International Journal of Number Theory
(2019)
© World Scientific Publishing Company
DOI: 10.1142/S1793042119500362

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

The non-congruent numbers via Monsky's formula

Weidong Cheng* and Xuejun Guo†

Department of Mathematics, Nanjing University
22 Hankou Road, Gulou Nanjing 210093, Jiangsu, P. R. China
*chengwd@smail.nju.edu.cn
†guoxj@nju.edu.cn

Received 18 September 2017
Revised 3 October 2018
Accepted 8 October 2018
Published 16 November 2018

This paper gives some new families of non-congruent numbers with arbitrarily many prime divisors. The main idea is based on Monsky's formula for the 2-Selmer rank of congruent elliptic curves.

Keywords: Elliptic curve; non-congruent number; 2-Selmer rank; Monsky's matrix.

Mathematics Subject Classification 2010: 11G05, 11C20

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 [9, Proposition 3.1 and Corollary 4.3]. Otherwise n is called a *non-congruent number*. The problem of determining which positive integers are congruent or non-congruent is one of long-standing problems in number theory. Without loss of generality we can restrict attention to square-free numbers. The famous conjecture of Birch and Swinnerton-Dyer predicts that each positive integer lying in the residue classes of 5, 6, and 7 modulo 8 should be a congruent number [18]. This paper is concerned in particular with non-congruent numbers. So in what follows, only positive integers lying in the residue classes of 1, 2, and 3 modulo 8 are involved.

There are many studies on non-congruent numbers. For the known results on non-congruent numbers with arbitrarily many prime divisors in recent years, see for instance [1–4, 8, 10, 12–15, 18, 19]. In order to estimate the Mordell–Weil rank $r(n)$ of the congruent elliptic curve E_n one may use the method of descents, for details we refer to Silverman's book [17, Chap. X]. We now 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 said to be 2-Selmer rank of the elliptic curve E_n.

The basic idea in this paper is to apply the fundamental inequality $0 \le r(n) \le s(n)$, which implies that one can use information about $s(n)$ to say something about $r(n)$. Particularly, we see that the upper bound $s(n) = 0$ implies $r(n) = 0$. In [6, Appendix], Monsky described the pure 2-Selmer group as the kernel of a square matrix M over the finite field $\mathbb{F}_2$, and gave an explicit formula to compute $s(n)$. Based on these two facts, Reinholz *et al.* [14, 15] described two families of odd non-congruent numbers whose odd prime divisors lying in at most two residue classes modulo 8.

In this paper, we are going to give some new families of non-congruent numbers including both odd and even cases with arbitrarily many number of prime divisors. In particular, Theorems 1.3 and 1.4 described some non-congruent numbers whose odd prime divisors lying in more than two residue classes modulo 8. Following Theorems 1.1–1.4, we see that these non-congruent numbers are described by the parity of the number of odd prime divisors lying in each residue classes modulo 8.

Throughout this paper, we study the square-free positive integers given by

$$n = \epsilon \cdot \prod_{p_i \in P} p_i \cdot \prod_{q_i \in Q} q_i \cdot \prod_{r_i \in R} r_i \cdot \prod_{s_i \in S} s_i, \qquad (*)$$

where

$$\epsilon = \begin{cases} 1 & \text{if } 2 \nmid n, \\ 2 & \text{if } 2 \mid n; \end{cases}$$

P, Q, R, S are finite sets which consist of odd prime numbers being congruent to 1, 3, 5, 7 modulo 8 respectively; and denote their cardinality by $g_1 := |P|$, $g_3 := |Q|$, $g_5 := |R|$ and $g_7 := |S|$; we also suppose that the following quadratic relationships between odd prime divisors are satisfied:

(i) $\left(\frac{p_j}{p_i}\right) = -1$ for $1 \le j < i \le g_1$;
(ii) $\left(\frac{q_j}{q_i}\right) = -1$ for $1 \le j < i \le g_3$;
(iii) $\left(\frac{r_j}{r_i}\right) = -1$ for $1 \le j < i \le g_5$;
(iv) $\left(\frac{s_j}{s_i}\right) = -1$ for $1 \le j < i \le g_7$;
(v) $\left(\frac{p_j}{q_i}\right) = -1$ for $1 \le i \le g_3, 1 \le j \le g_1$;
(vi) $\left(\frac{p_j}{r_i}\right) = -1$ for $1 \le i \le g_5, 1 \le j \le g_1$;
(vii) $\left(\frac{p_j}{s_i}\right) = -1$ for $1 \le i \le g_7, 1 \le j \le g_1$;
(viii) $\left(\frac{q_j}{r_i}\right) = -1$ for $1 \le i \le g_5, 1 \le j \le g_3$;
(ix) $\left(\frac{q_j}{s_i}\right) = -1$ for $1 \le i \le g_7, 1 \le j \le g_3$;
(x) $\left(\frac{r_j}{s_i}\right) = -1$ for $1 \le i \le g_7, 1 \le j \le g_5$.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Note that the non-negative integers g_i $(i = 1, 3, 5, 7)$ may equal zero, which means that the corresponding odd prime divisors and quadratic relationships do not appear.

Our main results are as follows. Theorems 1.1–1.4 describe the non-congruent numbers whose odd prime divisors lying in exactly one, two, three and four residue classes modulo 8, respectively. Actually, under the assumptions of above n, especially the restrictive quadratic relationships between the odd prime divisors, our proofs show that the following theorems are the only results that can be derived by using Monsky's formula.

Theorem 1.1. *Let n be a square-free positive integer defined by* $(*)$, *and suppose n satisfies one of the following conditions*:

(1) $g_1 = g_5 = g_7 = 0, \epsilon = 2$, $g_3 \geq 1$ *and* $g_3 \equiv 0 \pmod 2$;
(2) ([8, Theorem]) $g_1 = g_5 = g_7 = 0, \epsilon = 1$, $g_3 \geq 1$ *is an positive integer*;
(3) ([4, Lemma 1.1(1)] and [2, Corollary of Theorem 4.2]) $g_1 = g_3 = g_7 = 0, \epsilon = 2$ *and* $g_5 = 1$; *or* $g_1 = g_3 = g_7 = 0, \epsilon = 2$, $g_5 > 1$ *and* $g_5 \equiv 0 \pmod 2$.

Then n is a non-congruent number.

Note that Theorem 1.1(2) is just the result of [8], and Theorem 1.1(1) can be seen as an even analog of it. The first case of Theorem 1.1(3) is a classical result which can be found in [4, Lemma 1.1(1)], and the second case of (3) was given in [2, Corollary of Theorem 4.2] via algebraic graph theory.

Theorem 1.2. *Let n be a square-free positive integer defined by* $(*)$, *and suppose it satisfies one of the following conditions*:

(1) $g_1 = g_7 = 0, \epsilon = 1$, $g_3 \equiv 1 \pmod 2$, $g_5 \geq 1$ *and* $g_5 \equiv 0 \pmod 2$;
(2) $g_1 = g_7 = 0, \epsilon = 2$, $g_3 \geq 1, g_5 \geq 1$ *and* $g_3 \equiv g_5 \equiv 0 \pmod 2$; *or* $g_1 = g_7 = 0$, $\epsilon = 2$, $g_3 \geq 1, g_3 \equiv 0 \pmod 2$ *and* $g_5 = 1$;
(3) $g_1 = g_5 = 0, \epsilon = 2, g_3 \equiv 1 \pmod 2$ *and* $g_7 = 1$;
(4) ([16, Table 3.8, p. 232]) $g_1 = g_3 = 0, \epsilon = 1, g_5 = g_7 = 1$;
(5) $g_5 = g_7 = 0, \epsilon = 1$, $g_1 > 1, g_1 \equiv 0 \pmod 2$ *and* $g_3 \equiv 1 \pmod 2$; *or* $g_5 = g_7 = 0, \epsilon = 1$, $g_1 = 1$ *and* $g_3 \equiv 1 \pmod 2$;
(6) $g_3 = g_7 = 0, \epsilon = 2$, $g_1 = 1$ *and* $g_5 \equiv 1 \pmod 2$; *or* $g_3 = g_7 = 0, \epsilon = 2$, $g_1 > 1, g_1 \equiv 0 \pmod 2$ *and* $g_5 = 1$.

Then n is a non-congruent number.

Note that Theorem 1.2(4) was first given in [16] and can be found in [4, Lemma 1.1(3)].

Theorem 1.3. *Let n be a square-free positive integer defined by* $(*)$, *and suppose it satisfies one of the following conditions*:

(1) $g_1 = 0, \epsilon = 1$, $g_5 = g_7 = 1$ *and* $g_3 \geq 1$ *is a positive integer*; *or* $g_1 = 0, \epsilon = 1$, $g_5 \geq 2$, $g_3 \equiv g_5 \equiv 1 \pmod 2$ *and* $g_7 = 1$;

(2) $g_1 = 0, \epsilon = 2$, $g_3 \equiv 1 \pmod 2$, $g_5 \geq 1$, $g_5 \equiv 0 \pmod 2$ *and* $g_7 = 1$;
(3) $g_3 = 0, \epsilon = 1, g_1 \equiv g_5 \equiv 1 \pmod 2$ *and* $g_7 = 1$;
(4) $g_3 = 0, \epsilon = 2, g_1 \equiv 1 \pmod 2$ *and* $g_5 = g_7 = 1$;
(5) $g_5 = 0, \epsilon = 1$, $g_1 \geq 1, g_3 \geq 1$, $g_1 \equiv g_3 \equiv 0 \pmod 2$ *and* $g_7 = 1$;
(6) $g_5 = 0, \epsilon = 2$, $g_1 \geq 1, g_3 \geq 1$, $g_1 \equiv g_3 \equiv 1 \pmod 2$ *and* $g_7 = 1$;
(7) $g_7 = 0, \epsilon = 1$, $g_1 \geq 1, g_5 \geq 1$, $g_1 \equiv g_5 \equiv 0 \pmod 2$ *and* $g_3 \equiv 1 \pmod 2$;
(8) $g_7 = 0, \epsilon = 2$, $g_1 = 1$, $g_3 \geq 1, g_3 \equiv 0 \pmod 2$ *and* $g_5 \equiv 1 \pmod 2$; *or* $g_7 = 0$, $\epsilon = 2$, $g_1 \geq 1, g_3 \geq 1$, $g_1 \equiv g_3 \equiv 0 \pmod 2$ *and* $g_5 = 1$.

Then n is a non-congruent number.

Theorem 1.4. *Let n be a square-free positive integer defined by* $(*)$. *If* $\epsilon = 1$, $g_1 \geq 1$, $g_1 \equiv 0 \pmod 2$, $g_3 \equiv g_5 \equiv 1 \pmod 2$ *and* $g_7 = 1$; *or* $\epsilon = 1$, $g_1 \equiv g_5 \equiv 1 \pmod 2$, $g_3 \geq 1$, $g_3 \equiv 0 \pmod 2$ *and* $g_7 = 1$. *Then n is a non-congruent number.*

The organization of this paper is the following. In Sec. 2, we briefly sketch the Monsky formula for the 2-Selmer rank $s(n)$. In Sec. 3, we setup some matrix notations and state a proposition for block determinants. Theorems 1.1–1.4 are proved in Sec. 4 by using Monsky's formula.

2. Monsky's Formula for Counting 2-Selmer Rank

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

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

$$d_i := \begin{cases} 0 & \text{if } \left(\dfrac{l}{p_i}\right) = 1, \\ 1 & \text{if } \left(\dfrac{l}{p_i}\right) = -1; \end{cases} \quad a_{ij} := \begin{cases} 0 & \text{if } \left(\dfrac{p_j}{p_i}\right) = 1, \ \ j \neq i, \\ 1 & \text{if } \left(\dfrac{p_j}{p_i}\right) = -1, \ \ j \neq i; \end{cases} \quad a_{ii} := \sum_{1 \leq j \leq m, j \neq i} a_{ij}.$$

The *Monsky matrices* M_o and M_e are defined by

$$M_o := \begin{pmatrix} A + D_2 & D_2 \\ D_2 & A + D_{-2} \end{pmatrix}_{2m \times 2m} \tag{2.1}$$

and

$$M_e := \begin{pmatrix} D_2 & A + D_2 \\ A^t + D_2 & D_{-1} \end{pmatrix}_{2m \times 2m}. \tag{2.2}$$

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

$$s(n) = \begin{cases} 2m - \mathrm{rank}_{\mathbb{F}_2}(M_o) & \text{if } (2, n) = 1; \\ 2m - \mathrm{rank}_{\mathbb{F}_2}(M_e) & \text{if } (2, n) = 2. \end{cases} \tag{2.3}$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

3. Matrix Notations

We now state some notations of matrix which will be used throughout the paper. 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 $m \times n$ matrix with all entries 1. The set of all $m \times n$ matrices over $\mathbb{Z}$ is denoted by $\mathrm{Mat}_{m\times n}(\mathbb{Z})$, and we write it $\mathrm{Mat}_m(\mathbb{Z})$ when $m = n$. For abbreviation, we will omit the subscript which indicates when no confusion can arise.

Let $A = (a_{ij})$ and $B = (b_{ij})$ be two matrices with the same size. The matrix congruence $A \equiv B \pmod 2$ means that $a_{ij} \equiv b_{ij} \pmod 2$ for any possible i and j. And we write $A \sim B$ if B can be derived from A by a combination of types I and III elementary (row or column) operations [7, Definition 2.7(i) and (iii), Chap. VII]. According to [7, Theorem 3.5(viii), Chap. VII], if $A \sim B$ then $\det(A) \equiv \det(B) \pmod 2$.

For block matrix notations, especially the multiplication of block matrices, we refer the reader to [11, Chap. 3]. In Sec. 4, we will frequently use the following proposition to compute the determinants of M_o and M_e.

Proposition 3.1 (Block determinants [11, (6.2.1), Chap. 6]). *If A and D are square matrices, then*

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

4. Proof of Main Results

In this section, we give proofs of Theorems 1.1–1.4.

For any square-free positive integer n, according to the fundamental inequality $0 \le r(n) \le s(n)$, in order to show that n is non-congruent, it is sufficient to prove the 2-Selmer rank $s(n) = 0$. On account of Monsky's formula (2.3), we are reduced to proving the corresponding Monsky matrix is invertible over $\mathbb{F}_2$, i.e. the corresponding determinant is congruent to 1 modulo 2.

4.1. *Proof of Theorem* 1.1

Since the results stated in Theorem 1.1(2)–(3) are classical, we omit their proofs here. Now we give a simple proof for case (1). Note that the same method can be used to prove cases (2) and (3) as well.

In case (1), we consider the square-free positive integer $n = 2q_1q_2\cdots q_{g_3}$, where $q_i \equiv 3 \pmod 8$ for $1 \le i \le g_3$, and satisfying $(\frac{q_j}{q_i}) = -1$ for all $1 \le j < i \le g_3$. According to the law of quadratic reciprocity, it is easy to observe that $D_2 = D_{-1} = I_{g_3}$, and

$$A = \begin{pmatrix} 0 & & & \\ 1 & 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \cdots & 1 & g_3 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

where the ijth entries for $i < j$ lie in blank spaces which are equal to 0.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). By applying Proposition 3.1, we obtain

$$\det(M_e) = \det(I_{g_3} - (A^t + I_{g_3})(A + I_{g_3})).$$

It is easy to compute the inner matrix $(A^t + I_{g_3})(A + I_{g_3}) \equiv g_3 \mathbf{1}_{g_3 \times g_3} \pmod 2$, and then $\det(M_e) \equiv \det(I_{g_3} - g_3 \mathbf{1}_{g_3\times g_3}) \equiv g_3 + 1 \pmod 2$. It follows that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_3 \equiv 0 \pmod 2$. This is the desired conclusion.

4.2. *Proof of Theorem* 1.2

The following proof is quite similar to that of Theorem 1.1 but involves much more complicated block matrices operations.

(1) In this case, since $g_1 = g_7 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i$ defined by $(*)$. According to the law of quadratic reciprocity, it is easy to check that $D_{-1} = \begin{pmatrix} I_{g_3} & \\ & \mathbf{0}_{g_5} \end{pmatrix}$, $D_2 = \begin{pmatrix} I_{g_3} & \\ & I_{g_5} \end{pmatrix} = I_{g_3+g_5}$, $D_{-2} = \begin{pmatrix} \mathbf{0}_{g_3} & \\ & I_{g_5} \end{pmatrix}$, and $A = \begin{pmatrix} A_{11} & \mathbf{1} \\ \mathbf{1} & A_{22} \end{pmatrix}$, where

$$A_{11} = \begin{pmatrix} g_5 & & & \\ 1 & g_5+1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_5+g_3-1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_3+g_5-1 & 1 & \cdots & 1 \\ 1 & g_3+g_5-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_3+g_5-1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}).$$

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). By interchanging rows k and g_3+g_5+k for all $1 \le k \le g_3+g_5$ in M_o respectively, it is easy to see that $M_o \sim \begin{pmatrix} I_{g_3+g_5} & A+D_{-2} \\ A+D_2 & I_{g_3+g_5} \end{pmatrix}$. Thus [7, Theorem 3.5(viii), Chap. VII] and Proposition 3.1 make it obvious that

$$\det(M_o) \equiv \det(I_{g_3+g_5} - (A+D_2)(A+D_{-2})) \pmod 2. \tag{4.1}$$

In order to determine the right-hand determinant in Eq. (4.1), we first compute the inner matrix by using the block matrix multiplication (see for instance [11, Chap. 3]). That is

$$\begin{aligned}(A+D_2)(A+D_{-2}) &= \left(\begin{array}{c:c} A_{11}+I_{g_3} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{22}+I_{g_5} \end{array}\right) \left(\begin{array}{c:c} A_{11} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{22}+I_{g_5} \end{array}\right) \\ &\equiv \left(\begin{array}{c:c} g_5 \mathbf{1}_{g_3} & (g_3+g_5)\mathbf{1} \\ \hdashline g_5\mathbf{1} & \alpha_{22} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_3+g_5}(\mathbb{Z}),\end{aligned}$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

where $\alpha_{22} = (g_3+g_5)\mathbf{1}_{g_5} - (g_3+g_5-1)I_{g_5}$, and we omit the detail. It follows that

$$
\begin{aligned}
&I_{g_3+g_5} - (A+D_2)(A+D_{-2}) \\
&\equiv \begin{array}{c}
\left(\begin{array}{cccc:cccc}
g_5+1 & g_5 & \cdots & g_5 & g_3+g_5 & \cdots & \cdots & g_3+g_5 \\
g_5 & g_5+1 & \ddots & \vdots & \vdots & & & \vdots \\
\vdots & \ddots & \ddots & g_5 & \vdots & & & \vdots \\
g_5 & \cdots & g_5 & g_5+1 & g_3+g_5 & \cdots & \cdots & g_3+g_5 \\
\hdashline
g_5 & \cdots & \cdots & g_5 & 0 & g_3+g_5 & \cdots & g_3+g_5 \\
\vdots & & & \vdots & g_3+g_5 & 0 & \ddots & \vdots \\
\vdots & & & \vdots & \vdots & \ddots & \ddots & g_3+g_5 \\
g_5 & \cdots & \cdots & g_5 & g_3+g_5 & \cdots & g_3+g_5 & 0
\end{array}\right)
\begin{array}{l}
\left.\begin{array}{c}\\ \\ \\ \\ \end{array}\right\} g_3 \\
\left.\begin{array}{c}\\ \\ \\ \\ \end{array}\right\} g_5
\end{array} \\
\begin{array}{cc}
\underbrace{\hspace{10em}}_{g_3} & \underbrace{\hspace{12em}}_{g_5}
\end{array}
\end{array} \pmod 2.
\end{aligned} \tag{4.2}
$$

Here and subsequently, we use braces to count the corresponding rows or columns, and we will omit the below ones when all diagonal blocks are square.

In order to study the determinant of $I_{g_3+g_5} - (A+D_2)(A+D_{-2})$ in Eq. (4.1) modulo 2. We now perform more elementary row operations [7, Definition 2.7(i) and (iii), Chap. VII] on the left-hand matrix in Eq. (4.2) as follows.

First, we subtract all rows between row 2 and row g_3+g_5 by the first row, respectively. Second, we add the first row by rows between row g_3+1 and row g_3+g_5, and then add the first row by g_5 times of rows between row 2 and row g_3, respectively. It yields a lower triangular matrix as

$$
\begin{aligned}
&I_{g_3+g_5} - (A+D_2)(A+D_{-2}) \\
&\sim \left(\begin{array}{ccccc:ccc}
\triangle & & & & & & & \\
1 & 1 & & & & & & \\
1 & 0 & 1 & & & & & \\
\vdots & \vdots & \ddots & \ddots & & & & \\
1 & 0 & \cdots & 0 & 1 & & & \\
\hdashline
1 & 0 & \cdots & \cdots & 0 & g_3+g_5 & & \\
\vdots & \vdots & & & \vdots & & \ddots & \\
1 & 0 & \cdots & \cdots & 0 & & & g_3+g_5
\end{array}\right)
\begin{array}{l}
\left.\begin{array}{c}\\ \\ \\ \\ \\ \end{array}\right\} g_3 \\
\left.\begin{array}{c}\\ \\ \\ \end{array}\right\} g_5
\end{array} \pmod 2,
\end{aligned}
$$

where $\triangle = g_5 + 1 + g_5(g_3-1) + g_5 = g_3g_5 + g_5 + 1$.

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Now [7, Theorem 3.5(vii) and (viii), Chap. VII] gives that $\det(M_o) \equiv \det(I_{g_3+g_5} - (A + D_2)(A + D_{-2})) \equiv (g_3g_5 + g_5 + 1)(g_3 + g_5)^{g_5} \pmod 2$. By discussing the parity of g_3 and g_5, it follows immediately that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_3 \equiv 1 \pmod 2$ and $g_5 \equiv 0 \pmod 2$, where $g_3 \geq 1, g_5 \geq 1$.

(2) In this case, since $g_1 = g_7 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2\prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i$ defined by $(*)$. Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2), where A, D_{-1}, D_2 are the same as the proof of Theorem 1.2(1). Note that $D_2 = I_{g_3+g_5}$ and by Proposition 3.1, we get that

$$\det(M_e) = \det(D_{-1} - (A^t + D_2)(A + D_2)). \tag{4.3}$$

In order to determine the right-hand determinant modulo 2 in Eq. (4.3), we first compute the inner matrix $(A^t + D_2)(A + D_2)$ by applying the block matrix multiplication as before. That is

$$(A^t + D_2)(A + D_2) \equiv \left(\begin{array}{c|c} g_3\mathbf{1}_{g_3} & (g_5+1)\mathbf{1} \\ \hline (g_5+1)\mathbf{1} & \beta_{22} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_3+g_5}(\mathbb{Z}),$$

where $\beta_{22} = (g_3 + g_5)\mathbf{1}_{g_5} - (g_3 + g_5 - 1)I_{g_5}$. It follows that

$$\begin{aligned} &D_{-1} - (A^t + D_2)(A + D_2) \\ &\equiv \left(\begin{array}{cccc|cccc} g_3+1 & g_3 & \cdots & g_3 & g_5+1 & \cdots & \cdots & g_5+1 \\ g_3 & g_3+1 & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & g_3 & \vdots & & & \vdots \\ g_3 & \cdots & g_3 & g_3+1 & g_5+1 & \cdots & \cdots & g_5+1 \\ \hline g_5+1 & \cdots & \cdots & g_5+1 & 1 & g_3+g_5 & \cdots & g_3+g_5 \\ \vdots & & & \vdots & g_3+g_5 & 1 & \ddots & \vdots \\ \vdots & & & \vdots & \vdots & \ddots & \ddots & g_3+g_5 \\ g_5+1 & \cdots & \cdots & g_5+1 & g_3+g_5 & \cdots & g_3+g_5 & 1 \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_3 \\ \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_5 \end{array} \pmod 2. \end{aligned} \tag{4.4}$$

We now perform a finite sequence of elementary row and column operations [7, Definition 2.7(i) and (iii), Chap. VII] on the left-hand matrix in Eq. (4.4) as follows.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

First of all, we add rows between row 2 and row g_3 by the first row; and add rows between row g_3+2 and row g_3+g_5 by row g_3+1, respectively. This yields

$$
\begin{aligned}
&D_{-1}-(A^t+D_2)(A+D_2)\\
&\sim \left(\begin{array}{ccccc|cccc}
g_3+1 & g_3 & g_3 & \cdots & g_3 & g_5+1 & \cdots & \cdots & g_5+1\\
1 & 1 & 0 & \cdots & 0 & 0 & \cdots & \cdots & 0\\
1 & 0 & 1 & \ddots & \vdots & \vdots & & & \vdots\\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & & & \vdots\\
1 & 0 & \cdots & 0 & 1 & 0 & \cdots & \cdots & 0\\
\hline
g_5+1 & \cdots & \cdots & \cdots & g_5+1 & 1 & g_3+g_5 & \cdots & g_3+g_5\\
0 & \cdots & \cdots & \cdots & 0 & g_3+g_5+1 & g_3+g_5+1 & & \\
\vdots & & & & \vdots & \vdots & & \ddots & \\
0 & \cdots & \cdots & \cdots & 0 & g_3+g_5+1 & & & g_3+g_5+1
\end{array}\right)
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\end{array}}\right\} g_3\\
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_5
\end{array}\\
&\hspace{10cm}\pmod 2.
\end{aligned}
$$

We use the diagonal matrices appearing in the top left and bottom right blocks to eliminate the non-zero entries on rows (respectively, columns) one and g_3+1. We add the first row by g_3 times of rows from 2 to g_3; and subtract the first column by columns from 2 to g_3, respectively. Furthermore, we add row g_3+1 by g_5+1 times of rows from 2 to g_3; and add row (respectively, column) g_3+1 by rows (respectively, columns) from g_3+2 to g_3+g_5, respectively. We thus get

$$
\begin{aligned}
&D_{-1}-(A^t+D_2)(A+D_2)\\
&\equiv \left(\begin{array}{ccccc|cccc}
g_3+1 & 0 & 0 & \cdots & 0 & 0 & g_5+1 & \cdots & g_5+1\\
0 & 1 & 0 & \cdots & 0 & 0 & 0 & \cdots & 0\\
0 & 0 & 1 & \ddots & \vdots & \vdots & \vdots & & \vdots\\
\vdots & \vdots & \ddots & \ddots & 0 & \vdots & \vdots & & \vdots\\
0 & 0 & \cdots & 0 & 1 & 0 & 0 & \cdots & 0\\
\hline
g_3(g_5+1) & 0 & \cdots & \cdots & 0 & g_3(g_5+1)+1 & 1 & \cdots & 1\\
0 & \cdots & \cdots & \cdots & 0 & 0 & g_3+g_5+1 & & \\
\vdots & & & & \vdots & \vdots & & \ddots & \\
0 & \cdots & \cdots & \cdots & 0 & 0 & & & g_3+g_5+1
\end{array}\right)
\begin{array}{l}
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\\1\end{array}}\right\} g_3\\
\left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_5
\end{array}\\
&\hspace{10cm}\pmod 2.
\end{aligned}
\tag{4.5}
$$

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

We now only need to consider the right-hand matrix in Eq. (4.5) through the following two subcases:

Case (i). If $g_3 \equiv g_5 \pmod 2$. Then we have $g_3 + g_5 \equiv 0 \pmod 2$ and $g_3(g_5+1) \equiv 0 \pmod 2$. This implies that

$$D_{-1} - (A^t + D_2)(A + D_2) \sim \left(\begin{array}{cc:c} g_3+1 & & \\ & I_{g_3-1} & \mathfrak{S} \\ \hdashline & & I_{g_5} \end{array}\right) \pmod 2,$$

where we use $\mathfrak{S}$ to denote the block lying in the top left corner which does not contribute to the determinant of M_e. So we can now return to Eq. (4.3) and get that $\det(M_e) \equiv g_3 + 1 \pmod 2$. It is easy to see that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_3 \equiv g_5 \equiv 0 \pmod 2$ in this situation.

Case (ii). If $g_3 \not\equiv g_5 \pmod 2$. Then we must have $g_5 = 1$, otherwise the last row of the right-hand matrix in Eq. (4.5) is congruent to zero modulo 2. So we have $g_3 \equiv 0 \pmod 2$. It follows that $D_{-1} - (A^t + D_2)(A + D_2) \sim I_{g_3+1} \pmod 2$. Then it is clear that $\det(M_e) \equiv 1 \pmod 2$.

(3) In this case, since $g_1 = g_5 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2\prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that $D_{-1} = \left(\begin{smallmatrix} I_{g_3} & \\ & I_{g_7} \end{smallmatrix}\right) = I_{g_3+g_7}$, $D_2 = \left(\begin{smallmatrix} I_{g_3} & \\ & \mathbf{0}_{g_7} \end{smallmatrix}\right)$, $D_{-2} = \left(\begin{smallmatrix} \mathbf{0}_{g_3} & \\ & I_{g_7} \end{smallmatrix}\right)$, and $A = \left(\begin{smallmatrix} A_{11} & \mathbf{0} \\ \mathbf{1} & A_{22} \end{smallmatrix}\right)$, where

$$A_{11} = \begin{pmatrix} 0 & & & \\ 1 & 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_3 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_3 & & & \\ 1 & g_3+1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_3 + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}).$$

Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). Note that $D_{-1} = I_{g_3+g_7}$ and use Proposition 3.1 again, we see that

$$\det(M_e) = \det(D_2 - (A + D_2)(A^t + D_2)). \tag{4.6}$$

In order to determine the right-hand determinant in Eq. (4.6), we first compute the inner matrix $(A + D_2)(A^t + D_2)$ by block matrix multiplication. That is

$$(A + D_2)(A^t + D_2) \equiv \left(\begin{array}{c:c} \mathbf{1}_{g_3} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{0}_{g_7} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_3+g_7}(\mathbb{Z}).$$

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

It follows that

$$D_2 - (A + D_2)(A^t + D_2) \equiv \left(\begin{array}{c:c} \gamma_{g_3} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{0}_{g_7} \end{array}\right) \pmod 2, \tag{4.7}$$

where $\gamma_{g_3} = \mathbf{1}_{g_3} - I_{g_3}$. In order to make $\det(M_e) \equiv 1 \pmod 2$, it is easy to see that there must be $g_7 = 1$, otherwise the last two rows in the right-hand matrix in Eq. (4.7) will be equal when modulo 2. So we have

$$\begin{aligned} D_2 - (A + D_2)(A^t + D_2) &\equiv \left(\begin{array}{c:c} \gamma_{g_3} & \mathbf{1}_{g_3\times 1} \\ \hdashline \mathbf{1}_{1\times g_3} & 0 \end{array}\right) \\ &\sim \left(\begin{array}{c:c} I_{g_3} & \mathbf{1}_{g_3\times 1} \\ \hdashline \mathbf{1}_{1\times g_3} & 0 \end{array}\right) \sim \left(\begin{array}{c:c} I_{g_3} & \mathbf{1}_{g_3\times 1} \\ \hdashline \mathbf{0}_{1\times g_3} & g_3 \end{array}\right), \end{aligned}$$

where we add rows between row one and row g_3 by row $g_3 + 1$ respectively for the first $\sim$, and then add row $g_3 + 1$ by the resulting rows from 1 to g_3 for the second $\sim$. This implies that $\det(M_e) \equiv g_3 \pmod 2$. Consequently, $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_3 \equiv 1 \pmod 2$ and $g_7 = 1$.

Remark 4.1. A similar discussion shows that if $g_1 = g_5 = 0$, $\epsilon = 1$, and n is given by $(*)$, then $\det(M_o) \equiv 0 \pmod 2$ always holds.

(4) As we know, the result stated in case (4) is classical, see for instance [16, Table 3.8, p. 232] or [4, Lemma 1.1(3)]. Here we give a new proof for it by using Monsky's formula.

Since $g_1 = g_3 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_5} r_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that $D_{-1} = \begin{pmatrix} \mathbf{0}_{g_5} & \\ & I_{g_7} \end{pmatrix}$, $D_2 = \begin{pmatrix} I_{g_5} & \\ & \mathbf{0}_{g_7} \end{pmatrix}$, $D_{-2} = \begin{pmatrix} I_{g_5} & \\ & I_{g_7} \end{pmatrix} = I_{g_5+g_7}$, and $A = \begin{pmatrix} A_{11} & \mathbf{1} \\ \mathbf{1} & A_{22} \end{pmatrix}$, where

$$A_{11} = \begin{pmatrix} g_5 + g_7 - 1 & 1 & \cdots & 1 \\ 1 & g_5 + g_7 - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & 1 & g_5 + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_5 & & & \\ 1 & g_5 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \cdots & 1 & g_5 + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}).$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Since n is odd, one only need to consider the Monsky matrix M_o defined by formula (2.1). First of all, we interchange rows k and g_5+g_7+k for all $1 \le k \le g_5+g_7$ in M_o, respectively. It follows that $M_o \sim \left(\begin{smallmatrix} D_2 & A+D_{-2} \\ A+D_2 & D_2 \end{smallmatrix}\right)$. Here we denote the right-hand matrix by $\left(\begin{smallmatrix} I_{g_5} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{smallmatrix}\right)$, where $\alpha_{12} = \left(0 \,\vdots\, A_{11} + I_{g_5} \,\vdots\, \mathbf{1}_{g_5 \times g_7} \right) \in \mathrm{Mat}_{g_5 \times (g_7+g_5+g_7)}(\mathbb{Z})$, $\alpha_{21} = \alpha_{12}^t \in \mathrm{Mat}_{(g_7+g_5+g_7)\times g_5}(\mathbb{Z})$, and

$$\alpha_{22} = \left(\begin{array}{c|c|c} \mathbf{0}_{g_7} & \mathbf{1} & A_{22} + I_{g_7} \\ \hline \mathbf{1} & I_{g_5} & \\ \hline A_{22} & & \mathbf{0}_{g_7} \end{array}\right) \in \mathrm{Mat}_{g_7+g_5+g_7}(\mathbb{Z}).$$

According to Proposition 3.1, we see

$$\det(M_o) \equiv \det(\alpha_{22} - \alpha_{21}\alpha_{12}) \pmod 2.$$

By block matrix multiplication again, it is easy to compute that

$$\alpha_{21}\alpha_{12} \equiv \left(\begin{array}{c|c|c} \mathbf{0}_{g_7} & \mathbf{0} & \mathbf{0} \\ \hline \mathbf{0} & g_5\mathbf{1}_{g_5} + (g_7+1-g_5)I_{g_5} & (g_7+1)\mathbf{1} \\ \hline \mathbf{0} & (g_7+1)\mathbf{1} & g_5\mathbf{1}_{g_7} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_7+g_5+g_7}(\mathbb{Z}).$$

Then it follows that

$$\begin{aligned} &\alpha_{22} - \alpha_{21}\alpha_{12} \\ &\equiv \left(\begin{array}{cccc|cccc|cccc} & & & & 1 & \cdots & \cdots & 1 & g_5+1 & & & \\ & & & & \vdots & & & \vdots & 1 & g_5+2 & & \\ & & & & \vdots & & & \vdots & \vdots & \ddots & \ddots & \\ & & & & 1 & \cdots & \cdots & 1 & 1 & \cdots & 1 & g_5+g_7 \\ \hline 1 & \cdots & \cdots & 1 & g_7 & g_5 & \cdots & g_5 & g_7+1 & \cdots & \cdots & g_7+1 \\ \vdots & & & \vdots & g_5 & g_7 & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & & & \vdots & \vdots & \ddots & \ddots & g_5 & \vdots & & & \vdots \\ 1 & \cdots & \cdots & 1 & g_5 & \cdots & g_5 & g_7 & g_7+1 & \cdots & \cdots & g_7+1 \\ \hline g_5 & & & & g_7+1 & \cdots & \cdots & g_7+1 & g_5 & \cdots & \cdots & g_5 \\ 1 & g_5+1 & & & \vdots & & & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & & \vdots & & & \vdots & \vdots & & & \vdots \\ 1 & \cdots & 1 & g_5+g_7-1 & g_7+1 & \cdots & \cdots & g_7+1 & g_5 & \cdots & \cdots & g_5 \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_7 \\ \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_5 \\ \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} g_7 \end{array} \\ &\pmod 2. \end{aligned} \tag{4.8}$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

We now only need to consider the right-hand matrix in Eq. (4.8) through the following three subcases:

Case (i). If $g_5 \equiv g_7 \pmod 2$. Then there must be $g_5 = 1$. Otherwise, if $g_5 \geq 2$ then rows between row g_7+1 and row g_7+g_5 are equal when modulo 2 in the right-hand matrix in (4.8), which implies that the determinant of M_o is congruent to 0 modulo 2. And then we also have $g_7 \equiv 1 \pmod 2$ in this situation. It follows that

$$\alpha_{22} - \alpha_{21}\alpha_{12} \equiv \left(\begin{array}{cccc|c|cccc} & & & & 1 & 0 & & & \\ & & & & \vdots & 1 & 1 & & \\ & & & & \vdots & \vdots & \ddots & \ddots & \\ & & & & 1 & 1 & \cdots & 1 & g_7-1 \\ \hline 1 & \cdots & \cdots & 1 & 1 & & & & \\ \hline 1 & & & & & 1 & \cdots & \cdots & 1 \\ 1 & 2 & & & & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & & & \vdots & & & \vdots \\ 1 & \cdots & 1 & g_7 & & 1 & \cdots & \cdots & 1 \end{array}\right) \begin{array}{l} \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} g_7 \\ g_5 = 1 \\ \left.\begin{matrix} \\ \\ \\ \\ \end{matrix}\right\} g_7 \end{array} \pmod 2. \tag{4.9}$$

By comparing rows g_7+g_5+1 and g_7+g_5+2 in the right-hand matrix in Eq. (4.9), we get $g_7 = 1$, otherwise these two rows are equal when modulo 2. Then we see that

$$\alpha_{22} - \alpha_{21}\alpha_{12} \equiv \left(\begin{array}{c|c|c} & 1 & \\ \hline 1 & 1 & \\ \hline 1 & & 1 \end{array}\right) \pmod 2.$$

Now it is obvious that $\det(M_o) \equiv \det(\alpha_{22} - \alpha_{21}\alpha_{12}) \equiv 1 \pmod 2$.

Case (ii). If $g_5 \not\equiv g_7 \pmod 2$ and $g_7 \geq 2$. By considering the first two rows in the right-hand matrix in Eq. (4.8), there must be $g_5 \equiv 1 \pmod 2$, otherwise these two rows are equal when modulo 2 and thus cannot lead to $\det(M_o) \equiv 1 \pmod 2$. But if we consider rows $g_7 + g_5 + 1$ and $g_7 + g_5 + 2$, then there must be $g_5 \equiv 0 \pmod 2$ for the same reason. This leads to a contradiction.

Case (iii). If $g_5 \not\equiv g_7 \pmod 2$ and $g_7 = 1$. Then $g_5 \equiv 0 \pmod 2$. It follows that the last row in the right-hand matrix in Eq. (4.8) is equal to zero when modulo 2, which also implies that $\det(M_o) \equiv 0 \pmod 2$.

In summary, the desired conclusion is proved.

Remark 4.2. A similar discussion shows that if $g_1 = g_3 = 0$, $\epsilon = 2$, and n is given by $(*)$, then $\det(M_e) \equiv 0 \pmod 2$ always holds.

(5) In this case, since $g_5 = g_7 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that $D_{-1} = D_2 = \begin{pmatrix} \mathbf{0}_{g_1} & \\ & I_{g_3} \end{pmatrix}$, $D_{-2} = \mathbf{0}_{g_1+g_3}$, and $A = \begin{pmatrix} A_{11} & \mathbf{1} \\ \mathbf{1} & A_{22} \end{pmatrix}$,

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

where

$$A_{11} = \begin{pmatrix} g_1+g_3-1 & 1 & \cdots & 1 \\ 1 & g_1+g_3-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_1+g_3-1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1 & & & \\ 1 & g_1+1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1+g_3-1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}).$$

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). We write M_o as a 4×4 block matrix

$$M_o = \left(\begin{array}{c:c:c:c} A_{11} & \mathbf{1} & \mathbf{0}_{g_1} & \mathbf{0} \\ \hdashline \mathbf{1} & A_{22}+I_{g_3} & \mathbf{0} & I_{g_3} \\ \hdashline \mathbf{0}_{g_1} & \mathbf{0} & A_{11} & \mathbf{1} \\ \hdashline \mathbf{0} & I_{g_3} & \mathbf{1} & A_{22} \end{array}\right) \in \mathrm{Mat}_{g_1+g_3+g_1+g_3}(\mathbb{Z}). \tag{4.10}$$

Now we perform elementary row and column operations on M_o in Eq. (4.10). First, we interchange rows k and g_1+g_3+k for all $1 \le k \le g_1+g_3$, respectively. Second, we interchange block rows (respectively, columns) one and two to produce a block matrix whose top left corner and lower right corner are the identity matrix I_{g_3}. Then we get

$$M_o \sim \left(\begin{array}{c:c:c:c} I_{g_3} & \mathbf{0} & \mathbf{1} & A_{22} \\ \hdashline \mathbf{0} & \mathbf{0}_{g_1} & A_{11} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{11} & \mathbf{0}_{g_1} & \mathbf{0} \\ \hdashline A_{22}+I_{g_3} & \mathbf{1} & \mathbf{0} & I_{g_3} \end{array}\right) \in \mathrm{Mat}_{g_3+g_1+g_1+g_3}(\mathbb{Z}). \tag{4.11}$$

Here we denote the right-hand matrix in Eq. (4.11) by $\left(\begin{smallmatrix} I_{g_3} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{smallmatrix}\right)$. Due to Proposition 3.1, it follows that

$$\det(M_o) \equiv \det(\alpha_{22} - \alpha_{21}\alpha_{12}) \pmod 2.$$

And according to the block matrix multiplication, it is easy to compute that

$$\alpha_{22} - \alpha_{21}\alpha_{12} \equiv \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & A_{11} & \mathbf{1} \\ \hdashline A_{11} & g_3\mathbf{1}_{g_1} & (g_1+g_3-1)\mathbf{1} \\ \hdashline \mathbf{1} & (g_1+g_3)\mathbf{1} & I_{g_3} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_1+g_1+g_3}(\mathbb{Z}). \tag{4.12}$$

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Denote the right-hand matrix in Eq. (4.12) by $\left(\begin{smallmatrix}\beta_{11} & \beta_{12} \\ \beta_{21} & I_{g_3}\end{smallmatrix}\right)$. By Proposition 3.1 again, we see

$$\det(\alpha_{22} - \alpha_{21}\alpha_{12}) \equiv \det(\beta_{11} - \beta_{12}\beta_{21}) \pmod 2.$$

As before, we can compute that $\beta_{12}\beta_{21} \equiv \left(\begin{smallmatrix} g_3\mathbf{1}_{g_1} & g_3(g_1+1)\mathbf{1} \\ g_1g_3\mathbf{1} & \mathbf{0}_{g_1}\end{smallmatrix}\right) \pmod 2 \in \mathrm{Mat}_{g_1+g_1}(\mathbb{Z})$, and

$$\begin{aligned}
&\beta_{11} - \beta_{12}\beta_{21} \\
&\quad\equiv \left(\begin{array}{c:c} g_3\mathbf{1}_{g_1} & A_{11} + g_3(g_1+1)\mathbf{1} \\ \hdashline A_{11} + g_1g_3\mathbf{1} & g_3\mathbf{1}_{g_1}\end{array}\right) \\
&\quad\equiv \begin{cases}
\left(\begin{array}{cccc:cccc}
 & & & & g_1+1 & 1 & \cdots & 1 \\
 & & & & 1 & g_1+1 & \ddots & \vdots \\
 & & & & \vdots & \ddots & \ddots & 1 \\
 & & & & 1 & \cdots & 1 & g_1+1 \\ \hdashline
g_1+1 & 1 & \cdots & 1 & & & & \\
1 & g_1+1 & \ddots & \vdots & & & & \\
\vdots & \ddots & \ddots & 1 & & & & \\
1 & \cdots & 1 & g_1+1 & & & &
\end{array}\right)\begin{matrix}\left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}g_1 \\ \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}g_1\end{matrix} & \text{if } 2 \mid g_3; \\[2ex]
\left(\begin{array}{cccc:cccc}
1 & \cdots & \cdots & 1 & 1 & g_1 & \cdots & g_1 \\
\vdots & & & \vdots & g_1 & 1 & \ddots & \vdots \\
\vdots & & & \vdots & \vdots & \ddots & \ddots & g_1 \\
1 & \cdots & \cdots & 1 & g_1 & \cdots & g_1 & 1 \\ \hdashline
0 & g_1+1 & \cdots & g_1+1 & 1 & \cdots & \cdots & 1 \\
g_1+1 & 0 & \ddots & \vdots & \vdots & & & \vdots \\
\vdots & \ddots & \ddots & g_1+1 & \vdots & & & \vdots \\
g_1+1 & \cdots & g_1+1 & 0 & 1 & \cdots & \cdots & 1
\end{array}\right)\begin{matrix}\left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}g_1 \\ \left.\vphantom{\begin{matrix}1\\1\\1\\1\end{matrix}}\right\}g_1\end{matrix} & \text{if } 2 \nmid g_3.
\end{cases} \pmod 2
\end{aligned} \tag{4.13}$$

We now remain to consider the following four subcases:

Case (i). If $g_3 \equiv 0 \pmod 2$ and $g_1 \geq 2$. Then there must be $g_1 \equiv 1 \pmod 2$, otherwise the rows between row one and row g_1 in the upper right-hand matrix in

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Eq. (4.13) are equal when modulo 2. It follows that

$$\det(\beta_{11} - \beta_{12}\beta_{21}) \equiv \det(\gamma_{g_1})^2 \equiv \det(\gamma_{g_1}) \pmod 2,$$

where $\gamma_{g_1} = \mathbf{1}_{g_1} + I_{g_1} \in \mathrm{Mat}_{g_1}(\mathbb{Z})$. It is easy to compute that $\det(\gamma_{g_1}) \equiv g_1 - 1 \equiv 0 \pmod 2$. Thus we have $\det(M_o) \equiv 0 \pmod 2$.

Case (ii). If $g_3 \equiv 0 \pmod 2$ and $g_1 = 1$. Then we see that Eq. (4.13) becomes $\beta_{11} - \beta_{12}\beta_{21} \equiv \begin{pmatrix} 0 & g_1+1 \\ g_1+1 & 0 \end{pmatrix} \pmod 2$. It also follows that $\det(M_o) \equiv 0 \pmod 2$.

Case (iii). If $g_3 \equiv 1 \pmod 2$ and $g_1 \geq 2$. Then there must be $g_1 \equiv 0 \pmod 2$ for the same reason as in case (i). It follows that

$$\beta_{11} - \beta_{12}\beta_{21} \equiv \left(\begin{array}{c:c} \mathbf{1}_{g_1} & I_{g_1} \\ \hdashline \gamma_{g_1} & \mathbf{1}_{g_1} \end{array}\right) \pmod 2 \sim \left(\begin{array}{c:c} \gamma_{g_1} & \mathbf{1}_{g_1} \\ \hdashline \mathbf{1}_{g_1} & I_{g_1} \end{array}\right),$$

where γ_{g_1} is the same as in case (i). Using Proposition 3.1 once again, we see that $\det(\beta_{11} - \beta_{12}\beta_{21}) \equiv \det(\gamma_{g_1} - \mathbf{1}_{g_1}\mathbf{1}_{g_1}) \equiv \det(\gamma_{g_1} - g_1\mathbf{1}_{g_1}) \equiv \det(\gamma_{g_1}) \equiv g_1 - 1 \equiv 1 \pmod 2$. So we have $\det(M_o) \equiv 1 \pmod 2$.

Case (iv). If $g_3 \equiv 1 \pmod 2$ and $g_1 = 1$. Then Eq. (4.13) becomes $\beta_{11} - \beta_{12}\beta_{21} \equiv \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \pmod 2$. It also follows that $\det(M_o) \equiv 1 \pmod 2$.

In summary, the desired conclusion is proved.

Remark 4.3. A similar discussion shows that if $g_5 = g_7 = 0$, $\epsilon = 2$, and n is given by $(*)$, then $\det(M_e) \equiv 0 \pmod 2$ always holds.

(6) In this case, since $g_3 = g_7 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2\prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_5} r_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that $D_{-1} = \mathbf{0}_{g_1+g_5}$, $D_2 = D_{-2} = \begin{pmatrix} \mathbf{0}_{g_1} & \\ & I_{g_5} \end{pmatrix}$, and $A = \begin{pmatrix} A_{11} & \mathbf{1} \\ \mathbf{1} & A_{22} \end{pmatrix}$, where

$$A_{11} = \begin{pmatrix} g_1+g_5-1 & 1 & \cdots & 1 \\ 1 & g_1+g_5-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \ldots & 1 & g_1+g_5-1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1+g_5-1 & 1 & \cdots & 1 \\ 1 & g_1+g_5-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \ldots & 1 & g_1+g_5-1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}).$$

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). Note that A is symmetric, it is easy to see $\det(M_e) \equiv \det(A + D_2)\det(A^t + D_2) \equiv (\det(A + D_2))^2 \equiv \det(A + D_2) \pmod 2$, where

$$A + D_2 = \left(\begin{array}{cccc:cccc} g_1+g_5-1 & 1 & \cdots & 1 & 1 & \cdots & \cdots & 1 \\ 1 & g_1+g_5-1 & \ddots & \vdots & \vdots & & & \vdots \\ \vdots & \ddots & \ddots & 1 & \vdots & & & \vdots \\ 1 & \cdots & 1 & g_1+g_5-1 & 1 & \cdots & \cdots & 1 \\ \hdashline 1 & \cdots & \cdots & 1 & g_1+g_5 & 1 & \cdots & 1 \\ \vdots & & & \vdots & 1 & g_1+g_5 & \ddots & \vdots \\ \vdots & & & \vdots & \vdots & \ddots & \ddots & 1 \\ 1 & \cdots & \cdots & 1 & 1 & \cdots & 1 & g_1+g_5 \end{array}\right) \begin{array}{l} \left.\vphantom{\begin{array}{c} 1\\1\\1\\1 \end{array}}\right\} g_1 \\ \left.\vphantom{\begin{array}{c} 1\\1\\1\\1 \end{array}}\right\} g_5 \end{array}. \tag{4.14}$$

Now it is sufficient to consider the following two subcases:

Case (i). If $g_1 = g_5 = 1$. Then $A+D_2 \equiv \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right) \pmod 2$. It is obvious that $\det(M_e) \equiv \det(A + D_2) \equiv 1 \pmod 2$.

Case (ii). If $g_1 = 1$ and $g_5 \geq 2$. Then there must be $g_5 \equiv 1 \pmod 2$, otherwise the last g_5 rows of $A + D_2$ in Eq. (4.14) are equal when modulo 2, which follows that $\det(M_e) \equiv 0 \pmod 2$. We thus have

$$A + D_2 \equiv \left(\begin{array}{c:c} 1 & \mathbf{1}_{1\times g_5} \\ \hdashline \mathbf{1}_{g_5\times 1} & \gamma_{g_5} \end{array}\right) \sim \left(\begin{array}{c:c} 1 & \mathbf{1}_{1\times g_5} \\ \hdashline \mathbf{0}_{g_5\times 1} & I_{g_5} \end{array}\right) \pmod 2,$$

where $\gamma_{g_5} = I_{g_5} + \mathbf{1}_{g_5}$. This implies that $\det(M_e) \equiv \det(A + D_2) \equiv 1 \pmod 2$.

Case (iii). If $g_1 \geq 2$. Then there must be $g_1 + g_5 \equiv 1 \pmod 2$, otherwise the first g_1 rows of $A + D_2$ in Eq. (4.14) are equal when modulo 2, which follows that $\det(M_e) \equiv 0 \pmod 2$. And for the same reason, there must be $g_5 = 1$ by considering rows between row $g_1 + 1$ and row $g_1 + g_5$. This implies that $g_1 \equiv 0 \pmod 2$. So we have

$$A + D_2 \equiv \left(\begin{array}{c:c} \gamma_{g_1} & \mathbf{1}_{g_1\times 1} \\ \hdashline \mathbf{1}_{1\times g_1} & 1 \end{array}\right) \sim \left(\begin{array}{c:c} I_{g_1} & \mathbf{0}_{g_1\times 1} \\ \hdashline \mathbf{1}_{1\times g_1} & 1 \end{array}\right) \pmod 2,$$

where $\gamma_{g_1} = I_{g_1} + \mathbf{1}_{g_1}$. And we get that $\det(M_e) \equiv \det(A + D_2) \equiv 1 \pmod 2$.

Remark 4.4. A similar discussion shows that if $g_3 = g_7 = 0$, $\epsilon = 1$, and n is given by $(*)$, then $\det(M_e) \equiv 0 \pmod 2$ always holds.

Remark 4.5. A similar discussion shows that if $g_3 = g_5 = 0$, n is given by $(*)$, then $\det(M_e) \equiv 0 \pmod 2$ always holds.

4.3. *Proof of Theorem* 1.3

(1) In this case, since $g_1 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that

$$D_2 = \left(\begin{array}{c:c:c} I_{g_3} & & \\ \hdashline & I_{g_5} & \\ \hdashline & & \mathbf{0}_{g_7} \end{array}\right), \quad D_{-2} = \left(\begin{array}{c:c:c} \mathbf{0}_{g_3} & & \\ \hdashline & I_{g_5} & \\ \hdashline & & I_{g_7} \end{array}\right),$$

$$D_{-1} = \left(\begin{array}{c:c:c} I_{g_3} & & \\ \hdashline & \mathbf{0}_{g_5} & \\ \hdashline & & I_{g_7} \end{array}\right), \quad \text{and} \quad A = \left(\begin{array}{c:c:c} A_{11} & \mathbf{1} & \mathbf{0} \\ \hdashline \mathbf{1} & A_{22} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{1} & A_{33} \end{array}\right),$$

where

$$A_{11} = \begin{pmatrix} g_5 & & & \\ 1 & g_5+1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_5+g_3-1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1'-1 & 1 & \cdots & 1 \\ 1 & g_1'-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_1'-1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}),$$

$$A_{33} = \begin{pmatrix} g_3+g_5 & & & \\ 1 & g_3+g_5+1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_3+g_5+g_7-1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}),$$

here and subsequently, we write $g_1' = g_3 + g_5 + g_7$.

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). First of all, we interchange rows k and $g_1' + k$ for all $1 \le k \le g_1'$. It follows that

$$M_o \sim \left(\begin{array}{ccc:ccc} I_{g_3} & & & A_{11} & \mathbf{1} & \mathbf{0} \\ & I_{g_5} & & \mathbf{1} & A_{22}+I_{g_5} & \mathbf{1} \\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33}+I_{g_7} \\ \hdashline A_{11}+I_{g_3} & \mathbf{1} & \mathbf{0} & I_{g_3} & & \\ \mathbf{1} & A_{22}+I_{g_5} & \mathbf{1} & & I_{g_5} & \\ \mathbf{1} & \mathbf{1} & A_{33} & & & \mathbf{0}_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g_1'}(\mathbb{Z}). \tag{4.15}$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Note that if $g_7 \geq 2$, then we see $g_1' \equiv 1 \pmod 2$ by considering rows $g_1' - 1$ and g_1' in the right-hand matrix in Eq. (4.15), otherwise these two rows must be equal when modulo 2. For the same reason, we see $g_1' \equiv 0 \pmod 2$ by considering rows $2g_1' - 1$ and $2g_1'$. This implies a contradiction. So there must be $g_7 = 1$.

Now we perform more elementary row operations on the right-hand matrix in Eq. (4.15). We add row g_1' to rows between row one and row $g_3 + g_5$, respectively; and add the last row to rows between row $g_1' + 1$ and row $g_1' + g_3 + g_5$, respectively. Note that $g_1' = g_3 + g_5 + 1$ and $g_1' + 1 \equiv g_3 + g_5 \pmod 2$. We denote the resulting matrix by $\begin{pmatrix} I_{g_3+g_5} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{pmatrix}$, where

$$\alpha_{12} \equiv \left(\begin{array}{c:c:c:c} \mathbf{0} & A_{11}^t + I_{g_3} & \mathbf{0} & (g_3+g_5+1)\mathbf{1} \\ \hdashline \mathbf{0} & \mathbf{0} & (g_1'+1)I_{g_5} & (g_3+g_5)\mathbf{1} \end{array}\right) \pmod 2,$$

$$\alpha_{21}^t \equiv \left(\begin{array}{c:c:c:c} \mathbf{0} & A_{11} & \mathbf{0} & \mathbf{1} \\ \hdashline \mathbf{0} & \mathbf{0} & (g_1'+1)I_{g_5} & \mathbf{1} \end{array}\right) \pmod 2,$$

both α_{12} and α_{21}^t belong to $\mathrm{Mat}_{(g_3+g_5)\times(g_7+g_3+g_5+g_7)}(\mathbb{Z})$, and

$$\alpha_{22} \equiv \left(\begin{array}{c:c:c:c} 0 & \mathbf{1} & \mathbf{1} & g_3+g_5+1 \\ \hdashline (g_3+g_5)\mathbf{1} & I_{g_3} & \mathbf{0} & \mathbf{0} \\ \hdashline (g_3+g_5+1)\mathbf{1} & \mathbf{0} & I_{g_5} & \mathbf{0} \\ \hdashline g_3+g_5 & \mathbf{0} & \mathbf{0} & 0 \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_7+g_3+g_5+g_7}(\mathbb{Z}).$$

On account of Proposition 3.1, we have

$$\det(M_o) \equiv \det(\alpha_{22} - \alpha_{21}\alpha_{12}) \pmod 2.$$

It is easy to compute that

$$\begin{aligned} &\alpha_{22} - \alpha_{21}\alpha_{12} \\ &\equiv \left(\begin{array}{c:c:c:c} 0 & \mathbf{1}_{1\times g_3} & \mathbf{1}_{1\times g_5} & g_3+g_5+1 \\ \hdashline (g_3+g_5)\mathbf{1}_{g_3\times 1} & I_{g_3} & \mathbf{0} & (g_3+g_5+1)\mathbf{1}_{g_3\times 1} \\ \hdashline (g_3+g_5+1)\mathbf{1}_{g_5\times 1} & \mathbf{0} & g_1' I_{g_5} & (g_3+g_5)\mathbf{1}_{g_5\times 1} \\ \hdashline g_3+g_5 & (g_5+1)\mathbf{1}_{1\times g_3} & (g_3+g_5)\mathbf{1}_{1\times g_5} & g_5 \end{array}\right) \\ &\pmod 2. \end{aligned} \tag{4.16}$$

We now divide the proof into two subcases as follows:

Case (i). If $g_5 = 1$. Now add all rows between row $g_7 + 1$ and row $g_7 + g_3$ to row one in the right-hand matrix in Eq. (4.16), respectively. Then each column between column $g_7 + 1$ and column $g_7 + g_3$ in the resulting matrix has a unique nonzero entry. And note that $g_3(g_3 + g_5 + 1) + (g_3 + g_5 + 1) \equiv g_3 + g_3^2 \equiv 0 \pmod 2$,

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

then there is also a unique non-zero entry on the first row. According to [7, Proposition 3.6, Chap. VII], by considering the expansion of $\det(\alpha_{22}-\alpha_{21}\alpha_{12})$ along these special columns and the first row respectively, then we get that $\det(M_o)\equiv\det(\alpha_{22}-\alpha_{21}\alpha_{12})\equiv\det\begin{pmatrix} g_3 & g_3+1\\ g_3+1 & 1\end{pmatrix}\equiv g_3-(g_3+1)^2\equiv 1 \pmod 2$. Note that the last congruence holds for any positive integer g_3.

Case (ii). If $g_5\geq 2$. We consider rows between row g_7+g_3+1 and row $g_7+g_3+g_5$ in the right-hand matrix of Eq. (4.16), which follows that $g_1'\equiv 1 \pmod 2$, otherwise these rows are equal when modulo 2. It follows that $g_3+g_5\equiv 0 \pmod 2$ and $g_3\equiv g_5 \pmod 2$ since $g_7=1$. Then Eq. (4.16) becomes

$$\alpha_{22}-\alpha_{21}\alpha_{12}\equiv\left(\begin{array}{c:c:c:c} 0 & \mathbf{1}_{1\times g_3} & \mathbf{1}_{1\times g_5} & 1\\ \hdashline \mathbf{0}_{g_3\times 1} & I_{g_3} & \mathbf{0} & \mathbf{1}_{g_3\times 1}\\ \hdashline \mathbf{1}_{g_5\times 1} & \mathbf{0} & I_{g_5} & \mathbf{0}_{g_5\times 1}\\ \hdashline 0 & (g_5+1)\mathbf{1}_{1\times g_3} & \mathbf{0}_{1\times g_5} & g_5 \end{array}\right) \pmod 2.$$

In order to compute the determinant of the right-hand matrix, we add g_5+1 times of rows between row g_7+1 and row g_7+g_3 to the last row, and also add columns between column g_7+g_3+1 and column $g_7+g_3+g_5$ to the first column. Then we get a upper triangular matrix when modulo 2 and $\det(M_o)\equiv\det(\alpha_{22}-\alpha_{21}\alpha_{12})\equiv\det\begin{pmatrix} g_5 & *\\ 0 & g_5+g_3(g_5+1)\end{pmatrix}\equiv g_5^3\equiv g_5 \pmod 2$. So $\det(M_o)\equiv 1 \pmod 2$ if and only if $g_5\geq 2$ and $g_3\equiv g_5\equiv 1 \pmod 2$ in this subcase.

(2) In this case, since $g_1=0$ and $\epsilon=2$, we consider the square-free positive integer $n=2\cdot\prod_{i=1}^{g_3}q_i\cdot\prod_{i=1}^{g_5}r_i\cdot\prod_{i=1}^{g_7}s_i$ defined by $(*)$. Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). Following the same notation and computational results as in the proof of Theorem 1.3(1), we see that

$$M_e=\left(\begin{array}{ccc:ccc} I_{g_3} & & & A_{11}+I_{g_3} & \mathbf{1} & \mathbf{0}\\ & I_{g_5} & & \mathbf{1} & A_{22}+I_{g_5} & \mathbf{1}\\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33}\\ \hdashline A_{11}^t+I_{g_3} & \mathbf{1} & \mathbf{1} & I_{g_3} & & \\ \mathbf{1} & A_{22}^t+I_{g_5} & \mathbf{1} & & \mathbf{0}_{g_5} & \\ \mathbf{0} & \mathbf{1} & A_{33}^t & & & I_{g_7} \end{array}\right)\in \mathrm{Mat}_{2g_1'}(\mathbb{Z}), \quad (4.17)$$

where $g_1'=g_3+g_5+g_7$ as before.

First of all, note that there must be $g_7\leq 2$ by considering rows between row g_3+g_5+1 and row $g_3+g_5+g_7$ in M_e. Otherwise, there exist two adjacent rows being equal when modulo 2, this implies that $\det(M_e)\equiv 0 \pmod 2$.

We now divide the proof into subcases as follows:

Case (i). Suppose that $g_5\geq 2$. In order to ensure $\det(M_e)\equiv 1 \pmod 2$, there must be $g_1'\equiv 0 \pmod 2$ by considering rows between row $g_1'+g_3+1$ and row $g_1'+g_3+g_5$ modulo 2 in Eq. (4.17). Otherwise, these rows are equal when modulo 2.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Note that if $g_7 = 2$ then $g_3 + g_5 \equiv 0 \pmod 2$ and $g_3 \equiv g_5 \pmod 2$. After adding rows $2g_1'$ and $2g_1' - 1$ to row g_1', we see that rows g_1' and $g_1' - 1$ are equal when modulo 2. This implies that $\det(M_e) \equiv 0 \pmod 2$.

Now we discuss the situation when $g_7 = 1$, which implies that $g_3 + g_5 \equiv 1 \pmod 2$ and $g_3 \not\equiv g_5 \pmod 2$. We add rows (respectively, columns) between row (respectively, column) one and row (respectively, column) $g_3 + g_5$ by row (respectively, column) g_1', respectively, in Eq. (4.17). And denote the resulting block matrix by $\left(\begin{smallmatrix} I_{g_3+g_5} & \beta_{12} \\ \beta_{21} & \beta_{22} \end{smallmatrix}\right)$, where $\beta_{21} \equiv \beta_{12}^t \pmod 2 \in \mathrm{Mat}_{(g_7+g_3+g_5+g_7)\times(g_g+g_5)}(\mathbb{Z})$,

$$\beta_{12} \equiv \left(\begin{array}{c:c:c:c} \mathbf{0} & A_{11}^t & \mathbf{0} & \mathbf{1} \\ \hdashline \mathbf{0} & \mathbf{0} & I_{g_5} & \mathbf{0} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{(g_3+g_5)\times(g_7+g_3+g_5+g_7)}(\mathbb{Z}),$$

and

$$\beta_{22} \equiv \left(\begin{array}{c:c:c:c} 0 & \mathbf{1} & \mathbf{1} & 1 \\ \hdashline \mathbf{1} & I_{g_3} & & \\ \hdashline \mathbf{1} & & \mathbf{0}_{g_5} & \\ \hdashline 1 & & & 1 \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_7+g_3+g_5+g_7}(\mathbb{Z}).$$

According to Proposition 3.1, we see

$$\det(M_e) \equiv \det(\beta_{22} - \beta_{21}\beta_{12}) \pmod 2.$$

It is easy to compute the inner matrix

$$\beta_{22} - \beta_{21}\beta_{12} \equiv \left(\begin{array}{c:c:c:c} 0 & \mathbf{1}_{1\times g_3} & \mathbf{1}_{1\times g_5} & 1 \\ \hdashline \mathbf{1}_{g_3\times 1} & I_{g_3} + g_5\mathbf{1}_{g_3} & & g_5\mathbf{1}_{g_3\times 1} \\ \hdashline \mathbf{1}_{g_5\times 1} & & I_{g_5} & \\ \hdashline 1 & g_5\mathbf{1}_{1\times g_3} & & g_3+1 \end{array}\right) \pmod 2. \tag{4.18}$$

We now perform more elementary row and column operations on the right-hand matrix in Eq. (4.18). We add all columns between column $g_7 + g_3 + 1$ and column $g_7 + g_3 + g_5$ to column one; and add the last row to rows between row $g_7 + 1$ and row $g_7 + g_3$, respectively. Remind that $g_5 + g_3 + 1 = g_1' \equiv 0 \pmod 2$. It follows that

$$\beta_{22} - \beta_{21}\beta_{12} \sim \left(\begin{array}{c:c:c:c} g_5 & \mathbf{1}_{1\times g_3} & \mathbf{1}_{1\times g_5} & 1 \\ \hdashline & I_{g_3} & & \\ \hdashline & & I_{g_5} & \\ \hdashline 1 & g_5\mathbf{1}_{1\times g_3} & & g_3+1 \end{array}\right) \pmod 2.$$

And then using [7, Proposition 3.6, Chap. VII], we get $\det(M_e) \equiv \det(\beta_{22} - \beta_{21}\beta_{12}) \equiv \det\left(\begin{smallmatrix} g_5 & 1 \\ 1 & g_3+1 \end{smallmatrix}\right) \equiv g_5(g_3 + 1) + 1 \pmod 2$. So it is easy to see that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_3 \equiv 1 \pmod 2$, $g_5 \geq 2$ and $g_5 \equiv 0 \pmod 2$. Here we have used the fact that $g_3 \not\equiv g_5 \pmod 2$ given at the beginning of this subcase.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Case (ii). Suppose that $g_5 = 1$. Now we denote M_e by $\begin{pmatrix} I_{g_3+g_5} & \delta_{12} \\ \delta_{21} & \delta_{22} \end{pmatrix}$, where $\delta_{21} \equiv \delta_{12}^t \pmod 2 \in \mathrm{Mat}_{(g_g+g_5)\times(1+g_3+g_5+1)}(\mathbb{Z})$,

$$\delta_{12} \equiv \left(\begin{array}{c:c:c:c} \mathbf{0} & A_{11}+I_{g_3} & \mathbf{1} & \mathbf{0} \\ \hdashline \mathbf{0} & \mathbf{1} & g_1' & \mathbf{1} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{(g_3+g_5)\times(g_7+g_3+g_5+g_7)}(\mathbb{Z}),$$

and

$$\delta_{22} \equiv \left(\begin{array}{c:c:c:c} \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33} \\ \hdashline \mathbf{1} & I_{g_3} & & \\ \hdashline \mathbf{1} & & 0 & \\ \hdashline A_{33}^t & & & I_{g_7} \end{array}\right) \pmod 2 \in \mathrm{Mat}_{g_7+g_3+g_5+g_7}(\mathbb{Z}).$$

By Proposition 3.1, we see $\det(M_e) \equiv \det(\delta_{22} - \delta_{21}\delta_{12}) \pmod 2$. As before, it is easy to compute the inner matrix

$$\delta_{22} - \delta_{21}\delta_{12} \equiv \left(\begin{array}{c:c:c:c} \mathbf{0}_{g_7} & \mathbf{1}_{g_7\times g_3} & \mathbf{1}_{g_7\times 1} & A_{33} \\ \hdashline \mathbf{1}_{g_3\times g_7} & I_{g_3} + g_3\mathbf{1}_{g_3} & g_7\mathbf{1}_{g_3\times 1} & \mathbf{1}_{g_3\times g_7} \\ \hdashline \mathbf{1}_{1\times g_7} & g_7\mathbf{1}_{1\times g_3} & g_7+1 & g_1'\mathbf{1}_{1\times g_7} \\ \hdashline A_{33}^t & \mathbf{1}_{g_7\times g_3} & g_1'\mathbf{1}_{g_7\times 1} & I_{g_7}+\mathbf{1}_{g_7} \end{array}\right) \pmod 2. \tag{4.19}$$

Remember that $g_7 \leq 2$. First, if $g_7 = 1$, then $g_1' \equiv g_3 \pmod 2$. We see that $g_3 \equiv 1 \pmod 2$ by considering rows g_1' and $g_1' + g_7$ in the right-hand matrix in Eq. (4.19). Otherwise, these two rows are equal when modulo 2. However, this also causes rows one and $g_1' + g_7$ to be equal, too. It follows that $\det(M_e) \equiv 0 \pmod 2$ always holds.

Second, if $g_7 = 2$, then $g_1' \equiv g_3 + 1 \pmod 2$. We see that $g_3 \equiv 1 \pmod 2$ by considering the first two rows in the right-hand matrix in Eq. (4.19). Otherwise, these two rows are equal when modulo 2. However, if we add the last two rows to the second row, then the first two rows in the resulting matrix are equal when modulo 2, which also follows that $\det(M_e) \equiv 0 \pmod 2$.

In summary, the desired conclusion is proved.

(3) In this case, since $g_3 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_5} r_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that

$$D_2 = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & I_{g_5} & \\ \hdashline & & \mathbf{0}_{g_7} \end{array}\right), \quad D_{-2} = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & I_{g_5} & \\ \hdashline & & I_{g_7} \end{array}\right),$$

$$D_{-1} = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & \mathbf{0}_{g_5} & \\ \hdashline & & I_{g_7} \end{array}\right), \quad \text{and} \quad A = \left(\begin{array}{c:c:c} A_{11} & \mathbf{1} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{22} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{1} & A_{33} \end{array}\right),$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

where

$$A_{11} = \begin{pmatrix} g_3' - 1 & 1 & \cdots & 1 \\ 1 & g_3' - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_3' - 1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_3' - 1 & 1 & \cdots & 1 \\ 1 & g_3' - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_3' - 1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}),$$

$$A_{33} = \begin{pmatrix} g_1 + g_5 & & & \\ 1 & g_1 + g_5 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1 + g_5 + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}),$$

here and subsequently, we write $g_3' = g_1 + g_5 + g_7$.

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). It is easy to see that

$$M_o = \left(\begin{array}{ccc:ccc} A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22} + I_{g_5} & \mathbf{1} & & I_{g_5} & \\ \mathbf{1} & \mathbf{1} & A_{33} & & & \mathbf{0}_{g_7} \\ \hdashline \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_5} & & \mathbf{1} & A_{22} + I_{g_5} & \mathbf{1} \\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33} + I_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g_3'}(\mathbb{Z}). \quad (4.20)$$

Note that $g_1 \geq 1$ and $g_7 \geq 1$. In order to ensure $\det(M_o) \equiv 1 \pmod 2$, we see that $g_3' \equiv 1 \pmod 2$ by considering the first row and row g_3' of M_o in Eq. (4.20). Furthermore, suppose that $g_7 \geq 2$, then rows $g_3' - 1$ and g_3' are equal when modulo 2, so there must be $g_7 = 1$. This implies that $g_1 + g_5 \equiv 0 \pmod 2$ and $g_1 \equiv g_5 \pmod 2$.

We now perform elementary row and column operations on M_o. We adding rows between row one and row $g_1 + g_5$ by row g_3'; and add rows between row $g_3' + 1$ and row $g_3' + g_1 + g_5$ by row $2g_3'$, respectively. Then apply [7, Proposition 3.6, Chap. VII] to the resulting matrix finitely many times, we get $\det(M_o) \equiv \det\begin{pmatrix} I_{g_1} & \mathbf{1}_{g_1 \times 1} \\ \mathbf{1}_{1 \times g_1} & 0 \end{pmatrix} \equiv g_1 \pmod 2$. It follows that $\det(M_o) \equiv 1 \pmod 2$ if and only if $g_1 \equiv g_5 \equiv 1 \pmod 2$ and $g_7 = 1$.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

(4) In this case, since $g_3 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2 \cdot \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_5} r_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). Following the same notation and computational results as in the proof of Theorem 1.3(3), we see

$$M_e = \left(\begin{array}{ccc|ccc} \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_5} & & \mathbf{1} & A_{22}+I_{g_5} & \mathbf{1} \\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33} \\ \hline A_{11}^t & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22}^t+I_{g_5} & \mathbf{1} & & \mathbf{0}_{g_5} & \\ \mathbf{1} & \mathbf{1} & A_{33}^t & & & I_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g_3'}(\mathbb{Z}), \tag{4.21}$$

where $g_1' = g_3 + g_5 + g_7$ as before.

Note that $g_1 \geq 1$ and $g_7 \geq 1$. In order to ensure $\det(M_o) \equiv 1 \pmod 2$, we get that $g_3' \equiv 1 \pmod 2$ by considering the first row and row g_3' of M_o in (4.21). Furthermore, if $g_5 \geq 2$ then $g_3' \equiv 1 \pmod 2$ implies that the rows between row $g_3' + g_1 + 1$ and row $g_3' + g_1 + g_5$ are equal when modulo 2. So we only need to consider the situation when $g_5 = 1$. This implies $g_1 + g_7 \equiv 0 \pmod 2$ and $g_1 \equiv g_7 \pmod 2$.

Similarly, if $g_7 \geq 2$, then rows g_3' and $g_3' - 1$ are equal when modulo 2 because of $g_3' \equiv 1 \pmod 2$. So we also only need to consider the situation when $g_7 = 1$. This implies $g_1 \equiv 1 \pmod 2$.

We now perform elementary row and column operations on M_e. First, we add rows (respectively, columns) between row (respectively, column) $g_3' + 1$ and row (respectively, column) $g_3' + g_1$ by row (respectively, column) $g_3' + g_1 + g_5$, respectively. Second, we add the last row (respectively, column) by row (respectively, column) $g_3' + g_1 + g_5$. And then we apply [7, Proposition 3.6, Chap. VII] to the resulting matrix finitely many times, which follows that $\det(M_e) \equiv g_1 \det\begin{pmatrix} 1 & 1 \\ 0 & g_1 \end{pmatrix} \equiv g_1^2 \equiv 1 \pmod 2$ always holds.

(5) In this case, since $g_5 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that

$$D_2 = \left(\begin{array}{c|c|c} \mathbf{0}_{g_1} & & \\ \hline & I_{g_3} & \\ \hline & & \mathbf{0}_{g_7} \end{array}\right), \quad D_{-2} = \left(\begin{array}{c|c|c} \mathbf{0}_{g_1} & & \\ \hline & \mathbf{0}_{g_3} & \\ \hline & & I_{g_7} \end{array}\right),$$

$$D_{-1} = \left(\begin{array}{c|c|c} \mathbf{0}_{g_1} & & \\ \hline & I_{g_3} & \\ \hline & & I_{g_7} \end{array}\right), \quad \text{and} \quad A = \left(\begin{array}{c|c|c} A_{11} & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & A_{22} & \mathbf{0} \\ \hline \mathbf{1} & \mathbf{1} & A_{33} \end{array}\right),$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

where

$$A_{11} = \begin{pmatrix} g_5' - 1 & 1 & \cdots & 1 \\ 1 & g_5' - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_5' - 1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1 & & & \\ 1 & g_1 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1 + g_3 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

$$A_{33} = \begin{pmatrix} g_1 + g_3 & & & \\ 1 & g_1 + g_3 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1 + g_3 + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}),$$

here and subsequently, we write $g_5' = g_1 + g_3 + g_7$.

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). That is

$$M_o = \left(\begin{array}{ccc:ccc} A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22} + I_{g_3} & \mathbf{0} & & I_{g_3} & \\ \mathbf{1} & \mathbf{1} & A_{33} & & & \mathbf{0}_{g_7} \\ \hdashline \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_3} & & \mathbf{1} & A_{22} & \mathbf{0} \\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33} + I_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g_5'}(\mathbb{Z}). \tag{4.22}$$

Note that $g_1 \geq 1$ and $g_7 \geq 1$. In order to ensure $\det(M_o) \equiv 1 \pmod 2$, we get that $g_5' \equiv 1 \pmod 2$ by considering row one and row g_5' in M_o, for otherwise these two rows are equal when modulo 2. Furthermore, if $g_7 \geq 2$, then row g_5' is equal to row $g_5' - 1$ when modulo 2. So we only need to consider the situation when $g_7 = 1$. It follows that $g_1 + g_3 \equiv 0 \pmod 2$ and $g_1 \equiv g_3 \pmod 2$.

We now perform elementary row and column operations on M_o in Eq. (4.22). We add rows between row one and row $g_1 + g_3$ by row g_5'; and add rows between row $g_5' + 1$ and row $g_5' + g_1$ by row $2g_5'$, respectively. After this, we continue to add all columns between column one and column g_1 to column g_5'. For the resulting matrix, we use [7, Proposition 3.6, Chap. VII], and get that

$$\det(M_o) \equiv \det\left(\begin{array}{c:c} A_{22}^t & I_{g_3} \\ \hdashline I_{g_3} & A_{22} \end{array}\right) \equiv \det\left(\begin{array}{c:c} I_{g_3} & A_{22} \\ \hdashline A_{22}^t & I_{g_3} \end{array}\right) \pmod 2, \tag{4.23}$$

where we performed type I elementary row operations for the second congruence.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

As before, we compute the right-hand determinant in Eq. (4.23) by using Proposition 3.1. It is easy to compute that $A_{22}^t A_{22} \equiv (g_1 + g_3 + 1)\mathbf{1}_{g_3} \equiv \mathbf{1}_{g_3} \pmod 2$. So Proposition 3.1 implies that $\det(M_o) \equiv \det(I_{g_3} - A_{22}^t A_{22}) \equiv \det\gamma_{g_3} \equiv g_3 - 1 \pmod 2$. Now it is obvious that $\det(M_o) \equiv 1 \pmod 2$ if and only if $g_1 \equiv g_3 \equiv 0 \pmod 2$ and $g_7 = 1$.

(6) In this case, since $g_5 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2\prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. Since n is even, we only need to consider the Monsky matrix M_e defined by formula (2.2). Following the same notation and computational results as in the proof of Theorem 1.3(5), we see that

$$M_e = \left(\begin{array}{ccc:ccc} \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_3} & & \mathbf{1} & A_{22} + I_{g_3} & \mathbf{0} \\ & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & A_{33} \\ \hdashline A_{11}^t & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22}^t + I_{g_3} & \mathbf{1} & & I_{g_3} & \\ \mathbf{1} & \mathbf{0} & A_{33}^t & & & I_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g_5'}(\mathbb{Z}), \tag{4.24}$$

where $g_5' = g_1 + g_3 + g_7$ as before.

Note that $g_1 \geq 1$ and $g_7 \geq 1$. In order to ensure $\det(M_e) \equiv 1 \pmod 2$, we get $g_5' \equiv 1 \pmod 2$ by considering row one and row g_5' in M_e, for otherwise these two rows are equal when modulo 2. Furthermore, if $g_7 \geq 2$, then row g_5' is equal to row $g_5' - 1$ when modulo 2. So we also only need to consider the situation when $g_7 = 1$. It follows that $g_1 + g_3 \equiv 0 \pmod 2$ and $g_1 \equiv g_3 \pmod 2$.

We now perform elementary row and column operations on M_e in Eq. (4.24). Fisrt, we add rows between row one and row $g_1 + g_3$ by row g_5', and add rows between row $g_5' + 1$ and row $g_5' + g_1 + g_3$ by row $2g_5'$, respectively. Second, we add all rows (respectively, columns) between row (respectively, column) one and row (respectively, column) g_1 to row (respectively, column) g_5'. Finally, continue to add g_1 times column $2g_5'$ to column g_5'. This yields

$$M_e \sim \left(\begin{array}{ccc:ccc} \mathbf{0}_{g_1} & & & I_{g_1} & \mathbf{0} & \mathbf{1} \\ & I_{g_3} & & \mathbf{0} & A_{22}^t & \mathbf{0} \\ & & 0 & \mathbf{0} & \mathbf{1} & g_1 \\ \hdashline I_{g_1} & \mathbf{0} & \mathbf{0} & \mathbf{0}_{g_1} & & \\ \mathbf{0} & A_{22} & \mathbf{1} & & I_{g_3} & \\ \mathbf{1} & \mathbf{0} & 0 & & & 1 \end{array}\right) \in \mathrm{Mat}_{2g_5'}(\mathbb{Z}). \tag{4.25}$$

For the right-hand matrix in Eq. (4.25), we use [7, Proposition 3.6, Chap. VII] finitely many times, and get that

$$\det(M_e) \equiv \det\left(\begin{array}{c:c:c} I_{g_3} & \mathbf{0} & A_{22}^t \\ \hdashline \mathbf{0} & g_1 & \mathbf{1} \\ \hdashline A_{22} & \mathbf{1} & I_{g_3} \end{array}\right) \pmod 2. \tag{4.26}$$

As before, we use Proposition 3.1 again to compute the right-hand determinant in Eq. (4.26). It is easy to see that $\begin{pmatrix} A_{22}^t \\ \mathbf{1} \end{pmatrix} (A_{22}\ \mathbf{1}) \equiv (g_1 + g_3 + 1)\mathbf{1}_{g_3} \equiv \mathbf{1}_{g_3} \pmod 2$. So Proposition 3.1 implies that $\det(M_e) \equiv \det\left(\begin{pmatrix} I_{g_3} & \mathbf{0} \\ \mathbf{0} & g_1 \end{pmatrix} - \begin{pmatrix} A_{22}^t \\ \mathbf{1} \end{pmatrix} (A_{22}\ \mathbf{1})\right) \equiv \det\begin{pmatrix} \gamma_{g_3} & \mathbf{1} \\ \mathbf{1} & 0 \end{pmatrix} \equiv \det\begin{pmatrix} I_{g_3} & \mathbf{1} \\ \mathbf{0} & g_3 \end{pmatrix} \equiv g_3 \pmod 2$. Now it is obvious that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_1 \equiv g_3 \equiv 1 \pmod 2$ and $g_7 = 1$.

(7) In this case, since $g_7 = 0$ and $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that

$$D_2 = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & I_{g_3} & \\ \hdashline & & I_{g_5} \end{array}\right), \quad D_{-2} = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & \mathbf{0}_{g_3} & \\ \hdashline & & I_{g_5} \end{array}\right),$$

$$D_{-1} = \left(\begin{array}{c:c:c} \mathbf{0}_{g_1} & & \\ \hdashline & I_{g_3} & \\ \hdashline & & \mathbf{0}_{g_5} \end{array}\right), \quad \text{and} \quad A = \left(\begin{array}{c:c:c} A_{11} & \mathbf{1} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{22} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{1} & A_{33} \end{array}\right),$$

where

$$A_{11} = \begin{pmatrix} g_7' - 1 & 1 & \cdots & 1 \\ 1 & g_7' - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_7' - 1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1 + g_5 & & & \\ 1 & g_1 + g_5 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1 + g_5 + g_3 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}), \tag{4.27}$$

$$A_{33} = \begin{pmatrix} g_7' - 1 & 1 & \cdots & 1 \\ 1 & g_7' - 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g_7' - 1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}),$$

here and subsequently, we write $g_7' = g_1 + g_3 + g_5$.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). That is

$$M_o = \left(\begin{array}{ccc:ccc} A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22}+I_{g_3} & \mathbf{1} & & I_{g_3} & \\ \mathbf{1} & \mathbf{1} & A_{33}+I_{g_5} & & & I_{g_5} \\ \hdashline \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_3} & & \mathbf{1} & A_{22} & \mathbf{1} \\ & & I_{g_5} & \mathbf{1} & \mathbf{1} & A_{33}+I_{g_5} \end{array}\right) \in \mathrm{Mat}_{2g_7'}(\mathbb{Z}).$$

We now perform elementary row operations on M_o by adding the first row to rows between row 2 and row g_7', and adding row $g_7'+1$ to rows between row $g_7'+2$ and row $2g_7'$, respectively. It follows that $M_o \sim M_o' := \left(\begin{smallmatrix} M_{11}' & D_2 \\ D_2 & M_{22}' \end{smallmatrix}\right) \pmod 2$, where $M_{22}' = M_{11}' + D_{-1}$, and

$$M_{11}' \equiv \left(\begin{array}{cccc:cccc:ccc} g_7'-1 & 1 & \cdots & 1 & 1 & \cdots & \cdots & 1 & 1 & \cdots & 1 \\ g_7' & g_7' & & & & & & & & & \\ \vdots & & \ddots & & & & & & & & \\ g_7' & & & g_7' & & & & & & & \\ \hdashline g_7' & & & & g_1+g_5 & 1 & \cdots & 1 & & & \\ \vdots & & & & & g_1+g_5+1 & \ddots & \vdots & & & \\ \vdots & & & & & & \ddots & 1 & & & \\ g_7' & & & & & & & g_1+g_5+g_3-1 & & & \\ \hdashline g_7' & & & & & & & & g_7'+1 & & \\ \vdots & & & & & & & & & \ddots & \\ g_7' & & & & & & & & & & g_7'+1 \end{array}\right) \begin{array}{l} \left.\rule{0pt}{3.5em}\right\} g_1 \\ \left.\rule{0pt}{3.5em}\right\} g_3 \\ \left.\rule{0pt}{2.5em}\right\} g_5 \end{array}$$

$$\pmod 2. \tag{4.28}$$

Note that if $g_7' \equiv 0 \pmod 2$ then row g_1+g_3+k is equal to row $g_7'+g_1+g_3+k$ for $1 \le k \le g_5$ in M_o', which implies that $\det(M_o) \equiv 0 \pmod 2$ since $g_5 \ge 1$. Thus we only need to consider the situation when $g_7' \equiv 1 \pmod 2$.

Now we perform more elementary row and column operations on M_o'. First, we add all rows (respectively, columns) between row (respectively, column) 2 and row (respectively, column) g_1 to the first row (respectively, column); and add all rows (respectively, columns) between row (respectively, column) $g_7'+2$ and row (respectively, column) $g_7'+g_1$ to row (respectively, column) $g_7'+1$ in M_o'. Second,

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

we interchange rows l and $g_7'+l$ for all $1 \le l \le g_7'$. Then we get $M_o \sim M_o' \sim M_o'' := \left(\begin{smallmatrix} D_2 & M_{22}'' \\ M_{11}'' & D_2 \end{smallmatrix}\right) \pmod 2$, where $M_{22}'' = M_{11}'' + D_{-1}$, and

$$M_{11}'' \equiv \left(\begin{array}{cccc:cccc:ccc}
g_1-1 & & & & 1 & \cdots & \cdots & 1 & 1 & \cdots & 1 \\
 & 1 & & & & & & & & & \\
 & & \ddots & & & & & & & & \\
 & & & 1 & & & & & & & \\
\hdashline
1 & & & & g_1+g_5 & 1 & \cdots & 1 & & & \\
\vdots & & & & & g_1+g_5+1 & \ddots & \vdots & & & \\
\vdots & & & & & & \ddots & 1 & & & \\
1 & & & & & & & g_1+g_5+g_3-1 & & & \\
\hdashline
1 & & & & & & & & & & \\
\vdots & & & & & & & & & & \\
1 & & & & & & & & & &
\end{array}\right)
\begin{array}{l}
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} g_1 \\
\left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} g_3 \\
\left.\vphantom{\begin{array}{c}a\\a\\a\end{array}}\right\} g_5
\end{array}
\pmod 2.$$

We denote the resulting matrix $\left(\begin{smallmatrix} D_2 & M_{22}'' \\ M_{11}'' & D_2 \end{smallmatrix}\right)$ by $\left(\begin{smallmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & I_{g_3+g_5} \end{smallmatrix}\right)$. By Proposition 3.1, we see $\det(M_o) \equiv \det(\alpha_{11} - \alpha_{12}\alpha_{21}) \pmod 2$. And according to block matrix multiplication, it is easy to compute that

$$\alpha_{11} - \alpha_{12}\alpha_{21} \equiv \left(\begin{array}{c:c:c:c}
(g_3+g_5)\delta_{g_1} & (g_1+g_5)\xi_{g_3\times g_1}^t & \mathbf{0} & g_1\delta_{g_1} + I_{g_1} \\
\hdashline
\xi_{g_3\times g_1} & I_{g_3} & \mathbf{0} & \xi_{g_3\times g_1} \\
\hdashline
\mathbf{0} & \mathbf{0} & I_{g_5} & \xi_{g_5\times g_1} \\
\hdashline
g_1\delta_{g_1} + I_{g_1} & \xi_{g_3\times g_1}^t & \xi_{g_5\times g_1}^t & \mathbf{0}_{g_1}
\end{array}\right) \pmod 2$$

$$\in \mathrm{Mat}_{g_7'+g_1}(\mathbb{Z}), \tag{4.29}$$

here and subsequently, we write $\delta_k = \mathrm{diag}(1, 0, \ldots, 0) \in \mathrm{Mat}_k(\mathbb{Z})$ and $\xi_{k\times l} = \left(\mathbf{1}_{k\times 1}\ \mathbf{0}_{k\times(l-1)}\right) \in \mathrm{Mat}_{k\times l}(\mathbb{Z})$.

We now perform elementary column operations on the right-hand matrix in Eq. (4.29). We add the first column by columns between column g_1+1 and column g_1+g_3, respectively; and also add column $g_7'+1$ by columns between column g_1+1 and column g_7', respectively. Then we get

$$\alpha_{11} - \alpha_{12}\alpha_{21}$$

$$\sim \left(\begin{array}{c:c:c:c}
\kappa\delta_{g_1} & (g_1+g_5)\xi_{g_3\times g_1}^t & \mathbf{0} & \lambda\delta_{g_1} + I_{g_1} \\
\hdashline
\mathbf{0} & I_{g_3} & \mathbf{0} & \mathbf{0} \\
\hdashline
\mathbf{0} & \mathbf{0} & I_{g_5} & \mathbf{0} \\
\hdashline
(g_1+g_3)\delta_{g_1} + I_{g_1} & \xi_{g_3\times g_1}^t & \xi_{g_5\times g_1}^t & (g_3+g_5)\delta_{g_1}
\end{array}\right) \pmod 2,$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

where $\kappa = g_3 + g_5 + g_3(g_1 + g_5)$ and $\lambda = g_1 + g_3(g_1 + g_5)$. By using [7, Proposition 3.6, Chap. VII] finitely many times on the right-hand matrix, then we get $\det(M_o) \equiv \det\begin{pmatrix} \kappa & \lambda+1 \\ g_1+g_3+1 & g_3+g_5 \end{pmatrix} \equiv g_3(g_1+1) \pmod 2$. We thus see that $\det(M_o) \equiv 1 \pmod 2$ if and only if $g_1 \equiv 0 \pmod 2$, $g_3 \equiv 1 \pmod 2$ and $g_5 \equiv 0 \pmod 2$.

(8) In this case, since $g_7 = 0$ and $\epsilon = 2$, we consider the square-free positive integer $n = 2 \cdot \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i$ defined by $(*)$. Since n is even, we only need to consider the determinant of the Monsky matrix M_e defined by formula (2.2). Following the same notation and computational results as in the proof of Theorem 1.3(7), it is easy to see that

$$M_e = \left(\begin{array}{ccc:ccc} \mathbf{0}_{g_1} & & & A_{11} & \mathbf{1} & \mathbf{1} \\ & I_{g_3} & & \mathbf{1} & A_{22}+I_{g_3} & \mathbf{1} \\ & & I_{g_5} & \mathbf{1} & \mathbf{1} & A_{33}+I_{g_5} \\ \hdashline A_{11}^t & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & \\ \mathbf{1} & A_{22}^t+I_{g_3} & \mathbf{1} & & I_{g_3} & \\ \mathbf{1} & \mathbf{1} & A_{33}^t+I_{g_5} & & & \mathbf{0}_{g_5} \end{array}\right) \in \mathrm{Mat}_{2g_7'}(\mathbb{Z}), \tag{4.30}$$

where $g_7' = g_1 + g_3 + g_5$ as before.

We now perform elementary row operations on M_e by adding the first row to rows between row 2 and row g_7', and adding row $g_7'+1$ to rows between row $g_7'+2$ and row $2g_7'$, respectively. It follows that

$$M_o \sim M_o' := \left(\begin{array}{c:c} D_2 & M_{12}' \\ \hdashline M_{21}' & D_{-1} \end{array}\right) \pmod 2, \tag{4.31}$$

where M_{12}' is equal to the right-hand block matrix in Eq. (4.28), and

$$M_{21}' \equiv \left(\begin{array}{cccc:cccc:ccc} g_7'-1 & 1 & \cdots & 1 & 1 & \cdots & \cdots & 1 & 1 & \cdots & 1 \\ g_7' & g_7' & & & & & & & & & \\ \vdots & & \ddots & & & & & & & & \\ g_7' & & & g_7' & & & & & & & \\ \hdashline g_7' & & & & g_1+g_5 & & & & & & \\ \vdots & & & & 1 & g_1+g_5+1 & & & & & \\ \vdots & & & & \vdots & \ddots & \ddots & & & & \\ g_7' & & & & 1 & \cdots & 1 & g_1+g_5+g_3-1 & & & \\ \hdashline g_7' & & & & & & & & g_7'+1 & & \\ \vdots & & & & & & & & & \ddots & \\ g_7' & & & & & & & & & & g_7'+1 \end{array}\right) \begin{array}{l} \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} g_1 \\ \left.\begin{array}{c} \\ \\ \\ \\ \end{array}\right\} g_3 \\ \left.\begin{array}{c} \\ \\ \\ \end{array}\right\} g_5 \end{array} \pmod 2.$$

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

We now divide the proof into two subcases as below:

Case (i). For $g_7' \equiv 0 \pmod 2$. Note that if $g_1 \geq 2$ then all rows between row 2 and row g_1 are zero rows when modulo 2. So there must be $g_1 = 1$. We thus also have $g_3 + g_5 \equiv 1 \pmod 2$ and $g_3 \not\equiv g_5 \pmod 2$.

We perform elementary column and row operations on the right-hand matrix in Eq. (4.31). First, we add the first column to columns between column $g_1 + 1$ and column g_7', and add column $g_7' + 1$ to columns between column $g_7' + 2$ and column $2g_7'$, respectively. Second, we add row $g_7' + g_1 + g_3 + k$ to row $g_1 + g_3 + k$ for all $1 \leq k \leq g_5$, respectively. And then by applying [7, Proposition 3.6, Chap. VII] to the resulting matrix finitely many times, we get

$$\det(M_o) \equiv \det\left(\begin{array}{c|c} I_{g_3} & A_{22}^t \\ \hline A_{22} & I_{g_3} \end{array}\right) \pmod 2,$$

where A_{22} was given by Eq. (4.27) for $g_1 = 1$.

Now Proposition 3.1 implies that

$$\det(M_o) \equiv \det(I_{g_3} - A_{22}^t A_{22}) \pmod 2.$$

It is easy to compute that $A_{22}^t A_{22} \equiv (g_3 + g_5)\mathbf{1}_{g_3} \equiv \mathbf{1}_{g_3} \pmod 2$, and $\det(M_o) \equiv g_3 - 1 \pmod 2$. So we get $\det(M_o) \equiv 1 \pmod 2$ if and only if $g_3 \equiv 0 \pmod 2$, and thus $g_5 \equiv 1 \pmod 2$.

Case (ii). For $g_7' \equiv 1 \pmod 2$. Note that rows from $g_7' + g_1 + g_3 + 1$ to $2g_7'$ are equal when modulo 2 in this situation, which implies that $g_5 = 1$. Otherwise $\det(M_o) \equiv 0 \pmod 2$ follows. So we also have $g_1 + g_3 \equiv 0 \pmod 2$ and $g_1 \equiv g_3 \pmod 2$.

Similarly, we perform elementary row and column operations on the right-hand matrix in Eq. (4.31) under the assumption that $g_7' \equiv 1 \pmod 2$. First, we add the last row (respectively, column) to rows (respectively, columns) between row (respectively, column) $g_7' + 2$ and row (respectively, column) $g_7' + g_1 + g_3$, respectively. Second, we add all rows (respectively, columns) between row (respectively, column) $g_7' + 2$ and row (respectively, column) $g_7' + g_1$ to row (respectively, column) $g_7' + 1$. Third, we add row (respectively, column) g_7' to row (respectively, column) $g_7' + 1$. Finally, add row (respectively, column) $g_7' + 1$ to rows (respectively, columns) between row (respectively, column) $g_1 + 1$ and row (respectively, column) $g_1 + g_3$, respectively. Also apply [7, Proposition 3.6, Chap. VII] to the resulting matrix finitely many times, we get

$$\det(M_o) \equiv \det\left(\begin{array}{c|c} \gamma_{g_3} & A_{22}^t \\ \hline A_{22} & I_{g_3} \end{array}\right) \pmod 2,$$

where A_{22} was given by Eq. (4.27) for $g_5 = 1$, and $\gamma_{g_3} = I_{g_3} + \mathbf{1}_{g_3}$. Now use Proposition 3.1 again, it follows that

$$\det(M_o) \equiv \det(\gamma_{g_3} - A_{22}^t A_{22}) \pmod 2.$$

It is easy to compute that $A_{22}^t A_{22} \equiv (g_7' + 1)\mathbf{1}_{g_3} \equiv 0 \pmod 2$, and $\det(M_o) \equiv \det(\gamma_{g_3}) \equiv g_3 - 1 \pmod 2$. Thus we get that $\det(M_o) \equiv 1 \pmod 2$ if and only if $g_1 \equiv g_3 \equiv 0 \pmod 2$.

In summary, the desired conclusion is proved.

4.4. *Proof of Theorem* 1.4

In this case, since $\epsilon = 1$, we consider the square-free positive integer $n = \prod_{i=1}^{g_1} p_i \cdot \prod_{i=1}^{g_3} q_i \cdot \prod_{i=1}^{g_5} r_i \cdot \prod_{i=1}^{g_7} s_i$ defined by $(*)$. By the law of quadratic reciprocity, it is easy to check that

$$D_2 = \left(\begin{array}{c:c:c:c} \mathbf{0}_{g_1} & & & \\ \hdashline & I_{g_3} & & \\ \hdashline & & I_{g_5} & \\ \hdashline & & & \mathbf{0}_{g_7} \end{array}\right), \quad D_{-2} = \left(\begin{array}{c:c:c:c} \mathbf{0}_{g_1} & & & \\ \hdashline & \mathbf{0}_{g_3} & & \\ \hdashline & & I_{g_5} & \\ \hdashline & & & I_{g_7} \end{array}\right),$$

$$D_{-1} = \left(\begin{array}{c:c:c:c} \mathbf{0}_{g_1} & & & \\ \hdashline & I_{g_3} & & \\ \hdashline & & \mathbf{0}_{g_5} & \\ \hdashline & & & I_{g_7} \end{array}\right), \quad \text{and} \quad A = \left(\begin{array}{c:c:c:c} A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ \hdashline \mathbf{1} & A_{22} & \mathbf{1} & \mathbf{0} \\ \hdashline \mathbf{1} & \mathbf{1} & A_{33} & \mathbf{1} \\ \hdashline \mathbf{1} & \mathbf{1} & \mathbf{1} & A_{44} \end{array}\right),$$

where

$$A_{11} = \begin{pmatrix} g-1 & 1 & \cdots & 1 \\ 1 & g-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g-1 \end{pmatrix} \in \mathrm{Mat}_{g_1}(\mathbb{Z}),$$

$$A_{22} = \begin{pmatrix} g_1 + g_5 & & & \\ 1 & g_1 + g_5 + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_1 + g_5 + g_3 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_3}(\mathbb{Z}),$$

$$A_{33} = \begin{pmatrix} g-1 & 1 & \cdots & 1 \\ 1 & g-1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 1 & \dots & 1 & g-1 \end{pmatrix} \in \mathrm{Mat}_{g_5}(\mathbb{Z}),$$

$$A_{44} = \begin{pmatrix} g_7' & & & \\ 1 & g_7' + 1 & & \\ \vdots & \ddots & \ddots & \\ 1 & \dots & 1 & g_7' + g_7 - 1 \end{pmatrix} \in \mathrm{Mat}_{g_7}(\mathbb{Z}),$$

here and subsequently, we write $g = g_1 + g_3 + g_5 + g_7$ and $g_7' = g - g_7$.

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

Since n is odd, we only need to consider the Monsky matrix M_o defined by formula (2.1). By interchanging rows k and $g+k$ for all $1 \leq k \leq g$ in M_o, it is easy to see that

$$M_o \sim \left(\begin{array}{cccc|cccc} \mathbf{0}_{g_1} & & & & A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{1} \\ & I_{g_3} & & & \mathbf{1} & A_{22} & \mathbf{1} & \mathbf{0} \\ & & I_{g_5} & & \mathbf{1} & \mathbf{1} & A_{33}+I_{g_5} & \mathbf{1} \\ & & & \mathbf{0}_{g_7} & \mathbf{1} & \mathbf{1} & \mathbf{1} & A_{44}+I_{g_7} \\ \hline A_{11} & \mathbf{1} & \mathbf{1} & \mathbf{1} & \mathbf{0}_{g_1} & & & \\ \mathbf{1} & A_{22}+I_{g_3} & \mathbf{1} & \mathbf{0} & & I_{g_5} & & \\ \mathbf{1} & \mathbf{1} & A_{33}+I_{g_5} & \mathbf{1} & & & I_{g_5} & \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & A_{44} & & & & \mathbf{0}_{g_7} \end{array}\right)$$

$$\in \mathrm{Mat}_{2g}(\mathbb{Z}). \tag{4.32}$$

Note that $g_1 \geq 1$, $g_7 \geq 1$ and $g_7' + g_7 = g$. By considering rows $g+1$ and $2g$, we get $g \equiv 1 \pmod 2$, otherwise these two rows are equal when modulo 2. Furthermore, since $g \equiv 1 \pmod 2$ implies $g_7' + g_7 - 1 \equiv 0 \pmod 2$, we have $g_7 = 1$, otherwise rows $2g$ and $2g-1$ are equal when modulo 2. And then $g_7' = g_1 + g_3 + g_5 \equiv 0 \pmod 2$ holds.

We now perform more elementary row and column operations on the right-hand matrix in Eq. (4.32). First, we add row g to rows between row one and row $g_1+g_3+g_5$; and add row $2g$ to rows between row $g+1$ and row $g+g_1+g_3+g_5$, respectively. Second, add all columns between column one and column g_1 to column g; and add all columns between column $g+g_1+g_3+1$ and column $g+g_1+g_3+g_5$ to column g, respectively. Finally, add column $2g$ to columns between column $g+g_1+1$ to column $g+g_1+g_3$, respectively. Then we get

$$M_o \sim \left(\begin{array}{cccc|cccc} \mathbf{0}_{g_1} & & & & I_{g_1} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ & I_{g_3} & & & \mathbf{0} & A_{22} & \mathbf{0} & \mathbf{1} \\ & & I_{g_5} & & \mathbf{0} & \mathbf{0} & \mathbf{0}_{g_5} & \mathbf{0} \\ & & & g_5 & \mathbf{1} & \mathbf{0} & \mathbf{1} & 1 \\ \hline I_{g_1} & \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{0}_{g_1} & & & \\ \mathbf{0} & A_{22}^t & \mathbf{0} & \mathbf{0} & & I_{g_5} & & \\ \mathbf{0} & \mathbf{0} & \mathbf{0}_{g_5} & \mathbf{0} & & & I_{g_5} & \\ \mathbf{1} & \mathbf{1} & \mathbf{1} & g_1 & & & & \mathbf{0}_{g_7} \end{array}\right) \in \mathrm{Mat}_{2g}(\mathbb{Z}).$$

According to [7, Proposition 3.6, Chap. VII], we have

$$\det(M_o) \equiv \det \left(\begin{array}{c|c|c|c} I_{g_3} & & A_{22} & \mathbf{1} \\ \hline & g_5 & \mathbf{0} & 1 \\ \hline A_{22}^t & \mathbf{0} & I_{g_3} & \\ \hline \mathbf{1} & g_1 & & 0 \end{array}\right) \pmod 2. \tag{4.33}$$

We denote the right-hand matrix in (4.33) by $\left(\begin{smallmatrix} I_{g_3} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{smallmatrix}\right)$. Then Proposition 3.1 implies that

$$\det(M_o) \equiv \det(\alpha_{22} - \alpha_{21}\alpha_{12}) \pmod 2.$$

By using block matrix multiplication and noting that $g_7' + 1 \equiv 1 \pmod 2$, it is easy to compute that

$$\alpha_{21}\alpha_{12} \equiv \left(\begin{array}{c:c:c} 0 & \mathbf{0} & 0 \\ \hdashline \mathbf{0} & \mathbf{1}_{g_3} & \mathbf{1} \\ \hdashline 0 & \mathbf{1} & g_3 \end{array}\right) \pmod 2,$$

and

$$\alpha_{22} - \alpha_{21}\alpha_{12} \equiv \left(\begin{array}{c:c:c} g_5 & \mathbf{0} & 1 \\ \hdashline \mathbf{0} & I_{g_3} + \mathbf{1}_{g_3} & \mathbf{1} \\ \hdashline g_1 & \mathbf{1} & g_3 \end{array}\right) \pmod 2. \tag{4.34}$$

Now we still perform elementary row operations on the right-hand matrix in Eq. (4.34). First, we add the last row to rows between row 2 and row $g_3 + 1$ respectively, then the central block becomes I_{g_3}. Second, we add all rows between row 2 and row $g_3 + 1$ to the last row. And then apply [7, Proposition 3.6, Chap. VII] to the resulting matrix, we get

$$\det(M_o) \equiv \det \begin{pmatrix} g_5 & 1 \\ \mu & \nu \end{pmatrix} \pmod 2,$$

where $\mu = g_1(g_3 + 1)$ and $\nu = g_3 + g_3(g_3 + 1) \equiv g_3 \pmod 2$. Then it is easy to compute that $\det(M_o) \equiv g_1 + g_1 g_3 + g_3 g_5 \pmod 2$. By discussing the parity of g_1, g_3 and g_5, we see that $\det(M_e) \equiv 1 \pmod 2$ if and only if $g_1 \equiv 0 \pmod 2$ and $g_3 \equiv g_5 \equiv 1 \pmod 2$, or $g_1 \equiv g_5 \equiv 1 \pmod 2$ and $g_3 \equiv 0 \pmod 2$.

Remark 4.6. A similar discussion shows that if n is defined by $(*)$ and $\epsilon = 2$, then $\det(M_e) \equiv 0 \pmod 2$ always holds.

Acknowledgments

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

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

References

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

Int. J. Number Theory Downloaded from www.worldscientific.com by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.

[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] K. Feng and Y. Xue, Constructing new non-congruent numbers by graph theory, in *Number Theory*, Series on Number Theory and its Applications, Vol. 2 (World Scientific, Hackensack, NJ, 2007), pp. 24–38.
[5] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, *Invent. Math.* **111**(1) (1993) 171–195.
[6] D. R. Heath-Brown, The size of Selmer groups for the congruent number problem, II, *Invent. Math.* **118**(2) (1994) 331–370, with an appendix by P. Monsky.
[7] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics, Vol. 73 (Springer, New York, 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**(7) (1996) 168–169.
[9] A. W. Knapp, *Elliptic Curves*, Mathematical Notes, Vol. 40 (Princeton University Press, Princeton, NJ, 1992).
[10] 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.
[11] C. Meyer, *Matrix Analysis and Applied Linear Algebra* (Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2000), With 1 CD-ROM (Windows, Macintosh and UNIX) and a solutions manual, iv+171 pp.
[12] Y. Ouyang and S. Zhang, On non-congruent numbers with 1 modulo 4 prime factors, *Sci. China Math.* **57**(3) (2014) 649–658.
[13] Y. Ouyang and S. Zhang, On second 2-descent and non-congruent numbers, *Acta Arith.* **170**(4) (2015) 343–360.
[14] 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.
[15] L. Reinholz, B. K. Spearman and Q. Yang, On the prime factors of non-congruent numbers, *Colloq. Math.* **138**(2) (2015) 271–282.
[16] P. Serf, Congruent numbers and elliptic curves, in *Computational Number Theory* (de Gruyter, Berlin, 1991), pp. 227–238.
[17] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn., Graduate Texts in Mathematics, Vol. 106 (Springer, Dordrecht, 2009).
[18] Y. Tian, X. Yuan and S.-W. Zhang, Genus periods, genus points and congruent number problem, *Asian J. Math.* **21**(4) (2017) 721–773.
[19] Z. Wang, Congruent elliptic curves with nontrivial Shafarevich–Tate groups, *Sci. China Math.* **59**(11) (2016) 2145–2166.

Int. J. Number Theory Downloaded from www.worldscientific.com
by NANJING UNIVERSITY on 11/25/18. Re-use and distribution is strictly not permitted, except for Open Access articles.