Journal of Number Theory 196 (2019) 291–305

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Some new families of non-congruent numbers ☆

Weidong Cheng, Xuejun Guo *

Department of Mathematics, Nanjing University, Nanjing, 210093, China

ARTICLE INFO

Article history:
Received 5 July 2017
Received in revised form 5 July 2018
Accepted 16 September 2018
Available online 15 October 2018
Communicated by A. Pal

MSC:
primary 11G05
secondary 11C20, 15B33, 15A03

Keywords:
Elliptic curve
Non-congruent number
2-Selmer rank
Analytic Tate–Shafarevich invariant
Genus class number

ABSTRACT

We construct several new families of non-congruent numbers with arbitrarily many prime factors congruent to 3 modulo 8. Our results generalize the work of Reinholz, Spearman and Yang [14]. Our methods are based on Monsky's formula on the 2-Selmer rank of the congruent elliptic curve and the recent results by Tian, Yuan and Zhang on the congruent number problem.

Contents

☆ The work was supported by Postgraduate Research & Practice Innovation Program of Jiangsu Province (Grant No. KYZZ16_0035) and National Natural Science Foundation of China (Grant No. 11571163, 11631009).

* Corresponding author.
E-mail addresses: chengwd@smail.nju.edu.cn (W. Cheng), guoxj@nju.edu.cn (X. Guo).

https://doi.org/10.1016/j.jnt.2018.09.009
0022-314X/

1. Introduction

A positive integer n is called a *congruent number* if it is the area of a right triangle with rational lengths, or equivalently if the congruent elliptic curve

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

has positive Mordell–Weil rank. Otherwise n is called a *non-congruent number*. Without loss of generality, we shall restrict attention to square-free number n throughout this paper.

To determine all congruent numbers and non-congruent numbers is one of long-standing problems in number theory. Many eminent mathematicians have worked on this problem. For the known results on the construction of non-congruent numbers with arbitrarily many prime factors, see for instance, Iskra [8], Feng [1–4], Reinholz, Spearman and Yang [14,15] Ouyang and Zhang [11,12], Wang [21] and the recent works of Tian, Yuan and Zhang [10,18–20].

In order to estimate the *Mordell–Weil rank* $r(n)$ of E_n one may use the method of descents, for details we refer to Silverman's book [16, Chapter X]. We first introduce the notion of 2-Selmer rank, following Heath-Brown [5,6]. The number of 2-descents is the order of the Selmer group $S^{(2)}$. This is a power of 2, and will be a multiple of 4, on account of the rational points of order 2 on E_n. We shall therefore write $|S^{(2)}| = 2^{2+s(n)}$. The exponent $s(n)$ is called the 2-*Selmer rank* of the elliptic curve E_n. Recall that $0 \leq r(n) \leq s(n)$. Hence if $s(n) = 0$, then $r(n) = 0$. Moreover, Monsky [6, Appendix] represented the 2-Selmer group as the kernel of a square matrix M over the finite field $\mathbb{F}_2$, and thus gave an explicit formula to compute $s(n)$.

Based on above well-known facts, Reinholz, Spearman and Yang recently constructed a family of odd non-congruent numbers with all prime factors congruent to 3 modulo 8 in [14]. Later they constructed another family of odd non-congruent numbers with one prime factor congruent to 1 modulo 8 and all other prime factors congruent to 3 modulo 8 in [15]. Note that only odd non-congruent numbers were studied in [14,15].

In Section 2, we prove the following main theorem which gives both odd and even non-congruent numbers explicitly (see Theorems 2.1 and 2.2 for details). Our result generalizes the result of [14] according to Example 2.1. And the proof is also based on applications of the fundamental inequality $r(n) \leq s(n)$.

Theorem 1.1. *Let g, k and l be any positive integers satisfying $g \geq k > l$. Let $p_1, p_2, \cdots, p_g$ be distinct primes congruent to 3 modulo 8, such that for all $i > j$,*

$$\left(\frac{p_j}{p_i}\right) = \begin{cases} 1, & \text{if } (i,j) \neq (k,l); \\ -1, & \text{otherwise.} \end{cases}$$

Here $\left(\frac{\cdot}{\cdot}\right)$ *denotes the Legendre symbol. Define*

$$\mathcal{N}_{k,l}^{odd} := \{n = p_1 p_2 \cdots p_g\}, \tag{1}$$

$$\mathcal{N}_{k,l}^{even} := \left\{n = 2p_1 p_2 \cdots p_g \;\middle|\; g \text{ is even}\right\}. \tag{2}$$

If $k - l$ *is not divisible by* 2*, then each element of* $\mathcal{N}_{k,l}^{odd} \cup \mathcal{N}_{k,l}^{even}$ *is a non-congruent number.*

The recent work of Tian, Yuan and Zhang [20] combining with a theorem of Smith [17] give a totally new approach to construct non-congruent numbers explicitly. Their results establish a sufficient condition for n to be non-congruent in terms of the parity of the analytic Tate–Shafarevich invariant $\mathcal{L}(n)$ defined by equation (12). The parity of $\mathcal{L}(n)$ is described by that of the genus class numbers of imaginary quadratic fields, and thus by the Legendre symbols given by the prime factors of n.

In Section 3, we use Tian, Yuan and Zhang's results to prove the following theorem, which is the even analogue of Iskra's theorem in [8].

Theorem 1.2. *Let* $p_1, p_2, \cdots, p_t$ *be distinct primes congruent to* 3 *modulo* 8*, such that* $\left(\frac{p_j}{p_i}\right) = -1$ *for* $i > j$*. If* t *is an even positive integer, then the product* $n = 2p_1 \cdots p_t$ *is a non-congruent number.*

This new approach is effective to find out almost all non-congruent numbers. One can see the examples in Subsection 3.2. In fact one may use [20] to rewrite the proof of Theorem 1.1 when the number of prime factors is small. However, this procedure will involve tedious computations of genus class numbers in the general situation with arbitrary number of prime factors.

2. Non-congruent numbers via Monsky's formula

In this section, we first review some of the standard facts on Monsky's formula for the 2-Selmer rank $s(n)$ and properties of block matrices. Theorem 1.1 will be proved in Subsections 2.2 and 2.3.

First of all, we state some notations of matrices which will be used throughout this section. Let I_m denote the $m \times m$ identity matrix; $\mathbf{0}_{m\times n}$ denote the zero matrix with size $m \times n$; and $\mathbf{1}_{m\times n}$ denote the $m \times n$ scalar matrix with all entries 1. For abbreviation, we may omit the subscript indicates when no confusion can arise. We say two matrices $X = (x_{ij})$ and $Y = (x_{ij})$ with the same size are congruent to each other, denote by $X \equiv Y \pmod 2$, means that $x_{ij} \equiv y_{ij} \pmod 2$ for any possible i and j.

2.1. Monsky's formula for the 2-Selmer rank

In the appendix of Heath-Brown's paper [6], Monsky proved the following formula to compute the 2-Selmer rank $s(n)$ of the congruent elliptic curve E_n.

Let n be a square-free positive integer with odd prime factors $p_1, p_2, \cdots, p_m$. We define three diagonal $m \times m$ matrices $D_l = \mathrm{diag}(d_{ii})$ for $l \in \{-1, \pm 2\}$; and one $m \times m$ matrix $A = (a_{ij})$ by

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

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

$$a_{ii} := \sum_{1 \leq j \leq m, j \neq i} a_{ij}.$$

The *Monsky matrices* M_o and M_e are defined by

$$M_o := \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_{-2} \end{pmatrix}_{2m \times 2m} \tag{3}$$

and

$$M_e := \begin{pmatrix} D_2 & A + D_2 \\ A^t + D_2 & D_{-1} \end{pmatrix}_{2m \times 2m}. \tag{4}$$

Here and subsequently, A^t denotes the transpose matrix of A. Then *Monsky's formula* for the 2-Selmer rank $s(n)$ says that

$$s(n) = \begin{cases} 2m - \mathrm{rank}_{\mathbb{F}_2}(M_o), & \text{if } (2, n) = 1; \\ 2m - \mathrm{rank}_{\mathbb{F}_2}(M_e), & \text{if } (2, n) = 2. \end{cases} \tag{5}$$

In order to compute the determinants of M_o and M_e, we require the following properties of block determinants, and the proofs are left to the reader.

Lemma 2.1. *If A and D are square matrices, then*

$$\det \begin{pmatrix} A & \mathbf{0} \\ C & D \end{pmatrix} = \det \begin{pmatrix} A & B \\ \mathbf{0} & D \end{pmatrix} = \det(A)\det(D).$$

Lemma 2.2. *If A and D are square matrices, then*

$$\det\begin{pmatrix} A & B \\ C & D \end{pmatrix} = \begin{cases} \det(A)\det(D-CA^{-1}B), & \text{if } A^{-1} \text{ exists;} \\ \det(D)\det(A-BD^{-1}C), & \text{if } D^{-1} \text{ exists.} \end{cases}$$

2.2. Odd non-congruent numbers

The following theorem gives a new family of odd non-congruent numbers explicitly. It generalizes the result of [14].

Theorem 2.1. *With the notation of Theorem 1.1, if $k-l$ is not divisible by 2, then each element of $\mathcal{N}_{k,l}^{odd}$ is a non-congruent number.*

Note that if $l=1$ and $k=m$ is a positive even integer. Then $\mathcal{N}_{m,1}^{odd}$ gives exactly the non-congruent numbers described by Reinholz, Spearman and Yang in [14]. Moreover, it is easy to check that if $k-l=1$, then $\mathcal{N}_{k,l}^{odd}=\mathcal{N}_{2,1}^{odd}$. However, according to Example 2.1 after the proof of Theorem 2.1, we see that [14, Theorem 1] does not work for $\mathcal{N}_{5,2}^{odd}$. In fact, it is a simple matter to construct such kind of examples when $k-l\geq 3$ and $g\geq 5$. And hence Theorem 2.1 does give new non-congruent numbers.

Proof. Given a square-free positive integer $n=p_1p_2\cdots p_g\in\mathcal{N}_{k,l}^{odd}$. The aim is to show that n is non-congruent. Since $0\leq r(n)\leq s(n)$, it is sufficient to prove that the 2-Selmer rank $s(n)=0$. Furthermore, by Monsky's formula (5), we are reduced to prove that the Monsky matrix M_o has $\mathbb{F}_2$-rank $2g$, i.e., to prove $\det(M_o)\equiv 1 \pmod 2$.

Since $p_i\equiv 3 \pmod 8$ for $1\leq i\leq g$, it is immediate that $\left(\frac{-1}{p_i}\right)=-1$, $\left(\frac{2}{p_i}\right)=-1$ and $\left(\frac{-2}{p_i}\right)=1$. So we have $D_{-1}=D_2=I_g$ and $D_{-2}=\mathbf{0}_{g\times g}$. And by the law of quadratic reciprocity, we have $\left(\frac{p_j}{p_i}\right)=-\left(\frac{p_i}{p_j}\right)$ for any $1\leq i\neq j\leq g$. Therefore we can write A as a 3×3 block matrix

$$A=\begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \\ A_{31} & A_{32} & A_{33} \end{pmatrix}\begin{matrix} l-1 \\ k-l+1 \\ g-k \end{matrix}, \qquad (6)$$

$$\begin{matrix} l-1 & k-l+1 & g-k \end{matrix}$$

where A_{ij} designates the i–jth-block. Specifically, the upper triangular blocks A_{12}, A_{13} and A_{23} are zero matrices, the lower triangular blocks A_{21}, A_{31} and A_{32} are scalar matrices with all entries 1, and

$$A_{11}=\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 \\ 1 & 1 & 0 & \cdots & 0 \\ 1 & 1 & 2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & 1 & \cdots & 1 & l-2 \end{pmatrix}_{(l-1)\times(l-1)},$$

$$A_{22} = \left(\begin{array}{c|cccc|c} l & 0 & 0 & \cdots & 0 & 1 \\ \hline 1 & l & 0 & \cdots & 0 & 0 \\ 1 & 1 & l+1 & \ddots & \vdots & 0 \\ \vdots & \vdots & \ddots & \ddots & 0 & \vdots \\ 1 & 1 & \cdots & 1 & k-2 & 0 \\ \hline 0 & 1 & 1 & \cdots & 1 & k-2 \end{array}\right)_{(k-l+1)\times(k-l+1)},$$

$$A_{33} = \begin{pmatrix} k & 0 & 0 & \cdots & 0 \\ 1 & k+1 & 0 & \cdots & 0 \\ 1 & 1 & k+2 & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ 1 & 1 & \cdots & 1 & g-1 \end{pmatrix}_{(g-k)\times(g-k)}.$$

Since n is odd, we only need to consider the Monsky matrix $M_o = \left(\begin{smallmatrix} A+I_g & I_g \\ I_g & A \end{smallmatrix}\right)$. By performing the elementary row operations of Type I on M_o [7, Chapter VII, Definition 2.7 (i)], i.e., interchanging rows of M_o finite times. One can change M_o into $\left(\begin{smallmatrix} I_g & A \\ A+I_g & I_g \end{smallmatrix}\right)$. By [7, Chapter VII, Theorem 2.8], these operations are equivalent to multiplying finite number of $2g \times 2g$ elementary matrices with determinants ± 1 on the left-hand side of M_o. Thus there exists a square matrix L with determinant ± 1 such that

$$LM_o = \begin{pmatrix} I_g & A \\ A+I_g & I_g \end{pmatrix}.$$

Computing the determinants on both sides of this equation. Lemma 2.2 makes it obvious that

$$\det(M_o) \equiv \det(I_g - (A+I_g)A) \pmod 2. \tag{7}$$

In order to determine the determinant of the right hand side of (7), we first need to compute $(A+I_g)A$. By the above, we write $(A+I_g)A$ as a 3×3 block matrix

$$(\alpha_{ij})_{1\le i,j\le 3},$$

which is partitioned conformably with A. By the multiplication law of block matrices, we have $\alpha_{11} = (A_{11} + I_{l-1})A_{11}, \alpha_{12} = \mathbf{0}_{(l-1)\times(k-l+1)}, \alpha_{13} = \mathbf{0}_{(l-1)\times(g-k)}, \alpha_{22} = (A_{22} + I_{k-l+1})A_{22}, \alpha_{23} = \mathbf{0}_{(k-l+1)\times(g-k)}$, and $\alpha_{33} = (A_{33} + I_{g-k})A_{33}$.

The main diagonal blocks of $(A+I_g)A$ are determined as follows. First of all, we have

$$\alpha_{11} = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ * & 1\times 2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & (l-2)(l-1) \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 & \cdots & 0 \\ * & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ * & \dots & * & 0 \end{pmatrix} \pmod 2. \tag{8}$$

Here and subsequently, we use symbols $*$ to denote the elements which do not contribute to the determinant of M_o. And similarly, we get that α_{33} is also congruent to a strictly lower triangular matrix modulo 2.

In order to compute α_{22}. Let us denote by α_i the row i of $A_{22}+I_{k-l+1}$, and denote by β_j the column j of A_{22}. We need to determine the i–jth-entry modulo 2 in the following cases.

(i) If $2 \le j < i \le k-l$. Then $\alpha_i = (1,\dots,1,l+i-1,0,\dots,0)$ and $\beta_j = (0,\dots,0,l+j-2,1,\dots,1)^t$, where $l+i-1$ lies in column i of α_i, and $l+j-2$ lies in row j of β_j. Since $l+i-1 > l+j-2$, the i–jth-entry of α_{22} is equal to $\alpha_i \cdot \beta_j = (l+i-1)+(l+j-2)+(i-j-1) = 2l+2i-4 \equiv 0 (\mathrm{mod}\ 2)$.

(ii) If $j=1$ and $2 \le i \le k-l$, then the i–1th-entry of α_{22} is equal to $\alpha_i \cdot \beta_1 = (1,\dots,1,l+i-1,0,\dots,0)\cdot(l,1,\dots,1,0)^t = 2l+2i-3 \equiv 1 (\mathrm{mod}\ 2)$.

(iii) If $i = k-l+1$ and $2 \le j \le k-l$, then the $(k-l+1)$–jth-entry of α_{22} is equal to $\alpha_{k-l+1}\cdot\beta_j = (0,1,\dots,1,k-1)^t \cdot (0,\dots,0,l+j-2,1,\dots,1)^t = 2k-5 \equiv 1 (\mathrm{mod}\ 2)$.

Except above three cases, the other entries of α_{22} can be determined easily by applying the law of quadratic reciprocity. It follows that

$$\alpha_{22} = \left(\begin{array}{c|ccccc|c} l(l+1) & 1 & 1 & \cdots & 1 & k+l-1 \\ \hline * & l(l+1) & 0 & \cdots & 0 & 1 \\ * & * & (l+1)(l+2) & \ddots & \vdots & \vdots \\ * & * & * & \ddots & 0 & \vdots \\ * & * & * & * & (k-2)(k-1) & 1 \\ \hline k-l-1 & * & * & * & * & (k-2)(k-1) \end{array}\right)$$

$$\equiv \left(\begin{array}{c|ccc|c} 0 & 1 & \cdots & 1 & k+l-1 \\ \hline 1 & 0 & \cdots & 0 & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 1 \\ \hline k-l-1 & 1 & \cdots & 1 & 0 \end{array}\right) \quad (\mathrm{mod}\ 2). \tag{9}$$

Now substituting (8) and (9) into (7). Because $\det(I_{l-1}-\alpha_{11}) \equiv \det(I_{g-k}-\alpha_{33}) \equiv 1 \pmod 2$. So Lemma 2.1 shows that

$$\det(M_o) \equiv \det(I_{k-l+1}-\alpha_{22}) \pmod 2.$$

By applying [7, Chapter VII, Theorem 2.8 and Theorem 3.5] to the determinant of the right hand side. Specifically, we add the first row (resp. the last column) by rows (resp. columns) from 2 to $k-l$ in $I_{k-l+1}-\alpha_{22}$, which make this matrix become lower triangular when modulo 2. It follows that

$$\det(I_{k-l+1}-\alpha_{22}) \equiv \det\left(\begin{array}{c:c:c} -k+l+2 & \mathbf{0} & -2k+2 \\ \hdashline -\mathbf{1} & I_{k-l-1} & \mathbf{0} \\ \hdashline -2k+2l+2 & -\mathbf{1} & -k+l+2 \end{array}\right)$$
$$\equiv (k-l)^2 \pmod 2.$$

In conclusion, if $k-l$ is not divisible by 2. Then obviously $\det(M_o) \equiv (k-l)^2 \equiv 1 \pmod 2$. The proof is completed. □

Example 2.1. We consider the square-free positive integer $n = p_1p_2p_3p_4p_5$, where $p_1, p_2, \ldots, p_5$ are distinct odd primes congruent to 3 modulo 8, such that for all $i > j$,

$$\left(\frac{p_j}{p_i}\right) = \begin{cases} 1, & \text{if } (i,j) \neq (5,2); \\ -1, & \text{otherwise.} \end{cases}$$

Obviously, this n belongs to $\mathcal{N}_{5,2}^{odd}$ and consequently it is a non-congruent number by Theorem 2.1.

Nevertheless, one can't determine whether or not this n is a non-congruent number by the result of Reinholz [14, Theorem 1]. If otherwise, then there must exist a permutation σ which belongs to the symmetric group S_5 such that $n = p_{\sigma(1)}p_{\sigma(2)}p_{\sigma(3)}p_{\sigma(4)}p_{\sigma(5)}$ satisfies the requirement of [14, Theorem 1]. It follows that there exists one and only one Legendre symbol between $\left(\frac{p_{\sigma(1)}}{p_{\sigma(2)}}\right)$ and $\left(\frac{p_{\sigma(1)}}{p_{\sigma(4)}}\right)$ which equals 1, and the other $\left(\frac{p_{\sigma(j)}}{p_{\sigma(i)}}\right)$ with $i > j$ are equal to -1.

We now show that this can not happen by reduction to absurdity. First of all, if $\sigma(1) = 5$ or $\sigma(2) = 5$, then at least two Legendre symbols among $\left(\frac{p_5}{p_{\sigma(3)}}\right)$, $\left(\frac{p_5}{p_{\sigma(4)}}\right)$ and $\left(\frac{p_5}{p_{\sigma(5)}}\right)$ are equal to 1. This contradicts the requirement of [14, Theorem 1]. Second, if $\sigma(3) = 5$ then one Legendre symbol between $\left(\frac{p_5}{p_{\sigma(4)}}\right)$ and $\left(\frac{p_5}{p_{\sigma(5)}}\right)$ equals 1, also a contradiction. Third, if $\sigma(4) = 5$ then $\sigma(5) = 2$, otherwise there must be $\left(\frac{p_5}{p_{\sigma(5)}}\right) = 1$. This leads to a contradiction since then at least two Legendre symbols among $\left(\frac{p_{\sigma(1)}}{p_2}\right)$, $\left(\frac{p_{\sigma(2)}}{p_2}\right)$ and $\left(\frac{p_{\sigma(3)}}{p_2}\right)$ equal 1. Finally, the only possibility is $\sigma(5) = 5$. This implies $\sigma(1) = 2$ since there exists exactly one Legendre symbol equals 1, which also contradicts [14, Theorem 1] because $2 \nmid \sigma(5) = 5$. In conclusion, we see that [14, Theorem 1] does not work for above n.

2.3. Even non-congruent numbers

Note that only odd non-congruent numbers were involved in [14,15]. The following theorem may be viewed as the even case of Theorem 2.1, which gives a new family of even non-congruent numbers with arbitrarily many prime factors explicitly.

Theorem 2.2. *With the notation of Theorem 1.1, if $k-l$ is not divisible by 2, then each element of $\mathcal{N}_{k,l}^{even}$ is a non-congruent number.*

Proof. The proof is quite similar to that of Theorem 2.1 but involves much more complicated block matrix operations. Following the notation of previous subsection, for any $n = 2p_1p_2\cdots p_g \in \mathcal{N}_{k,l}^{even}$, we consider the Monsky matrix M_e defined by (4). Then Lemma 2.2 implies that

$$\det(M_e) = \det(I_g - (A + I_g)(A^t + I_g)), \tag{10}$$

where A is given by (6).

In order to determine the determinant of the left hand side of (10), we first compute the $g \times g$ symmetric matrix $(A + I_g)(A^t + I_g)$. We regard this matrix as a 3×3 block matrix

$$(\beta_{ij})_{1\leq i,j\leq 3},$$

which is partitioned conformably with A. By applying the multiplication law of block matrices again, it is easy to compute that $\beta_{11} = (A_{11}+I_{l-1})(A_{11}^t+I_{l-1}), \beta_{21} = A_{21}(A_{11}^t+I_{l-1}), \beta_{22} = A_{21}A_{21}^t+(A_{22}+I_{k-l+1})(A_{22}^t+I_{k-l+1}), \beta_{31} = A_{31}(A_{11}^t+I_{l-1}), \beta_{32} = A_{31}A_{21}^t+A_{32}(A_{22}^t+I_{k-l+1}), \beta_{33} = A_{31}A_{31}^t+A_{32}A_{32}^t+(A_{33}+I_{g-k})(A_{33}^t+I_{g-k})$, and the symmetric implies that $\beta_{12} = \beta_{21}^t, \beta_{13} = \beta_{31}^t, \beta_{23} = \beta_{32}^t$.

The task is now to compute the blocks $\beta_{ij}(1 \leq j \leq i \leq 3)$ modulo 2 in above matrix. Since the method is elementary, we only write down the details for β_{11} and β_{22} as below.

$$\begin{aligned}\beta_{11} =&(A_{11} + I_{l-1})(A_{11}^t + I_{l-1})\\ =&\begin{pmatrix} 1 & 1 & 1 & 1 & \cdots & 1\\ 1 & 2^2+1 & 3 & 3 & \cdots & 3\\ 1 & 3 & 3^2+2 & 5 & \cdots & 5\\ 1 & 3 & 5 & 4^2+3 & * & \vdots\\ \vdots & \vdots & \vdots & * & \ddots & 2l-5\\ 1 & 3 & 5 & \cdots & 2l-5 & (l-1)^2+(l-2)\end{pmatrix},\end{aligned}$$

where the i–jth-entry equals $2j-1$ for $l-1 \geq i > j \geq 1$, and equals i^2+i-1 for $l-1 \geq i = j \geq 1$. Note that β_{11} is symmetric. Thus we have $\beta_{11} \equiv \mathbf{1}_{(l-1)\times(l-1)} \pmod 2$.

$$\begin{aligned}\beta_{22} =&A_{21}A_{21}^t + (A_{22} + I_{k-l+1})(A_{22}^t + I_{k-l+1})\\ =&(l-1)\mathbf{1}_{(k-l+1)\times(k-l+1)}\\ &+\left(\begin{array}{c|c|ccc|c} l+2 & l+1 & l+1 & \cdots & l+1 & k-1\\ \hline l+1 & (l+1)^2+1 & l+2 & \cdots & l+2 & l+1\\ l+1 & l+2 & (l+2)^2+2 & * & l+4 & l+3\\ \vdots & \vdots & * & \ddots & * & \vdots\\ l+1 & l+2 & l+4 & * & (k-1)^2+k-l+1 & 2k-l-3\\ \hline k-1 & l+1 & l+3 & \cdots & 2k-l-3 & (k-1)^2+k-l+1\end{array}\right)\end{aligned}$$

where the i–jth-entry of the second summand on the right hand side equals $l+2(j-1)$ for $k-l \geq i > j \geq 2$, and equals $(l+i-1)^2+i-1$ for $k-l \geq i = j \geq 2$; and all other i–jth-entries for $i = 1$ or $k-l+1$ and $j = 1$ or $k-l+1$ are easy to be determined. It follows that

$$\beta_{22} \equiv \left(\begin{array}{c:ccc:c} 1 & 0 & \cdots & 0 & k+l \\ \hdashline 0 & 1 & \cdots & 1 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & \cdots & 1 & 0 \\ \hdashline k+l & 0 & \cdots & 0 & 1 \end{array}\right)_{(k-l+1)\times(k-l+1)} \pmod 2.$$

In the same manner, we see that $\beta_{12} \equiv \mathbf{1}_{(l-1)\times(k-l+1)}, \beta_{13} \equiv \mathbf{1}_{(l-1)\times(g-k)}, \beta_{21} \equiv \mathbf{1}_{(k-l+1)\times(l-1)}, \beta_{23} \equiv \mathbf{1}_{(k-l+1)\times(g-k)}, \beta_{31} \equiv \mathbf{1}_{(g-k)\times(l-1)}, \beta_{32} \equiv \mathbf{1}_{(g-k)\times(k-l+1)}, \beta_{33} \equiv \mathbf{1}_{(g-k)\times(g-k)}$.

Now combining above results yields

$$I_g - (A+I_g)(A^t+I_g) \equiv$$

$$\left(\begin{array}{c:c:c} \begin{matrix} 0 & -1 & \cdots & -1 \\ -1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & 0 \end{matrix} & \mathbf{-1} & \mathbf{-1} \\ \hdashline \mathbf{-1} & \begin{matrix} 0 & 0 & 0 & \cdots & 0 & -k-l \\ 0 & 0 & -1 & \cdots & -1 & 0 \\ 0 & -1 & 0 & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & -1 & 0 \\ 0 & -1 & \cdots & -1 & 0 & 0 \\ -k-l & 0 & \cdots & 0 & 0 & 0 \end{matrix} & \mathbf{-1} \\ \hdashline \mathbf{-1} & \mathbf{-1} & \begin{matrix} 0 & -1 & \cdots & -1 \\ -1 & 0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \cdots & -1 & 0 \end{matrix} \end{array}\right)_{g\times g} \begin{matrix} \} l-1 \\ \} k-l+1 \\ \} g-k \end{matrix}$$

$$\underbrace{\qquad}_{l-1} \quad \underbrace{\qquad\qquad}_{k-l+1} \quad \underbrace{\qquad}_{g-k}$$

$$\pmod 2. \tag{11}$$

We now return to determine the determinant of $I_g-(A+I_g)(A^t+I_g)$ in (10) modulo 2. For this purpose, we need to perform a finite sequence of elementary row operations of type I and type III [7, Chapter VII, Definition 2.7 (i) and (iii)] on the block matrix of the left hand side of (11), to make it become lower triangular. This process is not difficult but is too long to give here, so we omit the details. The main diagonal elements of the final lower triangular matrix are the same as

$$\mathrm{diag}(g-1, I_{l-2}, k-l, k-l, I_{K-L-1}, I_{g-k}) \pmod 2.$$

Now applying Lemma 2.2 and [7, Chapter VII, Theorem 2.8 and Theorem 3.5] again, we see that the Monsky matrix M_e has determinant

$$\det(M_e) \equiv (g-1)(k-l)^2 \pmod 2.$$

Since g is even and $k-l$ is not divisible by 2, it follows immediately that $\det(M_e) \equiv 1 \pmod 2$, and this is the desired conclusion. □

3. New approach according to Tian, Yuan and Zhang

In this section, we use the recent work of Tian, Yuan and Zhang [20] to construct non-congruent numbers explicitly. In [20], the authors defined an analytic Tate–Shafarevich invariant $\mathcal{L}(n)$ of E_n as follows:

$$\mathcal{L}(n) := \begin{cases} (L(E_n,1)/(2^{2k(n)-2-\alpha(n)}\Omega_{n,\infty}))^{1/2}, & \text{if } \mathrm{ord}_{s=1}L(E_n,s)=0; \\ (L'(E_n,1)/(2^{2k(n)-2-\alpha(n)}\Omega_{n,\infty}R_n))^{1/2}, & \text{if } \mathrm{ord}_{s=1}L(E_n,s)=1; \\ 0, & \text{if } \mathrm{ord}_{s=1}L(E_n,s)>1. \end{cases} \tag{12}$$

Here

- $k(n)$ is the number of odd prime factors of n;
- $\alpha(n)=0$ if n is even, and 1 if n is odd;
- the real period

$$\Omega_{n,\infty} = \frac{2}{\sqrt{n}} \int_1^\infty \frac{dx}{\sqrt{x^3-x}};$$

- R_n is twice of the Néron–Tate height of a generator of $E_n(\mathbb{Q})/E_n(\mathbb{Q})_{tor}$ (in the case of rank one).

The main results relating to the non-congruent numbers in [20] are the following two theorems.

Theorem 3.1. ([20, Theorem 1.1]) *Let $n \equiv 1,2,3 \pmod 8$ be a positive and square-free integer. Then $\mathcal{L}(n)$ is an integer, and*

$$\mathcal{L}(n) \equiv \sum_{\substack{n=d_0d_1\cdots d_l \\ d_i\equiv 1 \pmod 8, i>0}} \prod_i g(d_i) \pmod 2. \tag{13}$$

Here all decompositions $n = d_0 d_1 \cdots d_l$ are non-ordered with $d_i > 1$ for all $i \geq 0$. $g(d_i) := \#(2\mathrm{Cl}(\mathbb{Q}(\sqrt{-d_i})))$ are the genus class numbers. And the right-hand side is considered to be 1 if $n = 1$.

Theorem 3.2. ([20, Corollary 1.3]) *For every square-free positive integer n congruent to $1, 2$ or 3 modulo 8, we have that $\mathcal{L}(n)$ is odd if and only if $E_n(\mathbb{Q})$ is finite and $Ш(E_n)[2^\infty] = 0$. Moreover, when these statements hold, $Ш(E_n)$ is finite, and its order is as predicted by the conjecture of Birch and Swinnerton–Dyer.*

Theorem 3.2 states that if $n \equiv 1, 2, 3 \pmod 8$ is a positive and square-free integer such that the analytic Tate–Shafarevich invariant $\mathcal{L}(n)$ is odd, then n is a non-congruent number. Note that if the number of prime factors of n is very small, or most of the genus class numbers coming from the right hand side of (13) are even. Then the parity of $\mathcal{L}(n)$ is determinable. We are thus led to the following applications of [20].

3.1. Even analogue of [8]

The following theorem is an easy corollary of Theorems 3.1 and 3.2. We may view it as the even analogue of Iskra's theorem in [8].

Theorem 3.3. *Let $p_1, p_2, \cdots, p_t$ be distinct primes congruent to 3 modulo 8, such that $\left(\frac{p_j}{p_i}\right) = -1$ for $i > j$. If t is an even positive integer, then the product $n = 2p_1 \cdots p_t$ is a non-congruent number.*

Proof. Note that the genus class number $g(d)$ is odd if and only if the ideal class group $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ has no nonzero element of order 4, and the 4-ranks of $\mathrm{Cl}(\mathbb{Q}(\sqrt{-d}))$ can be determined by studying the $\mathbb{F}_2$-rank of the Rédei matrices (see, for example, [13,9]). Based on these facts, we have

- $g(2) \equiv 1 \pmod 2$;
- $g(2p_ip_j) \equiv g(2p_ip_jp_kp_l) \equiv \cdots \equiv g(n) \equiv 0 \pmod 2$;
- $g(p_ip_j) \equiv 1 \pmod 2$;
- $g(p_ip_jp_kp_l) \equiv g(p_ip_jp_kp_lp_up_v) \equiv \cdots \equiv g(p_1p_2\cdots p_{t-1}p_t) \equiv 0 \pmod 2$.

Here i, j, k, l, u, v are distinct integers belong to $\{1, 2, \cdots, t\}$.

This implies that to study the parity of the right hand side of congruence (13), we only need to consider the decompositions of n with the form $n = 2 \cdot d_1 \cdot d_2 \cdots d_l$, where each d_i has exactly two odd prime factors. The number of such decompositions is equal to

$$\frac{\binom{t}{2}\binom{t-2}{2}\cdots\binom{4}{2}}{(\frac{t}{2})!}.$$

By induction on t, it is easy to check that this number is congruent to 1 modulo 2.

Now apply Theorems 3.1 and 3.2, we have $\mathcal{L}(n) \equiv g(2) \cdot \prod_{i,j} g(p_i p_j) \cdot \frac{\binom{t}{2}\binom{t-2}{2}\cdots\binom{4}{2}}{(\frac{t}{2})!} \equiv 1 \pmod 2$. This completes the proof. □

3.2. More examples

The following examples show that by applying the results of [20]. One may find out almost all of the non-congruent numbers with small number of prime factors.

Example 3.1. Let $n = p_1p_2p_3$ be a square-free positive integer such that $p_i \equiv 3 \pmod 8$ for $1 \le i \le 3$. If the triple $\left[\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{p_3}\right), \left(\frac{p_2}{p_3}\right)\right]$ belongs to

$$\{[1,1,1],[1,1,-1],[1,-1,-1],[-1,1,1],[-1,-1,1],[-1,-1,-1]\}.$$

Then n is a non-congruent number.

Proof. Note that $n = p_1p_2p_3 = p_1 \cdot p_2p_3 = p_2 \cdot p_1p_3 = p_3 \cdot p_1p_2$. Theorem 3.1 implies that

$$\mathcal{L}(n) \equiv g(p_1p_2p_3) + g(p_1)g(p_2p_3) + g(p_2)g(p_1p_3) + g(p_3)g(p_1p_2) \pmod 2. \tag{14}$$

Now we only need to verify the parities of the genus class numbers on the right hand side of (14) one by one.

Since $n = p_1p_2p_3 \equiv 3 \pmod 8$, we consider the Rédei matrix

$$\begin{aligned} R^{(1)} &= \begin{pmatrix} (p_1,d)_{p_1} & (p_1,d)_{p_2} & (p_1,d)_{p_3} \\ (p_2,d)_{p_1} & (p_2,d)_{p_2} & (p_2,d)_{p_3} \\ (p_3,d)_{p_1} & (p_3,d)_{p_2} & (p_3,d)_{p_3} \end{pmatrix} \\ &= \begin{pmatrix} \left(\frac{p_2p_3}{p_1}\right) & \left(\frac{p_1}{p_2}\right) & \left(\frac{p_1}{p_3}\right) \\ \left(\frac{p_2}{p_1}\right) & \left(\frac{p_1p_3}{p_2}\right) & \left(\frac{p_2}{p_3}\right) \\ \left(\frac{p_3}{p_1}\right) & \left(\frac{p_3}{p_2}\right) & \left(\frac{p_1p_2}{p_3}\right) \end{pmatrix}, \end{aligned} \tag{15}$$

where $d = -p_1p_2p_3$, and $(p,d)_q$ denotes the Hilbert symbol for primes p and q. It is easy to check that only when the triple $\left[\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{p_3}\right), \left(\frac{p_2}{p_3}\right)\right]$ takes value from the following set

$$\{[1,1,1],[1,1,-1],[1,-1,-1],[-1,1,1],[-1,-1,1],[-1,-1,-1]\}.$$

Then the $\mathbb{F}_2$-rank of $R^{(1)}$ is equal to 1. By Rédei's formula for the 4-rank of $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$ [9, Theorem 3.1], we have $\mathrm{rk}_4(\mathrm{Cl}(\mathbb{Q}(\sqrt{d})) = 1$. It follows that the $g(p_1p_2p_3) \equiv 0 \pmod 2$.

By similar computations, we see that $g(p_1) \equiv g(p_2) \equiv g(p_3) \equiv g(p_1p_2) \equiv g(p_1p_3) \equiv g(p_2p_3) \equiv 1 \pmod 2$. Now substituting these congruences back to (14), it follows that $\mathcal{L}(n) \equiv 1 \pmod 2$. This completes the proof. □

Similar argument applies to the situation of 4 prime factors. The proof of the following example will be omitted.

Example 3.2. Let $n = p_1p_2p_3p_4$ be a square-free positive integer such that $p_i \equiv 3 \pmod 8$ for $1 \leq i \leq 4$. Denote by $\alpha = \left(\frac{p_1}{p_2}\right)\left(\frac{p_3}{p_4}\right)$, $\beta = \left(\frac{p_1}{p_3}\right)\left(\frac{p_2}{p_4}\right)$ and $\gamma = \left(\frac{p_1}{p_4}\right)\left(\frac{p_2}{p_3}\right)$. Then in the following cases, n is a non-congruent number:

(i) $\alpha = \beta = \gamma = 1$;
(ii) $\alpha = \beta = 1, \gamma = -1$;
(iii) $\alpha = 1, \beta = \gamma = -1$;
(iv) $\alpha = -1, \beta = \gamma = 1$;
(v) $\alpha = \beta = -1, \gamma = 1$;
(vi) $\alpha = \beta = \gamma = -1$.

Acknowledgments

The authors thank the referees for their careful readings of the manuscript and many valuable suggestions that helped improving the presentation of this paper.

References

[1] K. Feng, Non-congruent numbers, odd graphs and the Birch–Swinnerton–Dyer conjecture, Acta Arith. 75 (1996) 71–83.
[2] K. Feng, M. Xiong, On elliptic curves $y^2 = x^3 - n^2x$ with rank zero, J. Number Theory 109 (2004) 1–26.
[3] K. Feng, Y. Xue, New series of odd non-congruent numbers, Sci. China Ser. A 49 (2006) 1642–1654.
[4] K. Feng, Y. Xue, Constructing new non-congruent numbers by graph theory, in: Number Theory, in: Ser. Number Theory Appl., vol. 2, World Sci. Publ., Hackensack, NJ, 2007, pp. 24–38.
[5] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem, Invent. Math. 111 (1993) 171–195.
[6] D.R. Heath-Brown, The size of Selmer groups for the congruent number problem. II, Invent. Math. 118 (1994) 331–370, with an appendix by P. Monsky.
[7] T.W. Hungerford, Algebra, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, New York–Berlin, 1980, reprint of the 1974 original.
[8] 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.
[9] M. Kolster, The 2-part of the narrow class group of a quadratic number field, Ann. Sci. Math. Québec 29 (2005) 73–96.
[10] D. Li, 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 (2000) 229–236.
[11] Y. Ouyang, S. Zhang, On non-congruent numbers with 1 modulo 4 prime factors, Sci. China Math. 57 (2014) 649–658.
[12] Y. Ouyang, S. Zhang, On second 2-descent and non-congruent numbers, Acta Arith. 170 (2015) 343–360.

[13] L. Rédei, Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, J. Reine Angew. Math. 171 (1934) 55–60.
[14] L. Reinholz, B.K. Spearman, Q. Yang, Families of non-congruent numbers with arbitrarily many prime factors, J. Number Theory 133 (2013) 318–327.
[15] L. Reinholz, B.K. Spearman, Q. Yang, On the prime factors of non-congruent numbers, Colloq. Math. 138 (2015) 271–282.
[16] J.H. Silverman, The Arithmetic of Elliptic Curves, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.
[17] A.D. Smith, An Approach to the Full BSD Conjecture at Two in Quadratic Twist Families of Elliptic Curves, Princeton University Undergraduate Senior Theses, 2015.
[18] Y. Tian, Congruent numbers with many prime factors, Proc. Natl. Acad. Sci. USA 109 (2012) 21256–21258.
[19] Y. Tian, Congruent numbers and Heegner points, Cambridge J. Math. 2 (2014) 117–161.
[20] Y. Tian, X. Yuan, S.-W. Zhang, Genus periods, genus points and congruent number problem, Asian J. Math. 21 (2017) 721–773.
[21] Z. Wang, Congruent elliptic curves with non-trivial Shafarevich–Tate groups, Sci. China Math. 59 (2016) 2145–2166.