Families of non-congruent numbers with arbitrarily many prime factors

Lindsey Reinholz, Blair K. Spearman*, Qiduan Yang

Department of Mathematics and Statistics, University of British Columbia Okanagan, Kelowna, BC V1V 1V7, Canada

Article info

Article history:
Received 18 January 2012
Revised 24 July 2012
Accepted 31 July 2012
Available online 29 September 2012
Communicated by David Goss

MSC:
11G05

Keywords:
Elliptic curve
Congruent numbers
Non-congruent numbers
Rank

Abstract

A method is given for generating families of non-congruent numbers with arbitrarily many prime factors. We then use this method to construct an infinite set of new families of these numbers with prime factors of the form $8k + 3$.

© 2012 Elsevier Inc. All rights reserved.

1. Introduction

A positive integer $n$ is called congruent if it is equal to the area of a right triangle with rational sides. Equivalently, the rank of the elliptic curve

$$y^2 = x(x^2 - n^2)$$

(1)

* Research supported by the Natural Sciences and Engineering Research Council of Canada.
* Corresponding author.
E-mail addresses: reinholz@interchange.ubc.ca (L. Reinholz), blair.spearman@ubc.ca (B.K. Spearman), qiduan.yang@ubc.ca (Q. Yang).

0022-314X/$ – see front matter © 2012 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.jnt.2012.07.011
is positive. Otherwise \( n \) is non-congruent. An extensive discussion of congruent numbers and elliptic curves is given by Koblitz [5]. Families of congruent numbers and non-congruent numbers have been studied with many of the classifications depending on the prime factors of \( n \) combined with values of Legendre symbols which relate the prime factors. A theorem of Heath-Brown [3, Theorem 2] indicates that a positive proportion of the quadratic twists of (1) have rank zero. Positive integers with a bounded number of prime factors have a density of zero as can be deduced from [7, Corollary], so it follows that there exist infinitely many odd squarefree non-congruent numbers with arbitrarily many prime factors. Of particular interest is the following family of non-congruent numbers due to Iskra [4], which contain arbitrarily many prime factors.

**Proposition 1.** Let \( p_1, p_2, \ldots, p_t \) be distinct primes such that \( p_i \equiv 3 \pmod{8} \) and \( (\frac{p_j}{p_i}) = -1 \) for \( j < i \). Then \( n = p_1 p_2 \cdots p_t \) is a non-congruent number.

In this paper, we give a method for explicitly generating these types of families of non-congruent numbers and apply it to construct infinitely many distinct new families. The main idea involves a specially chosen positive integer \( n \) for which the rank of (1) is equal to zero, as well as an infinite set of squarefree integers \( d \) for which the quadratic twist of (1) by \( d \) also has rank zero. This idea has already been investigated by Ono [9, Theorem 1], who for certain elliptic curves \( E \) gives a set of primes \( S \) of density 1/3 for which any twist of \( E \) by a product of primes in \( S \) produces a rank zero curve. Iskra’s theorem on non-congruent numbers with arbitrarily many prime factors [4] is proved by using a complete 2-descent to show that the rank of the elliptic curves (1) is equal to zero. This requires the demonstration of the insolvability of arbitrarily many pairs of quadratic equations over \( \mathbb{Q} \), a method which involves a rapidly increasing amount of computation according to the number of prime factors of \( n \) and the values of the Legendre symbols relating those prime factors. Indeed, even in the case of three primes, Ono notes that a careful analysis is required to demonstrate the property of non-congruence when using a 2-descent [9, p. 350]. As a result, for purposes of efficiency in proof, it is often worthwhile to make use of a different approach to produce non-congruent numbers with arbitrarily many prime factors. For example, Feng [2, Theorem 3.1] employs graph theory. In the proof of our theorem we make use of the Monsky matrix and its rank to bound the rank of (1). Background reading on this matrix is available in [1,8], and in the appendix of [3]. In Section 2 we recall the theory of Monsky matrices, while in Section 3 we use linear algebra to establish conditions necessary for the construction of new families of non-congruent numbers. Finally in Section 4, we prove our theorem. We state our main theorem next.

**Theorem 1.** Let \( m \) be a fixed nonnegative even integer and let \( t \) be any positive integer satisfying \( t \geq m \). Let \( N_m \) denote the set of positive integers with prime factorization \( p_1 p_2 \cdots p_t \), where \( p_1, p_2, \ldots, p_t \) are distinct primes of the form \( 8k + 3 \) such that

\[
\left( \frac{p_j}{p_i} \right) = \begin{cases} 
-1 & \text{if } 1 \leq j < i \text{ and } (j, i) \neq (1, m), \\
+1 & \text{if } 1 \leq j < i \text{ and } (j, i) = (1, m). 
\end{cases}
\]

If \( n \in N_m \), then \( n \) is non-congruent. Moreover for \( m > 0 \), the sets \( N_m \) are pairwise disjoint.

We note that the sets \( N_m \) are nonempty as a consequence of Dirichlet’s theorem on primes in arithmetic progression and that by the Law of Quadratic Reciprocity we have

\[
\left( \frac{p_i}{p_j} \right) = -\left( \frac{p_j}{p_i} \right),
\]

for primes of the form \( 8k + 3 \) with \( i \neq j \).
2. An upper bound for the rank

In this section we will review the Monsky matrix whose entries are defined modulo 2. In order to bound the rank of the elliptic curves (1) in our theorem, we need to recall Monsky’s formula for \( s(n) \), the 2-Selmer rank \([1,8]\). Let \( n \) be a squarefree positive integer with odd prime factors \( P_1, P_2, \ldots, P_t \). We define diagonal \( t \times t \) matrices \( D_l = (d_{ii}) \) for \( l \in \{-2, -1, 2\} \), and the square \( t \times t \) matrix \( A = (a_{ij}) \) by

\[
d_{ii} = \begin{cases} 
0, & \text{if } \left( \frac{1}{P_i} \right) = 1, \\
1, & \text{if } \left( \frac{1}{P_i} \right) = -1, 
\end{cases}
\]

\[
a_{ij} = \begin{cases} 
0, & \text{if } \left( \frac{P_j}{P_i} \right) = 1, \ j \neq i, \\
1, & \text{if } \left( \frac{P_j}{P_i} \right) = -1, \ j \neq i, 
\end{cases}
\]

Then

\[
s(n) = \begin{cases} 
2t - \text{rank}_{\mathbb{F}_2}(M_o), & \text{if } n = P_1 P_2 \cdots P_t, \\
2t - \text{rank}_{\mathbb{F}_2}(M_e), & \text{if } n = 2P_1 P_2 \cdots P_t, 
\end{cases} \quad \text{(3)}
\]

where \( M_o \) and \( M_e \) are the \( 2t \times 2t \) matrices:

\[
M_o = \begin{bmatrix} \frac{A + D_2}{D_2} & \frac{D_2}{A + D_{-2}} \\
\frac{D_2}{A + D_{-2}} & \frac{A + D_2}{D_2} \end{bmatrix}, \quad M_e = \begin{bmatrix} D_2 & \frac{A + D_2}{A^T + D_2} \\
\frac{A + D_2}{A^T + D_2} & D_{-1} \end{bmatrix} \quad \text{(4)}
\]

The fundamental inequality that we use is

\[
r(n) \leq s(n), \quad \text{(5)}
\]

where \( r(n) \) is the rank of (1).

3. Linear algebra and the generation of non-congruent numbers

Our linear algebra will be carried out over the finite field with two elements. In order to apply Monsky’s formula, we need the following identity for block determinants, and a proof of this can be found in Meyer \([6, p. 475]\).

**Proposition 2.** If \( A \) and \( D \) are square matrices, then

\[
\det \left( \begin{bmatrix} A & B \\ C & D \end{bmatrix} \right) = \begin{cases} 
\det(A) \det(D - CA^{-1}B), & \text{when } A^{-1} \text{ exists}, \\
\det(D) \det(A - BD^{-1}C), & \text{when } D^{-1} \text{ exists}. 
\end{cases}
\]

We will also make use of the following identity \([6, p. 483, Exercise 6.2.7]\).

**Proposition 3.** If \( B \) is an invertible \( n \times n \) matrix, and if \( D \) and \( C \) are \( n \times k \) matrices then

\[
\det(B + CD^T) = \det(B) \det(I + D^T B^{-1}C).
\]

For convenience we define three matrices which will be used in our construction of non-congruent numbers.
**Definition 1.** For a positive integer $r$, we define the matrices $U$, $Q$, and $A$ by

$$U = U_r = \begin{bmatrix} r-1 & 1 & 1 & \cdots & 1 & 1 \\ 0 & r-2 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 2 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 0 & 0 \end{bmatrix},$$

$$Q = Q_r = \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ 1 & 0 & 0 & \cdots & 0 & 1 \end{bmatrix},$$

and

$$A = A_r = \begin{bmatrix} r-2 & 1 & 1 & \cdots & 1 & 0 \\ 0 & r-2 & 1 & \cdots & 1 & 1 \\ 0 & 0 & \ddots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & 2 & 1 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 1 \end{bmatrix}.$$

As usual $I = I_r$ denotes the identity matrix and $0 = 0_r$ denotes the zero matrix.

Our first lemma is a direct calculation.

**Lemma 1.** With $Q$ defined as in Definition 1, we have

$$Q^2 = 2Q \equiv 0_r \pmod{2}.$$

The next lemma establishes an identity involving $U$.

**Lemma 2.** With $U$ defined as in Definition 1, we have

$$U(U + I) \equiv 0_r \pmod{2}.$$

**Proof.** We apply mathematical induction on $r$. The lemma is true when $r = 1$ since $U = [0]$ and $U + I = [1]$. Now assume that

$$U_{r-1}(U_{r-1} + I_{r-1}) \equiv 0_{r-1} \pmod{2}.$$

We can write

$$U_r = \begin{bmatrix} r-1 & 1 \cdots & 1 \\ 0 & U_{r-1} \end{bmatrix}.$$
\[
U_r(U_r+I_r) = \begin{bmatrix}
    r-1 & 1 & \cdots & 1 \\
    0 & U_{r-1} \\
\end{bmatrix}
\begin{bmatrix}
    r & 1 & \cdots & 1 \\
    0 & U_{r-1} \end{bmatrix},
\]

which for some \(1 \times (r-1)\) matrix \(W\), simplifies to

\[
\begin{bmatrix}
    r(r-1) & W \\
    0 & U_{r-1}(U_{r-1} + I_{r-1})
\end{bmatrix} \equiv \begin{bmatrix}
    0 & W \\
    0 & 0
\end{bmatrix} \pmod{2}
\]

by the induction hypothesis. It remains to calculate \(W\). We see that

\[
W = [r-1][1 \ 1 \ \cdots \ 1] + [1 \ 1 \ \cdots \ 1][U_{r-1} + I_{r-1}]
\]

\[
= [r-1 \ r-1 \ \cdots \ r-1] + [1 \ 1 \ \cdots \ 1]
\]

\[
= [r-1 \ r-1 \ \cdots \ r-1] + [r-1 \ r-1 \ \cdots \ r-1]
\]

\[
\equiv [0 \ 0 \ \cdots \ 0] \pmod{2}.
\]

The proofs of the next three lemmas use direct calculation.

**Lemma 3.** With \(U\) and \(Q\) as given in Definition 1, we have

\[
UQ = \begin{bmatrix}
    r & 0 & 0 & \cdots & 0 & r \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    0 & 0 & 0 & \cdots & 0 & 0
\end{bmatrix}
\]

**Lemma 4.** With \(U\) and \(Q\) as given in Definition 1, we have

\[
Q(U + I) \equiv \begin{bmatrix}
    r & 1 & 1 & \cdots & 1 & 0 \\
    0 & 0 & 0 & \cdots & 0 & 0 \\
    0 & 0 & 0 & \cdots & 0 & 0 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    0 & 0 & 0 & \cdots & 0 & 0 \\
    r & 1 & 1 & \cdots & 1 & 0
\end{bmatrix} \pmod{2}.
\]

**Lemma 5.** With \(A\) as given in Definition 1, we have

\[
A(A + I) \equiv \begin{bmatrix}
    0 & 1 & 1 & \cdots & 1 & r \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
    1 & 0 & 0 & \cdots & 0 & 1 \\
    r & 1 & 1 & \cdots & 1 & 0
\end{bmatrix} \pmod{2}.
\]
Proof. From Definition 1 we have

\[ A(A + I) \equiv (U + Q)(U + I + Q) \equiv U(U + I) + UQ + Q(U + I) + Q^2 \pmod{2} \]

Applying Lemmas 1, 2, 3, and 4 yields the desired result. \( \square \)

The next lemma provides the starting point for our families of non-congruent numbers.

Lemma 6. With \( A = A_r \) as given in Definition 1, \( r \) even, and \( T \) defined by

\[ T = \begin{bmatrix} 1 & A \\ A + I & 1 \end{bmatrix}, \]

we have \( \det(T) \equiv 1 \pmod{2} \).

Proof. Recalling Lemma 5, we have

\[
A(A + I) \equiv \begin{bmatrix}
0 & 1 & 1 & \cdots & 1 & r \\
1 & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 1 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 \\
r & 1 & 1 & \cdots & 1 & 0
\end{bmatrix} \equiv \begin{bmatrix}
0 & 1 & 1 & \cdots & 1 & 0 \\
0 & 0 & 0 & \cdots & 0 & 1 \\
1 & 0 & 0 & \cdots & 0 & 1 \\
0 & 1 & 1 & \cdots & 1 & 0
\end{bmatrix} \equiv CD^T \pmod{2},
\]

where

\[
C = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \end{bmatrix} \quad \text{and} \quad D^T = \begin{bmatrix} 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix}.
\]

Setting \( B = I_r \) with \( r \) even, using the determinant of block matrices, and applying Proposition 3, allows us to determine that

\[
\det(T) = \det(I - A(A + I)) \\
= \det(I_2 - D^T C) \\
= \det \left( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & 1 & \cdots & 1 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ \vdots & \vdots \\ 0 & 1 \end{bmatrix} \right) \\
= \det \left( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} - \begin{bmatrix} 0 & r - 2 \\ 2 & 0 \end{bmatrix} \right) \\
\equiv \det \left( \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \right) \pmod{2} \\
\equiv 1 \pmod{2}. \quad \square \]
Our final lemma is a crucial step in producing families of non-congruent numbers with arbitrarily many prime factors. This lemma implies that by carefully choosing the primes which we append to an existing non-congruent number, we can preserve the obvious pattern in each of the $U$ and $A$ matrices, thereby producing non-congruent numbers with arbitrarily many prime factors.

**Lemma 7.** Let $m$ be a fixed nonnegative even integer and let $t$ be any positive integer satisfying $t \geq m$. Suppose that the matrix $M = M_{2t}$ is given by

$$
M = \begin{bmatrix}
U + I & I \\
I & U
\end{bmatrix},
$$

with

$$
U = \begin{bmatrix}
U_{11} & U_{12} \\
0 & U_{22}
\end{bmatrix}.
$$

$U_{11}$ is a $(t - m) \times (t - m)$ (possibly empty) matrix given by

$$
U_{11} = \begin{bmatrix}
t - 1 & 1 & 1 & \cdots & 1 \\
0 & t - 2 & 1 & \cdots & 1 \\
0 & 0 & \ddots & \ddots & \vdots \\
\vdots & \vdots & \ddots & \ddots & 1 \\
0 & 0 & \cdots & 0 & m
\end{bmatrix}.
$$

$U_{12}$ is a $(t - m) \times m$ (possibly empty) matrix with all of its entries equal to 1, and $U_{22}$ is a (possibly empty) $m \times m$ matrix of integers with

$$
\det \begin{bmatrix}
I & U_{22} \\
U_{22} + I & I
\end{bmatrix} \equiv 1 \pmod{2}.
$$

Then $\det(M) \equiv 1 \pmod{2}$. We note that by convention the empty matrix has determinant 1 and if $U_{22}$ is empty then $U_{22} + I_0$ is equal to the empty matrix.

**Proof.** After performing row changes on $M$, we obtain the matrix $N$ given by

$$
N = \begin{bmatrix}
I & U \\
U + I & I
\end{bmatrix},
$$

so that

$$
\det(M) = (-1)^t \det(N).
$$

Applying the formula for block determinants given in Proposition 2 we obtain

$$
\det(N) = \det(I) \det(I - UI^{-1}(U + I)) = \det(I - U(U + I)).
$$

Now we see from (6) that

$$
\det(I_m - U_{22}(U_{22} + I_m)) \equiv 1 \pmod{2}.
$$
Meanwhile, $U_{11}(U_{11} + I_{t-m})$ is an upper triangular matrix which has each of its diagonal entries equal to the product of two consecutive integers so that
\[
\det(U_{11}(U_{11} + I_{t-m})) \equiv 0 \pmod{2}. \tag{7}
\]
Therefore,
\[
I_t - U(U + I_t) = I_t - \begin{bmatrix} U_{11} & U_{12} \\ 0 & U_{22} \end{bmatrix} \begin{bmatrix} U_{11} + I_{t-m} & U_{12} \\ 0 & U_{22} + I_m \end{bmatrix} \\
\equiv I_t - \begin{bmatrix} U_{11}(U_{11} + I_{t-m}) & U_{12} \\ 0 & U_{22}(U_{22} + I_m) \end{bmatrix} \pmod{2} \\
\equiv \begin{bmatrix} I_{t-m} - U_{11}(U_{11} + I_{t-m}) & \ast \\ 0 & I_m - U_{22}(U_{22} + I_m) \end{bmatrix} \pmod{2}.
\]
Finally,
\[
\det(M) = (-1)^t \det(N) \\
\equiv \det(I_t - U(U + I_t)) \pmod{2} \\
\equiv \det(I_m - U_{22}(U_{22} + I_m)) \pmod{2} \text{ by (7)} \\
\equiv 1 \pmod{2}. \qedhere
\]

4. Proof of the theorem

Proof. We apply Lemma 7 to generate our families of non-congruent numbers. For the choice of prime factors with Legendre symbols as specified in our theorem, the Monsky matrix (4) becomes
\[
M = \begin{bmatrix} U + I & 1 \\ 1 & U \end{bmatrix},
\]
where
\[
U = \begin{bmatrix} U_{11} & U_{12} \\ 0 & U_{22} \end{bmatrix},
\]
with $U_{11}$ and $U_{12}$ as given in Lemma 7. The matrix $U_{22}$ is chosen to be the empty matrix if $m = 0$, while $U_{22}$ is chosen to equal $A_m$ if $m > 0$. Lemma 6 shows that the conditions of Lemma 7 are fulfilled with these choices so that we can use Lemma 7 to deduce that
\[
\det(M) \equiv 1 \pmod{2}.
\]
Thus the rank of $M$ is equal to $2t$. It follows from (3) that $s(n) = 0$ if $n \in N_m$ and by inequality (5) that the rank of (1) is equal to zero. Hence $n$ is non-congruent. We note that $N_0$ is the family of non-congruent numbers due to Iskra and that $N_2 \subseteq N_0$ by permuting the first two primes in any $n \in N_2$. We now prove that all other sets $N_m$ are new. Assume that the positive integer $n$ satisfies
\[
n \in N_m \cap N_m',
\]
for even integers $m$ and $m'$ with $m' > m \geq 4$. Suppose that the prime factorization of the integer $n$, satisfying (2) is given by
\[ n = p_1 p_2 \cdots p_t \in N_m \]

and that a permutation \( \pi \) of the prime factors \( p_i \) of \( n \) results in

\[ n = q_1 q_2 \cdots q_t \in N_{m'} , \]

where the \( q_i \) are the prime factors of \( n \) and

\[
\left( \frac{q_j}{q_i} \right) = \begin{cases} 
-1 & \text{if } 1 \leq j < i \text{ and } (j, i) \neq (1, m') , \\
1 & \text{if } 1 \leq j < i \text{ and } (j, i) = (1, m') . 
\end{cases} \tag{8}
\]

Let \( k \) denote the largest subscript for which \( p_k \) is not fixed by the permutation \( \pi \). Clearly \( k \geq 2 \).

If \( k = 2 \) then \( q_1 = p_2 \) and \( q_2 = p_1 \) so that \( \left( \frac{q_1}{q_2} \right) = +1 \), contradicting \( 8 \) as \( m' > m \geq 4 \). If \( k = 3 \), then the ordered set \( \{q_1, q_2, q_3\} \) is one of the ordered sets \( \{p_3, p_1, p_2\}, \{p_3, p_2, p_1\}, \{p_1, p_3, p_2\} \) or \( \{p_2, p_3, p_1\} \).

Considering these choices in order leads to the Legendre symbol values

\[
\left( \frac{q_1}{q_2} \right) = +1, \quad \left( \frac{q_1}{q_3} \right) = +1, \quad \left( \frac{q_2}{q_3} \right) = +1, \quad \left( \frac{q_2}{q_3} \right) = +1, \tag{8}
\]

each of which contradicts \( 8 \) and the inequality \( m' > m \geq 4 \). Therefore, \( k \geq 4 \). By the definition of \( k \) we know that \( p_k = q_j \) for some \( j \) satisfying \( 1 \leq j < k \). If \( p_k = q_1 \) then as

\[
\{p_1, p_2, \ldots, p_{k-1}\} = \{q_2, q_3, \ldots, q_k\} \tag{9}
\]

and

\[
\left( \frac{q_1}{q_i} \right) = -1 \tag{10}
\]

for \( 2 \leq i \leq k \) and \( i \neq m' \), we conclude by \( 9 \), \( 10 \) and the inequality \( k \geq 4 \) that the symbol \( \left( \frac{p_k}{p_i} \right) \) has a value of \( -1 \) for at least two values of \( \ell \) satisfying \( 1 \leq \ell \leq k - 1 \). This contradicts \( 2 \). If \( q_k = p_1 \) then we obtain a contradiction in a similar manner. Therefore, \( p_k = q_j \) for some \( j \) satisfying \( 2 \leq j \leq k - 1 \). We also have that \( q_k = p_i \) for some \( i \) satisfying \( 2 \leq i \leq k - 1 \). From \( 8 \) we must have

\[
\left( \frac{q_j}{q_k} \right) = -1,
\]

so that

\[
\left( \frac{p_k}{p_i} \right) = -1
\]

which contradicts \( 2 \). Thus, the sets \( N_m \) and \( N_{m'} \) are distinct. A similar argument shows that for \( m \geq 4 \) the integers in the sets \( N_m \) are different from the integers in Iskra’s theorem \([4]\). \( \square \)

**Remark 1.** The proof of Lemma 6 actually shows that \( T \) does not have full rank if \( m \) is odd and \( m \geq 3 \). Going further, by making use of Schinzel’s hypothesis H \([11]\), we can offer the following evidence that congruent numbers whose prime factors are of the form \( 8k + 3 \) and satisfy \( 2 \) exist whenever \( m \) is odd and \( m \geq 3 \). A similar approach appears in the previously mentioned paper of Ono \([9, Theorem 2]\), where the statement that a family of elliptic curves has positive rank is related to Schinzel’s hypothesis H (called Bouniakowsky’s conjecture). To establish our claim we note that for any positive
rational number \( v \neq 1 \), the form \( v(v-1)(v+1) \), properly scaled to an integer by squares of rational numbers, produces a congruent number [10]. Let \( m \geq 3 \) be odd, and suppose that \( p_2, p_3, \ldots, p_{m-1} \) are distinct prime numbers of the form \( 8k+3 \) satisfying \( (\frac{p_i}{p_j}) = -1 \) if \( 1 \leq j < i \). Define the integer \( d \) by \( d = p_2 p_3 \cdots p_{m-1} \) so that \( d \equiv 3(\text{mod } 8) \). Let \( v = \frac{dx^2}{16y^2} \) for positive integers \( x \) and \( y \). Scaling by squares yields the congruent number

\[
(d^2 - 16y^2) (dx^2 + 16y^2).
\]

We recall Schinzel’s hypothesis H [11] which states that if a finite product \( Q(x) = \prod_{i=1}^{m} f_i(x) \) of polynomials \( f_i(x) \in \mathbb{Z}[x] \) has no fixed divisors, then all of the \( f_i(x) \) will be simultaneously prime, for infinitely many integral values of \( x \). From this hypothesis we deduce that the two forms

\[
dx^2 - 16y^2 \quad \text{and} \quad dx^2 + 16y^2
\]

assume prime values infinitely often. These primes have the form \( 8k+3 \). Furthermore, if \( p \) is any prime divisor of \( d \) then

\[
\left( \frac{dx^2 - 16y^2}{p} \right) = \left( \frac{-1}{p} \right) = -1,
\]

\[
\left( \frac{dx^2 - 16y^2}{dx^2 + 16y^2} \right) = \left( \frac{-2}{dx^2 + 16y^2} \right) = +1,
\]

while

\[
\left( \frac{p}{dx^2 + 16y^2} \right) = -\left( \frac{dx^2 + 16y^2}{p} \right) = -1.
\]

Thus, when \( m \) is odd and \( m \geq 3 \), we cannot generate families of non-congruent numbers.

References