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

VINCENT GIRARD, MATILDE N. LALÍN, AND SIVASANKAR C. NAIR

ABSTRACT. The concept of θ-congruent numbers was introduced by Fujiwara [Fu97], who showed that for primes $p \equiv 5, 7, 19 \pmod{24}$, p is not a $\pi/3$-congruent number. In this paper we show the existence of two infinite families of composite non-$\pi/3$-congruent numbers and non-$2\pi/3$-congruent numbers, obtained from products of primes which are congruent to 5 modulo 24 and to 13 modulo 24 respectively. This is achieved by generalizing a result obtained by Serf [Se91] based on descent on certain elliptic curves, and by extending a method of Iskra [Is96] involving the classical (or $\pi/2$-) congruent numbers.

1. INTRODUCTION

A natural number is said to be a *congruent number* if it occurs as the area of a right triangle which has rational side lengths. The congruent number problem consists of deciding whether a given natural number n is congruent. It has been generalized in several directions (see the work of Top and Yui [TY08] for a survey on the topic). In particular, Fujiwara [Fu97] generalized the concept of congruent numbers to include triangles other than right triangles as well.

Definition 1.1 (θ-congruent number)**.** Let $0 < \theta < \pi$ be a real number such that $\cos(\theta)$ is rational, say, $\cos(\theta) = \dfrac{s}{r}$, where $s, r \in \mathbb{Z}$, $|s| \leq r$ and $\gcd(s, r) = 1$. A natural number n is said to be a θ-congruent number if $n\sqrt{r^2 - s^2}$ occurs as the area of a triangle with rational sides and containing the angle θ.

By means of the cosine theorem, n is θ-congruent if and only if there exist a, b, c rationals such that

$$\begin{cases} c^2 = a^2 + b^2 - 2ab(s/r), \\ 2nr = ab. \end{cases}$$

We remark that classical congruent numbers satisfy the definition above by chosing $\theta = \pi/2$. In this case, Nagel [Na29] proved, for example, that primes of the form $p \equiv 3 \pmod{8}$ are non-congruent while Monsky [Mo90], extending results of Heegner [He52], proved that primes of the form $p \equiv 5, 7 \pmod{8}$ are congruent. Similar results are known for products of a few prime factors such as $2p$, pq, etc, (see for instance the paper of Serf [Se91]).

If we consider the question of composite numbers with arbitrary many prime factors, we find the following result.

Theorem 1.2 (Iskra, [Is96])**.** *Let $p_1, \ldots, p_\ell$ be distinct primes such that $p_i \equiv 3 \pmod{8}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_\ell$ is a non-congruent number.*

Some generalizations and extensions of Iskra's result can be found in [RSY13, RSY15].

2010 *Mathematics Subject Classification.* Primary 11G05; Secondary 14H52.

Key words and phrases. θ-congruent numbers, non-congruent numbers, elliptic curves.

The complete characterization of congruent numbers was given by Tunnell [Tu83] (see also [Ko93] for many details) and it relies on the Birch and Swinnerton-Dyer conjecture.

After $\theta = \pi/2$, the next natural values to consider are $\theta = \pi/3, 2\pi/3$, since they are the only other $0 < \theta < \pi$ that are rational multiples of π and such that $\cos(\theta)$ is rational. In this realm, Fujiwara [Fu97] proved that a prime p is not $\pi/3$-congruent if $p \equiv 5, 7, 19 \pmod{24}$. In addition, Kan [Ka00] proved that a prime p is not $2\pi/3$-congruent if $p \equiv 7, 11, 13 \pmod{24}$ and further proved that the primes $p \equiv 23 \pmod{24}$ are $\pi/3$ and $2\pi/3$-congruent. In these cases, complete characterizations analogous to Tunnell's results were given conditionally on the Birch and Swinnerton-Dyer conjecture by Yoshida [Yo01, Yo02].

Our goal is to prove two results for products of arbitrarily many primes that are analogous to the result of Iskra [Is96].

Theorem 1.3. *Let $p_1, \ldots, p_{2\ell+1}$ be distinct primes such that $p_i \equiv 5 \pmod{24}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = p_1 \cdots p_{2\ell+1}$ is a non-$\pi/3$-congruent number.*

Theorem 1.4. *Let $p_1, \ldots, p_{2\ell}$ be distinct primes with $\ell > 0$ such that $p_i \equiv 13 \pmod{24}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$. Then the product $n = 2p_1 \cdots p_{2\ell}$ is a non-$2\pi/3$-congruent number.*

Our proofs are relatively elementary, building upon a generalization of the work of Serf [Se91] for classical congruent numbers. This generalization, stated in Theorem 2.6, is interesting in its own right due to its potential applications to other values of θ and families of composite numbers different from the ones considered in Theorems 1.3 and 1.4.

2. 2-descent on $E_{n,\theta}$

The classical congruent number problem has been related to a condition on the arithmetics of certain elliptic curves. The same is true for its generalization.

Proposition 2.1 (Fujiwara, [Fu97])**.** *Let n be a natural integer such that $n \neq 1, 2, 3, 6$. The following are equivalent.*

(1) n is θ-congruent.

(2) The elliptic curve $E_{n,\theta}$ given by:

$$E_{n,\theta}: \ y^2 = x\big(x - n(r-s)\big)\big(x + n(r+s)\big)$$

has positive rank over the rationals.

For $n \nmid 6$, the elliptic curve $E_{n,\theta}$ has torsion $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} = \{\mathcal{O}, (n(r-s), 0), (0, 0), (-n(r+s), 0)\}$. Fujiwara [Fu02] further investigated the cases of $n \mid 6$. Depending on certain conditions on r and s, the torsion in these cases may be $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\ell\mathbb{Z}$ with $\ell = 1, 2, 3, 4$, as predicted by Mazur's Theorem.

We will show that for some particular values of $n \nmid 6$ and θ, the rank of $E_{n,\theta}$ will always be 0 which implies, by Proposition 2.1, that n cannot be θ-congruent. We will need two statements, which are generalizations of theorems in Serf [Se91]. The first one corresponds to Theorem 3.1 in [Se91] and can be obtained with the help of Proposition 1.4, Chapter X in Silverman [Si86].

Before proceeding, we establish some notation. Let $M_{\mathbb{Q}}$ be the set of all places of $\mathbb{Q}$. For a finite place p, let v_p be the valuation defined by p.

Let $\Delta_{n,\theta}$ be the discriminant of $E_{n,\theta}$. Then

$$\Delta_{n,\theta} = 4^3 n^6 r^2 (r^2 - s^2)^2.$$

Theorem 2.2 (Complete 2-descent for $E_{n,\theta}$ over $\mathbb{Q}$ – Proposition 1.4, Chapter X in [Si86]). *Let n be a square-free natural number. Let $p_1, p_2, \ldots, p_k$ denote the odd primes that divide $\Delta_{n,\theta}$, and consider*

$$S = \{\infty, 2, p_1, p_2, \ldots, p_k\} \subset M_{\mathbb{Q}}.$$

Let

$$\mathbb{Q}(S,2) = \{a \in \mathbb{Q}^*/\mathbb{Q}^{*2} \mid v_p(a) \equiv 0 \pmod 2 \quad \forall p \in M_{\mathbb{Q}} \setminus S\}.$$

(1) There exists an injective homomorphism such that

$$\phi: E_{n,\theta}(\mathbb{Q})/2E_{n,\theta}(\mathbb{Q}) \hookrightarrow \quad \mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$$

$$P = (x,y) \mapsto \begin{cases} (x, x - n(r-s)) & \text{if } x \neq 0, n(r-s), \\ \left(\frac{r+s}{s-r}, -n(r-s)\right) & \text{if } x = 0, \\ \left(n(r-s), \frac{2r}{r-s}\right) & \text{if } x = n(r-s), \\ (1,1) & \text{if } x = \infty \text{ (i.e } P = \mathcal{O}). \end{cases}$$

(2) If $(b_1, b_2) \in \mathbb{Q}(S,2) \times \mathbb{Q}(S,2) \setminus \mathrm{Im}\{\mathcal{O}, (0,0), (n(r-s),0)\}$, then $(b_1,b_2) \in \mathrm{Im}(\phi)$ if and only if there exists a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$ to the system of equations

$$\begin{cases} b_1 z_1^2 - b_2 z_2^2 = n(r-s), \\ b_1 z_1^2 - b_1 b_2 z_3^2 = -n(r+s). \end{cases} \tag{2.1}$$

In this case, $(b_1, b_2) = \phi(P)$, where $P = (x,y) = (b_1 z_1^2, b_1 b_2 z_1 z_2 z_3)$.

As mentioned before, when $n \nmid 6$, the torsion subgroup of $E_{n,\theta}(\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. By the Mordell–Weil Theorem,

$$E_{n,\theta}(\mathbb{Q})/2E_{n,\theta}(\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^{\rho+2},$$

where ρ is the rank of $E_{n,\theta}(\mathbb{Q})$. Thus $\rho > 0$ iff there is an element $(b_1,b_2) \in \mathrm{Im}(\phi) \backslash \mathrm{Im}\{\mathcal{O}, (0,0), (n(r-s),0)\}$ iff the System (2.1) has a nontrivial solution in $\mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}$.

Remark 2.3. If we also exclude the image of $(-n(r+s), 0)$ (given by $(-n(r+s), -2nr)$) as a possibility for (b_1, b_2), we obtain that the rank of $E_{n,\theta}$ is strictly positive if and only if there exists a solution $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ to the system of equations (2.1).

Remark 2.4. By subtracting the first equation from the second equation in (2.1) we obtain

$$b_2 z_2^2 - b_1 b_2 z_3^2 = -2nr, \tag{2.2}$$

which must also be verified.

Remark 2.5. A system of representatives of classes in $\mathbb{Q}(S,2)$ is given by

$$R = \{(-1)^\alpha 2^\beta p_1^{\varepsilon_1} \cdots p_k^{\varepsilon_k} \mid \alpha, \beta, \varepsilon_1, \ldots, \varepsilon_k \in \{0,1\}\}.$$

The next statement in this section is a generalization of Theorem 3.3 in Serf [Se91] giving sufficient conditions for n not to be a θ-congruent number for arbitrary θ. Part of this result will be crucially used to prove Theorems 1.3 and 1.4. However, as remarked in the Introduction, this result is interesting on its own.

Theorem 2.6 (Unsolvability Conditions). *Let $n = p_1 p_2 \cdots p_\ell$, with $p_1, p_2, \ldots, p_\ell$ primes. For $p \in \{p_1, p_2 \ldots p_\ell\}$, denote $n' = n/p$, $b_1' = b_1/p$ (if $p \mid b_1$) and $b_2' = b_2/p$ (if $p \mid b_2$). Then the system of equations* (2.1) *has no solution (z_1, z_2, z_3) under the following conditions.*

General unsolvability condition.

I) If $b_1 b_2 < 0$.

Unsolvability conditions modulo 2.

II.1) If $2 \nmid n$, $2 \mid b_1$ *and* $2 \nmid (r+s)$.
II.1') If $2 \nmid n$, $(v_2(b_1), v_2(b_2)) = (0,1)$, $r \equiv 2 \pmod 4$, *and* $b_1 \equiv 1 \pmod 4$.

For II.2) we suppose that $2 \mid n$.

- *If* $(v_2(b_1), v_2(b_2)) = (0,0)$ *and any one of the following is satisfied*

II.2.a) $2 \nmid (r+s)$ *and* $b_1 \equiv 3 \pmod 4$,
II.2.a') $2 \mid r$ *and* $b_1 \not\equiv 1 \pmod 8$.

- *If* $(v_2(b_1), v_2(b_2)) = (0,1)$ *and any one of the following is satisfied*

II.2.b) $2 \nmid r$ *and* $b_1 \equiv 1 \pmod 4$,
II.2.b') $r \equiv 2 \pmod 4$ *and* $b_1 \not\equiv 5 \pmod 8$,
II.2.b") $4 \mid r$ *and* $b_1 \not\equiv 1 \pmod 8$.

- *If* $(v_2(b_1), v_2(b_2)) = (1,0)$ *and any one of the following is satisfied*

II.2.c) $2 \nmid (r+s)$ *and* $n' b_1' (r+s) \equiv 1 \pmod 4$,
II.2.c') $2 \mid r$ *and* $n' b_1' (r-s) \not\equiv 1 \pmod 8$.

- *If* $(v_2(b_1), v_2(b_2)) = (1,1)$ *and any one of the following is satisfied*

II.2.d) $2 \mid s$ *and* $n' b_1' (r+s) \equiv 3 \pmod 4$,
II.2.d') $2 \mid r$ *and* $n' b_1' (r+s) \not\equiv 7 \pmod 8$.

Unsolvability conditions modulo p **for** $p \in \{p_1, \dots, p_\ell\}$.

- *If* $(v_p(b_1), v_p(b_2)) = (0,0)$ *and any one of the following is satisfied*

III.a) $p \nmid r$ *and* $\left(\dfrac{b_1}{p}\right) = -1$,
III.a') $p \nmid (r+s)$ *and* $\left(\dfrac{b_2}{p}\right) = -1$,
III.a") $p \nmid (r-s)$ *and* $\left(\dfrac{b_1 b_2}{p}\right) = -1$.

- *If* $(v_p(b_1), v_p(b_2)) = (0,1)$ *and any one of the following is satisfied*

III.b) $p \mid r$ *and* $\left(\dfrac{b_1}{p}\right) = -1$,
III.b') $p \nmid (r+s)$ *and* $\left(\dfrac{n' b_1 b_2' (r+s)}{p}\right) = -1$,
III.b") $p \nmid (r-s)$ *and* $\left(\dfrac{-n' b_2' (r-s)}{p}\right) = -1$.

- *If* $(v_p(b_1), v_p(b_2)) = (1,0)$ *and any one of the following is satisfied*

III.c) $p \nmid r$ *and* $\left(\dfrac{2 n' b_1' b_2 r}{p}\right) = -1$,
III.c') $p \mid (r+s)$ *and* $\left(\dfrac{b_2}{p}\right) = -1$,
III.c") $p \nmid (r-s)$ *and* $\left(\dfrac{n' b_1' (r-s)}{p}\right) = -1$.

- *If* $(v_p(b_1), v_p(b_2)) = (1,1)$ *and any one of the following is satisfied*

III.d) $p \nmid r$ *and* $\left(\dfrac{-2 n' b_2' r}{p}\right) = -1$,

III.d') $p \nmid (r+s)$ and $\left(\dfrac{-n'b_1'(r+s)}{p}\right) = -1$,

III.d") $p \mid (r-s)$ and $\left(\dfrac{b_1'b_2'}{p}\right) = -1$.

Before proceeding with the proof of Theorem 2.6 we will prove some auxiliary results.

Lemma 2.7. *Let $(z_1, z_2, z_3) \in \mathbb{Q}^* \times \mathbb{Q}^* \times \mathbb{Q}^*$ be a solution to the system (2.1). Then there exist $a_1, a_2, a_3 \in \mathbb{Z}$ and m, d positive integers with*

$$z_1 = \frac{a_1}{d}, \quad z_2 = \frac{a_2}{d}, \quad z_3 = \frac{a_3}{md},$$

such that

$$(a_1, d) = (a_2, d) = (a_3, d) = (a_3, m) = (m, 2nr(r+s)d) = 1,$$
$$m \mid b_1, \quad m \mid b_2, \text{ and } m \mid (r-s).$$

Proof. Write $z_i = \frac{a_i}{d_i}$ for $i = 1, 2, 3$ as irreducible fractions with $d_i > 0$. After clearing denominators, the first equation in (2.1) becomes

$$b_1 a_1^2 d_2^2 - b_2 a_2^2 d_1^2 = n(r-s) d_1^2 d_2^2. \tag{2.3}$$

By simple inspection, we conclude that $d_1^2 \mid b_1 d_2^2$ and $d_2^2 \mid b_2 d_1^2$. Since b_1, b_2 are square-free, we must have $d_1 \mid d_2$ and $d_2 \mid d_1$ which implies $d_1 = d_2$. We set $d := d_1 = d_2$. We now look at the second equation in (2.1). After clearing denominators,

$$b_1 a_1^2 d_3^2 - b_1 b_2 a_3^2 d^2 = -n(r+s) d^2 d_3^2.$$

We then conclude that $d^2 \mid b_1 d_3^2$, and since b_1 is square-free, $d \mid d_3$. Thus we write $d_3 = md$. By dividing by d^2, we obtain

$$b_1 a_1^2 m^2 - b_1 b_2 a_3^2 = -n(r+s) d^2 m^2.$$

From this we conclude that $m^2 \mid b_1 b_2$ and since the b_i are square-free, $m \mid b_1$ and $m \mid b_2$. In particular m is square-free. Let p be a prime dividing $(m, n(r+s)d)$. Then $v_p(b_1 a_1^2 m^2) = 3$ and $v_p(b_1 b_2 a_3^2) = 2$, but $v_p(n(r+s)d^2m^2) \geq 3$, which leads to a contradiction. Therefore, $(m, n(r+s)d) = 1$. Now we look at Equation (2.2) which yields

$$b_2 a_2^2 m^2 - b_1 b_2 a_3^2 = -2nr d^2 m^2.$$

Applying the same ideas, $(m, 2r) = 1$.

Back to Equation (2.3), since $m \mid b_1, b_2$, we have that $m \mid n(r-s)d^4$, which implies that $m \mid (r-s)$. □

Remark 2.8. We rewrite System (2.1) and Equation (2.2) as

$$b_1 a_1^2 - b_2 a_2^2 = n(r-s) d^2, \tag{2.4}$$

$$b_1 a_1^2 m^2 - b_1 b_2 a_3^2 = -n(r+s) d^2 m^2, \tag{2.5}$$

$$b_2 a_2^2 m^2 - b_1 b_2 a_3^2 = -2nr d^2 m^2. \tag{2.6}$$

Lemma 2.9. *With the previous notation, we have that*

$$(b_1, d) = (b_2, d) = 1.$$

Proof. Let p be a prime such that $p \mid (b_1, d)$. By Equation (2.4), we conclude that $p \mid b_2$ since $(d, a_2) = 1$. By Equation (2.5), $p^2 \mid b_1 a_1^2 m^2$, but this is a contradiction since $(d, a_1) = (d, m) = 1$ and b_1 is square-free. Analogously, $p \mid (b_2, d)$ also leads to a contradiction. □

Corollary 2.10. *With the previous notation,*

$$b_1 \mid n(r+s)m, \qquad b_2 \mid 2nrm.$$

Proof. Equation (2.5) implies that $b_1 \mid n(r+s)d^2m^2$. We conclude that $b_1 \mid n(r+s)m$ because $(b_1, d) = 1$ and b_1 is square-free.

Equation (2.6) implies that $b_2 \mid 2nrd^2m^2$. We conclude that $b_2 \mid 2nrm$ because $(b_2, d) = 1$ and b_2 square-free. □

Lemma 2.11. *With the previous notation,*

$$(a_1, a_2) \mid (r-s), \qquad (a_1, a_3) \mid (r+s), \qquad (a_2, a_3) \mid 2r.$$

Proof. Let p be a prime dividing both a_1 and a_2. By looking at Equation in (2.4), $p^2 \mid n(r-s)d^2$. Since $(a_i, d) = 1$ and n is square-free, we conclude that $p \mid (r-s)$. Thus $(a_1, a_2) \mid (r-s)$.

The other two statements follow similarly by looking at Equations (2.5) and (2.6). □

We have now all the necessary elements to proceed to the proof of Theorem 2.6.

Proof of Theorem 2.6. I) We have $b_1b_2 < 0$. The right-hand sides of Equations (2.5) and (2.6) are negative. If $b_1b_2 < 0$, the left-hand side of one of these two equations is positive, leading to a contradiction.

II.1) We have $2 \nmid n$, $2 \mid b_1$, and $2 \nmid (r+s)$. By Lemma 2.7, $2 \nmid m$. By Corollary 2.10, we obtain a contradiction since $2 \mid b_1$ and $b_1 \mid n(r+s)m$.

II.1') We have $2 \nmid n$, $(v_2(b_1), v_2(b_2)) = (0, 1)$, $r \equiv 2 \pmod 4$, and $b_1 \equiv 1 \pmod 4$. By Lemma 2.7, $2 \nmid m$ and by Lemma 2.9, $2 \nmid d$. By dividing Equation (2.6) by 2, we obtain $b_2'(a_2^2m^2 - b_1a_3^2) = -nrd^2m^2 \equiv 2 \pmod 4$, which leads to a contradiction for $b_1 \equiv 1 \pmod 4$ and b_2' odd.

II.2.a) We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (0, 0)$, $2 \nmid (r+s)$ and $b_1 \equiv 3 \pmod 4$. By Lemma 2.7, $2 \nmid m$. Since $2 \nmid (r+s)$ and $(r, s) = 1$, we also have that $2 \nmid (r-s)$. Suppose that $2 \mid d$. By Lemma 2.7, $2 \nmid a_1, a_2, a_3$. By looking at Equation (2.6), since $2 \nmid b_2$ and $4 \mid 2nrd^2m^2$, we conclude that $a_2^2m^2 \equiv b_1a_3^2 \pmod 4$, and since $b_1 \equiv 3 \pmod 4$ and m, a_2, a_3 are odd, we get a contradiction.

Now suppose that $2 \nmid d$. Equation (2.5) then implies that $a_1^2m^2 - b_2a_3^2 \equiv 2 \pmod 4$ since b_1 is odd. The only possible case is with a_1, a_3 odd and $b_2 \equiv 3 \pmod 4$. Thus Equation (2.4) becomes $3a_1^2 - 3a_2^2 \equiv 2 \pmod 4$ which has no solution.

II.2.a') We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (0, 0)$, $2 \mid r$ and $b_1 \not\equiv 1 \pmod 8$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid r$, we have that $2 \nmid (r+s)$. By looking at Equation (2.6), we get that $a_2^2 \equiv b_1a_3^2 \pmod 8$ since b_2 is odd. Since $b_1 \not\equiv 1 \pmod 8$, this is only possible if a_2, a_3 are even. Now we look at Equation (2.4). Since $2 \mid a_2$ and $2 \mid n$, we have that $2 \mid b_1a_1^2$. But this implies that a_1 is even, since b_1 is odd. By Lemma 2.11, $(a_1, a_2) \mid (r-s)$ and we obtain a contradiction since $r-s$ is odd.

II.2.b) We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (0, 1)$, $2 \nmid r$, and $b_1 \equiv 1 \pmod 4$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_2$, Lemma 2.9 implies $2 \nmid d$. By dividing Equation (2.6) by 2, $b_2'(a_2^2m^2 - b_1a_3^2) = -nrd^2m^2 \equiv 2 \pmod 4$. This implies that $a_2^2 - a_3^2 \equiv 2 \pmod 4$, which has no solution.

II.2.b') We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (0, 1)$, $r \equiv 2 \pmod 4$, and $b_1 \not\equiv 5 \pmod 8$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_2$, Lemma 2.9 implies $2 \nmid d$. Since $2 \mid r$, we have that $2 \nmid (r \pm s)$. By looking at Equation (2.4), we have $b_1a_1^2 - b_2a_2^2 = n(r-s)d^2 \equiv 2 \pmod 4$ and we conclude that $2 \mid a_1$ and $2 \nmid a_2$. Analogously, by looking at Equation (2.5), $2 \nmid a_3$. By dividing Equation (2.6) by 2, we obtain $b_2'(a_2^2m^2 - b_1a_3^2) = -nrd^2m^2 \equiv 4 \pmod 8$, leading to a contradiction if $b_1 \not\equiv 5 \pmod 8$.

II.2.b") We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (0, 1)$, $4 \mid r$, and $b_1 \not\equiv 1 \pmod 8$. This is proved analogously to the previous case. At the end, by dividing Equation (2.6) by 2, we obtain $b_2'(a_2^2m^2 - b_1a_3^2) = -nrd^2m^2 \equiv 0 \pmod 8$, leading to a contradiction if $b_1 \not\equiv 1 \pmod 8$.

II.2.c) We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (1,0)$, $2 \nmid (r+s)$, and $n'b_1'(r+s) \equiv 1 \pmod 4$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_1$, Lemma 2.9 implies $2 \nmid d$. Since $2 \nmid (r+s)$, then $2 \nmid (r-s)$. By looking at Equation (2.4), $2 \mid a_2$ and $2 \nmid a_1$. By dividing Equation (2.5) by 2 and by multiplying by b_1' we obtain $(b_1')^2(a_1^2m^2 - b_2a_3^2) = -n'b_1'(r+s)d^2m^2 \equiv -1 \pmod 4$ leading to $1 - b_2a_3^2 \equiv -1 \pmod 4$, a contradiction.

II.2.c') We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (1,0)$, $2 \mid r$, and $n'b_1'(r-s) \not\equiv 1 \pmod 8$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_1$, Lemma 2.9 implies $2 \nmid d$. Since $2 \mid r$, then $2 \nmid (r-s)$. By looking at Equation (2.6) modulo 8, $4 \mid a_2$ and $2 \mid a_3$. By dividing Equation (2.4) by 2 and multiplying by b_1', and by looking modulo 8, we obtain $(b_1')^2a_1^2 \equiv n'b_1'(r-s)d^2 \not\equiv 1 \pmod 8$, but this is a contradiction since $(b_1'a_1)^2$ is a square and can only be $\equiv 1, 4, 0 \pmod 8$ but $n'b_1'(r-s)d^2$ is odd.

II.2.d) We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (1,1)$, $2 \mid s$, and $n'b_1'(r+s) \equiv 3 \pmod 4$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_1$, Lemma 2.9 implies $2 \nmid d$. Since $2 \mid s$, we have that $2 \nmid r(r \pm s)$. By dividing Equation (2.6) by 2, $b_2'(a_2^2m^2 - b_1a_3^2) = -nrd^2m^2 \equiv 2 \pmod 4$, and this is only possible when $2 \mid a_2$ and $2 \nmid a_3$. Lemma 2.11 implies that $2 \nmid a_1$, since $2 \mid a_2$ and $r-s$ is odd. By dividing Equation (2.5) by 2 and by multiplying by b_1', we obtain $(b_1')^2(a_1^2m^2 - b_2a_3^2) = -n'b_1'(r+s)d^2m^2 \equiv 1 \pmod 4$ and $1 - b_2 \equiv 1 \pmod 4$, a contradiction since b_2 is even and square-free.

II.2.d') We have $2 \mid n$, $(v_2(b_1), v_2(b_2)) = (1,1)$, $2 \mid r$ and $n'b_1'(r+s) \not\equiv 7 \pmod 8$. By Lemma 2.7, $2 \nmid m$. Since $2 \mid b_1$, Lemma 2.9 implies $2 \nmid d$. Since $2 \mid r$, then $2 \nmid (r \pm s)$. By looking at Equation (2.6) modulo 8, $2 \mid a_2$ and $2 \mid a_3$. Lemma 2.11 implies that $2 \nmid a_1$, since $2 \mid a_2$ and $r-s$ is odd. By dividing Equation (2.5) by 2 and by multiplying by b_1', we have $(b_1')^2(a_1^2m^2 - b_2a_3^2) = -n'b_1'(r+s)d^2m^2 \not\equiv 7 \pmod 8$ leading to a contradiction.

III.a) We have $(v_p(b_1), v_p(b_2)) = (0,0)$, $p \nmid r$, and $\left(\dfrac{b_1}{p}\right) = -1$. Multiply Equation (2.6) by b_2 and look modulo p. We get a contradiction unless $p \mid a_3$ and $p \mid a_2$. But then Lemma 2.11 implies that $p \mid 2r$, a contradiction.

III.a') We have $(v_p(b_1), v_p(b_2)) = (0,0)$, $p \nmid (r+s)$, and $\left(\dfrac{b_2}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.5) by b_1.

III.a") We have $(v_p(b_1), v_p(b_2)) = (0,0)$, $p \nmid (r-s)$, and $\left(\dfrac{b_1b_2}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.4) by b_1.

III.b) We have $(v_p(b_1), v_p(b_2)) = (0,1)$, $p \mid r$, and $\left(\dfrac{b_1}{p}\right) = -1$. By Lemma 2.7, $p \nmid m$. Since $p \mid b_2$, Lemma 2.9 implies $p \nmid d$. By multiplying Equation (2.6) by b_2', by dividing by p, and by looking modulo p, $p \mid a_2, a_3$. By looking at Equation (2.4), $p \mid a_1$. By Lemma 2.11, $p \mid (r-s)$ and since $p \mid r$, then $p \mid s$, and we get a contradiction.

III.b') We have $(v_p(b_1), v_p(b_2)) = (0,1)$, $p \nmid (r+s)$, and $\left(\dfrac{n'b_1b_2'(r+s)}{p}\right) = -1$. By Lemma 2.7, $p \nmid m$. Since $p \mid b_2$, Lemma 2.9 implies $p \nmid d$. By looking at Equation (2.5) modulo p, $p \mid a_1$. Now multiply Equation (2.5) by b_1b_2' and divide by p. We look modulo p and we get a contradiction.

III.b") We have $(v_p(b_1), v_p(b_2)) = (0,1)$, $p \nmid (r-s)$, and $\left(\dfrac{-n'b_2'(r-s)}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.4) by b_2' and by dividing it by p.

III.c) We have $(v_p(b_1), v_p(b_2)) = (1,0)$, $p \nmid r$, and $\left(\dfrac{2n'b_1'b_2r}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.6) by $b_1'b_2$ and by dividing it by p.

III.c') We have $(v_p(b_1), v_p(b_2)) = (1,0)$, $p \mid (r+s)$, and $\left(\frac{b_2}{p}\right) = -1$. By Lemma 2.7, $p \nmid m$. Since $p \mid b_1$, Lemma 2.9 implies $p \nmid d$. By multiplying Equation (2.5) by b_1', by dividing by p, and by looking modulo p, $p \mid a_1, a_3$. By looking at Equation (2.4), $p \mid a_2$. By Lemma 2.11, $p \mid (r-s)$ and since $p \mid (r+s)$, then $p \mid r, s$ and we get a contradiction.

III.c") We have $(v_p(b_1), v_p(b_2)) = (1,0)$, $p \nmid (r-s)$ and $\left(\frac{n'b_1'(r-s)}{p}\right) = -1$. This is proved analogously to *III.b')* by multiplying Equation (2.4) by b_1' and by dividing it by p.

III.d) We have $(v_p(b_1), v_p(b_2)) = (1,1)$, $p \nmid r$, and $\left(\frac{-2n'b_2'r}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.6) by b_2' and by dividing it by p.

III.d') We have $(v_p(b_1), v_p(b_2)) = (1,1)$, $p \nmid (r+s)$, and $\left(\frac{-n'b_1'(r+s)}{p}\right) = -1$. This is proved analogously to the previous case by multiplying Equation (2.5) by b_1' and by dividing it by p.

III.d") We have $(v_p(b_1), v_p(b_2)) = (1,1)$, $p \mid (r-s)$, and $\left(\frac{b_1'b_2'}{p}\right) = -1$. By Lemma 2.7, $p \nmid m$. Since $p \mid b_1$, Lemma 2.9 implies $p \nmid d$. By multiplying Equation (2.4) by b_2', by dividing by p, and by looking modulo p, $p \mid a_1, a_2$. By looking at Equation (2.5), $p^2 \mid n(r+s)$ and then $p \mid (r+s)$. Since $p \mid (r-s)$, then $p \mid r, s$ and we get a contradiction.

□

3. Proof of the main results

We proceed to the proof of Theorem 1.3. For this, we will use Theorem 2.6 for the particular case $\theta = \pi/3$.

Recall that if $p \mid b$, we denote b/p by b'.

Proof of Theorem 1.3. We first notice that the condition $\left(\frac{p_j}{p_i}\right) = -1$ for $i < j$ can be easily extended to $i \neq j$ due to the Law of Quadratic Reciprocity, which guarantees that the order of i and j does not matter when computing the Legendre symbol, since $p_i, p_j \equiv 1 \pmod 4$. More precisely, for the selection of primes in the statement, we summarize the following properties.

(1) Since $p_i \equiv 5 \pmod{24}$, we have

$$\begin{aligned} \left(\frac{-1}{p_i}\right) &= 1, \\ \left(\frac{2}{p_i}\right) &= -1, \\ \left(\frac{3}{p_i}\right) &= -1, \\ \left(\frac{p_j}{p_i}\right) &= -1 \quad \text{for } i \neq j. \end{aligned}$$

(2) Since n is a product of an odd number of primes,

$$\left(\frac{n'}{p_i}\right) = 1 \text{ for all } i.$$

Recall from Remark 2.5 that $R := \{(-1)^\alpha 2^\beta p_1^{\varepsilon_1} \dots p_k^{\varepsilon_k} \mid \alpha, \beta, \varepsilon_1, \dots, \varepsilon_k \in \{0,1\}\}$ is a system of representatives for $\mathbb{Q}(S,2)$. From Theorem 2.2, we have to consider the system of equations (2.1) for $(b_1, b_2) \in R \times R$. The primes to be considered are the given ones $p_1, \dots, p_{2\ell+1}$ that divide n and the remaining ones $p_{2\ell+2}, \dots, p_k$ that divide $r, (r-s)$ and $(r+s)$ but do not divide n.

Since $\theta = \pi/3$, we have that $r = 2$ and $s = 1$. Therefore, $r - s = 1$ and $r + s = 3$. Then we need to examine the solvability of (2.1) with b_1, b_2 elements of

$$R := \{(-1)^\alpha 2^\beta 3^\gamma p_1^{\varepsilon_1} \cdots p_{2\ell+1}^{\varepsilon_{2\ell+1}} \mid \alpha, \beta, \gamma, \varepsilon_1, \dots, \varepsilon_{2\ell+1} \in \{0,1\}\}.$$

By Lemma 2.7, $m \mid (r-s)$, and therefore $m = 1$. By Corollary 2.10 $b_1 \mid 3n$ and $b_2 \mid 4n$.

We will now group the possibilites of b_1 and b_2 into four cases depending on the number of primes that divide them. As seen above, the primes that can divide b_1 are $3, p_1, p_2, \dots, p_{2\ell+1}$ and those that can divide b_2 are $2, p_1, p_2, \dots, p_{2\ell+1}$. For what it follows, p_i denotes a prime of the set $\{p_1, \dots, p_{2\ell+1}\}$. We consider the following cases:

(1) **b_1 and b_2 are both divisible by an odd number of primes (including 3 and 2 respectively).**

- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,0)$. Then,
$$\left(\frac{b_1}{p_i}\right) = \left(\frac{b_2}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.a.*
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,0)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = 1, \quad \left(\frac{b_2}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{2n'b_1'b_2r}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.c.*
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,1)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = \left(\frac{b_2'}{p_i}\right) = 1 \quad \Longrightarrow \quad \left(\frac{-n'b_1'(r+s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.d'.*

Thus, if the system is to be solvable, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$ for $1 \le i \le 2\ell+1$. Hence, in this case, we must have that all primes p_i dividing n must also divide b_2 and must not divide b_1. Since both b_1, b_2, n are products of an odd number of primes and we have the extra condition $b_1 b_2 > 0$ for a solution to exist (by Theorem 2.6.*I*), we are left with only the following cases:

$$(b_1, b_2) \in \{(3, n), (-3, -n)\}.$$

Consider $(b_1, b_2) = (3, n)$. Equation (2.4) can be written as

$$3a_1^2 = n(a_2^2 + d^2).$$

Since $b_1 = 3$, Lemma 2.9 implies that $3 \nmid d$ and $d^2 \equiv 1 \pmod 3$. Since $3 \nmid n$, the right-hand side of the above equation is never divisible by 3, leading to a contradiction.

Hence, the only possibility in this case is that $(b_1, b_2) = (-3, -n) = \left(\frac{r+s}{s-r}, -n(r-s)\right)$.

(2) **b_1 is divisible by an odd number of primes and b_2 by an even number of primes.**

- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,0)$. Then,
$$\left(\frac{b_1}{p_i}\right) = -1, \quad \left(\frac{b_2}{p_i}\right) = 1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.a.*

- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$. Then,
$$\left(\frac{b_1}{p_i}\right) = \left(\frac{b_2'}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{n'b_1b_2'(r+s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.b'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,1)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = 1, \quad \left(\frac{b_2'}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{-n'b_1'(r+s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.d'*.

Therefore, we obtain that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,0)$ for $1 \leq i \leq 2\ell+1$ if the system is to be solvable. Hence, in this case, all primes p_i dividing n must also divide b_1 and must not divide b_2. This time we are left with the following cases:
$$(b_1, b_2) \in \{(n,1), (-n,-1)\}.$$
Consider $(b_1, b_2) = (-n,-1)$. After some simplification Equation (2.5) becomes
$$a_1^2 + a_3^2 = 3d^2.$$
By looking at the above equation modulo 3, we conclude that $3 \mid a_1, a_3$. Looking again at the right-hand side, $3 \mid d^2$. But then we have that $3 \mid a_1$ and $3 \mid d$, a contradiction by Lemma 2.7.

We are left with the only possibility, $(b_1, b_2) = (n,1) = \left(n(r-s), \frac{2r}{r-s}\right)$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$.

(3) b_1 **is divisible by an even number of primes and** b_2 **by an odd number of primes.**
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,0)$. Then,
$$\left(\frac{b_1}{p_i}\right) = 1, \quad \left(\frac{b_2}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.a'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$. Then,
$$\left(\frac{b_1}{p_i}\right) = \left(\frac{b_2'}{p_i}\right) = 1 \quad \Longrightarrow \quad \left(\frac{n'b_1b_2'(r+s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.b'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,0)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = \left(\frac{b_2}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{n'b_1'(r-s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.c"*.

Thus, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,1)$ for $1 \leq i \leq 2\ell+1$, which means all primes p_i must divide both b_1 and b_2. We have the following possibilities:
$$(b_1, b_2) \in \{(3n,n), (-3n,-n)\}.$$
Consider $(b_1, b_2) = (3n, n)$. Equation (2.4) becomes
$$3a_1^2 = a_2^2 + d^2.$$
Since $b_1 = 3n$, Lemma 2.9 implies that $3 \nmid d$. Thus $d^2 \equiv 1 \pmod 3$ and the right-hand side of the above equation is never divisible by 3, leading to a contradiction.

Therefore, we are left with the only possibility of $(b_1, b_2) = (-3n,-n) = (-n(r+s), -2nr)$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$.

(4) **Both** b_1 **and** b_2 **are divisible by an even number of primes.**

- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$. Then,
$$\left(\frac{b_1}{p_i}\right) = 1, \quad \left(\frac{b_2'}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{-n'b_2'(r-s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.b"*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,0)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = -1, \quad \left(\frac{b_2}{p_i}\right) = 1 \quad \Longrightarrow \quad \left(\frac{n'b_1'(r-s)}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.c"*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,1)$. Then,
$$\left(\frac{b_1'}{p_i}\right) = \left(\frac{b_2'}{p_i}\right) = -1 \quad \Longrightarrow \quad \left(\frac{-2n'b_2'r}{p_i}\right) = -1,$$
and System (2.1) is unsolvable by Theorem 2.6.*III.d*.

Therefore, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,0)$ for $1 \leq i \leq 2\ell+1$, which means none of the primes p_i divide either b_1 or b_2. We have the following possibilities:
$$(b_1, b_2) \in \{(1,1), (-1,-1)\}.$$
Consider $(b_1, b_2) = (-1,-1)$. Replacing these values in Equation (2.5), we have:
$$a_1^2 + a_3^2 = 3nd^2.$$
By looking at the above equation modulo 3, we conclude that $3 \mid a_1, a_3$. Looking again at the right-hand side, $3 \mid d^2$. But then we have that $3 \mid a_1$ and $3 \mid d$, a contradiction by Lemma 2.7.

Hence we are left with $(b_1, b_2) = (1,1)$.

We have shown that the system of equations (2.1) has a solution only when $(b_1, b_2) \in \{(1,1), (n,1), (-3,-n), (-$ which are the images of the torsion points of $E_{n,\theta}$. Since the map defined in Theorem 2.2 is injective, these are the only rational points on $E_{n,\theta}(\mathbb{Q})$. Thus its rank has to be zero and, by Proposition 2.1, n is not $\pi/3$-congruent.

This concludes the proof of Theorem 1.3. □

We now proceed to the proof of Theorem 1.4. In this case, we will use Theorem 2.6 when $\theta = 2\pi/3$.

Proof of Theorem 1.4. For the selection of odd primes in the statement, we summarize the following properties.

(1) Since $p_i \equiv 13 \pmod{24}$, we have
$$\begin{aligned} \left(\frac{-1}{p_i}\right) &= 1, \\ \left(\frac{2}{p_i}\right) &= -1, \\ \left(\frac{3}{p_i}\right) &= 1, \\ \left(\frac{p_j}{p_i}\right) &= -1 \quad \text{for } i \neq j. \end{aligned}$$

(2) Since n is a product of an odd number of primes (including 2),

$$\left(\frac{n'}{p_i}\right) = 1 \text{ for all } i.$$

Since $\theta = 2\pi/3$, we have that $r = 2$ and $s = -1$. Therefore, $r - s = 3$ and $r + s = 1$. Then we need to examine the solvability of (2.1) with b_1, b_2 elements of

$$R := \{(-1)^\alpha 2^\beta 3^\gamma p_1^{\varepsilon_1} \cdots p_{2\ell}^{\varepsilon_{2\ell}} \mid \alpha, \beta, \gamma, \varepsilon_1, \ldots, \varepsilon_{2\ell} \in \{0, 1\}\}.$$

By Lemma 2.7, $m \mid (r - s)$, and therefore $m = 1$ or $m = 3$. By Lemma 2.7 and Corollary 2.10, $3 \mid b_1, b_2$ iff $m = 3$.

For the time being we will ignore the factor of 3 dividing b_i when $m = 3$. For what it follows, p_i denotes a prime of the set $\{p_1, \ldots, p_{2\ell}\}$. We consider the following cases:

(1) **b_1 and b_2 are both divisible by an odd number of primes (including 2 but excluding 3).**
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0, 0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.a*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0, 1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.b'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.c*.

Thus, if the system is to be solvable, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 1)$ for $1 \leq i \leq 2\ell$. This implies that

$$(b_1, b_2) \in \{(\pm n, \pm n), (\pm 3n, \pm 3n)\}.$$

Now consider the unsolvability conditions modulo 2. Since n' is odd, $(n')^2 \equiv 1 \pmod 8$ and Theorem 2.6.*II.2.d'* gives a contradiction unless $(b_1, b_2) = (-n, -n) = (-n(r + s), -2nr)$ in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$.

(2) **b_1 is divisible by an odd number of primes and b_2 by an even number of primes.**
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0, 0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.a*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0, 1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.b"*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.d*.

Therefore, we obtain that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 0)$ for $1 \leq i \leq 2\ell$. Hence, in this case,

$$(b_1, b_2) \in \{(\pm n, \pm 1), (\pm 3n, \pm 3)\}.$$

Applying Theorem 2.6.*II.2.c'* gives a contradiction unless $(b_1, b_2) = (3n, 3) = \left(n(r - s), \frac{2r}{r-s}\right)$ in $\mathbb{Q}(S, 2) \times \mathbb{Q}(S, 2)$.

(3) **b_1 is divisible by an even number of primes and b_2 by an odd number of primes.**
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0, 0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.a'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.c"*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1, 1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.d'*.

Thus, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$ for $1 \leq i \leq 2\ell$, and we have the following possibilities:

$$(b_1, b_2) \in \{(\pm 1, \pm n), (\pm 3, \pm 3n)\}.$$

Now Theorem 2.6.*II.2.b'* gives a contradiction except for $(b_1, b_2) = (-3, -3n) = \left(\frac{r+s}{s-r}, -n(r-s)\right)$ in $\mathbb{Q}(S,2) \times \mathbb{Q}(S,2)$.

(4) **Both b_1 and b_2 are divisible by an even number of primes.**
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.b'*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,0)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.c*.
- Suppose $\exists p_i$ such that $(v_{p_i}(b_1), v_{p_i}(b_2)) = (1,1)$. Then System (2.1) is unsolvable by Theorem 2.6.*III.d*.

Therefore, $(v_{p_i}(b_1), v_{p_i}(b_2)) = (0,0)$ for $1 \leq i \leq 2\ell$ and

$$(b_1, b_2) \in \{(\pm 1, \pm 1), (\pm 3, \pm 3)\}.$$

Applying Theorem 2.6.*II.2.a'* gives a contradiction unless $(b_1, b_2) = (1,1)$.

We have shown that the system of equations (2.1) has a solution only when $(b_1, b_2) \in \{(1,1), (3n,3), (-3,-3n)\}$, which are the images of the torsion points of $E_{n,\theta}$. Since the map defined in Theorem 2.2 is injective, these are the only rational points on $E_{n,\theta}(\mathbb{Q})$. Thus its rank has to be zero and, by Proposition 2.1, n is not $2\pi/3$-congruent.

This concludes the proof of Theorem 1.4. □

As a final note, we can combine Theorem 1.3 with Dirichlet's Theorem on arithmetic progressions and the Chinese Remainder Theorem in order to prove the following result.

Corollary 3.1. *There exists an infinite sequence of distinct primes such that any product of an odd number of primes in this sequence cannot be a $\pi/3$-congruent number.*

Proof. To prove this result, it suffices to show the existence of an infinite sequence of primes p_i such that $p_i \equiv 5 \pmod{24}$ and $\left(\frac{p_j}{p_i}\right) = -1$ for $j < i$, since the product of any odd number of such primes is not $\pi/3$-congruent by Theorem 1.3.

First notice that by Dirichlet's Theorem on arithmetic progressions, there are infinitely many primes congruent to $5 \pmod{24}$. Also notice that by Quadratic Reciprocity, $\left(\frac{p_j}{p_i}\right) = \left(\frac{p_i}{p_j}\right)$.

We construct the set by induction. Suppose that we have already k primes $p_1, \ldots, p_k$ that satisfy the desired conditions. For each $1 \leq i \leq k$, let s_i be an integer that is a quadratic non-residue modulo p_i. By the Chinese Remainder Theorem, we can find an integer x such that $x \equiv s_i \pmod{p_i}$ for $1 \leq i \leq k$ and $x \equiv 5 \pmod{24}$. Applying Dirichlet's Theorem, we obtain an infinite sequence of primes $p \equiv x \pmod{24p_1 \cdots p_k}$. We can choose any of them to be p_{k+1}. This process can be repeated indefinitely.

This concludes the proof of the corollary. □

A similar corollary can be deduced from Theorem 1.4.

4. Conclusion

Several directions of further exploration arise from this work. Theorem 2.6 may be used to obtain results for n a product of a few primes. For example, one can directly recover known results such

as the fact that $p \equiv 5, 7, 19 \pmod{24}$ are not $\pi/3$-congruent and $p \equiv 7, 11 \pmod{24}$ are not $2\pi/3$-congruent. One can further prove that $n = 2p$ is not $\pi/3$-congruent for $p \equiv 19 \pmod{24}$ and that $n = 2p$ is not $2\pi/3$-congruent for $p \equiv 13, 19 \pmod{24}$. The procedure for these proofs is straightforward but long.

A natural question to ask is whether similar results to Theorems 1.3 and 1.4 can be found with different congruence conditions and/or different values of θ. It would be also interesting to explore other methods for doing analogous constructions in the case of classical non-congruent numbers, such as the ones considered in [RSY13, RSY15], and see how they can be adapted to other values of θ.

Acknowledgements

The authors would like to thank Dimitris Koukoulopoulos for helpful discussions and the referee for their very careful and detailed reading of the manuscript and for their useful corrections.

This research was supported by the Natural Sciences and Engineering Research Council of Canada [Undergraduate Student Research Award to VG, Discovery Grant 355412-2013 to ML] and Mitacs [Globalink Research Internship to SN].

References

[Fu97] M. Fujiwara, *θ-congruent numbers*, Number Theory, K. Györy, A. Pethö and V. Sós (eds.), de Gruyter, Berlin, 1997, pp. 235–241.

[Fu02] M. Fujiwara, *Some properties of θ-congruent numbers*, Natur. Sci. Rep. Ochanomizu Univ. 52 (2002), no. 2, 1–8.

[He52] K. Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56, (1952). 227–253.

[Is96] B. Iskra, *Non-congruent numbers with arbitrarily many prime factors congruent to* 3 *modulo* 8, Proc. Japan Acad. Ser. A Math. Sci. **72** , 1996, no. 7, 168–169.

[Ka00] M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith. **9**4 no.2, 2000, pp. 153–160.

[Ko93] N. Koblitz, *Introduction to elliptic curves and modular forms*, Grad. Texts Math. 97, 2nd edition, Springer-Verlag, Berlin, 1993.

[Mo90] P. Monsky, *Mock Heegner points and congruent numbers*, Math. Z. 204 (1990), no. 1, 45–67.

[Na29] T. Nagell, *L'analyse indéterminée de degré supérieur*, vol. 39, Gauthier-Villars, Paris, 1929.

[RSY13] L. Reinholz, B. K. Spearman, Q. Yang, *Families of non-congruent numbers with arbitrarily many prime factors*, J. Number Theory 133 (2013), no. 1, 318–327.

[RSY15] L. Reinholz, B. K. Spearman, Q. Yang, *On the prime factors of non-congruent numbers*, Colloq. Math. 138 (2015), no. 2, 271–282.

[Se91] P. Serf, *Congruent Numbers and Elliptic Curves*, Computational Number Theory, A. Pethö, M. Pohst, H. Williams and H. Zimmer (eds.), Walter de Gruyter and Co. Berlin, New York, 1991, pp. 227–238.

[Si86] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[ST92] J. H. Silverman, J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer, New York, 1992.

[Tu83] J. B. Tunnell, *A classical Diophantine problem and modular forms of weight 3/2*, Invent. Math. 72 (1983), no. 2, 323–334.

[TY08] J. Top, N. Yui, Noriko, *Congruent number problems and their variants*, Algorithmic number theory: lattices, number fields, curves and cryptography, 613–639, Math. Sci. Res. Inst. Publ., 44, Cambridge Univ. Press, Cambridge, 2008.

[Yo01] S. Yoshida, *Some variants of the congruent number problem. I.* Kyushu J. Math. 55 (2001), no. 2, 387–404.

[Yo02] S. Yoshida, *Some variants of the congruent number problem. II.* Kyushu J. Math. 56 (2002), no. 1, 147–165.

Département de Mathématiques et de Statistique, Université de Montréal, Canada
E-mail address: girardvin@dms.umontreal.ca

Département de Mathématiques et de Statistique, Université de Montréal, Canada
E-mail address: mlalin@dms.umontreal.ca

Department of Mathematics and Statistics, Indian Institute of Technology Kanpur, India
E-mail address: sivasankar.nair@gmail.com