Functiones et Approximatio
58.1 (2018), 69–77
doi: 10.7169/facm/1641

AN EXTENSION THEOREM FOR GENERATING NEW FAMILIES OF NON-CONGRUENT NUMBERS

Lindsey Reinholz, Blair K. Spearman, Qiduan Yang

Abstract: A technique for generating new families of non-congruent numbers by appending a tail of primes to extend known families of non-congruent numbers is presented. These new non-congruent numbers are comprised of arbitrarily many prime factors belonging to two or three odd congruence classes modulo 8.

Keywords: elliptic curve, congruent number, non-congruent number, rank.

1. Introduction

A positive integer n is called a congruent number if it is equal to the area of a right triangle with rational side lengths. Otherwise n is said to be a non-congruent number. Equivalently, n is non-congruent if and only if the rank of the elliptic curve

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

is equal to zero [15].

Both congruent and non-congruent numbers have been widely studied for centuries. Though a complete solution to the congruent number problem continues to elude mathematicians, success has been made in finding particular families of these numbers. A thorough overview of this problem and the progress that has been made towards its solution can be found in [15]. The classification of numbers into families often requires imposing conditions on the prime factors of the numbers and the associated values of the Legendre symbols relating these primes. Lagrange [7] presented numerous different families of non-congruent numbers containing a maximum of four distinct prime factors. Over two decades after the publication of Lagrange's work, Iskra [6] described the first family of non-congruent numbers with arbitrarily many distinct prime factors; these numbers are a product of primes of the form $8k + 3$ satisfying a specific pattern of Legendre symbols.

Research supported by the Natural Sciences and Engineering Research Council of Canada.
2010 Mathematics Subject Classification: primary: 11G05

Since then many others, including Feng [1], Feng and Xiong [2], Feng and Xue [3], Goto [4], Li and Tian [8], Ouyang and Zhang [10, 11], and Reinholz et al. [13, 14], have produced new, more complex families of non-congruent numbers that contain an unlimited number of prime factors. Nevertheless, there exist numerous families of non-congruent numbers awaiting discovery.

In this paper, we present a novel technique for generating families of non-congruent numbers. The idea is, given a non-congruent number with 2-Selmer rank equal to zero and prime factors of a specified form, we can produce new non-congruent numbers by appending a tail of primes of the form $8k+1$ to the original non-congruent number. This enables us to generalize known families of non-congruent numbers and construct many new families of non-congruent numbers. Our extension technique for generating new families of non-congruent numbers is summarized in our main theorem, which we state next.

Theorem 1. *Let* $p_1, p_2, ..., p_t, q_1, q_2, ..., q_u$ *be distinct primes with* $p_i \equiv 5 \pmod 8$ *and* $q_j \equiv 3 \pmod 8$ *for all* $i \in [1,t]$ *and* $j \in [1,u]$. *Set*

$$b = \left(\prod_{i=1}^{t} p_i\right)^{e_p} \left(\prod_{j=1}^{u} q_j\right)^{e_q},$$

where $e_p, e_q \in \{0,1\}$ *and* $(e_p + e_q) > 0$, *and suppose that the elliptic curve*

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

has 2-Selmer rank of zero, so $s(b) = 0$ *(as given by Equation (2.1)). Define the positive integer* n *by*

$$n = br_1 r_2 \cdots r_v,$$

where $r_1, r_2, ..., r_v$ *are distinct primes satisfying* $r_k \equiv 1 \pmod 8$ *for all* $k \in [1,v]$. *If for each* k *with* $1 \le k \le v$ *the set* S_k *defined by*

$$S_k = \left\{ \left(\frac{r_k}{p_i}\right), \left(\frac{r_k}{q_j}\right), \left(\frac{r_k}{r_h}\right) \text{ with } 1 \le i \le t,\ 1 \le j \le u,\ \text{and } 1 \le h < k \le v \right\}$$

has exactly one Legendre symbol equal to -1, *then* n *is a non-congruent number.*

In Section 3, we present the proof of Theorem 1 and in Section 4, we provide examples that illustrate how this extension theorem can be applied to construct new families of non-congruent numbers. We now direct our attention to Section 2, where we discuss the theory and preliminary information that is necessary for the proof of the main theorem.

2. The 2-Selmer rank and a condition for non-congruence

The proof of Theorem 1 requires the use of linear algebra carried out over $\mathbb{F}_2$ in conjunction with Monsky's formula for the 2-Selmer rank. This formula computes the 2-Selmer rank, $s(n)$, of the elliptic curve given by Equation (1.1), which provides an upper bound for the curve's Mordell-Weil rank, $r(n)$. In this section we provide a brief overview of Monsky's formula, but for more details regarding the intricate theory behind the formula, we direct the reader to Monsky's appendix in Heath-Brown's paper [5].

Let n be a squarefree positive integer with odd prime factors $P_1, P_2, \dots, P_m$. We define diagonal $m \times m$ matrices $\mathbf{D}_l = [d_i]$ for $l \in \{-2, 2\}$, and the $m \times m$ matrix $\mathbf{A} = [a_{ij}]$ by

$$d_i = \begin{cases} 0, & \text{if } \left(\frac{l}{P_i}\right) = 1, \\ 1, & \text{if } \left(\frac{l}{P_i}\right) = -1, \end{cases} \qquad a_{ij} = \begin{cases} 0, & \text{if } \left(\frac{P_j}{P_i}\right) = 1,\, j \neq i, \\ 1, & \text{if } \left(\frac{P_j}{P_i}\right) = -1,\, j \neq i, \end{cases} \qquad a_{ii} = \sum_{j:j\neq i} a_{ij}.$$

Then

$$s(n) = 2m - \operatorname{rank}_{\mathbb{F}_2}(\mathbf{M}), \tag{2.1}$$

where $\mathbf{M}$ is the $2m \times 2m$ matrix given by

$$\mathbf{M} = \left[\begin{array}{c|c} \mathbf{A} + \mathbf{D}_2 & \mathbf{D}_2 \\ \hline \mathbf{D}_2 & \mathbf{A} + \mathbf{D}_{-2} \end{array}\right]. \tag{2.2}$$

The rank, $r(n)$, of the elliptic curve given by Equation (1.1) satisfies the inequality

$$r(n) \leq s(n).$$

Consequently if $\mathbf{M}$ has nonzero determinant, then $r(n) = 0$.

In order to compute the determinant of $\mathbf{M}$, we require the following property of block determinants; a proof of this result can be found in Meyer [9, p. 475].

Proposition 1. *If $\mathbf{A}$ and $\mathbf{D}$ are square matrices, then*

$$\det\left(\left[\begin{array}{c|c} \mathbf{A} & \mathbf{B} \\ \hline \mathbf{C} & \mathbf{D} \end{array}\right]\right) = \begin{cases} \det(\mathbf{A}) \det\left(\mathbf{D} - \mathbf{C}\mathbf{A}^{-1}\mathbf{B}\right), & \textit{when } \mathbf{A}^{-1} \textit{ exists,} \\ \det(\mathbf{D}) \det\left(\mathbf{A} - \mathbf{B}\mathbf{D}^{-1}\mathbf{C}\right), & \textit{when } \mathbf{D}^{-1} \textit{ exists.} \end{cases}$$

3. Proof of Theorem 1

We now give the proof of Theorem 1.

Proof. Begin by forming the $(t+u) \times (t+u)$ $\mathbf{A}$ matrix, as defined in Section 2, for $b = p_1 p_2 \cdots p_t q_1 q_2 \cdots q_u$. We denote this matrix by $\mathbf{A_b}$ and the corresponding $(t+u) \times (t+u)$ diagonal matrices for b by

$$\mathbf{D_2^b} = \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & & \vdots \\ \vdots & & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{bmatrix} = \mathbf{I_{t+u}}$$

and

$$\mathbf{D^b_{-2}} = \begin{bmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & \vdots \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & 1 & & & \vdots \\ \vdots & & & & 0 & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots\cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}.$$

Note that the first t diagonal entries in $\mathbf{D^b_{-2}}$ are equal to one. The Monsky matrix corresponding to b is

$$\mathbf{M_b} = \left[\begin{array}{c|c} \mathbf{A_b} + \mathbf{D^b_2} & \mathbf{I_{t+u}} \\ \hline \mathbf{I_{t+u}} & \mathbf{A_b} + \mathbf{D^b_{-2}} \end{array}\right]. \tag{3.1}$$

Similarly the $(2t+2u+2v) \times (2t+2u+2v)$ Monsky matrix associated with $n = br_1r_2\cdots r_v$ is given by

$$\mathbf{M_n} = \left[\begin{array}{c|c} \mathbf{A_n} + \mathbf{D^n_2} & \mathbf{D^n_2} \\ \hline \mathbf{D^n_2} & \mathbf{A_n} + \mathbf{D^n_{-2}} \end{array}\right],$$

where

$$\mathbf{D^n_2} = \begin{bmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & \vdots \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & 1 & & & \vdots \\ \vdots & & & & 0 & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots\cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}$$

and

$$\mathbf{D^n_{-2}} = \begin{bmatrix} 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & & & & & \vdots \\ \vdots & & \ddots & & & & \vdots \\ \vdots & & & 1 & & & \vdots \\ \vdots & & & & 0 & & \vdots \\ \vdots & & & & & \ddots & \vdots \\ 0 & \cdots\cdots & \cdots & \cdots & \cdots & \cdots & 0 \end{bmatrix}$$

are the $(t+u+v) \times (t+u+v)$ diagonal matrices for n and $\mathbf{A_n}$ is the $(t+u+v) \times (t+u+v)$ $\mathbf{A}$ matrix corresponding to n. The first $(t+u)$ diagonal entries in $\mathbf{D_2^n}$ are equal to one, whereas the first t diagonal entries in $\mathbf{D^n_{-2}}$ are equal to one.

Guided by the conditions imposed on the Legendre symbols in the statement of our theorem, we use elementary row and column operations to reduce $\mathbf{M_n}$ until the value of its determinant can be computed. Since we are working over $\mathbb{F}_2$, the operations that we make use of yield a matrix with the same determinant. Let m_{ij} denote the entry in the i^{th} row and j^{th} column of $\mathbf{M_n}$. Apply the following sequence of steps to $\mathbf{M_n}$. Consider those entries with $m_{ij} = 1$ where $1 \leq i \leq (t+u+v)$, $(t+u) < j \leq (t+u+v)$ and $i < j$. Begin with $j = (t+u+v)$, and determine the corresponding value of i for which $m_{ij} = 1$. Subtract column j from column i and then subtract row j from row i. Following this, decrease the value of j by one and repeat the previously described column and row subtraction operations. Continue this process for each $j = (t+u+v-1), (t+u+v-2), ..., (t+u+1)$. Upon completing the v column subtractions and v row subtractions, we find that the upper left block of $\mathbf{M_n}$ is reduced to

$$\left[\begin{array}{c|c} \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right].$$

Now repeat the aforementioned procedure, but with the rows i and the columns j satisfying $(t+u+v+1) \leq i \leq (2t+2u+2v)$, $(2t+2u+v) < j \leq (2t+2u+2v)$, and $i < j$. Begin with $j = (2t+2u+2v)$ and complete the necessary v column subtractions and v row subtractions, thus reducing the lower right block of $\mathbf{M_n}$ to

$$\left[\begin{array}{c|c} \mathbf{A_b} + \mathbf{D^b_{-2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right].$$

By carrying out these operations, we have transformed $\mathbf{M_n}$ into

$$\mathbf{M_n^*} = \left[\begin{array}{c|c||c|c} \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{0} & \mathbf{I_{t+u}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} & \mathbf{0} & \mathbf{0} \\ \hline\hline \mathbf{I_{t+u}} & \mathbf{0} & \mathbf{A_b} + \mathbf{D^b_{-2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{I_v} \end{array}\right].$$

We now add rows $(2t+2u+v+1)$ through $(2t+2u+2v)$ to rows $(t+u+1)$ through $(t+u+v)$ respectively to get

$$\mathbf{M_n^{**}} = \left[\begin{array}{c||c} \begin{array}{c|c} \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} & \mathbf{I_{t+u+v}} \\ \hline\hline \mathbf{D_2^n} & \begin{array}{c|c} \mathbf{A_b} + \mathbf{D^b_{-2}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} \end{array}\right].$$

Following this, we perform $(t+u+v)$ row interchanges to $\mathbf{M_n^{**}}$ to obtain the matrix

$$\mathbf{M_n^{***}} = \left[\begin{array}{c|c} \mathbf{D_2^n} & \begin{array}{c|c} \mathbf{A_b} + \mathbf{D_{-2}^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} \\ \hline \begin{array}{c|c} \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array} & \mathbf{I_{t+u+v}} \end{array}\right].$$

Note that since we are working over $\mathbb{F}_2$

$$\det(\mathbf{M_n}) = \det(\mathbf{M_n^*}) = \det(\mathbf{M_n^{**}}) = \det(\mathbf{M_n^{***}}). \tag{3.2}$$

Applying Proposition 1 to $\mathbf{M_n^{***}}$ yields

$$\begin{aligned} &\det(\mathbf{M_n^{***}}) \\ &= \det(\mathbf{I_{t+u+v}}) \det\left(\mathbf{D_2^n} - \left[\begin{array}{c|c} \mathbf{A_b} + \mathbf{D_{-2}^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right] \mathbf{I_{t+u+v}^{-1}} \left[\begin{array}{c|c} \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right]\right) \\ &= \det\left(\left[\begin{array}{c|c} \mathbf{I_{t+u}} & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{0} \end{array}\right] - \left[\begin{array}{c|c} (\mathbf{A_b} + \mathbf{D_{-2}^b})(\mathbf{A_b} + \mathbf{D_2^b}) & \mathbf{0} \\ \hline \mathbf{0} & \mathbf{I_v} \end{array}\right]\right) \\ &= \det\left(\mathbf{I_{t+u}} - \left(\mathbf{A_b} + \mathbf{D_{-2}^b}\right)\left(\mathbf{A_b} + \mathbf{D_2^b}\right)\right) \det\left(\mathbf{I_v}\right) \\ &= \det\left(\mathbf{I_{t+u}} - \left(\mathbf{A_b} + \mathbf{D_{-2}^b}\right)\left(\mathbf{A_b} + \mathbf{D_2^b}\right)\right). \end{aligned} \tag{3.3}$$

In order to compute this determinant, we need to consider the matrix $\mathbf{M_b}$ described by Equation (3.1). By assumption $s(b) = 0$, so Equation (2.1) implies that $\mathbf{M_b}$ has full rank and hence

$$\det(\mathbf{M_b}) \neq 0. \tag{3.4}$$

In addition, if we perform $(t+u)$ row interchanges to $\mathbf{M_b}$ to obtain

$$\mathbf{M_b^*} = \left[\begin{array}{c|c} \mathbf{I_{t+u}} & \mathbf{A_b} + \mathbf{D_{-2}^b} \\ \hline \mathbf{A_b} + \mathbf{D_2^b} & \mathbf{I_{t+u}} \end{array}\right]$$

and apply Proposition 1 to $\mathbf{M_b^*}$, then it follows that

$$\begin{aligned} \det\left(\mathbf{M_b}\right) = \det\left(\mathbf{M_b^*}\right) &= \det\left(\mathbf{I_{t+u}}\right) \det\left(\mathbf{I_{t+u}} - \left(\mathbf{A_b} + \mathbf{D_{-2}^b}\right) \mathbf{I_{t+u}^{-1}} \left(\mathbf{A_b} + \mathbf{D_2^b}\right)\right) \\ &= \det\left(\mathbf{I_{t+u}} - \left(\mathbf{A_b} + \mathbf{D_{-2}^b}\right)\left(\mathbf{A_b} + \mathbf{D_2^b}\right)\right). \end{aligned} \tag{3.5}$$

Combining Equations (3.2), (3.3), (3.4), and (3.5) enables us to conclude that

$$\det(\mathbf{M_n}) \neq 0.$$

Thus $r(n) = 0$, so n is a non-congruent number.

■

4. Applying Theorem 1 to generate new families of non-congruent numbers

In this section we provide some examples to show how our extension theorem can be used to generate new non-congruent numbers from known families of non-congruent numbers. The numbers that we generate clearly belong to new families of non-congruent numbers because their prime factorizations differ from those of other existing families of non-congruent numbers [1, 2, 3, 4, 6, 8, 10, 11, 13, 14].

The first family we extend is Iskra's [6].

Theorem 2 (Iskra). *Let t be a positive integer and suppose that $p_1, p_2, \ldots, p_t$ are distinct primes satisfying $p_i \equiv 3 \pmod 8$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then $b = p_1 p_2 \cdots p_t$ is a non-congruent number.*

In Section 4.2 of Reinholz's master's thesis [12], the non-congruent numbers described by Iskra's theorem are shown to have 2-Selmer rank of zero. As a result, new non-congruent numbers can be produced by utilizing Theorem 1 to append a tail of primes of the form $8k+1$ to Iskra's non-congruent numbers. Some numerical examples are given in Table **??** on the next page.

Furthermore, Theorem 1 can be applied to the following result by Reinholz et al. [13].

Theorem 3 (Reinholz et al.). *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 $p_1, p_2, \cdots, p_t$ 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 $b \in N_m$, then n is non-congruent.

In the proof of this theorem in [13], the non-congruent numbers are shown to have 2-Selmer rank equal to zero. Therefore, Theorem 1 can be directly applied to Theorem 3 to generate infinitely many new non-congruent numbers, including the two listed in Table **??**.

Finally, Theorem 1 can be used to extend an important result by Ouyang and Zhang [11].

Theorem 4 (Ouyang and Zhang). *Let*

$$\left[\frac{x}{h}\right] = \left(1 - \left(\frac{x}{h}\right)\right)/2$$

and suppose that $b = p_1 \cdots p_k \equiv 1, 3 \pmod 8$ and $p_i \equiv \pm 3 \pmod 8$. Define $\mathbf{B}$ to be the $k \times k$ matrix with (i,j)-entries $\left[\frac{p_j}{p_i}\right]$ for $i \neq j$ and with (i,i)-entries $\left[\frac{m/p_i}{p_i}\right]$, and $\mathbf{C} = diag\left\{\left[\frac{-1}{p_1}\right], \ldots, \left[\frac{-1}{p_k}\right]\right\}$. If $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ is invertible, then b is a non-congruent number.

With a little effort one can prove that for the integer b in Theorem 4, the condition that $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ is invertible is equivalent to the Monsky matrix, given by Equation (2.2), having full rank. Thus, the matrix $\mathbf{B}^2 + \mathbf{CB} + \mathbf{C}$ is invertible if and only if $s(b) = 0$. As a result, Theorem 1 can be used to extend Ouyang and Zhang's work and generate new non-congruent numbers containing arbitrarily many prime factors belonging to two or three odd congruence classes modulo 8. Table **??** lists a couple numerical examples.

Table 1. Theorem 1 Numerical Examples

b	$n = br_1r_2 \cdots r_k$	**Theorem that b satisfies**
$19 \cdot 11 \cdot 163 \cdot 419$	$19 \cdot 11 \cdot 163 \cdot 419 \cdot 97 \cdot 313 \cdot 617 \cdot 1697 \cdot 1721 \cdot 6521 \cdot 15361 \cdot 16889$	Theorem 2
$347 \cdot 83 \cdot 11 \cdot 3 \cdot 499 \cdot 1123 \cdot 2803$	$347 \cdot 83 \cdot 11 \cdot 3 \cdot 499 \cdot 1123 \cdot 2803 \cdot 673 \cdot 2953 \cdot 3617 \cdot 7417 \cdot 8713$	Theorem 2
$11 \cdot 59 \cdot 163 \cdot 307 \cdot 947$	$11 \cdot 59 \cdot 163 \cdot 307 \cdot 947 \cdot 41 \cdot 1361 \cdot 2017 \cdot 4057 \cdot 4673 \cdot 8969$	Theorem 3
$3 \cdot 11 \cdot 67 \cdot 163 \cdot 691 \cdot 1483 \cdot 3019 \cdot 2179 \cdot 16987$	$3 \cdot 11 \cdot 67 \cdot 163 \cdot 691 \cdot 1483 \cdot 3019 \cdot 2179 \cdot 16987 \cdot 2137 \cdot 4273 \cdot 13553 \cdot 36793$	Theorem 3
$3 \cdot 11 \cdot 19 \cdot 43 \cdot 59 \cdot 5 \cdot 13 \cdot 29 \cdot 37$	$3 \cdot 11 \cdot 19 \cdot 43 \cdot 59 \cdot 5 \cdot 13 \cdot 29 \cdot 37 \cdot 27481 \cdot 31321 \cdot 52561 \cdot 78049$	Theorem 4
$3 \cdot 19 \cdot 67 \cdot 83 \cdot 13 \cdot 61 \cdot 101 \cdot 149$	$3 \cdot 19 \cdot 67 \cdot 83 \cdot 13 \cdot 61 \cdot 101 \cdot 149 \cdot 4177 \cdot 9649 \cdot 9721 \cdot 17449 \cdot 26953 \cdot 49297$	Theorem 4

References

[1] K. Feng, *Non-congruent numbers, odd graphs and the Birch-Swinnerton-Dyer conjecture*, Acta Arith. **75**(1) (1996), 71–83.

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

[3] K. Feng and Y. Xue, *New series of odd non-congruent numbers*, Sci. China Ser. A **49**(11) (2006), 1642–1654.

[4] T. Goto, *A note on the Selmer group of the elliptic curve $y^2 = x^3 + Dx$*, Proc. Japan Acad. Ser. A Math. Sci. **77**(7) (2001), 122–125.

[5] D.R. Heath-Brown, *The size of Selmer groups for the congruent number problem, II*, Invent. Math. **118**(2) (1994), 331–370.

[6] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8*, Proc. Japan Acad. Ser. A Math. Sci. **72**(7) (1996), 168–169.

[7] J. Lagrange, *Nombres congruents et courbes elliptiques*, Séminaire Delange-Pisot-Poitou, Théorie des nombres **16e** année (16) (1974–1975).

[8] D. Li and Y. Tian, *On the Birch-Swinnerton-Dyer conjecture of elliptic curves $E_D : y^2 = x^3 - D^2x$*, Acta Math. Sin. (Engl. Ser.) **16**(2) (2000), 229–236.

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

[10] Y. Ouyang and S. Zhang, *On non-congruent numbers with 1 modulo 4 prime factors*, Sci. China Math. **57**(3) (2014), 649–658.

[11] Y. Ouyang and S. Zhang, *On second 2-descent and non-congruent numbers*, Acta Arith. **170**(4) (2015), 343–360.

[12] L. Reinholz, *Families of Congruent and Non-Congruent Numbers*, Master's Thesis, The University of British Columbia, 2013.

[13] L. Reinholz, B.K. Spearman and Q. Yang, *Families of non-congruent numbers with arbitrarily many prime factors*, J. Number Theory **133**(1) (2013), 318–327.

[14] L. Reinholz, B.K. Spearman and Q. Yang, *On the prime factors of non-congruent numbers*, Colloq. Math. **138**(2) (2015), 271–282.

[15] J. Top and N. Yui, *Congruent number problems and their variants*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ. **44** (2008), 613–639.

Address: Lindsey Reinholz, Blair K. Spearman, and Qiduan Yang: Department of Computer Science, Mathematics, Physics 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: 12 October 2016; **revised:** 15 December 2016