FAMILIES OF NON-CONGRUENT NUMBERS WITH ARBITRARILY MANY PAIRS OF PRIME FACTORS

Shamik Das [1]
Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati, Assam, India
shamikdas@iitg.ac.in

Anupam Saikia[2]
Department of Mathematics, Indian Institute of Technology Guwahati, Guwahati, Assam, India
a.saikia@iitg.ac.in

Received: 10/30/19, Accepted: 6/23/20, Published: 7/24/20

Abstract

In this article we show the existence of infinitely many new families, each containing infinitely many non-congruent numbers. These non-congruent numbers are obtained as products of an arbitrary number of pairs of primes (p_j, q_j), all of which are equivalent either to $(1, 3)$ or to $(5, 7)$ modulo 8.

1. Introduction

A natural number n is called a congruent number if it is the area of a right triangle with rational lengths. Equivalently, n is a non-congruent number if the elliptic curve

$$E_n : y^2 = x^3 - n^2 x \tag{1}$$

has Mordell-Weil rank 0, i.e., Equation (1) has no rational solution other than the four 2-torsion points $(0, 0)$, $(\pm n, 0)$ and the point $\mathcal{O}$ at infinity on E_n. The elliptic curve E_n is referred to as the *congruent number elliptic curve*. Without loss of generality, we shall restrict our attention to square-free natural numbers n throughout this article. To determine all congruent and non-congruent numbers is one of the long-standing problems in number theory. The Birch and Swinnerton-Dyer Conjecture for a rational elliptic curve predicts that a square-free natural number n is congruent if $n \equiv 5$, 6 or 7 (mod 8). Tunnel [9], Monsky [4] and Tian [8]

[1]The first author has been supported by Senior Research Fellowship from IIT Guwahati.
[2]The second author has been supported by Professional Development Allowance from IIT Guwahati.

are some of the eminent mathematicians who have made significant contributions toward identifying congruent numbers. For the known results on the construction of non-congruent numbers with arbitrarily many prime factors of the form $8k+3$, one can refer to [2] and [5] for instance.

In [3], Lagrange proved that a composite number of the form pq must be non-congruent when p and q are primes with $\left(\frac{p}{q}\right) = -1$ and $(p,q) \equiv (1,3)$ or $(5,7) \pmod 8$. Serf ([6]) proved that a composite number of the form $(p_1q_1)(p_2q_2)$ must be non-congruent where the prime factors $p_1, p_2 \equiv 5 \pmod 8$ and $q_1, q_2 \equiv 7 \pmod 8$ with certain conditions on the associated Legendre symbols. In this article we show the existence of infinitely many new families of composite non-congruent numbers, obtained as products of arbitrary numbers of pairs of primes (p_j, q_j), all of which are equivalent either to $(1,3)$ or to $(5,7)$ modulo 8. The main result of this article can be stated as follows.

Theorem 1. *Let t be a positive integer. Suppose p_1, p_2, ..., p_t and q_1, q_2, ..., q_t are distinct primes such that all pairs (p_j, q_j) are equivalent either to $(1,3)$ or to $(5,7)$ modulo 8. Suppose*

$$\begin{aligned} &\left(\frac{q_j}{q_i}\right) = -1 \quad \text{if } i > j, \qquad \left(\frac{p_i}{p_j}\right) = 1 \quad \text{if } i \neq j, \quad \text{and} \\ &\left(\frac{p_i}{q_j}\right) = \begin{cases} 1 & \text{if } i \neq j \\ -1 & \text{if } i = j, \end{cases} \end{aligned} \tag{2}$$

where $\left(\frac{\cdot}{\cdot}\right)$ denotes the Legendre symbol. Then

$$n = (p_1q_1)(p_2q_2)\cdots(p_tq_t)$$

is a non-congruent number.

The following theorem guarantees that for each positive integer t, we do have infinitely many pairs of primes $(p_1, q_1), \ldots, (p_t, q_t)$ satisfying the conditions of Theorem 1.

Theorem 2. *Let H_t denote the collection of positive integers with prime factorization $(p_1q_1)(p_2q_2)\cdots(p_tq_t)$, where all the pairs (p_j, q_j) are equivalent to $(1,3)$ modulo 8 and satisfy the conditions (2). For any natural number t, the set H_t contains infinitely many elements. The analogous statement for pairs $(p_j, q_j) \equiv (5,7)$ (mod 8) holds as well.*

The method of complete 2-descent is a convenient tool in computing Mordell-Weil rank of an elliptic curve (see [8]). In Section 2, we briefly discuss how 2-descent leads to an 'unsolvability condition' for ruling out existence of non-torsion rational points on E_n (see Corollary 1). In Section 3, we show that the unsolvability condition holds for composite numbers of the form given in Theorem 1. Finally, we show in Section

4 that Theorem 1 provides infinitely many families, each containing infinitely many non-congruent numbers. We furnish a few examples of non-congruent numbers to illustrate our results.

2. An Unsolvability Condition

In this section we first recall the key aspects of the method of complete 2-descent that we need. Then we state an 'unsolvability condition' for the Mordell-Weil group $E_n(\mathbb{Q})$ to have rank zero, which rules out additional rational points on E_n. The method of 2-descent is an algorithm used for computing the rank of an elliptic curve. For elliptic curves given by the general Weierstrass equation $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in K$, where K is a number field, the process involved in carrying out the method of complete 2-decent is described in Proposition 1.4 on page 315 of [7]. For curves of the form, $y^2 = x(x^2 - n^2)$ the procedure can be summarized by the following proposition (see [6]).

Proposition 1 (Complete 2-Descent). *Let*

$$n = 2^{\epsilon} r_1 r_2 \cdots r_k$$

be a square-free positive integer where $\epsilon \in \{0, 1\}$, k is a natural number, and r_1, r_2, ..., r_k are odd primes. Let E_n be the elliptic curve over $\mathbb{Q}$ defined by

$$E_n : y^2 = x(x-n)(x+n),$$

and

$$S = \{\infty,\ 2,\ r_1,\ r_2,\ \ldots,\ r_k\}$$

be a finite subset of $M_{\mathbb{Q}}$, the set of all places of $\mathbb{Q}$. In addition, define

$$\mathbb{Q}(S,2) := \{c \in \mathbb{Q}^*/\left(\mathbb{Q}^*\right)^2 \ \mid\ \nu_p(c) \equiv 0 \pmod 2 \quad \forall\, p \in M_{\mathbb{Q}} \setminus S\},$$

where $\nu_p(c)$ is the p-adic valuation of c. Then there exists an injective homomorphism

$$b : E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \longhookrightarrow \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \tag{3}$$

defined by

$$P = (x,y) \longmapsto \begin{cases} (1,1), & \text{if } P = \mathcal{O} \\ (-1,-n), & \text{if } P = (0,0) \\ (n,2), & \text{if } P = (n,0) \\ (x, x-n), & \text{if } P \neq \mathcal{O}, (0,0), (n,0). \end{cases}$$

If $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \setminus Im\{\mathcal{O}, (0,0), (\pm n, 0)\}$, then $(b_1, b_2) \in Im(b)$ if and only if there exist $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ such that the following two equations simultaneously hold:

$$b_1 z_1^2 - b_2 z_2^2 = n, \tag{4}$$

$$b_1 z_1^2 - b_1 b_2 z_3^2 = -n. \tag{5}$$

In this case, $(b_1, b_2) = b(P)$ *for* $P = (b_1 z_1^2, b_1 b_2 z_1 z_2 z_3)$.

Remark 1. A system of representatives of classes in $\mathbb{Q}(S, 2)$ is given by

$$R = \{(-1)^\alpha 2^\beta r_1^{\epsilon_1} \cdots r_k^{\epsilon_k} \mid \quad \alpha,\ \beta,\ \epsilon_1,\ \ldots,\ \epsilon_k = 0 \text{ or } 1\}.$$

Let r be the rank of the Mordell-weil group $E_n(\mathbb{Q})$ of rational points on the elliptic curve E_n. Then $E_n(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}^r$, and consequently,

$$E_n(\mathbb{Q})/2E_n(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{r+2}.$$

For n to be a non-congruent number, we require that $r = 0$. In other words, we need to show that the system of equations given by (4) and (5) does not have a solution for any pair

$$(b_1, b_2) \in R \times R \setminus \{(1, 1),\ (-1, -n),\ (n, 2),\ (-n, -2n)\}. \tag{6}$$

The following proposition rules out simultaneous solutions of Equations (4) and (5) in certain cases (see [6]).

Proposition 2 (Unsolvability Condition). *Let*

$$n = 2^\epsilon r_1 r_2 \cdots r_k$$

be a square-free positive integer where $\epsilon \in \{0, 1\}$, k *is a natural number, and* r_1, r_2, *...,* r_k *are odd primes. Let* $(b_1, b_2) \in R \times R$, *where* R *is as defined in Remark 1. The system of equations given by (4) and (5) has no solution* $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ *in the following cases:*

(a) $b_1 b_2 < 0$ *or*

(b) $2 \nmid n$ *and* $2 \mid b_1$.

It is convenient for us to express the unsolvability condition in terms of integral solutions rather than rational solutions as follows.

Lemma 1. *Let* $(z_1, z_2, z_3) \in (\mathbb{Q}^*)^3$ *be a solution to Equations (4) and (5). Then there exist a positive integer* d *and pairwise coprime integers* a_1, a_2 *and* a_3 *such that*

$$z_1 = \frac{a_1}{d}, \quad z_2 = \frac{a_2}{d}, \quad z_3 = \frac{a_3}{d}, \quad \text{and } (a_i, d) = 1.$$

Proof. We write $z_i = \frac{a_i}{d_i}$ for $i = 1, 2, 3$ as fractions in irreducible form with $d_i > 0$. After clearing denominators, Equation (4) becomes

$$b_1 a_1^2 d_2^2 - b_2 a_2^2 d_1^2 = n d_1^2 d_2^2. \tag{7}$$

By simple inspection, we can say that $d_1^2|b_1d_2^2$ and $d_2^2|b_2d_1^2$. Since b_1 and b_2 are square-free, we must have $d_1|d_2$ and $d_2|d_1$, hence $d_1 = d_2$. We set $d := d_1 = d_2$. Now, after clearing denominators, Equation (5) becomes

$$b_1a_1^2d_3^2 - b_1b_2a_3^2d^2 = -nd^2d_3^2. \tag{8}$$

It is easy to see $d^2|b_1d_3^2$ and since b_1 is square-free, $d|d_3$. Thus we write $d_3 = md$. By dividing both sides by d^2 in Equation (8), we get

$$b_1a_1^2m^2 - b_1b_2a_3^2 = -nd^2m^2. \tag{9}$$

Equation (9) gives us $m^2|b_1b_2$, and since b_1 and b_2 are square-free, we have $m|b_1$ and $m|b_2$, and m is also square-free. Our target is to show $m = 1$. It can be shown that $(m, nd) = 1$. Suppose p is a prime dividing (m, nd), then $\nu_p(b_1a_1^2m^2) \geq 3$ and $\nu_p(b_1b_2a_3^2) = 2$ but $\nu_p(nm^2d^2) \geq 3$, a contradiction to Equation (8). Now since $b_i \equiv 0 \pmod{m}$ for $i = 1, 2$, from Equation (7) we get $m = 1$, hence $d_3 = d$.

Now, we can rewrite (4) and (5) as

$$b_1a_1^2 - b_2a_2^2 = nd^2, \tag{10}$$

$$b_1a_1^2 - b_1b_2a_3^2 = -nd^2. \tag{11}$$

By taking the sum and the difference of the pair of equations above, we further obtain

$$2b_1a_1^2 - b_2a_2^2 - b_1b_2a_3^2 = 0, \tag{12}$$

$$b_2a_2^2 - b_1b_2a_3^2 = -2nd^2. \tag{13}$$

Since n is square-free and $(a_i, d) = 1$ for $i = 1,\ 2,\ 3$, we can easily deduce from above that $(a_1, a_2) = (a_1, a_3) = (a_2, a_3) = 1$. □

Corollary 1. *If $(b_1, b_2) \in \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2) \setminus Im\{\mathcal{O}, (0, 0), (\pm n, 0)\}$ then $(b_1, b_2) \in Im(b)$ if and only if there exist pairwise coprime integers a_1, a_2, a_3 and d satisfying the system of equations (10) and (11), or equivalently, (12) and (13).*

3. Proof of Theorem 1

In order to prove that $n = (p_1q_1)(p_2q_2)\cdots(p_tq_t)$ is a non-congruent number as stated in Theorem 1, we need to use the Legendre symbols listed as follows.

Remark 2. (*a*) Suppose $n = n_j'q_j = n_j''p_j$ for all $j \in \{1,\ 2,\ \ldots,\ t\}$. Then

$$\left(\frac{n_j'}{q_j}\right) = (-1)^j, \quad \text{and } \left(\frac{n_j''}{p_j}\right) = -1. \tag{14}$$

Moreover,

$$\left(\frac{q_j}{q_i}\right) = -1 \quad \text{for } i > j \text{ implies } \left(\frac{q_j}{q_i}\right) = 1 \quad \text{for } j > i. \tag{15}$$

(b) When all the prime pairs in the factorization of n in Theorem 1 satisfy $(p_j, q_j) \equiv (5, 7) \pmod 8$, we have

$$\left(\frac{-1}{p_j}\right) = -\left(\frac{2}{p_j}\right) = 1, \qquad \left(\frac{-1}{q_j}\right) = -\left(\frac{2}{q_j}\right) = -1. \tag{16}$$

(c) When all the prime pairs in the factorization of n in Theorem 1 satisfy $(p_j, q_j) \equiv (1, 3) \pmod 8$, we have

$$\left(\frac{-1}{p_j}\right) = \left(\frac{2}{p_j}\right) = 1, \qquad \left(\frac{-1}{q_j}\right) = \left(\frac{2}{q_j}\right) = -1. \tag{17}$$

By Corollary 1, it suffices to show that the system of equations (10) and (11) or equivalently, (12) and (13), cannot simultaneously be solved for any pair

$$\begin{aligned} &(b_1, b_2) \in D := R \times R \ \setminus \ \{(1,1), (-1,-n), (n,2), (-n,-2n)\}, \\ &\text{with } R = \{\pm 2^{\epsilon} p_1^{\epsilon_1} \dots p_t^{\epsilon_t} q_1^{\mu_1} \cdots q_t^{\mu_t} \mid \epsilon, \epsilon_1, \dots, \epsilon_t, \mu_1, \dots, \mu_t \in \{0,1\}\}. \end{aligned} \tag{18}$$

By Proposition 2, we know that the equivalent system of equations (4) and (5) do not have a solution when $b_1 b_2 < 0$, or when $2 \nmid n$ and $2 | b_1$. Therefore, we only need to consider pairs (b_1, b_2) for which $b_1 b_2 > 0$ and $2 \nmid b_1$. The following lemma shows that it is enough to consider pairs (b_1, b_2) for which b_2 is positive and odd.

Lemma 2. *Let $(b_1, b_2) \in D$ represent an element in the image of the map b given by (3). Then, there is a pair (b_1^*, b_2^*) in D representing an element in $Im(b)$ such that b_2^* is positive and odd.*

Proof. Let us first assume that b_2 is positive and even. Then the set of points

$$L = \{(1,1), (-1,-n), (n,2), (-n,-2n), (b_1, b_2)\}$$

generates a subgroup of $Im(b)$ inside $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$. By closure, the pair

$$(b_1, b_2) \cdot (n, 2) = (nb_1, 2b_2) \in Im(b).$$

By our assumption $2 | b_2$, hence we can write $2b_2 = 2^2 b_2^*$, where $b_2^* \in \mathbb{Q}/\left(\mathbb{Q}^*\right)^2$ and $2 \nmid b_2^*$. If we set $b_1^* = nb_1$, then we have

$$(nb_1, 2b_2) = (b_1^*, b_2^*) \in Im(b) \subset \mathbb{Q}(S,2) \times \mathbb{Q}(S,2),$$

where b_2^* is odd.

Next, let us assume that b_2 is negative and odd. As before, we have

$$(b_1, b_2) \cdot (-n, -2n) = (-nb_1, -2b_2n) = (b_1^*, b_2^*) \in Im(b),$$

where $b_2^* = -2b_2n$ is positive and even. But it leads us to the previous case.

Finally, let b_2 be negative and even. Then the pair

$$(b_1, b_2) \cdot (-n, -2n) = (-b_1n, -2b_2n) \in Im(b)$$

as well. Equivalently, the pair

$$(b_1^*, b_2^*) \in Im(b) \subset \mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2),$$

where $b_1^* = -b_1n$, $-2b_2n = 2^2b_2^*$ with b_2^* as positive and odd. □

By Corollary 1, (18) and Lemma 2, it now suffices to show that for a pair (b_1, b_2) in D with b_2 positive and odd, the system of equations (10), (11) has a solution only when $(b_1, b_2) = (1, 1)$. Since b_1, b_2 are factors of n, we next show that none of the q_j divides b_1b_2 in Lemma 3 and that none of the p_j divides b_1b_2 in Lemma 4. We extend the argument employed by Iskra in [2] that dealt with the case when n has all its prime factors in the form $8k + 3$.

Lemma 3. *Let (b_1, b_2) be an element of $R \times R$ such that b_2 is odd and positive. If $(b_1, b_2) \in Im(b)$, then q_j does not divide b_1b_2 for $j = 1,\ 2,\ \cdots, t$.*

Proof. We provide the argument when all pairs $(p_j, q_j) \equiv (5, 7) \pmod 8$. The proof is similar when all pairs $(p_j, q_j) \equiv (1, 3) \pmod 8$. Define

$$U = \{j : q_j | b_1 \text{ or } q_j | b_2\}.$$

It is enough to show that U is the empty set. Suppose otherwise, and let u be the least element of U. Let

$$b_i' = \begin{cases} \frac{b_i}{q_u}, & \text{if } q_u | b_i \\ b_i, & \text{if } q_u \nmid b_i \end{cases} \quad \text{and} \quad b_i'' = \begin{cases} \frac{b_i}{p_u}, & \text{if } p_u | b_i \\ b_i, & \text{if } p_u \nmid b_i \end{cases} \quad i = 1 \text{ or } 2.$$

By Remark 2,

$$\left(\frac{b_i'}{q_u}\right) = \begin{cases} -1, & \text{if } p_u | b_i \\ 1, & \text{if } p_u \nmid b_i, \end{cases} \quad \text{for } i = 1,\ 2. \tag{19}$$

According to the definition of u, q_u divides both b_1 and b_2 or exactly one of them. We consider these three cases separately.

`Case 1:` $q_u | b_1$ and $q_u | b_2$. We have the following possibilities.

`Subcase I:` $p_u \nmid b_1$ and $p_u \nmid b_2$. From Equation (11) we obtain $b_1a_1^2 - b_1b_2a_3^2 \equiv 0 \pmod{p_u}$, i.e.,

$$a_1^2 \equiv b_2a_3^2 \pmod{p_u}.$$

As $(a_1, a_3) = 1$, we have $\left(\frac{b_2}{p_u}\right) = 1$. But it is not possible, since q_u is a divisor of b_2.

`Subcase II:` $p_u \mid b_1$ and $p_u \mid b_2$. Dividing both side of Equation (13) by p_u, we obtain $b_2'' a_2^2 - b_1 b_2'' a_3^2 = -2n_u'' d^2$, i.e.,

$$b_2'' a_2^2 \equiv -2n_u'' d^2 \pmod{p_u}.$$

Since $(a_2, d) = 1$, we have $\left(\frac{-2n_u'' b_2''}{p_u}\right) = 1$. Consequently, $\left(\frac{b_2''}{p_u}\right) = 1$. It is not possible, since q_u is a divisor of b_2''.

`Subcase III:` $p_u | b_1$ but $p_u \nmid b_2$. In this case,

$$\left(\frac{b_2'}{q_u}\right) = -\left(\frac{b_1'}{q_u}\right) = 1.$$

Dividing both sides of Equation (11) by q_u, we obtain $b_1' a_1^2 - b_1' b_2 a_3^2 = -n_u' d^2$. Hence,

$$b_1' a_1^2 \equiv -n_u' d^2 \pmod{q_u}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_u' b_1'}{q_u}\right) = \left(\frac{-1}{q_u}\right)\left(\frac{n_u'}{q_u}\right)\left(\frac{b_1'}{q_u}\right) = 1$. It follows that

$$\left(\frac{n_u'}{q_u}\right) = 1. \tag{20}$$

On the other hand, division of both sides of (13) by q_u yields $b_2' a_2^2 - b_1 b_2' a_3^2 = -2n_u' d^2$. Hence,

$$b_2' a_2^2 \equiv -2n_u' d^2 \pmod{q_u}.$$

As $(a_2, d) = 1$, we have $\left(\frac{-2n_u' b_2'}{q_u}\right) = \left(\frac{-1}{q_u}\right)\left(\frac{2}{q_u}\right)\left(\frac{b_2'}{q_u}\right)\left(\frac{n_u'}{q_u}\right) = 1$. It follows that $\left(\frac{n_u'}{q_u}\right) = -1$, which contradicts (20).

`Subcase IV:` $p_u \nmid b_1$ and $p_u | b_2$. This case can be ruled out in a similar way as above.

`Case 2:` $q_u | b_1$ and $q_u \nmid b_2$. As before, we consider the following subcases.

`Subcase I:` $p_u \nmid b_1$ and $p_u \nmid b_2$. From Equation (10) we have

$$b_1 a_1^2 \equiv b_2 a_2^2 \pmod{p_u}.$$

Since $(a_1, a_2) = 1$, we have $\left(\frac{b_1 b_2}{p_u}\right) = 1$, which is impossible, since $q_u | b_1$ but not b_2.

`Subcase II:` $p_u | b_1$ and $p_u \mid b_2$. Equation (10) gives us $b_2 a_2^2 \equiv 0 \pmod{q_u}$. It follows that a_2 is divisible by q_u, and $\frac{a_2^2}{q_u}$ is divisible by q_u. Dividing both sides of Equation (12) by q_u, we obtain $2b_1' a_1^2 - b_2 \frac{a_2^2}{q_u} - b_1' b_2 a_3^2 = 0$ and consequently,

$$2a_1^2 \equiv b_2 a_3^2 \pmod{q_u}.$$

Now, $(a_1, a_3) = 1$ implies $\left(\frac{2b_2}{q_u}\right) = 1$, which is a contradiction since p_u divides b_2.

Subcase III: $p_u|b_1$ and $p_u \nmid b_2$. Equation (10) gives us a_2 is divisible by p_u. Now dividing both sides of Equation (13) by p_u, we obtain $b_2\frac{a_2^2}{p_u} - b_1''b_2a_3^2 = -2n_u''d^2$, i.e.,

$$b_1''b_2a_3^2 \equiv 2n_u''d^2 \pmod{p_u}. \tag{21}$$

Since $(a_3, d) = 1$, it follows that $\left(\frac{2n_u''b_1''b_2}{p_u}\right) = 1$. But

$$\left(\frac{2n_u''b_1''b_2}{p_u}\right) = \left(\frac{2}{p_u}\right)\left(\frac{n_u''}{p_u}\right)\left(\frac{b_1''}{p_u}\right)\left(\frac{b_2}{p_u}\right) = (-1)\cdot(-1)\cdot(-1)\cdot 1 = -1,$$

a contradiction to (21).

Subcase IV: $p_u \nmid b_1$ and $p_u \mid b_2$. The argument is similar to the previous one.

Case 3: $q_u \nmid b_1$ and $q_u \mid b_2$. We consider following subcases.

Subcase I: $p_u \nmid b_1$. Equation (10) gives us $b_1a_1^2 \equiv 0 \pmod{q_u}$. It follows that a_1 is divisible by q_u, and $\frac{a_1^2}{q_u}$ is divisible by q_u. Dividing both sides of Equation (12) by q_u, we obtain $2b_1\frac{a_1^2}{q_u} - b_2'a_2^2 - b_1b_2'a_3^2 = 0$ and consequently,

$$a_2^2 \equiv -b_1a_3^2 \pmod{q_u}.$$

Now, $(a_2, a_3) = 1$ implies $\left(\frac{-b_1}{q_u}\right) = 1$, which is a contradiction because p_u does not divide b_1.

Subcase II: $p_u \mid b_1$ and $p_u \mid b_2$. From Equation (11) we have

$$b_1''a_1^2 \equiv -n_u''d^2 \pmod{p_u}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_u''b_1''}{p_u}\right) = 1$, which is impossible since $q_u \nmid b_1$.

Subcase III: $p_u|b_1$ and $p_u \nmid b_2$. Equation (10) gives us a_2 is divisible by p_u. Dividing both sides of Equation (10) by p_u, we obtain $b_1''a_1^2 - b_2\frac{a_2^2}{p_u} = n_u''d^2$. Clearly,

$$b_1''a_1^2 \equiv n_u''d^2 \pmod{p_u}. \tag{22}$$

Since $(a_1, d) = 1$, $\left(\frac{n_u''b_1''}{p_u}\right) = 1$. But

$$\left(\frac{n_u''b_1''}{p_u}\right) = \left(\frac{n_u''}{p_u}\right)\left(\frac{b_1''}{p_u}\right) = (-1)\cdot 1 = -1,$$

a contradiction to (22).

Therefore, we can conclude that $u = \min U$ does not exist, i.e., U is empty. So, none of the prime factors q_j of n divides b_1b_2. □

Lemma 4. *Let (b_1, b_2) be an element of $R \times R$ such that b_2 is odd and positive. If $(b_1, b_2) \in Im(b)$, then p_j does not divide b_1b_2 for $j = 1, 2, \ldots, t$.*

Proof. We provide the argument when all prime pairs in the factorization of n satisfy $(p_j, q_j) \equiv (5, 7) \pmod 8$. The proof is similar when all pairs $(p_j, q_j) \equiv (1, 3) \pmod 8$. Let us define

$$V = \{j : p_j | b_1 \text{ or } p_j | b_2\}.$$

It suffices to show that V is empty. If possible, let V be non-empty and v be the least element of V. Let

$$b_{i,v} = \begin{cases} \frac{b_i}{p_v}, & \text{if } p_v | b_i \\ b_i, & \text{if } p_v \nmid b_i \end{cases} \qquad i = 1,\ 2.$$

Since $q_j \nmid b_1 b_2$, for all $j \in \{1, 2, \ldots t\}$, we have

$$\left(\frac{b_{1,v}}{p_v}\right) = \left(\frac{b_{2,v}}{p_v}\right) = 1.$$

We need to consider the following three cases.

`Case A:` $p_v | b_1$ and $p_v | b_2$. Dividing Equation (11) by p_v, we have $b_{1,v}a_1^2 - b_{1,v}b_2 a_3^2 = -n_v'' d^2$. Clearly,

$$b_{1,v}a_1^2 \equiv -n_v'' d^2 \pmod{p_v}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{-n_v'' b_{1,v}}{p_v}\right) = 1$. It follows that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (14).

`Case B:` $p_v | b_1$ and $p_v \nmid b_2$. From Equation (10) we have $a_2 \equiv 0 \pmod{p_v}$. Therefore, $b_{1,v}a_1^2 - b_2 \frac{a_2^2}{p_v} = n_v'' d^2$, and

$$b_{1,v}a_1^2 \equiv n_v'' d^2 \pmod{p_v}.$$

Since $(a_1, d) = 1$, we have $\left(\frac{n_v'' b_{1,v}}{p_v}\right) = 1$. It follows that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (14).

`Case C:` $p_v \nmid b_1$ and $p_v \mid b_2$. From Equation (10) we have $a_1 \equiv 0$ in modulo p_v. Therefore, $b_1 \frac{a_1^2}{p_v} - b_{2,v}a_2^2 = n_v'' d^2$ and

$$-b_{2,v}a_2^2 \equiv n_v'' d^2 \pmod{p_v}.$$

Since $(a_2, d) = 1$, we have $\left(\frac{-n_v'' b_{2,v}}{p_v}\right) = 1$. But it implies that $\left(\frac{n_v''}{p_v}\right) = 1$, a contradiction to (14). □

By Lemmas 3 and 4, we can conclude that if $(b_1, b_2) \in Im(b)$ with $b_1 b_2 > 0$ and b_2 odd as well as positive, then $b_2 = 1 = b_1$. Hence, Theorem 1 follows from Propositions 1 and 2, and Corollary 1.

4. Infinitude of the Families

In this section, we show that Theorem 1 provides infinitely many families of non-congruent numbers and each family has infinitely many members by proving Theorem 2.

Proof of Theorem 2. We use Dirichlet's theorem on primes in arithmetic progression and apply induction on t. The case when $t = 1$ is trivial, since we can take any $q_1 \equiv 3 \pmod 8$ and $p_1 \equiv 1 \pmod 8$, $p_1 \equiv 2 \pmod{q_1}$. Suppose $t > 1$. By the induction hypothesis, we know that there exists an integer $n_{t-1} = (p_1q_1)(p_2q_2)\cdots(p_{t-1}q_{t-1})$ where $p_1, p_2, \ldots, p_{t-1}$ and $q_1, q_2, \ldots, q_{t-1}$ are distinct primes such that $p_j \equiv 1 \pmod 8$ and $q_j \equiv 3 \pmod 8$ for all $1 \leq j \leq t-1$ satisfying (2).

It is enough if we can choose primes p_t and q_t satisfying

$$q_t \equiv \begin{cases} 3 & \pmod 8, \\ \alpha & \pmod{n_{t-1}}, \end{cases} \tag{23}$$

and

$$p_t \equiv \begin{cases} 1 & \pmod 8, \\ \beta & \pmod{n_{t-1}}, \\ \gamma & \pmod{q_t}, \end{cases} \tag{24}$$

where α, β is any quadratic residue modulo n_{t-1} and γ is any quadratic non-residue modulo q_t, e.g., $\alpha = 1 = \beta$, $\gamma = 2$. The Chinese Remainder Theorem guarantees that both the systems of congruences (23) and (24) have a solution. By applying this theorem in conjunction with Dirichlet's theorem on primes in arithmetic progression and quadratic reciprocity, we can conclude that there exist infinitely many primes p_t and q_t satisfying the system of congruences given by (24) and (23), respectively.

The analogous statement, when all the prime pairs (p_j, q_j) in the factorization of n are equivalent to $(5, 7)$ modulo 8, can be proved similarly. □

5. Examples

Example 1. Consider $n = (17 \cdot 3) \cdot (409 \cdot 19) \cdot (3697 \cdot 859)$, where each pair of prime factors is equivalent to $(1, 3)$ modulo 8 and satisfy the hypotheses (2) of Theorem 1. Using MAGMA [1], we verify that the rank of the elliptic curve $y^2 = x^3 - n^2x$ is 0, hence n is non-congruent. We further verify that $(17\cdot3)\cdot(409\cdot19)$, $(17\cdot3)\cdot(3697\cdot859)$ and $(409 \cdot 19) \cdot (3697 \cdot 859)$ are non-congruent too, as implied by Theorem 1.

Example 2. Consider $n = (5 \cdot 7) \cdot (29 \cdot 79) \cdot (821 \cdot 151)$ where each pair of prime factors is equivalent to $(5, 7)$ modulo 8 and satisfy the hypotheses (2) of Theorem 1. Using MAGMA [1], we verify that the rank of the elliptic curve $y^2 = x^3 - n^2x$ is 0,

hence n is non-congruent. We further verify that $(5 \cdot 7) \cdot (29 \cdot 79)$, $(5 \cdot 7) \cdot (821 \cdot 151)$ and $(29 \cdot 79) \cdot (821 \cdot 151)$ are non-congruent too, as implied by Theorem 1.

Acknowledgement. The authors would like to thank the anonymous referee for going through the manuscript very carefully and making helpful comments.

References

[1] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24**(3-4) (1997), 235–265.

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

[3] J. Lagrange, Nombres congruents et courbes elliptiques, in *Séminaire Delange-Pisot-Poitou (16e année: 1974/75), Théorie des Nombres, Fasc. 1,* **16**, 1975.

[4] P. Monsky, Mock Heegner points and congruent numbers, *Math. Z.* **204**(1) (1990), 45–67.

[5] L. Reinholz, B. K. Spearman, and Q. Yang, Families of even non-congruent numbers with prime factors in each odd congruence class modulo eight, *Int. J. Number Theory* **14**(3) (2018), 669–692.

[6] P. Serf, Congruent numbers and elliptic curves, in *Computational Number Theory (Debrecen, 1989)*, de Gruyter, Berlin, 1991.

[7] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer, Dordrecht, 2009.

[8] Y. Tian, Congruent numbers and Heegner points, *Camb. J. Math.* **2**(1) (2014), 117–161.

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