Bull. Aust. Math. Soc. **103** (2021), 218–229
doi:10.1017/S0004972720000672

ON θ-CONGRUENT NUMBERS OVER REAL NUMBER FIELDS

SHAMIK DAS and ANUPAM SAIKIA

(Received 15 April 2020; accepted 19 May 2020; first published online 9 September 2020)

Abstract

The notion of θ-congruent numbers is a generalisation of congruent numbers where one considers triangles with an angle θ such that $\cos\theta$ is a rational number. In this paper we discuss a criterion for a natural number to be θ-congruent over certain real number fields.

2020 *Mathematics subject classification*: primary 11G05; secondary 11R21, 11R16.

Keywords and phrases: congruent number, elliptic curve.

1. Introduction

A natural number $n \in \mathbb{N}$ is called a *congruent number* if it occurs as the area of a rational right triangle, that is, there exist rational numbers a, b and c such that

$$a^2 + b^2 = c^2, \quad ab = 2n. \tag{1.1}$$

For example, 6 is a congruent number given by the Pythagorean triple $(3, 4, 5)$. Fermat showed that $n = 1$ is not a congruent number; this is equivalent to Fermat's Last Theorem for the exponent 4. Euler was the first to show that $n = 7$ is a congruent number (see [12]). It is known that the numbers 1, 2, 3 and 4 are not congruent numbers, but 5, 6 and 7 are. However, a straightforward criterion to tell whether or not a given n is a congruent number remains elusive. This is the classical *congruent number problem*. As n is a congruent number if and only if $n\alpha^2$ is congruent for any $\alpha \in \mathbb{Z} \setminus \{0\}$, it is enough to consider the problem for square-free natural numbers.

If n is a congruent number then it follows from (1.1) that there exist three rational squares in arithmetic progression with gap n, namely $x - n$, x, $x + n$ where $x = c^2/4$. Therefore we obtain the rational point $(c^2/4, c(a^2 - b^2)/8)$ on the elliptic curve

$$E_n : y^2 = x(x^2 - n^2). \tag{1.2}$$

Here, E_n is called the *congruent number elliptic curve*. It is well known that the torsion subgroup $E_n(\mathbb{Q})_{\text{tors}}$ of the Mordell–Weil group $E_n(\mathbb{Q})$ consists only of points of order dividing 2, namely $(0, 0)$, $(\pm n, 0)$ and the point at infinity $\mathcal{O}$ (see

The first author has been supported by a Senior Research Fellowship from IIT Guwahati and the second author has been supported by a Professional Development Allowance from IIT Guwahati.

[12, Proposition 17]). So the rational point $(c^2/4, c(a^2-b^2)/8)$ obtained from the Pythagorean triple (a,b,c) must be of infinite order. Conversely, a point P of infinite order on $E_n(\mathbb{Q})$ gives a rational point $2P=(x,y)$ where $x-n$, x and $x+n$ are rational squares (see Proposition 2.4). Taking $a=\sqrt{x+n}-\sqrt{x-n}$, $b=\sqrt{x+n}+\sqrt{x-n}$, and $c=2\sqrt{x}$, it can be easily checked that n is a congruent number from (1.1). This argument leads to the following well-known criterion.

CRITERION 1.1. *A positive integer n is a congruent number if and only if $E_n(\mathbb{Q})$ has a point of infinite order.*

This criterion led to significant progress on the congruent number problem by Tunnel [20], Monsky [13] and very recently by Tian [19], among several others.

If n is not a congruent number a natural question arises whether n appears as the area of a right triangle whose sides belong to some real number field, leading to the following generalisation. A positive integer n is called a congruent number over a number field K (or in short, a *K-congruent number*) if there exist $a,b,c\in K$ such that (1.1) holds. Study of the congruent number problem over algebraic number fields dates back at least to Tada [18] who considered real quadratic fields. Jędrzejak [9] gave some results for congruent numbers over certain other real number fields. Fujiwara [3] and Kan [10] considered another variant of congruent numbers called θ-congruent numbers and defined as follows.

DEFINITION 1.2. Let $0<\theta<\pi$ be an angle with rational cosine $\cos\theta=s/r$ where $0<|s|<r$ and $\gcd(r,s)=1$. Let $(u,v,w)_\theta$ denote a triangle with an angle θ between the sides u and v.

A positive integer n is called a θ-congruent number if there exists a triangle $(u,v,w)_\theta$ with sides in $\mathbb{Q}$ having area $n\alpha_\theta$, where $\alpha_\theta=\sqrt{r^2-s^2}$. In other words, n is a θ-congruent number if it satisfies

$$2rn=uv,\quad w^2=u^2+v^2-2uv\cdot\frac{s}{r}. \tag{1.3}$$

The θ-congruent numbers with $\theta=\pi/2$ are just the classical congruent numbers. For θ-congruent numbers we have a similar criterion to (1.1) in terms of the associated *θ-congruent number elliptic curve* given by

$$E_{n,\theta}: y^2=x(x+(r+s)n)(x-(r-s)n), \tag{1.4}$$

where r and s are defined as above. The following criterion is due to Fujiwara [3].

CRITERION 1.3. *Let $\theta\in(0,\pi)$ be an angle such that $\cos\theta$ is rational and let n be a square-free natural number.*

(1) *n is θ-congruent if and only if $E_{n,\theta}$ has a point of order greater than 2.*
(2) *If $n\neq 1,2,3,6$, then n is θ-congruent if and only if $E_{n,\theta}$ has positive rank.*

There is an extension of θ-congruent numbers over a number field K similar to that of congruent numbers over a number field K.

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

DEFINITION 1.4. With notation as in Definition 1.2, we call a natural number n a (K,θ)-congruent number if there is a triangle $(u,v,w)_\theta$ with sides in a number field K satisfying (1.3). We refer to the triangle $(u,v,w)_\theta$ as a (K,θ,n)-triangle.

Janfada and Salami [8] studied θ-congruent number over real quadratic fields. It is easy to see that when $n=1$ and $\theta=2\pi/3$, we have $r=2, s=-1, \alpha_\theta=\sqrt{3}$ and there is a $(\mathbb{Q}(\sqrt{3}),\theta,1)$-triangle with sides $(2,2,2\sqrt{3})$ of area $\sqrt{3}$. But we know that $\operatorname{rank}(E_{1,\theta}(\mathbb{Q}(\sqrt{3})))=0$, hence we can conclude that 1 occurs as a $2\pi/3$-congruent number for only finitely many triangles with sides in $\mathbb{Q}(\sqrt{3})$. This motivates the following definition, which is analogous to the notion of *properly K-congruent numbers* defined in [4] and [9].

DEFINITION 1.5. We say that a (K,θ)-congruent number n is properly (K,θ)-congruent if (1.3) has infinitely many solutions $u,v,w\in K$.

For example, all $(\mathbb{Q},\theta)$-congruent numbers not equal to 1, 2, 3 or 6 are properly $(\mathbb{Q},\theta)$-congruent by Criterion 1.3. The question whether n is a θ-congruent number is intimately connected with the torsion subgroup of the corresponding θ-congruent number elliptic curve $E_{n,\theta}$ over $\mathbb{Q}$. Much progress has been made concerning the torsion of base change of elliptic curves (defined over $\mathbb{Q}$) over number fields, especially when the degree of the number field is small (see [2, 5–7, 14]). When the elliptic curve has complex multiplication, more information is available for the torsion subgroup over number fields (see, for example, [15]). The congruent number elliptic curve has complex multiplication but the θ-congruent number elliptic curve in (1.4) does not have complex multiplication for $\theta\neq\pi/2$ (Proposition 2.11). Hence the study of the torsion subgroup of the latter requires somewhat more care. Motivated by [9], this paper provides a criterion for determining whether a square-free positive integer n is a θ-congruent number over certain classes of real number fields (Theorems 2.2, 2.12 and 2.14).

2. Main results

2.1. θ-congruent numbers over real multi-quadratic fields. For a number field K let $E_{n,\theta}(K)_{\text{tors}}$ denote the group of K-rational torsion points of $E_{n,\theta}$ defined in (1.4), where n is a square-free natural number and r,s are as defined in Definition 1.2. The rational torsion points on $E_{n,\theta}(\mathbb{Q})_{\text{tors}}$ are well known by the following result of Fujiwara [3, Proposition 4].

PROPOSITION 2.1. *For $n\neq 1,2,3,6$,*

$$E_{n,\theta}(\mathbb{Q})_{\text{tors}}=\mathbb{Z}/2\mathbb{Z}\oplus\mathbb{Z}/2\mathbb{Z}.$$

Let $K_{2,d}$ denote a real number field of type $(2,\dots,2)$, that is,

$$K_{2,d}=\mathbb{Q}(\sqrt{m_1},\dots,\sqrt{m_d}),$$

where m_i are distinct square-free natural numbers such that any two distinct m_i, m_j are coprime. It follows that $[K_{2,d}:\mathbb{Q}]=2^d$. We prove the following analogue of

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

Criterion 1.1 for a θ-congruent number over $K_{2,d}$. For a positive integer a, let $\mathrm{sqf}(a)$ denote the square-free part of a. We take n to be a square-free natural number and keep the same notation as in Definition 1.4 for the rest of the paper.

THEOREM 2.2. *Consider the number field $K_{2,d} = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_d})$ as above. Assume that:*

(1) *n and $\mathrm{sqf}(nm_i)$ do not divide 6 for all $i \in \{1, 2, \ldots, d\}$;*
(2) *$2r(r-s)$ is not a square in $K_{2,d}$.*

Then n is θ-congruent number over $K_{2,d}$ if and only if $E_{n,\theta}(K_{2,d})$ has a point of infinite order.

It is standard notation to denote the group of all 2-torsion points defined over K on the elliptic curve $E_{n,\theta}$ by $E_{n,\theta}(K)[2]$. We need the following lemma for the proof of the theorem.

LEMMA 2.3. *For every subfield K of $\mathbb{R}$, a natural number n is θ-congruent over K if and only if $E_{n,\theta}(K) \setminus E_{n,\theta}(K)[2] \neq \emptyset$.*

The essential argument for the proof of the lemma above is contained in Tada [18, Theorem 1] who considered the case $\theta = \pi/2$ for real quadratic fields K. The analogue for real quadratic fields for any θ with rational cosine in [8] adopts the same approach as in [18]. In the case of real multi-quadratic fields, the proof similarly follows from the following well-known result on elliptic curves.

PROPOSITION 2.4 [11]. *Let E be an elliptic curve over a field k (of characteristic $\neq 2, 3$) given by*

$$E : y^2 = (x - a_1)(x - a_2)(x - a_3) \quad \text{with } a_1, a_2, a_3 \in k.$$

Let (x_0, y_0) be a k-rational point of $E \setminus \{O\}$. Then there exists a k-rational point (x_1, y_1) of E with $2(x_1, y_1) = (x_0, y_0)$ if and only if $x_0 - a_1$, $x_0 - a_2$ and $x_0 - a_3$ are squares in k.

PROOF OF LEMMA 2.3. Let K be a real number field. For a positive integer n and θ such that $\cos\theta = s/r$ with $s, r \in \mathbb{Z}$, consider the two sets

$$S = \left\{(u, v, w) \in K^3 : 0 < u \leq v < w,\ uv = 2rn,\ u^2 + v^2 - 2uv \cdot \frac{s}{r} = w^2\right\}$$

and

$$T = \{(x, y) \in 2E_{n,\theta}(K) \setminus \{O\} : y \geq 0\}.$$

Define

$$\phi : S \to T, \quad (u, v, w) \mapsto \left(\frac{w^2}{4}, \frac{w(v^2 - u^2)}{8}\right),$$

and let $\psi : T \to S$ be the map sending (x, y) to the tuple

$$\left(\sqrt{x + (r+s)n} - \sqrt{x - (r-s)n},\ \sqrt{x + (r+s)n} + \sqrt{x - (r-s)n},\ 2\sqrt{x}\right).$$

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

Using Proposition 2.4, it is easy to see that the maps ϕ and ψ are well defined, and that $\phi \circ \psi = 1_T$ and $\psi \circ \phi = 1_S$. It follows that n is θ-congruent over K if and only if T is nonempty. □

The following corollary is immediate from Lemma 2.3.

COROLLARY 2.5. *Assume that $E_{n,\theta}(K)_{\text{tors}} = E_{n,\theta}(K)[2]$ for the real number field K. Then n is a θ-congruent number over K if and only if $E_{n,\theta}(K)$ has positive rank.*

LEMMA 2.6. *If n and $\text{sqf}(nm_i)$ do not divide 6 for all $i \in \{1, 2, \ldots, d\}$, then $E_{n,\theta}(K_{2,d})_{\text{tors}}$ is a 2-group.*

PROOF. By the remark below Theorem 2 and Lemma 3 in [16], $E_{n,\theta}(K_{2,d})_{\text{tors}}$ must be a 2-group if the torsion subgroup of the quadratic m_i-twist $E^{m_i}_{n,\theta}$ over $\mathbb{Q}$ is a 2-group for each i. Hence it suffices to show that

$$E^{m_i}_{n,\theta}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Observe that the quadratic m_i-twist of the θ-congruent number elliptic curve is

$$E^{m_i}_{n,\theta} : y^2 = x(x - m_i n(r - s))(x + m_i n(r + s)). \tag{2.1}$$

Thus $E^{m_i}_{n,\theta}$ is isomorphic to $E_{nm_i,\theta}$. By Proposition 2.1,

$$E^{m_i}_{n,\theta}(\mathbb{Q})_{\text{tors}} \cong E_{nm_i,\theta}(\mathbb{Q})_{\text{tors}} \cong E_{\text{sqf}(nm_i),\theta}(\mathbb{Q})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}.$$

Therefore, we can conclude that $E_{n,\theta}(K_{2,d})_{\text{tors}}$ is a 2-group. □

While Lemma 2.6 rules out torsion points of odd order, we still need to show that there is no torsion point of order 4 or a higher power of 2.

LEMMA 2.7. *Under the assumption of Theorem 2.2,*

$$E_{n,\theta}(K_{2,d})_{\text{tors}} = E_{n,\theta}(K_{2,d})[2].$$

PROOF. It is enough to show that $E_{n,\theta}(K_{2,d})_{\text{tors}} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Since we know that there are exactly three elements of order 2 and $E_{n,\theta}(K_{2,d})_{\text{tors}}$ is a 2-group by Lemma 2.6, it suffices to show that $E_{n,\theta}(K_{2,d})_{\text{tors}}$ has no point of order 4. Suppose, if possible, P has order 4. Then $2P$ has order 2 and

$$2P \in \{(0, 0),\ (-(r + s)n, 0),\ ((r - s)n, 0)\}.$$

By Proposition 2.4,

(1) $2P = (0, 0)$ if and only if both $-(r + s)n$ and $(r - s)n$ are squares in $K_{2,d}$, which is not possible because $K_{2,d}$ is a real subfield.
(2) $2P = (-(r + s)n, 0)$ if and only if both $-(r + s)n$ and $-2rn$ are squares in $K_{2,d}$, which is not possible for same reason as in (1).
(3) $2P = ((r - s)n, 0)$ if and only if both $(r - s)n$ and $2rn$ are squares in $K_{2,d}$. Then $2r(r - s)$ is a square in $K_{2,d}$, contrary to our assumption. □

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

Theorem 2.2 follows immediately from Corollary 2.5 and Lemma 2.7. We have the following consequences of Theorem 2.2.

COROLLARY 2.8. *Under the assumption of Theorem 2.2, n is a θ-congruent number over $K_{2,d}$ if and only if at least one of the 2^d numbers $nm_1^{e_1}\cdots m_d^{e_d}(e_i = 0, 1)$ is a θ-congruent number over $\mathbb{Q}$.*

We require the following well-known result to establish this corollary.

PROPOSITION 2.9 [1]. *Suppose E is an elliptic curve over a number field k. Suppose $D \in k \setminus k^2$ and E^D is the quadratic D-twist of E. Then*

$$\operatorname{rank}(E(k)) + \operatorname{rank}(E^D(k)) = \operatorname{rank}(E(k(\sqrt{D}))). \tag{2.2}$$

PROOF OF COROLLARY 2.8. Using (2.2) inductively and noting that $E_{n,\theta}^{m_i}$ is isomorphic to $E_{nm_i,\theta}$, we obtain

$$\operatorname{rank}(E_{n,\theta}(K_{2,d})) = \sum \operatorname{rank}(E_{nm_1^{e_1}\cdots m_d^{e_d},\theta}(\mathbb{Q})),$$

where the summation is over all d-tuples $e_i \in \{0, 1\}$. By Theorem 2.2 and Criterion 1.3, if n is a θ-congruent number then

$$\operatorname{rank}(E_{n,\theta}(K_{2,d})) > 0 \iff \operatorname{rank}(E_{nm_1^{e_1}\cdots m_d^{e_d},\theta}(\mathbb{Q})) > 0 \quad \text{for some } (e_1, \ldots, e_d),$$

which proves the corollary. □

COROLLARY 2.10. *Under the assumption of Theorem 2.2, n is a θ-congruent number over $K_{2,d}$ if and only if n is a θ-congruent number over $\mathbb{Q}$ or over some real quadratic field $\mathbb{Q}(\sqrt{m_1^{e_1}\cdots m_d^{e_d}})$ contained in $K_{2,d}$.*

PROOF. Suppose n is not a θ-congruent number over $\mathbb{Q}$. By Corollary 2.8, one of the 2^d numbers $nm_1^{e_1}\cdots m_d^{e_d}$, say nr ($\neq n$), is a θ-congruent number over $\mathbb{Q}$. Then

$$\operatorname{rank}(E_{nr,\theta}(\mathbb{Q})) > 0 \implies \operatorname{rank}(E_{n,\theta}^r(\mathbb{Q})) > 0 \implies \operatorname{rank}(E_{n,\theta}(\mathbb{Q}(\sqrt{r}))) > 0$$

by (2.1) and (2.2). Thus, n is θ-congruent number over $\mathbb{Q}(\sqrt{r})$. The converse is trivial. □

2.2. θ-congruent numbers over real number fields of degree coprime to 6. We now look for analogues of Theorem 2.2 for real number fields K other than multi-quadratic fields. We need to ensure that the torsion subgroup $E_{n,\theta}(K)_{\text{tors}}$ does not grow bigger than $E_{n,\theta}(\mathbb{Q})_{\text{tors}}$. When the degree of K over $\mathbb{Q}$ is not divisible by small primes, it is possible to restrict the torsion and obtain similar criteria for θ-congruent numbers over K as stated in Theorem 2.12 below.

In [9], it has been proved that n is a congruent number over K if and only if $E_n(K)$ has a point of infinite order, under the assumptions that (i) K is a real number field such that $[K : \mathbb{Q}]$ is odd or $2p$, where p is prime, and (ii) $\sqrt{2}$, $\sqrt{3}$ and $\sqrt{5} \notin K$. The proof depends crucially on the fact that congruent number elliptic curves have complex multiplication, hence their torsion groups over such number fields are well understood

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

due to work of Silverberg [17] and Prasad *et al.* [15]. But the torsion of a θ-congruent number elliptic curve poses somewhat more difficulty due to the next proposition.

PROPOSITION 2.11. *The θ-congruent number elliptic curve $E_{n,\theta}$ does not have complex multiplication for $\theta \neq \pi/2$.*

PROOF. Given any number field F, there are only finitely many $\mathbb{C}$-isomorphism classes of elliptic curves over F with complex multiplication, and each isomorphism class has a distinct j-invariant which must be an algebraic integer in F. By using SAGE, one can show that the j-invariant of a rational elliptic curve with complex multiplication must be one of the 13 integers -262537412640768000, -147197952000, -884736000, -12288000, -884736, -32768, -3375, 0, 1728, 8000, 54000, 287496 or 16581375. The j-invariant of the elliptic curve $E_{n,\theta}$ given by equation (1.4) is

$$j(E_{n,\theta}) = 2^6 \frac{(3r^2 + s^2)^3}{r^2(r^2 - s^2)^2}.$$

It is clear that $j(E_{n,\theta}) > 0$. By considering the numerator of $j(E_{n,\theta})$ modulo 5, we find that it is not divisible by 5 and hence it cannot be 8000, 54000 or 16581375 for any two coprime integers r and s. By considering the numerator of $j(E_{n,\theta})$ modulo 11, we find that it is not divisible by 11 and hence it cannot be 287496 for any two coprime integers r and s. Finally, $j(E_{n,\theta}) = 1728$ if and only if $s = 0$, that is, $\theta = \pi/2$. □

Exploiting recent work of González-Jiménez and Najman on the torsion subgroup of rational elliptic curves, we show that a generalised criterion for θ-congruent numbers can still be obtained.

THEOREM 2.12. *Suppose n is a square-free natural number other than 1, 2, 3 or 6. Let K be a real number field such that $[K : \mathbb{Q}]$ is coprime to 6 and not divisible by 55. Then n is a θ-congruent number over K if and only if $E_{n,\theta}(K)$ has a point of infinite order.*

The result of González-Jiménez and Najman in [6] that we use is as follows.

PROPOSITION 2.13. *Let B be a positive integer. Let $E/\mathbb{Q}$ be an elliptic curve and $K/\mathbb{Q}$ a number field of degree d, where the smallest prime divisor of d is $\geq B$. Let $E(K)[p^\infty]$ denote the p-primary torsion subgroup of $E(K)_{\text{tors}}$, that is, the p-Sylow subgroup of $E(K)$.*

(i) *If $B \geq 11$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes. In particular, we have $E(K)_{\text{tors}} = E(\mathbb{Q})_{\text{tors}}$.*
(ii) *If $B \geq 7$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 7$.*
(iii) *If $B \geq 5$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 5, 7, 11$.*
(iv) *If $B > 2$, then $E(K)[p^\infty] = E(\mathbb{Q})[p^\infty]$ for all primes $p \neq 2, 3, 5, 7, 11, 13, 19, 43, 67, 163$.*

PROOF OF THEOREM 2.12. By Proposition 2.1, $E_{n,\theta}(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Suppose K is a real number field satisfying the assumptions of Theorem 2.12. By

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

Proposition 2.13(iii), we need only rule out torsion points of order 5, 7 or 11 in $E_{n,\theta}(K)_{\text{tors}}$. We consider the following cases.

5-*torsion*. Suppose, if possible, $R = (x, y)$ is a point of order 5 in $E_{n,\theta}(K)_{\text{tors}}$. We consider the possibilities for the degree of the subextension $\mathbb{Q}(R)$ of K over $\mathbb{Q}$. The Galois group of the normal closure of $\mathbb{Q}(R)$ can be identified with a subgroup of $GL_2(\mathbb{F}_5)$, the general linear group over the finite field of order 5. By the fundamental theorem of Galois theory, $[\mathbb{Q}(R) : \mathbb{Q}]$ must divide $\#GL_2(\mathbb{F}_5) = 2^5 \cdot 3 \cdot 5$. By assumption, $[K : \mathbb{Q}]$ is coprime to 6, but $[\mathbb{Q}(R) : \mathbb{Q}]$ must divide 5 since $\mathbb{Q}(R) \subset K$. Further, $[\mathbb{Q}(R) : \mathbb{Q}] \neq 1$ as $E_{n,\theta}(\mathbb{Q})_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. Therefore, $\mathbb{Q}(R)$ is a quintic extension over $\mathbb{Q}$ and $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ is a subgroup of $E_{n,\theta}(Q(R))_{\text{tors}}$. But González-Jiménez showed that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/10\mathbb{Z}$ cannot appear as a torsion subgroup of a rational elliptic curve over a quintic field [5, Theorem 2]. Therefore, 5-torsion cannot occur over K.

7-*torsion*. Suppose $E_{n,\theta}(K)_{\text{tors}}$ contains a point of order 7, say $R = (x, y)$. By a similar argument to that above, $[\mathbb{Q}(R) : \mathbb{Q}] = 7$. It follows that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ appears as a subgroup of $E_{n,\theta}(\mathbb{Q}(R))_{\text{tors}}$. But González-Jiménez and Najman showed that $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/14\mathbb{Z}$ cannot appear as a torsion subgroup of a rational elliptic curve over a number field of degree 7 [6, Proposition 7.1]. Therefore, 7-torsion cannot occur over K.

11-*torsion*. Suppose $E_{n,\theta}(K)_{\text{tors}}$ contains a point of order 11, say $R = (x, y)$. By arguing as before, we find that $[\mathbb{Q}(R) : \mathbb{Q}]$ divides $5^2 \cdot 11$. Theorem 5.8 of [6] provides a complete list of possibilities for the degree of a number field generated by 11-torsion on a rational elliptic curve, and that list does not include 11, 5^2 and $5^2 \cdot 11$. So we must have either $[\mathbb{Q}(R) : \mathbb{Q}] = 5$ or $[\mathbb{Q}(R) : \mathbb{Q}] = 55$. If $[\mathbb{Q}(R) : \mathbb{Q}] = 5$ then $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$ would appear as a subgroup of $E_{n,\theta}(\mathbb{Q}(R))_{\text{tors}}$. But González-Jiménez has shown that a quintic field cannot have $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/22\mathbb{Z}$ as a subgroup of the torsion of a rational elliptic curve [5, Theorem 2]. If $[\mathbb{Q}(R) : \mathbb{Q}] = 55$ then $[K : \mathbb{Q}]$ is divisible by 55, which contradicts our assumption on the degree of K.

Thus we can conclude that $E_{n,\theta}(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. The theorem now follows from Corollary 2.5. □

2.3. θ-congruent numbers over real cubic fields. After $\theta = \pi/2$, the next natural values to be considered are $\theta = \pi/3$ and $2\pi/3$, since they are rational multiples of π with rational cosine. Fujiwara [3] proved that a prime p is not $\pi/3$-congruent if $p \equiv 5, 7, 19 \pmod{24}$. Kan [10] showed that a prime p is not $2\pi/3$-congruent in case $p \equiv 7, 11, 13 \pmod{24}$ and that primes $p \equiv 23 \pmod{24}$ are $\pi/3$- and $2\pi/3$-congruent over $\mathbb{Q}$. In this subsection we consider angles θ where $\cos\theta = s/r$ and r, s belong to certain congruence classes modulo 5 and obtain the following criterion over real cubic fields.

THEOREM 2.14. *Suppose n is a square-free natural number other than* 1, 2, 3 *or* 6. *Let K be a real cubic number field. Suppose s is divisible by* 5 *or* $(r, s) \equiv (\pm 2, \pm 1)$ *or* $(\pm 1, \pm 2) \pmod 5$. *Then n is a θ-congruent number over K if and only if $E_{n,\theta}(K)$ has a point of infinite order.*

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

In order to prove the theorem, we need to consider the growth of torsion on base change from $\mathbb{Q}$ to a cubic field K. Let d be a positive integer. Let $\Phi(d)$ be the set of possible torsion structures $E(K)_{\text{tors}}$, where K runs through all number fields K of degree d and E runs through all elliptic curves over K. Mazur established that

$$\Phi(1) = \{C_n : n = 1, \ldots, 10, 12\} \cup \{C_2 \times C_{2m} : m = 1, \ldots, 4\},$$

where C_n denotes the cyclic group of order n. Let $\Phi_{\mathbb{Q}}(d)$ be the set of possible torsion structures over a number field of degree d of an elliptic curve defined over $\mathbb{Q}$. Clearly, $\Phi_{\mathbb{Q}}(1) = \Phi(1)$. For each $G \in \Phi(1)$, let $\Phi_{\mathbb{Q}}(d, G)$ denote the set

$$\{E(K)_{\text{tors}} : E/\mathbb{Q} \text{ is an elliptic curve}, E(\mathbb{Q})_{\text{tors}} \simeq G, [K : \mathbb{Q}] = d\}.$$

In order to identify θ-congruent numbers over a number field of degree d, we need to examine $\Phi_{\mathbb{Q}}(d, \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$. We use the following result for a cubic extension of $\mathbb{Q}$.

PROPOSITION 2.15 [7]. *For $G = C_2 \times C_2$,*

$$\Phi_{\mathbb{Q}}(3, G) = \{C_2 \times C_2,\ C_2 \times C_6\}.$$

PROOF OF THEOREM 2.14. The Weierstrass form of a θ-congruent number elliptic curve $E_{n,\theta}$ is given by

$$y^2 = x^3 - 3^3(3r^2 + s^2)n^2x + 2 \cdot 3^3n^3s(9r^2 - s^2) \quad \text{where } \cos\theta = \frac{s}{r}.$$

For a cubic number field K,

$$E_{n,\theta}(K)_{\text{tors}} \simeq C_2 \times C_2 \quad \text{or} \quad E_{n,\theta}(K)_{\text{tors}} \simeq C_2 \times C_6$$

by Proposition 2.15. Our objective is to rule out $E_{n,\theta}(K)_{\text{tors}} \simeq C_2 \times C_6$ under the assumptions on r, s in Theorem 2.14. Suppose, if possible, $E_{n,\theta}(K)_{\text{tors}} \simeq C_2 \times C_6$. Then there is an element in $E_{n,\theta}(K)$ of order 3, say $P = (X, Y)$, where X is a root of the third division polynomial given by

$$\phi(x) = 3x^4 - 162n^2(3r^2 + s^2)x^2 + 648n^3s(9r^2 - s^2)x - 729n^4(3r^2 + s^2)^2. \tag{2.3}$$

It is not difficult to observe that $\phi(3nx) = 3^5n^4f(x)$, where

$$f(x) = x^4 - 6(3r^2 + s^2)x^2 + 8s(9r^2 - s^2)x - 3(3r^2 + s^2)^2 \in \mathbb{Z}[x].$$

Hence $\phi(x)$ has a solution in K if and only if $f(x)$ has a solution in K. Reducing the polynomial $f(x)$ modulo 5, we find that $f(x)$ is equivalent to either $x^4 + 2x^2 + 3$ or $x^4 + 3x^2 + 3 \in \mathbb{Z}/5\mathbb{Z}[x]$ under the assumption of Theorem 2.14. One can easily check that $x^4 + 2x^2 + 3$ and $x^4 + 3x^2 + 3$ are irreducible polynomials over $\mathbb{Z}/5\mathbb{Z}$. Therefore $f(x)$ is irreducible over $\mathbb{Q}$, hence Equation (2.3) does not possess a solution in K as 4 does not divide $[K : \mathbb{Q}]$. The theorem now follows from Corollary 2.5. □

EXAMPLE 2.16. To illustrate the theorem above, let us take $\cos\theta = 5/6$ where $r = 6$ and $s = 5 \equiv 0 \pmod 5$. The corresponding θ-congruent number curve with $n = 7$ is

$$E_{7,\theta} : y^2 = x^3 + 70x^2 - 539x.$$

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

We can verify by using MAGMA that the rank of $E_{7,\theta}(\mathbb{Q})$ is 0, therefore 7 is not a θ-congruent number over $\mathbb{Q}$. By putting $y = 1$, we find that the polynomial $x^3 + 70x^2 - 539x - 1$ has three real roots. If we denote the largest real root by $\alpha \approx 7.0017$, then $K = \mathbb{Q}(\alpha)$ is a real cubic field. The point $(\alpha, 1) \in E_{7,\theta}(K)$ is clearly not a 2-torsion point and hence 7 is θ-congruent over K. By Proposition 2.15,

$$E_{7,\theta}(K)_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \quad \text{or} \quad \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}.$$

Theorem 2.15 rules out the latter possibility, which we directly verify now. Clearly,

$$E_{7,\theta}(K)[2] = E_{7,\theta}(\mathbb{Q}) = \{(0,0),\ (7,0),\ (-77,0), O\}.$$

If the point $(\alpha, 1)$ were a 6-torsion point, then one of $P = (\alpha, 1)$, $Q = (\alpha, 1) + (0, 0)$, $R = (\alpha, 1) + (-77, 0)$ or $S = (\alpha, 1) + (7, 0)$ must be a 3-torsion point. By considering the x-coordinates of the points, it can be easily checked that

$$\begin{aligned} &x(2P) > 208 > x(-P) = \alpha, \\ &x(2Q) = x(2P) > 208 > 0 > x(-Q), \\ &x(2R) = x(2P) > 208 > 0 > x(-R), \\ &x(2S) = x(2P) < 303 < 24000 < x(-S). \end{aligned}$$

Therefore, $2P \neq -P$, $2Q \neq -Q$, $2R \neq -R$ or $2S \neq -S$, and none of P, Q, R or S is a 3-torsion point. Therefore, $P = (\alpha, 1)$ cannot be a 6-torsion on $E_{7,\theta}(K)$ and it must have infinite order.

REMARK 2.17. Suppose K is a real sextic field. It has been conjectured in [2] that $\Phi_{\mathbb{Q}}(6,\ \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z})$ is a subset of

$$\{\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2t\mathbb{Z} : t = 1, 2, 3, 4, 6\} \cup \{\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z},\ \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/12\mathbb{Z}\}.$$

If we put restrictions on (r, s) such that $2r(r - s)$ is a not a square element in K, we can rule out a 4-torsion point on $E_{n,\theta}(K)_{\text{tors}}$ by Lemma 2.7. If we further assume that s is divisible by 5 or $(r, s) \equiv (\pm 2, \pm 1)$ or $(\pm 1, \pm 2)$ mod 5, we can rule out a 3-torsion point on $E_{n,\theta}(K)_{\text{tors}}$ as in Theorem 2.14, noting that 4 does not divide $[K : \mathbb{Q}]$. Therefore, we have $E_{n,\theta}(K)_{\text{tors}} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, and by Corollary 2.5 a square-free integer $n \neq 1, 2, 3, 6$ will be a θ-congruent number over a real sextic field K under the above restrictions over r, s if and only if $E_{n,\theta}(K)$ has positive rank assuming the conjecture.

COROLLARY 2.18. *If a real number field satisfies the assumptions of Theorem 2.2, 2.12 or 2.14, then a number n is (K, θ)-congruent if and only if n is properly (K, θ)-congruent.*

PROOF. For such a field K, by our results, a number n is (K, θ)-congruent if and only if $\text{rank}(E_{n,\theta}(K))$ is positive. Moreover, n is properly (K, θ)-congruent if and only if $E_{n,\theta}$ has a point of infinite order. The corollary follows immediately. □

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

2.4. Questions.

(1) Must a θ-congruent number be properly θ-congruent for all real number fields of degree coprime to 6, if the assumption in Theorem 2.12 that the number field is a Galois extension over $\mathbb{Q}$ when its degree is divisible by 55 is dropped?
(2) For $\cos\theta = s/r \in \mathbb{Q}^\times$, must a θ-congruent number be properly θ-congruent for all real cubic fields, without the congruence conditions on r and s assumed in Theorem 2.14?
(3) Must θ-congruent numbers be properly θ-congruent over a number field K when the degree is not coprime to 6 (not covered by Theorem 2.12)?
(4) Explore the cases $n = 1, 2, 3, 6$ which are not covered by Theorems 2.2, 2.12 and 2.14.

Acknowledgement

The authors would like to thank the anonymous referee for reading the manuscript carefully and making valuable suggestions.

References

[1] J. E. Cremona and P. Serf, 'Computing the rank of elliptic curves over real quadratic number fields of class number 1', *Math. Comp.* **68**(227) (1999), 1187–1200.
[2] H. B. Daniels and E. González-Jiménez, 'On the torsion of rational elliptic curves over sextic fields', *Math. Comp.* **89**(321) (2020), 411–435.
[3] M. Fujiwara, 'θ-congruent numbers', in: *Number Theory: Diophantine, Combinatorial and Algebraic Aspects* (eds. K. Győry, A. Pethő and V. Sós) (de Gruyter, Berlin, 1998), 235–241.
[4] E. Girondo, G. González-Diez, E. González-Jiménez, R. Steuding and J. Steuding, 'Right triangles with algebraic sides and elliptic curves over number fields', *Math. Slovaca* **59**(3) (2009), 299–306.
[5] E. González-Jiménez, 'Complete classification of the torsion structures of rational elliptic curves over quintic number fields', *J. Algebra* **478** (2017), 484–505.
[6] E. González-Jiménez and F. Najman, 'Growth of torsion groups of elliptic curves upon base change', *Math. Comp.* **89**(323) (2020), 1457–1485.
[7] E. González-Jiménez, F. Najman and J. M. Tornero, 'Torsion of rational elliptic curves over cubic fields', *Rocky Mountain J. Math.* **46**(6) (2016), 1899–1917.
[8] A. S. Janfada and S. Salami, 'On θ-congruent numbers on real quadratic number fields', *Kodai Math. J.* **38**(2) (2015), 352–364.
[9] T. Jędrzejak, 'Congruent numbers over real number fields', *Colloq. Math.* **128**(2) (2012), 179–186.
[10] M. Kan, 'θ -congruent numbers and elliptic curves', *Acta Arith.* **94**(2) (2000), 153–160.
[11] A. W. Knapp, *Elliptic Curves*, Mathematical Notes, 40 (Princeton University Press, Princeton, NJ, 1992).
[12] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Graduate Texts in Mathematics, 97 (Springer-Verlag, New York, 1984).
[13] P. Monsky, 'Mock Heegner points and congruent numbers', *Math. Z.* **204**(1) (1990), 45–67.
[14] F. Najman, 'Torsion of rational elliptic curves over cubic fields and sporadic points on $X_1(n)$', *Math. Res. Lett.* **23**(1) (2016), 245–272.
[15] D. Prasad and C. S. Yogananda, 'Bounding the torsion in CM elliptic curves', *C. R. Math. Acad. Sci. Soc. R. Can.* **23**(1) (2001), 1–5.
[16] D. Qiu and X. Zhang, 'Elliptic curves and their torsion subgroups over number fields of type $(2, 2, \ldots, 2)$', *Sci. China Ser. A* **44**(2) (2001), 159–167.

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press

[17] A. Silverberg, 'Points of finite order on abelian varieties', in: *p-Adic Methods in Number Theory and Algebraic Geometry*, Contemporary Mathematics, 133 (American Mathematical Society, Providence, RI, 1992), 175–193.
[18] M. Tada, 'Congruent numbers over real quadratic fields', *Hiroshima Math. J.* **31**(2) (2001), 331–343.
[19] Y. Tian, 'Congruent numbers and Heegner points', *Camb. J. Math.* **2**(1) (2014), 117–161.
[20] J. B. Tunnell, 'A classical Diophantine problem and modular forms of weight 3/2', *Invent. Math.* **72**(2) (1983), 323–334.

SHAMIK DAS, Department of Mathematics,
Indian Institute of Technology Guwahati, Guwahati-781039, Assam, India
e-mail: shamikdas@iitg.ac.in

ANUPAM SAIKIA, Department of Mathematics,
Indian Institute of Technology Guwahati, Guwahati-781039, Assam, India
e-mail: a.saikia@iitg.ac.in

https://doi.org/10.1017/S0004972720000672 Published online by Cambridge University Press