank $\varrho - k$.

Thus the probability that $[AB]$ has rank ϱ is

$$\begin{aligned} P(\mathrm{rank}AB = \varrho) &= \sum_{k=0}^{\varrho}(P(\mathrm{rank}A = k)P(\mathrm{rank}B'' = \varrho - k)) \\ &= \sum_{k=0}^{\varrho}\mathrm{sym}(t,k)E_{t-k,s}(\varrho - k). \end{aligned}$$

□

We now have to deal with the special cases of $s = 1$ and $s = 0$:

(1) When $s = 1$ and when we remove the last column, we will have just the symmetric matrix A, so the probability that $M_1(n)$ has rankϱ is

$$\mathrm{sym}(t, \varrho).$$

(2) When $s = 0$ (therefore, $m = t$), $M_1(n)$ will be the Laplace matrix of an undirected graph, so by Lemma 2.5, the number of even partitions, 2^{e+1}, will be equal to $2^{t-\varrho}$, and thus $\varrho = t - e - 1$. Therefore, $M_1(n)$ will have rank ϱ if and only if the graph $G_1(n)$ has $2^{t-\varrho}$ even partitions, probability for which is

$$\mathrm{par}(m, t - \varrho - 1).$$

Remark 3.3. We now have the probability that $M_1(n)$ has rank ϱ. When we multiply this with the probability that n has t prime factors congruent to 1 (mod 4) and s prime factors congruent to 3 (mod 4), we will have the probability that an integer $n \leqslant X$ with m prime factors corresponds to the matrix $M_1(n)$ of dimension $t \times (t + s)$ with rank ϱ. However, we have not separated the cases when $n \equiv \pm 3 \pmod 8$ and when $n \equiv \pm 1 \pmod 8$.

To obtain $\alpha(X;p,q,m)$, we need to represent the probability that n has t prime factors congruent to 1 (mod 4) and s prime factors congruent to 3 (mod 4) as the sum of probabilities that n has:

▷ t_1 prime factors congruent to 1 (mod 8),
▷ t_2 prime factors congruent to 5 (mod 8),
▷ s_1 prime factors congruent to 3 (mod 8),
▷ s_2 prime factors congruent to 7 (mod 8).

Clearly, for fixed k, s and t, we have

$$\pi_k(X;4;t,s) = \sum_{\substack{t_1+t_2=t\\ s_1+s_2=s}} \pi_k(X;8;t_1,s_1,t_2,s_2).$$

However, probabilities where t_2+s_1 is even correspond to integers congruent to $\pm 1 \pmod 8$, and probabilities where t_2+s_1 is odd correspond to integers congruent to ± 3, so we only need to factor in those that have t_2+s_1 odd.

We have thus proved Theorem 1.2. □

4. Proof of Theorem 1.3

In this case, the Laplace matrix looks like this:

$$M_2(n) = \begin{bmatrix} A & B & 0 \\ 0 & 0 & 0 \\ b_1 & b_2 & * \end{bmatrix},$$

where the vector $\overline{b_1 b_2}$ is determined by Proposition 2.3 (edges going from -1 to prime factors congruent to ± 3). Since $n \equiv \pm 1 \pmod 8$, we have $* = 0$.

As in the case when $n \equiv \pm 3 \pmod 8$, in order to have $(s^{\Phi}(n), s^{\widehat{\Phi}}(n)) = (p,q)$, we need to have $s^{\Phi}(n) = t+1-\mathrm{rank}_{\mathbb{F}_2} M_2(n) = p$ and $s^{\widehat{\Phi}}(n) = s-1+t-\mathrm{rank}_{\mathbb{F}_2} M_2(n) = q$. Thus we have $s = q-p+2$, $t = m-s = m-q+p-2$, and $\mathrm{rank}_{\mathbb{F}_2} M_1(n) = t+1-p = m-q-1$. In addition to this, let t_1, t_2, s_1 and s_2 be as in Remark 3.3. We are thus left with determining the rank of $M_2(n)$:

$$M_2(n) = \left[\begin{array}{c|c|c|c} A_1 & A_2 & B_1 & B_2 \\ \hline A_3 & A_4 & B_3 & B_4 \\ \hline 0_{1\times t_1} & 1_{1\times t_2} & 1_{1\times s_1} & 0_{1\times s_2} \end{array}\right],$$

where A_1 and A_4 are symmetric matrices of dimensions $t_1 \times t_1$ and $t_2 \times t_2$, $A_2 = A_3^T$ and A_2 is a matrix of dimension $t_1 \times t_2$, and B_1, B_2, B_3 and B_4 are matrices of dimensions $t_1 \times s_1$, $t_1 \times s_2$, $t_2 \times s_1$ and $t_2 \times s_2$. We will be determining the rank in the same fashion as we did in the case when $n \equiv \pm 3 \pmod 8$, except we have 3 cases now:

(1) If we have $t_2 = s_1 = 0$, then the last row only has zeroes, so the probability is calculated in the same way as in Lemma 3.2:

$$\sum_{k=0}^{\varrho} (\mathrm{sym}(t,k) E_{t-k,s}(\varrho - k)).$$

(2) If $t_2 = 0$ and $s_1 \neq 0$, then $M_2(n)$ becomes:

$$\left[\begin{array}{c|c|c} A_1 & B_1 & B_2 \\ \hline 0_{1\times t_1} & 1_{1\times s_1} & 0_{1\times s_2} \end{array}\right].$$

We can use elementary column operations to add the first column which ends with 1 to the others that end with 1, after which we can exchange the last column of the matrix with the first. This will give us

$$\left[\begin{array}{c|c|c} A_1 & B_1 & B_2 \\ \hline 0_{1\times t} & 0_{1\times s_1} & 0\ldots01 \end{array}\right].$$

If matrix A has rank ϱ_1, we can use elementary operations to turn it into the canonical matrix, after which we can use column operations to zero out the top part of the B matrices. We get

$$\left[\begin{array}{c|c|c|c} E_{\varrho_1\times\varrho_1} & 0 & 0 & 0 \\ \hline 0_{(t-\varrho_1)\times\varrho_1} & 0 & B'_1 & B'_2 \\ \hline 0_{1\times\varrho_1} & 0_{1\times(t-\varrho_1)} & 0_{1\times s_1} & 0\ldots01 \end{array}\right].$$

We can rewrite the previous matrix as

$$\left[\begin{array}{c|c|c|c} E_{\varrho_1\times\varrho_1} & 0 & 0 & 0 \\ \hline 0_{(t-\varrho_1)\times\varrho_1} & 0 & B''_1 & B''_2 \\ \hline 0_{1\times\varrho_1} & 0_{1\times(t-\varrho_1)} & 0_{1\times(s-1)} & 1 \end{array}\right],$$

where B''_1 is a $(t-\varrho_1)\times(s-1)$ matrix and B''_2 is a $(t-\varrho_1)\times 1$ matrix. Transforming B''_1 into its canonical matrix (of rank ϱ_2, say), we have

$$\left[\begin{array}{c|c|c|c|c} E_{\varrho_1\times\varrho_1} & 0 & 0 & 0 & 0 \\ \hline 0_{\varrho_2\times\varrho_1} & 0 & E & 0 & 0 \\ \hline 0_{(t-\varrho_1-\varrho_2)\times\varrho_1} & 0 & 0 & 0 & u \\ \hline 0_{1\times\varrho_1} & 0_{1\times(t-\varrho_1)} & 0_{1\times\varrho_2} & 0_{1\times(s-1-\varrho_2)} & 1 \end{array}\right].$$

Therefore, the rank of $M_2(n)$ is $\varrho_1 + \varrho_2 + 1$, regardless of the column u. The probability that $M_2(n)$ has rank ϱ is thus

$$\sum_{\varrho_1+\varrho_2=\varrho-1} \operatorname{sym}(t, \varrho_1) E_{t-\varrho_1, s-1}(\varrho_2).$$

(3) If $t_2 \neq 0$, we can use column operations to zero out all the ones in the matrix using the last column in A. Every time we add that column to another column in A, we do the same thing with rows, to keep the matrix A symmetric. We have

$$\left[\begin{array}{c|c|c|c} A_1 & A_2 & B_1 & B_2 \\ \hline A_3 & A_4 & B_3 & B_4 \\ \hline 0_{1\times t_1} & 0\ldots01 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right].$$

As previously, this can be written down as

$$\left[\begin{array}{c|c|c|c} A'_1 & A'_2 & B'_1 & B'_2 \\ \hline A'_3 & A'_4 & B'_3 & B'_4 \\ \hline 0_{1\times(t-1)} & 1 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right],$$

where A'_1 is a $(t-1)\times(t-1)$ symmetric matrix, A'_2 is a column of length $t-1$ such that $A'_2 = A'^T_3$, and A'_4 is an entry. Transforming A'_1 into canonical shape (while keeping A symmetric), and zeroing out the top part of the matrix B, gives us

$$\left[\begin{array}{c|c|c|c|c} E_{\varrho_1\times\varrho_1} & 0 & 0 & 0 & 0 \\ \hline 0_{(t-1-\varrho_1)\times\varrho_1} & 0 & A''_2 & B''_1 & B''_2 \\ \hline 0_{1\times\varrho_1} & A''_3 & A'_4 & B'_3 & B'_4 \\ \hline 0_{1\times\varrho_1} & 0_{1\times(t-1-\varrho_1)} & 1 & 0_{1\times s_1} & 0_{1\times s_2} \end{array}\right].$$

Doing the same thing with B''_1, we get

$$\left[\begin{array}{c|c|c|c|c|c} E_{\varrho_1\times\varrho_1} & 0 & 0 & 0 & 0 & 0 \\ \hline 0_{\varrho_2\times\varrho_1} & 0 & 0 & 0 & E & 0 \\ \hline 0_{(t-1-\varrho_1-\varrho_2)\times\varrho_1} & 0 & 0 & u & 0 & 0 \\ \hline 0_{1\times\varrho_1} & v & u^T & A'_4 & 0 & w \\ \hline 0_{1\times\varrho_1} & 0_{1\times\varrho_2} & 0_{1\times(t-1-\varrho_1-\varrho_2)} & 1 & 0_{1\times\varrho_2} & 0_{1\times(s-\varrho_2)} \end{array}\right].$$

Therefore, $M_2(n)$ has rank $\varrho_1+\varrho_2+1$ if all the vectors u, v and w are zero vectors. Otherwise, $M_2(n)$ has rank $\varrho_1+\varrho_2+2$. The probability that $M_2(n)$ has rank ϱ is

$$\sum_{\varrho_1+\varrho_2=\varrho-1} \operatorname{sym}(t, \varrho_1) E_{t-\varrho_1, s-1}(\varrho_2) 2^{\varrho-m} + \sum_{\varrho_1+\varrho_2=\varrho-2} \operatorname{sym}(t, \varrho_1) E_{t-\varrho_1, s-1}(\varrho_2)(1 - 2^{\varrho-m}).$$

We are left with special cases when $s = 1$ or $s = 0$. The case when $s = 1$ splits off into two cases, when $t_2 + s_1 > 0$ and when $t_2 + s_1 = 0$. Because $n \equiv \pm 1 \pmod 8$, if $t_2 + s_1 > 0$, when we remove the last column, the final row will still be nonzero. Our matrix (with the final column removed and after elementary operations) will look like

$$\left[\begin{array}{c|c} A_1 & A_2 \\ \hline A_3 & A_4 \\ \hline 0_{1\times(t-1)} & 1 \end{array}\right],$$

where A_1 is a symmetric matrix with dimension $(t-1)\times(t-1)$, and $A_2 = A_3^T$. Turning A_1 into its canonical matrix while preserving the symmetric nature of A, we get

$$\left[\begin{array}{c|c|c} E & 0 & 0 \\ \hline 0 & 0 & A_2' \\ \hline 0 & A_2'^T & A_4 \\ \hline 0_{1\times\varrho_1} & 0_{1\times(t-1-\varrho_1)} & 1 \end{array}\right],$$

where ϱ_1 is the rank of A_1. If column A_2' has nonzero entries, then the rank of $M_2(n)$ is $\varrho_1 + 2$. Otherwise the rank is $\varrho_1 + 1$. Thus, $M_2(n)$ has rank ϱ with probability

$$\operatorname{sym}(t-1, \varrho-1)2^{\varrho-t} + \operatorname{sym}(t-1, \varrho-2)(1-2^{\varrho-t}).$$

If $t_2 + s_1 = 0$, then our matrix will be the symmetric matrix A after removing the last column. The probability that $M_2(n)$ has rankϱ is

$$\operatorname{sym}(t, \varrho).$$

When $s = 0$, we have that $t = m$, and $M_2(n)$ is a symmetric matrix with a row beneath it, which looks like

$$\left[\begin{array}{c|c} A_1 & A_2 \\ \hline 0_{1\times t_1} & 1_{1\times t_2} \end{array}\right]$$

If $t_2 = 0$, then $M_2(n)$ is a Laplace matrix of an undirected graph with m vertices. The probability that $M_2(n)$ has rank ϱ is (from Lemma 2.5)

$$\operatorname{par}(m, m-\varrho-1).$$

If $t_2 \neq 0$, due to the matrix $A = [A_1 A_2]$ being symmetric, the last row is the sum of all the others in addition to the last column of A being the sum of all the other columns. We shall therefore remove the last row of A and the last column of $M_2(n)$. Performing the usual operations, we get

$$\left[\begin{array}{c|c|c} E & 0 & 0 \\ \hline 0 & 0 & A_2' \\ \hline 0 & A_2'^T & A_4 \\ \hline 0_{1\times\varrho_1} & 0_{1\times(m-2-\varrho_1)} & 1 \end{array}\right].$$

The probability that $M_2(n)$ has rank ϱ is

$$\operatorname{sym}(m-2,\varrho-1)2^{\varrho-m+1}+\operatorname{sym}(m-2,\varrho-2)(1-2^{\varrho-m+1}).$$

Combining this with Proposition 2.7, and keeping in mind Remark 3.3 (except now we will demand that t_2+s_1 is even), the proof of Theorem 1.3 is complete. □

Acknowledgement. I wish to thank my graduate thesis advisor Goran Đanković for introducing me to the subject and for his continuous support. I also thank the anonymous referee for his remarks which helped improve the presentation of the results.

References

[1] *R. P. Brent, B. D. McKay*: Determinants and ranks of random matrices over $\mathbb{Z}_m$. Discrete Math. *66* (1987), 35–49. zbl MR doi

[2] *B. Faulkner, K. James*: A graphical approach to computing Selmer groups of congruent number curves. Ramanujan J. *14* (2007), 107–129. zbl MR doi

[3] *K. Feng*: Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture. Acta Arith. *75* (1996), 71–83. zbl MR doi

[4] *K. Feng, M. Xiong*: On elliptic curves $y^2=x^3-n^2x$ with rank zero. J. Number Theory *109* (2004), 1–26. zbl MR doi

[5] *D. R. Heath-Brown*: The size of Selmer groups for the congruent number problem. Invent. Math. *111* (1993), 171–195. zbl MR doi

[6] *D. R. Heath-Brown*: The size of Selmer groups for the congruent number problem II. Invent. Math. *118* (1994), 331–370. zbl MR doi

[7] *D. Kane, Z. Klagsbrun*: On the joint distribution of $\operatorname{Sel}_{\Phi}(E/\mathbb{Q})$ and $\operatorname{Sel}_{\widehat{\Phi}}(E'/\mathbb{Q})$ in quadratic twist families. Available at `https://arxiv.org/abs/1702.02687v1` (2007), 25 pages.

[8] *N. Koblitz*: Introduction to Elliptic Curves and Modular Forms. Graduate Texts in Mathematics 97, Springer, New York, 1984. zbl MR doi

[9] *R. C. Rhoades*: 2-Selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves. J. Number Theory *129* (2009), 1379–1391. zbl MR doi

[10] *M. Xiong, A. Zaharescu*: Selmer groups and Tate-Shafarevich groups for the congruent number problem. Comment. Math. Helv. *84* (2009), 21–56. zbl MR doi

Author's address: Ilija Vrećica, Department of Mathematics, University of Belgrade, Studentski trg 16, Belgrade, Serbia, e-mail: `ilijav@matf.bg.ac.rs`.