COLLOQUIUM MATHEMATICUM

VOL. 138 2015 NO. 2

ON THE PRIME FACTORS OF NON-CONGRUENT NUMBERS

BY

LINDSEY REINHOLZ, BLAIR K. SPEARMAN and QIDUAN YANG (Kelowna)

Abstract. We give infinitely many new families of non-congruent numbers where the first prime factor of each number is of the form $8k+1$ and the rest of the prime factors have the form $8k+3$. Products of elements in each family are shown to be non-congruent.

1. Introduction. A positive integer n is called *congruent* if it is equal to the area of a right triangle with rational sides. Otherwise n is *non-congruent*. Equivalently the rank of the associated congruent number elliptic curve

$$y^2 = x(x^2 - n^2) \tag{1.1}$$

is non-zero if and only if n is congruent. An extensive discussion of congruent numbers and elliptic curves is given by Koblitz [6]. Families of congruent numbers and non-congruent numbers have been intensively studied. The classification of these numbers often depends on congruence conditions on their prime factors combined with values of Legendre symbols relating the prime factors. For example, a prime number of the form $8k+3$ or a product of two such primes is non-congruent [3, 10]. These facts may be proved by utilizing a complete 2-descent to show that the ranks of the associated congruent number curves are equal to zero. A significant extension of this idea produced the following theorem of Iskra [5].

PROPOSITION 1.1 (Iskra). *Let t be a positive integer and suppose that $p_1, \dots, p_t$ are distinct primes satisfying $p_i \equiv 3 \pmod 8$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then $n = p_1 \cdots p_t$ is a non-congruent number.*

A sequence of primes $\{p_i\}$ that satisfies the conditions of this proposition has the additional property that any product of primes chosen from this sequence is non-congruent. We also mention a couple of results by Lagrange that are related to the main theorem in this paper, and involve non-congruent numbers with two or three prime factors [7]. Lagrange's non-congruent numbers have the form $n = pq$ with $\left(\frac{p}{q}\right) = -1$, or $n = pqr$ with $\left(\frac{p}{q}\right) = -\left(\frac{p}{r}\right)$, where $p \equiv 1 \pmod 8$ and $q \equiv r \equiv 3 \pmod 8$.

2010 *Mathematics Subject Classification*: Primary 11G05.
Key words and phrases: elliptic curve, congruent numbers, non-congruent numbers, rank.

DOI: 10.4064/cm138-2-11

Recently, ideas from graph theory have enabled authors, such as Feng, to construct new families of non-congruent numbers [2]. One of Feng's theorems generalizes Lagrange's non-congruent numbers in the case of two prime factors. However, in the present paper, we extend the aforementioned non-congruent numbers of Lagrange to produce infinitely many new families of non-congruent numbers without appealing to graph theory. Our non-congruent numbers are different from those of Feng, and we give details on this after completing the proof of our theorem. These new families have a property similar to that described immediately following Proposition 1.1, in that they give rise to a sequence of integers such that any product of them is non-congruent. Our method of proof makes use of the Monsky matrix in order to provide an upper bound of zero for the rank of the elliptic curve (1.1). Additionally we require some crucial results from linear algebra. These are recalled in Section 2. In Section 3 we prove our theorem, which we state now.

THEOREM 1.2. *Let m be a fixed positive integer and let t be any integer satisfying $t \geq m$. Let S_m denote the set of positive integers with prime factorization $pq_1 \cdots q_t$, where p is a prime of the form $8k+1$ and $q_1, \ldots, q_t$ are distinct primes of the form $8k+3$ such that*

$$\left(\frac{p}{q_i}\right) = \begin{cases} -1 & \text{if } i = m, \\ 1 & \text{if } i \neq m, \end{cases}$$

and

$$\left(\frac{q_j}{q_i}\right) = -1 \quad \text{if } j < i.$$

If $n \in S_m$, then n is non-congruent. Moreover, for different m, the sets S_m are pairwise disjoint.

We note that the sets S_m are non-empty as a consequence of Dirichlet's theorem on primes in arithmetic progression, and further, that we can form sequences

$$p, q_1, q_2, \ldots$$

of prime numbers satisfying the hypotheses of our theorem. This leads to the following corollary.

COROLLARY 1.3. *Let $\{p, q_1, \ldots, q_m, q_{m+1}, \ldots\}$ be a sequence of prime numbers satisfying the hypotheses of the previous theorem. Any product of integers from the set*

$$\{pq_1 \cdots q_m, q_{m+1}, q_{m+2}, \ldots\}$$

is non-congruent.

2. An upper bound for the rank. In this section we review the Monsky matrix whose entries are defined modulo 2. In order to bound the rank of the elliptic curves (1.1) in our theorem, we need to recall Monsky's formula for $s(n)$, the 2-*Selmer rank*. Background information on this matrix is available in [1, 9], and in the appendix of [4].

Let n be a square-free positive integer with odd prime factors $P_1, \dots, P_t$. We define diagonal $t \times t$ matrices $\mathbf{D}_l = [d_i]$ for $l \in \{-2, -1, 2\}$ and a square $t \times t$ matrix $\mathbf{A} = [a_{ij}]$ by

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

and

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

$$a_{ii} = \sum_{j:\, j \neq i} a_{ij}.$$

Then

$$s(n) = \begin{cases} 2t - \operatorname{rank}_{\mathbb{F}_2}(\mathbf{M}_o) & \text{if } n = P_1 \cdots P_t, \\ 2t - \operatorname{rank}_{\mathbb{F}_2}(\mathbf{M}_e) & \text{if } n = 2P_1 \cdots P_t, \end{cases} \tag{2.1}$$

where $\mathbf{M}_o$ and $\mathbf{M}_e$ are the $2t \times 2t$ matrices

$$\mathbf{M}_o = \left[\begin{array}{c|c} \mathbf{A} + \mathbf{D}_2 & \mathbf{D}_2 \\ \hline \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_{-2} \end{array}\right]$$

and

$$\mathbf{M}_e = \left[\begin{array}{c|c} \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_2 \\ \hline \mathbf{A}^T + \mathbf{D}_2 & \mathbf{D}_{-1} \end{array}\right].$$

The fundamental inequality that we use is

$$r(n) \leq s(n), \tag{2.2}$$

where $r(n)$ is the rank of (1.1).

Our linear algebra is carried out over the finite field with two elements. In order to apply Monsky's formula, we need the following identity for block determinants; a proof can be found in Meyer [8, p. 475].

PROPOSITION 2.1. *If* $\mathbf{A}$ *and* $\mathbf{D}$ *are square matrices, then*

$$\det\left(\begin{bmatrix} \mathbf{A} & \mathbf{B} \\ \mathbf{C} & \mathbf{D} \end{bmatrix}\right) = \begin{cases} \det(\mathbf{A}) \det(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}) & \textit{when } \mathbf{A}^{-1} \textit{ exists,} \\ \det(\mathbf{D}) \det(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C}) & \textit{when } \mathbf{D}^{-1} \textit{ exists.} \end{cases}$$

3. Proofs

Proof of Theorem 1.2. Going directly to the Monsky matrix we have

$\mathbf{M}_o =$

$$\left[\begin{array}{cccccccccccc|cccccccccccc}
1 & 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 1 & 2 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 1 & \ddots & & & & & & & \vdots \\
0 & 1 & 1 & 3 & & & & & & & 0 & \vdots & & \ddots & \ddots & \ddots & & & & & & \vdots \\
\vdots & \vdots & \vdots & & \ddots & & & & & & \vdots & \vdots & & & \ddots & \ddots & \ddots & & & & & \vdots \\
0 & 1 & 1 & \cdots & 1 & m{-}1 & 0 & \cdots & \cdots & \cdots & 0 & \vdots & & & & \ddots & \ddots & \ddots & & & & \vdots \\
1 & 1 & 1 & \cdots & \cdots & 1 & m{+}1 & 0 & \cdots & \cdots & 0 & \vdots & & & & & \ddots & \ddots & \ddots & & & \vdots \\
0 & 1 & 1 & \cdots & \cdots & \cdots & 1 & m{+}1 & 0 & \cdots & 0 & \vdots & & & & & & \ddots & \ddots & \ddots & & \vdots \\
\vdots & \vdots & \vdots & & & & & & \ddots & & \vdots & \vdots & & & & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \vdots & & & & & & & t{-}2 & 0 & \vdots & & & & & & & & \ddots & \ddots & 0 \\
0 & 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & t{-}1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \\
\hline
0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 1 & \ddots & & & & & & & \vdots & 0 & 1 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & \ddots & \ddots & \ddots & & & & & & \vdots & 0 & 1 & 1 & 2 & & & & & & & 0 \\
\vdots & & & \ddots & \ddots & \ddots & & & & & \vdots & \vdots & \vdots & \vdots & & \ddots & & & & & & \vdots \\
\vdots & & & & \ddots & \ddots & \ddots & & & & \vdots & 0 & 1 & 1 & \cdots & 1 & m{-}2 & 0 & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & \ddots & \ddots & \ddots & & & \vdots & 1 & 1 & 1 & \cdots & \cdots & 1 & m & 0 & \cdots & \cdots & 0 \\
\vdots & & & & & & \ddots & \ddots & \ddots & & \vdots & 0 & 1 & 1 & \cdots & \cdots & \cdots & 1 & m & 0 & \cdots & 0 \\
\vdots & & & & & & & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & & & & & & \ddots & & \vdots \\
\vdots & & & & & & & & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & & & & & & t{-}3 & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & 0 & 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & t{-}2
\end{array}\right].$$

Note that each block in $\mathbf{M}_o$ is a $t \times t$ matrix. We start by applying a sequence of elementary row and column operations on $\mathbf{M}_o$. Specifically, we add column 1 to column $t+1$ and then subtract column $t+(m+1)$ from column $t+1$. This is followed by adding row 1 to row $t+1$ and then subtracting row $t+(m+1)$ from row $t+1$. We obtain a matrix $\mathbf{M}'_o$:

$\mathbf{M}'_o =$

$$\left[\begin{array}{cccccccccccc|cccccccccccc}
1 & 0 & \cdots & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0 & 1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 1 & 2 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 1 & \ddots & & & & & & & \vdots \\
0 & 1 & 1 & 3 & & & & & & & 0 & \vdots & & \ddots & \ddots & \ddots & & & & & & \vdots \\
\vdots & \vdots & \vdots & & \ddots & & & & & & \vdots & \vdots & & & \ddots & \ddots & \ddots & & & & & \vdots \\
0 & 1 & 1 & \cdots & 1 & m{-}1 & 0 & \cdots & \cdots & \cdots & 0 & \vdots & & & & \ddots & \ddots & \ddots & & & & \vdots \\
1 & 1 & 1 & \cdots & \cdots & 1 & m{+}1 & 0 & \cdots & \cdots & 0 & \vdots & & & & & \ddots & \ddots & \ddots & & & \vdots \\
0 & 1 & 1 & \cdots & \cdots & \cdots & 1 & m{+}1 & 0 & \cdots & 0 & \vdots & & & & & & \ddots & \ddots & \ddots & & \vdots \\
\vdots & \vdots & \vdots & & & & & & \ddots & & \vdots & \vdots & & & & & & & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & \vdots & & & & & & & t{-}2 & 0 & \vdots & & & & & & & & \ddots & \ddots & 0 \\
0 & 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & t{-}1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 \\
\hline
1 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & m & -1 & \cdots & \cdots & \cdots & -1 & 1{-}m & 0 & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 0 & 0 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 1 & \ddots & & & & & & & \vdots & 0 & 1 & 1 & 0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\
\vdots & & \ddots & \ddots & \ddots & & & & & & \vdots & 0 & 1 & 1 & 2 & & & & & & & 0 \\
\vdots & & & \ddots & \ddots & \ddots & & & & & \vdots & \vdots & \vdots & \vdots & & \ddots & & & & & & \vdots \\
\vdots & & & & \ddots & \ddots & \ddots & & & & \vdots & 0 & 1 & 1 & \cdots & 1 & m{-}2 & 0 & \cdots & \cdots & \cdots & 0 \\
\vdots & & & & & \ddots & \ddots & \ddots & & & \vdots & 1{-}m & 1 & 1 & \cdots & \cdots & 1 & m & 0 & \cdots & \cdots & 0 \\
\vdots & & & & & & \ddots & \ddots & \ddots & & \vdots & -1 & 1 & 1 & \cdots & \cdots & \cdots & 1 & m & 0 & \cdots & 0 \\
\vdots & & & & & & & \ddots & \ddots & \ddots & \vdots & \vdots & \vdots & \vdots & & & & & \ddots & & \vdots \\
\vdots & & & & & & & & \ddots & \ddots & 0 & \vdots & \vdots & \vdots & & & & & & t{-}3 & 0 \\
0 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 0 & 1 & -1 & 1 & 1 & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & 1 & t{-}2
\end{array}\right].$$

We can write this matrix in the form

$$\mathbf{M}'_o = \begin{bmatrix} \mathbf{U} & \mathbf{I}_t \\ \mathbf{I}_t & \mathbf{V} \end{bmatrix},$$

where $\mathbf{I}_t$ is the $t \times t$ identity matrix,

$$\mathbf{U} = \left[\begin{array}{cccccc|ccccc}
1 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\
0 & 1 & 0 & \cdots & \cdots & 0 & \vdots & & & & \vdots \\
0 & 1 & 2 & \ddots & & \vdots & \vdots & & & & \vdots \\
\vdots & \vdots & & \ddots & \ddots & \vdots & \vdots & & & & \vdots \\
0 & 1 & \cdots & 1 & m-1 & 0 & \vdots & & & & \vdots \\
1 & 1 & \cdots & \cdots & 1 & m+1 & 0 & \cdots & \cdots & \cdots & 0 \\
\hline
0 & 1 & \cdots & \cdots & \cdots & 1 & m+1 & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & & & & \vdots & 1 & m+2 & \ddots & & \vdots \\
\vdots & \vdots & & & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & & & & \vdots & \vdots & & \ddots & t-2 & 0 \\
0 & 1 & \cdots & \cdots & \cdots & 1 & 1 & \cdots & \cdots & 1 & t-1
\end{array}\right] = \begin{bmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{bmatrix},$$

and

$$\mathbf{V} = \left[\begin{array}{ccccccc|ccccc}
m & -1 & -1 & \cdots & \cdots & -1 & 1-m & 0 & \cdots & \cdots & \cdots & 0 \\
0 & 0 & 0 & \cdots & \cdots & \cdots & 0 & \vdots & & & & \vdots \\
0 & 1 & 1 & 0 & & & \vdots & \vdots & & & & \vdots \\
0 & 1 & 1 & 2 & \ddots & & \vdots & \vdots & & & & \vdots \\
\vdots & \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & & & \vdots \\
0 & 1 & \cdots & \cdots & 1 & m-2 & 0 & \vdots & & & & \vdots \\
1-m & 1 & \cdots & \cdots & \cdots & 1 & m & 0 & \cdots & \cdots & \cdots & 0 \\
\hline
-1 & 1 & \cdots & \cdots & \cdots & \cdots & 1 & m & 0 & \cdots & \cdots & 0 \\
\vdots & \vdots & & & & & \vdots & 1 & m+1 & \ddots & & \vdots \\
\vdots & \vdots & & & & & \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\
\vdots & \vdots & & & & & \vdots & \vdots & & \ddots & t-3 & 0 \\
-1 & 1 & \cdots & \cdots & \cdots & \cdots & 1 & 1 & \cdots & \cdots & 1 & t-2
\end{array}\right] = \begin{bmatrix} \mathbf{V}_{11} & \mathbf{V}_{12} \\ \mathbf{V}_{21} & \mathbf{V}_{22} \end{bmatrix}.$$

The matrix resulting from performing t row interchanges on $\mathbf{M}_o'$ is

$$\mathbf{N} = \begin{bmatrix} \mathbf{I}_t & \mathbf{V} \\ \mathbf{U} & \mathbf{I}_t \end{bmatrix}.$$

Note that

$$\det(\mathbf{M}_o) = \det(\mathbf{M}_o') = (-1)^t \det(\mathbf{N}).$$

In addition, by the formula for block determinants given in Proposition 2.1,

$$\det(\mathbf{N}) = \det\left(\begin{bmatrix} \mathbf{I}_t & \mathbf{V} \\ \mathbf{U} & \mathbf{I}_t \end{bmatrix}\right) = \det(\mathbf{I}_t)\det(\mathbf{I}_t - \mathbf{U}\mathbf{I}_t^{-1}\mathbf{V}) = \det(\mathbf{I}_t - \mathbf{U}\mathbf{V}).$$

Consider

$$\begin{aligned}
&\mathbf{U}_{11}\mathbf{V}_{11} \\
&= \begin{bmatrix} 1 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & 2 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \vdots \\ 0 & 1 & \cdots & 1 & m-1 & 0 \\ 1 & 1 & \cdots & \cdots & 1 & m+1 \end{bmatrix} \begin{bmatrix} m & -1 & -1 & \cdots & \cdots & -1 & 1-m \\ 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 1 & 0 & & & \vdots \\ 0 & 1 & 1 & 2 & \ddots & & \vdots \\ \vdots & \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & 1 & \cdots & \cdots & 1 & m-2 & 0 \\ 1-m & 1 & \cdots & \cdots & \cdots & 1 & m \end{bmatrix} \\
&= \begin{bmatrix} m+(1-m) & 0 & 0 & \cdots & \cdots & 0 & (1-m)+m \\ 0 & 0 & 0 & \cdots & \cdots & 0 & 0 \\ 0 & 2 & 2 & \ddots & & & \vdots \\ \vdots & 4 & 4 & 6 & \ddots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & & & & & \ddots & 0 \\ m+(m+1)(1-m) & * & \cdots & \cdots & \cdots & * & (1-m)+m(m+1) \end{bmatrix}.
\end{aligned}$$

Notice that all of the diagonal entries in the matrix $\mathbf{U}_{11}\mathbf{V}_{11}$, except for the two corner ones, are equal to the product of two consecutive integers, so they are congruent to 0 modulo 2. Moreover all of the entries of $\mathbf{U}_{11}\mathbf{V}_{11}$, except for the corner ones, in the first and last row are even, which means that they are congruent to 0 modulo 2. We note that the entries denoted by $*$ are of the form

$$-1 + (m-2) + (m+1),$$

hence are even. We reduce $\mathbf{U}_{11}\mathbf{V}_{11}$ modulo 2 to obtain

$$\mathbf{U}_{11}\mathbf{V}_{11} \equiv \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ 0 & \vdots & & \vdots & 0 \\ -m^2+m+1 & 0 & \cdots & 0 & m^2+1 \end{bmatrix} \pmod 2.$$

Further reduction modulo 2 yields

$$\mathbf{U}_{11}\mathbf{V}_{11} \equiv \begin{cases} \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 1 \end{bmatrix} \pmod 2 & \text{if } m \text{ is even,} \\ \begin{bmatrix} 1 & 0 & \cdots & 0 & 1 \\ 0 & 0 & & & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & & & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 \end{bmatrix} \pmod 2 & \text{if } m \text{ is odd.} \end{cases}$$

Returning to the matrices $\mathbf{U}$ and $\mathbf{V}$, we notice that all of the entries in $\mathbf{U}_{12}$ and $\mathbf{V}_{12}$ are equal to zero. In addition,

$$\mathbf{U}_{22}\mathbf{V}_{22} = \begin{bmatrix} m+1 & 0 & \cdots & \cdots & 0 \\ 1 & m+2 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & t-2 & 0 \\ 1 & \cdots & \cdots & 1 & t-1 \end{bmatrix} \begin{bmatrix} m & 0 & \cdots & \cdots & 0 \\ 1 & m+1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & t-3 & 0 \\ 1 & \cdots & \cdots & 1 & t-2 \end{bmatrix}.$$

This product of lower triangular matrices is lower triangular. Each diagonal entry in the matrix $\mathbf{U}_{22}\mathbf{V}_{22}$ is equal to the product of two consecutive integers, hence is congruent to 0 modulo 2. Therefore,

$$\mathbf{I}_t - \mathbf{UV} = \mathbf{I}_t - \begin{bmatrix} \mathbf{U}_{11} & \mathbf{U}_{12} \\ \mathbf{U}_{21} & \mathbf{U}_{22} \end{bmatrix} \begin{bmatrix} \mathbf{V}_{11} & \mathbf{V}_{12} \\ \mathbf{V}_{21} & \mathbf{V}_{22} \end{bmatrix} = \mathbf{I}_t - \begin{bmatrix} \mathbf{U}_{11}\mathbf{V}_{11} & \mathbf{0} \\ * & \mathbf{U}_{22}\mathbf{V}_{22} \end{bmatrix}.$$

If m is even then

$$\mathbf{I}_t - \mathbf{UV} \equiv \left[\begin{array}{cccccc|cccccc} 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & 0 & \vdots & & & & \vdots \\ 0 & 0 & 1 & \ddots & & \vdots & \vdots & & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & & & \vdots \\ 0 & & & \ddots & 1 & 0 & \vdots & & & & \vdots \\ 1 & 0 & \cdots & \cdots & 0 & 0 & 0 & \cdots & \cdots & \cdots & 0 \\ \hline & & & & & & 1 & 0 & \cdots & \cdots & 0 \\ & & & & & & * & \ddots & \ddots & & \vdots \\ & & & * & & & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & & & \vdots & & \ddots & \ddots & 0 \\ & & & & & & * & \cdots & \cdots & * & 1 \end{array}\right] \pmod 2$$

and

$$\begin{aligned} \det(\mathbf{M}_o) &= (-1)^t \det(\mathbf{N}) = (-1)^t \det(\mathbf{I}_t - \mathbf{UV}) \\ &\equiv (-1)^t \det \left(\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & \ddots & 1 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \end{bmatrix} \right) \pmod 2. \end{aligned}$$

Since interchanging rows in a matrix changes the sign of its determinant, by exchanging the first and last rows, we have

$$\det(\mathbf{M}_o) \equiv -\det \left(\begin{bmatrix} 1 & 0 & \cdots & \cdots & 0 \\ 0 & 1 & \ddots & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & 1 & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{bmatrix} \right) \equiv 1 \pmod 2.$$

If m is odd then

$$\mathbf{I}_t - \mathbf{UV} \equiv \left[\begin{array}{cccccc|ccccc} 0 & 0 & 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & 0 & \vdots & & & & \vdots \\ 0 & 0 & 1 & \ddots & & \vdots & \vdots & & & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots & \vdots & & & & \vdots \\ 0 & & & \ddots & 1 & 0 & \vdots & & & & \vdots \\ 1 & 0 & \cdots & \cdots & 0 & 1 & 0 & \cdots & \cdots & \cdots & 0 \\ \hline & & & & & & 1 & 0 & \cdots & \cdots & 0 \\ & & & & & & * & \ddots & \ddots & & \vdots \\ & & & * & & & \vdots & \ddots & \ddots & \ddots & \vdots \\ & & & & & & \vdots & & \ddots & \ddots & 0 \\ & & & & & & * & \cdots & \cdots & * & 1 \end{array}\right] \pmod 2$$

and

$$\det(\mathbf{M}_o) = (-1)^t \det(\mathbf{N}) = (-1)^t \det(\mathbf{I}_t - \mathbf{UV})$$

$$\equiv (-1)^t \det\left(\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & \ddots & 1 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 1 \end{bmatrix}\right) \pmod 2.$$

Continuing by subtracting the first row of this matrix from the last row yields

$$\det(\mathbf{M}_o) \equiv (-1)^t \det\left(\begin{bmatrix} 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & \ddots & & \vdots \\ \vdots & & \ddots & \ddots & \ddots & \vdots \\ 0 & & & \ddots & 1 & 0 \\ 1 & 0 & \cdots & \cdots & 0 & 0 \end{bmatrix}\right) \pmod 2.$$

This matrix is the same as the one we obtained in the case where m was even. As a result, we conclude that

$$\det(\mathbf{M}_o) \equiv 1 \pmod 2$$

when m is odd. Thus, the matrix $\mathbf{M}_o$ has full rank for all m, so equations (2.1) and (2.2) imply that n is non-congruent.

Next we show that for different m, the sets S_m are pairwise disjoint. Suppose that for some positive integer n, two sets S_m and $S_{m'}$ satisfy

$$n \in S_m \cap S_{m'},$$

where we may assume that $m > m' \geq 1$. Let π denote a permutation of the prime factors q_i of n, and suppose that

$$pq_1 \cdots q_t \in S_m \quad \text{and} \quad p\pi(q_1) \cdots \pi(q_t) = pq'_1 \cdots q'_t \in S_{m'}.$$

By definition of the sets S_m and $S_{m'}$, we deduce that

$$q'_{m'} = q_m.$$

As $m > m' \geq 1$, we conclude that

$$\{q_1, \ldots, q_{m-1}\} \subseteq \{q'_1, \ldots, q'_{m'-1}\}$$

is impossible. Therefore, for some integer j with $1 \leq j \leq m-1$, we have

$$q_j \in \{q'_{m'+1}, q'_{m'+2}, \ldots, q'_t\}.$$

It follows that

$$\left(\frac{q'_{m'}}{q_j}\right) = -1 \quad \text{or} \quad \left(\frac{q_m}{q_j}\right) = -1,$$

contradicting the definition of S_m. Thus, the sets S_m and $S_{m'}$ are distinct. This completes the proof of Theorem 1.2. ∎

Proof of Corollary 1.3. Let w be a product of integers belonging to the set

$$\{pq_1 \cdots q_m, q_{m+1}, q_{m+2}, \ldots\}.$$

If this product does not contain the integer factor $pq_1 \cdots q_m$, then it is non-congruent by Proposition 1.1. If it does contain $pq_1 \cdots q_m$, then Theorem 1.2 implies that w is a non-congruent number. ∎

REMARK 3.1. For the purpose of comparison with Feng's non-congruent numbers, we note that the prime factorization of these numbers, given in [2, Theorem 3.1(I)], consists of one prime factor of the form $8k+3$ and an arbitrary number of prime factors of the form $8k+1$. By contrast, our non-congruent numbers consist of one prime factor of the form $8k+1$ and an arbitrary number of prime factors of the form $8k+3$. The only possible overlap is in the case of exactly two prime factors, which gives precisely the non-congruent numbers of Lagrange [7].

Acknowledgements. This research was supported by the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

[1] A. Dujella, A. S. Janfada, and S. Salami, *A search for high rank congruent number elliptic curves*, J. Integer Sequences 12 (2009), no. 5, article 09.5.8.

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

[3] A. Genocchi, *Note analitiche sopra tre scritti inediti di Leonardo Pisano pubblicati da Baldassarre Boncompagni*, Ann. Sci. Mat. Fis. 6 (1855), 273–317.

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

[5] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8*, Proc. Japan Acad. Ser. A Math. Sci. 72 (1996), 168–169.

[6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, New York, 1993.

[7] J. Lagrange, *Nombres congruents et courbes elliptiques*, in: Séminaire Delange–Pisot–Poitou, 16e année: 1974/75. Théorie des nombres, Fasc. 1, Secrétariat Math., Paris, 1975, exp. 16.

[8] C. D. Meyer, *Matrix Analysis and Applied Linear Algebra*, SIAM, Philadelphia, 2000.

[9] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. 204 (1990), 45–67.

[10] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. 72 (1983), 323–334.

Lindsey Reinholz, Blair K. Spearman, Qiduan Yang
Department of Mathematics and Statistics
University of British Columbia Okanagan
Kelowna, BC, Canada V1V 1V7
E-mail: reinholz@interchange.ubc.ca
blair.spearman@ubc.ca
qiduan.yang@ubc.ca

Received 2 March 2014;
revised 29 October 2014 (6179)