Some properties of θ-congruent numbers

Masahiko FUJIWARA
Department of Mathematics, Ochanomizu University

(Received December 5, 2001)

Abstract

The concept of θ-congruent numbers was first introduced by myself as a generalization of classical congruent numbers. Since then, several interesting properties have been found. This paper gives still further theorems related to θ-congruent numbers.

1 Introduction

A natural number n is called a congruent number if it is the area of a right triangle with rational sides. A lot of studies have been made on congruent numbers. Particularly, the recent approach through elliptic curves brought about some beautiful results ([4], [5], [7]).

Of special interest is the fact that square free natural numbers n congruent to 5, 6 or 7 modulo 8 are always congruent numbers, provided that the weak Birch and Swinnerton-Dyer conjecture is true.

The concept of congruent numbers was first generalized to θ-congruent numbers connected to arbitrary triangles with rational sides in [1].

Let us review the definition of θ-congruent numbers. Suppose that there is a triangle with rational sides X, Y, Z. Denote by θ the angle between X and Y. $\cos\theta$ is necessarily rational. Thus $\cos\theta = \frac{s}{r}$ $(r > 0, (r, s) = 1)$. Then $\sin\theta = \frac{\alpha_\theta}{r}$ where $\alpha_\theta = \sqrt{r^2 - s^2}$ is uniquely determined by θ. We now define θ-congruent numbers as follows:

Definition 1 *A natural number n is a θ-congruent number if there exists a triangle such that*

1. *three sides are rational*
2. *one angle is θ*
3. *the area is $n\alpha_\theta$*

A θ-congruent number for $\theta = \frac{\pi}{2}$ is nothing but an ordinary congruent number, since $\alpha_{\frac{\pi}{2}} = 1$. Thus 6 is a $\frac{\pi}{2}$-congruent number, since 6 is the area of the right triangle with $X = 3$, $Y = 4$, $Z = 5$. 1 is a $\frac{\pi}{3}$-congruent number since $\alpha_{\frac{\pi}{3}} = \sqrt{3}$ and $\sqrt{3}$ is the area of the equilateral triangle with $X = Y = Z = 2$. As a little more complicated example, 19 is $\frac{2\pi}{3}$-congruent since $\alpha_{\frac{2\pi}{3}} = \sqrt{3}$ and $19\sqrt{3}$ is the area of the triangle with $X = \frac{544}{105}$, $Y = \frac{1995}{136}$, $Z = \frac{254659}{14280}$.

Obviously n is θ-congruent if and only if nk^2, for some integer k, is θ-congruent. Therefore, henceforth we assume n square free and also assume that θ has rational cosine unless otherwise stated.

We introduced the following elliptic curve attached to n and θ ([1]):

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

Several theorems on θ-congruent numbers have been proved by way of this $E_{n,\theta}$. To mention a few, for any θ and $n(\neq 1, 2, 3, 6)$, n is θ-congruent if and only if $E_{n,\theta}(\mathbb{Q})$ has a positive rank ([1]). A prime p is not $\frac{\pi}{3}$-congruent (resp. not $\frac{2\pi}{3}$-congruent) if p is 5, 7 or 19 (resp. 7, 11 or 13) modulo 24 ([1], [2]), and is both $\frac{\pi}{3}$ and $\frac{2\pi}{3}$-congruent if $p \equiv 23 \pmod{24}$ ([2], [3]).

In the following, $E(\mathbb{Q})_{\mathrm{tor}}$ denotes the group of points of finite order in $E(\mathbb{Q})$. Our main results in the present paper are as follows, where Theorem 1 is a version of a theorem due to my student Miss M. Otsuka.

Theorem 1 *Let E be an elliptic curve defined by*

$$E\ :\ y^2 = x(x+A)(x+B)$$

where A, B are integers with $B < 0 < A$. Then

(I) $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_8$ *if and only if there exist integers $a, b, k > 0$ such that a and b are coprime, of opposite parity, and satisfy either of the following:*

(i) $-B = k^2(a^2-b^2)^4,\ \ A-B = 16k^2a^4b^4,\ \ (1+\sqrt{2})b > a > b$

(ii) $-B = 16k^2a^4b^4,\ \ A-B = k^2(a^2-b^2)^4,\ \ a > (1+\sqrt{2})b$

(II) $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$ *if and only if there exist integers $u, v, k > 0$ such that*

$(u,v) = 1,\quad u > 2v \quad$ *and* $\quad A = u^3(u-2v)k^2,\quad B = v^3(v-2u)k^2$

(III) $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$ *if and only if $-B$ and $A-B$ are squares but not satisfy* (I)

(IV) $E(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$, *otherwise.*

Applying the above theorem to our $E_{n,\theta}$, we have

Theorem 2 (I) $E_{n,\theta}(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_8$ *if and only if there exist integers $a, b > 0$ such that a and b are coprime, of opposite parity, and satisfy either of the following:*

(i) $n = 1,\ \ r = 8a^4b^4,\ \ r - s = (a^2-b^2)^4,\ \ (1+\sqrt{2})b > a > b$

(ii) $n = 2,\ \ r = (a^2-b^2)^4,\ \ r - s = 32a^4b^4,\ \ a > (1+\sqrt{2})b$

(II) $E_{n,\theta}(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6$ *if and only if there exist integers $u, v > 0$ such that $(u,v) = 1$, $u > 2v$ and satisfy either of the following:*

(i) $n = 1,\ \ r = \frac{1}{2}(u-v)^3(u+v),\ \ r + s = u^3(u-2v)$

(ii) $n = 2,\ \ r = (u-v)^3(u+v),\ \ r + s = 2u^3(u-2v)$

(iii) $n = 3,\ \ r = \frac{1}{6}(u-v)^3(u+v),\ \ r + s = \frac{1}{3}u^3(u-2v)$

(iv) $n = 6,\ \ r = \frac{1}{3}(u-v)^3(u+v),\ \ r + s = \frac{2}{3}u^3(u-2v)$

(III) $E_{n,\theta}(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_4$ *if and only if either of the following folds:*

(i) $n = 1$, $2r$ *and* $r - s$ *are squares but not satisfy* (i) *of* (I)

(ii) $n = 2$, r *and* $2(r-s)$ *are squares but not satisfy* (ii) *of* (I)

(IV) $E_{n,\theta}(\mathbb{Q})_{\mathrm{tor}} \simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2$, *otherwise.*

This theorem naturally gives rise to the following corollary that supplements Theorem 1 of [1].

Corollary *For those* $n = 1, 2, 3, 6$ *and* θ *prescrived in* (I), (II), (III) *of Th.2,* n *is* θ*-congruent. For all the other* n *and* θ, n *is* θ*-congruent if and only if* $E_{n,\theta}(\mathbb{Q})$ *has a positive rank.*

The following theorem is a generalization of Theorem 2 in [1] and signifies abundance of θ-congruent numbers.

Theorem 3 *For any* θ*, there exist infinitely many* θ*-congruent numbers in any arithmetic progression.*

The θ-congruent numbers in Theorem 3 can not always be square free, since, for example, integers congruent to 4 mod 8 are divisible by 4. The following theorem gives Diophantine approximation to arbitrary angle θ by $\theta_{r,s}$ for which given n, not necessarily square free, is $\theta_{r,s}$-congruent.

Theorem 4 *For any integer* $n > 0$ *and any* $\theta \in (0, \pi)$*, there exist infinitely many integers* r *and* s *such that*

$$r > 0, \quad (r, s) = 1, \quad r > |s|, \quad n \ \textit{ is } \ \theta_{r,s} - \textit{congruent and} \ \ |\theta_{r,s} - \theta| < \frac{c(\theta)}{r}$$

where $\cos\theta_{r,s} = \dfrac{s}{r}$, $c(\theta) = \dfrac{9}{\sin\theta}$.

Corollary *For any integer* $n > 0$, $\{\theta \in (0, \pi); n \textit{ is } \theta\textit{-congruent}\}$ *is dense in* $(0, \pi)$.

2 Proofs of Theorem 1 and Theorem 2

We first give two preliminary lemmas necessary to prove Theorem 1.

Lemma 1 (well-known [4], [5]) *Let* E *be an elliptic curve defined by*

$$E \ : \ y^2 = (x - \alpha)(x - \beta)(x - \gamma)$$

with $\alpha, \beta, \gamma \in \mathbb{Q}$*. Let* $P = (x_0, y_0)$ *be a point in* $E(\mathbb{Q})$*. Then* $P \in 2E(\mathbb{Q})$ *if and only if* $x_0 - \alpha, x_0 - \beta, x_0 - \gamma \in \mathbb{Q}^2$.

Lemma 2 *Let* E *be an elliptic curve in Theorem 1 and* $P = (x_0, y_0)$ *be a point in* $E(\mathbb{Q})$*. Then*

(I) *x-coordinate of* $2P = \dfrac{1}{4}\left(\dfrac{y_0}{x_0 + A} + \dfrac{y_0}{x_0 + B} - \dfrac{y_0}{x_0}\right)^2$

(II) *Suppose* (A, B) *square free, then* $P \in 2E(\mathbb{Q})_{\mathrm{tor}}$ *if and only if* $\dfrac{|y_0|}{x_0}, \dfrac{|y_0|}{x_0 + A}, \dfrac{|y_0|}{x_0 + B} \in \mathbb{Z}^2$.

Proof of lemma 2. Note first that

$$x_0 = \frac{y_0^2}{(x_0 + A)(x_0 + B)}, \quad x_0 + A = \frac{y_0^2}{x_0(x_0 + B)}, \quad x_0 + B = \frac{y_0^2}{x_0(x_0 + A)} \qquad (*)$$

(I) By addition formula, x-coordinate of $2P = (\dfrac{dy}{dx})_{x_0}^2 - (A + B) - 2x_0$. It is easy to show

$$\left(\frac{dy}{dx}\right)_{x_0} = \frac{1}{2}\left(\frac{y_0}{x_0 + A} + \frac{y_0}{x_0 + B} + \frac{y_0}{x_0}\right).$$

Taking $(*)$ into account, straightforward computation leads to the formula in (I).
(II) If $P \in 2E(\mathbb{Q})_{\text{tor}}$, then by lemma 1 and Lutz-Nagell theorem, $x_0, x_0+A, x_0+B \in \mathbb{Z}^2$. Therefore $\frac{y_0}{x_0}$, $\frac{y_0}{x_0+A}, \frac{y_0}{x_0+B} \in \mathbb{Z}$.

Remark that these three integers are pairwise coprime; in fact, suppose there exists a prime p dividing $(\frac{y_0}{x_0}, \frac{y_0}{x_0+A})$. Then from $(*)$, p divides x_0, x_0+A, x_0+B. It follows that p^2 divides x_0, x_0+A, x_0+B and therefore p^2 divides A and B, contradicting (A, B) being square free. Similarly, $(\frac{y_0}{x_0}, \frac{y_0}{x_0+B}) = (\frac{y_0}{x_0+A}, \frac{y_0}{x_0+B}) = 1$, as claimed.

Therefore, by $(*)$ again, we have the desired conclusion. We can follow the above argument backwards to prove the converse.

Proof of Theorem 1. Owing to Mazur's theorem on the structure of torsion group ([6]), $E(\mathbb{Q})_{\text{tor}}$ is isomorphic to either $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_4$, $\mathbb{Z}_2 \oplus \mathbb{Z}_6$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_8$, since $E(\mathbb{Q})_{\text{tor}}$ obviously contains $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.
(I)$\Leftarrow$) We have only to show existence of a point of order 8 in $E(\mathbb{Q})$. Put v (resp. w in case (ii))$= a^2-b^2$ and w (resp. v in case (ii))$= 2ab$. Then in both (i) and (ii), $v^2+w^2 = u^2$ for some integer u and $A = k^2(w^4-v^4)$, $B = -k^2v^4$. Put $P = (k^2u^2v^2, k^3u^2v^2w^2)$. Then direct computation shows that $P \in E(\mathbb{Q})$. Moreover

$$x_0 + A = k^2u^2v^2 + k^2(w^4 - v^4) = k^2w^2u^2, \quad x_0 + B = k^2u^2v^2 - k^2v^4 = k^4v^2w^2.$$

Therefore by lemma 1,

$$P \in 2E(\mathbb{Q}) \text{ and } \frac{y_0}{x_0} = kw^2, \quad \frac{y_0}{x_0+A} = kv^2, \quad \frac{y_0}{x_0+B} = ku^2.$$

By (I) of lemma 2, x coordinate of $2P = \frac{1}{4}(kv^2+ku^2-kw^2)^2 = k^2v^4 = -B$. Consequently $2P = (-B, 0)$ and order of P is 4.
$\Rightarrow$) Let E^* be an elliptic curve defined by $y^2 = x(x+\frac{A}{k^2})(x+\frac{B}{k^2})$ where k^2 is the square part of (A, B). Since $E(\mathbb{Q}) \simeq E^*(\mathbb{Q})$, there exists a point $P = (x_0, y_0)$ in $2E^*(\mathbb{Q})$ of order 4 and $y_0 > 0$. As $2P$ has order 2 and $B < 0 < A$, due to lemma 1, we obtain $2P = (-\frac{B}{k^2}, 0)$. By (II) of lemma 2, putting $\frac{y_0}{x_0} = w^2, \frac{y_0}{x_0+\frac{A}{k^2}} = v^2$ and $\frac{y_0}{x_0+\frac{B}{k^2}} = u^2$ for some positive integers u, v, w,

$$\frac{1}{4}(v^2+u^2-w^2) = x\text{-coordinate of } 2P = -\frac{B}{k^2} = x_0 - (x_0 + \frac{B}{k^2}) = v^2u^2 - w^2v^2.$$

It follows that $(v^2+w^2-u^2)^2 = 0$ and therefore $u^2 = v^2+w^2$. This in turn implies that

$$\frac{B}{k^2} = v^2w^2 - v^2u^2 = -v^4, \quad \frac{A}{k^2} = u^2w^2 - u^2v^2 = u^2(w^2-v^2) \text{ and } \frac{A-B}{k^2} = u^2(w^2-v^2) + v^2(u^2-w^4) = w^4.$$

Consequently $(v, w) = 1$. Thus, v, w and u are Pythagorean triple and therefore $v = a^2-b^2$ (resp. $2ab$) and $w = 2ab$ (resp. a^2-b^2) for some integers a, b with $(a, b) = 1$, $a > b > 0$, of opposite parity. Here

$$\begin{aligned} A > 0 > B &\Leftrightarrow w > v > 0 \\ &\Leftrightarrow 2ab > a^2 - b^2 > 0 \text{ (resp. } a^2-b^2 > 2ab) \\ &\Leftrightarrow (1+\sqrt{2})b > a > b \text{ (resp. } a > (1+\sqrt{2})b), \end{aligned}$$

as mentioned in (i) and (ii) of (I).
(II)$\Leftarrow$) Put $P = (u^2v^2k^2, u^2v^2(u-v)^2k^3)$. We have only to prove that P is of order 3. It is straightforward, by using $A = u^3(u-2v)k^2$ and $B = v^3(v-2u)k^2$, that P is on $E(\mathbb{Q})$. On the other hand, $x_0 + A = u^2v^2k^2 + u^3(u-2v)k^2 = u^2(u-v)^2k^2$ and similarly $x_0 + B = v^2(u-v)^2k^2$. It follows that

$$\frac{y_0}{x_0} = (u-v)^2k, \quad \frac{y_0}{x_0+A} = v^2k \text{ and } \frac{y_0}{x_0+B} = u^2k.$$

Using (I) of lemma 2,

$$x-\text{coordinate of } 2P=\frac{1}{4}(u^2k+v^2k-(u-v)^2k)^2=u^2v^2k^2=x_0.$$

Thus, order of $P=3$.
$\Rightarrow$) Let E^* be an elliptic curve defined by $E^*\ :\ y^2=x(x+\frac{A}{k^2})(x+\frac{B}{k^2})$ where k^2 is the square part of (A,B). Since $E(\mathbb{Q})\simeq E^*(\mathbb{Q})$, there exists a point $P=(x_0,y_0)\in 2E^*(\mathbb{Q})$ of order 3 and $y_0>0$. By (II) of lemma 2, $\frac{y_0}{x_0}=w^2$, $\frac{y_0}{x_0+\frac{A}{k^2}}=v^2$ and $\frac{y_0}{x_0+\frac{B}{k^2}}=u^2$ for some positive integers u,v,w. Because x-coordinate of $2P$ is x_0, by (I) of lemma 2, $\frac{1}{4}(v^2+u^2-w^2)^2=x_0=u^2v^2$. Therefore $u^2+v^2-w^2=\pm 2uv$. Thus $(u\mp v)^2=w^2$.

Since $\frac{B}{k^2}=(x_0+\frac{B}{k^2})-x_0=v^2w^2-u^2v^2=v^3(v\mp 2u)$ and $B<0$, $(u-v)^2=w^2$ and $\frac{B}{k^2}=v^3(v-2u)$. $\frac{A}{k^2}=u^2w^2-u^2v^2=u^3(u-2v)$. Note that $u>2v$ since $B<0<A$. Since $(\frac{A}{k^2},\frac{B}{k^2})$ is square free, $(u,v)=1$.
(III) There exists a point of order 4 in $E(\mathbb{Q})$ if and only if $(-B,0)\in 2E(\mathbb{Q})$, since $(0,0)$ and $(-A,0)$ can not belong to $2E(\mathbb{Q})$ owing to lemma 1. This in turn is equivalent to $-B, A-B\in\mathbb{Z}^2$, owing again to lemma 1. Taking (I) into account, the proof of (III) is finished. (q.e.d.)

Proof of Theorem 2. We apply Th.1 to our curve $E_{n,\theta}$ where $A=(r+s)n$ and $B=-(r-s)n$. We first remark that $r>|s|$ if and only if $A>0>B$. We also note here that, for our $E_{n,\theta}$, (I) or (III) in Th.1 takes place only when $n=1$ or 2; in fact, since $-B=(r-s)n$ and $A-B=2rn$ are squares, we can write $(r-s)n=t^2$, $2rn=m^2$ for some integers r,m. Suppose an odd prime p divides n, then p divides both t and m. Consequently, n being square free, p divides r and s. This implies $n=1$ or 2.
(I) In both (i) and (ii) of (I) in Th.1, there exist positive integers u,v,w,k such that $-B=(r-s)n=k^2v^4$, $A-B=2rn=k^2w^4$, $v^2+w^2=u^2$, $(v,w)=1$.
<u>subcase $n=1$.</u> We have

$$-B=r-s=k^2v^4,\quad A-B=2r=k^2w^4,\quad v^2+w^2=u^2.$$

Here k has to be equal to 1 since, if a prime p divides k, p divides r and s. Since w is clearly even, (i) of (I) in Th.1 must occur and obtain (i) in Th.2.
<u>subcase $n=2$.</u> We have

$$-B=2(r-s)=k^2v^4,\quad A-B=4r=k^2w^4,\quad v^2+w^2=u^2,\quad (v,w)=1,$$

in both (i) and (ii) of (I). If an odd prime p (resp. 4) divides k, then p (resp. 2) divides r and s. Therefore k must be 1 or 2. If $k=1$, then 2 divides v and w, which contradicts $(v,w)=1$. It follows that $k=2$ and we have

$$-B=2(r-s)=4v^4,\ A-B=4r=4w^4,\ v^2+w^2=u^2.$$

Hence, w must be odd and (ii) of (I) in Th.1 must occur, leading to (ii) of (I) in Th.2.
(III) $-B=(r-s)n$ and $A-B=2rn$ are squares but not satisfy (I). Since n is 1 or 2 as was mentioned in the beginning of the proof of Th.2, we have either

$$\begin{aligned} &n=1, \qquad -B=r-s \text{ and } A-B=2r, \qquad \text{or}\\ &n=2, \qquad -B=2(r-s) \text{ and } A-B=4r, \end{aligned}$$

corresponding respectively to (i) or (ii) of (I) in Th.2.
(II) From (II) of Th.1, there are integers $u,v,k>0$ such that

$$A=(r+s)n=u^3(u-2v)k^2,\ B=-(r-s)n=v^3(v-2u)k^2,\ (u,v)=1,\ u>2v>0.$$

Subtraction leads to $2rn=k^2(u-v)^3(u+v)$. Since k^2 divides $(r+s)n$ and $2rn$, n being square free and $(r,s)=1$, we conclude that $k=1$ or 2.

subcase $k=1$. W have

$$(r+s)n = u^3(u-2v), \quad -(r-s)n = v^3(v-2u) \ \text{ and } \ 2rn = (u-v)^3(u+v), \quad (u,v)=1, \quad u > 2v > 0.$$

We claim here that $n=1$ or 3 in our case. In fact, let p be a prime dividing u, then p does not divide n. That is, $(u,n)=1$. This implies u^3 divides $r+s$. Similarly we can show that $(v,n)=1$ and v^3 divides $r-s$. It follows that n divides both $u-2v$ and $v-2u$, hence divides $3(u-v)$. It is easy to see that n does not divides $u-v$. Therefore $n=1$ or 3 as claimed.

Consequently we have

- $n=1, \ r+s = u^3(u-2v), \ 2r = (u-v)^3(u+v)$ or
- $n=3, \ 3(r+s) = u^3(u-2v), \ 6r = (u-v)^3(u+v)$.

These respectively correspond to (i) or (iii) of (II) in Th.2.
subcase $k=2$. We have

$$(r+s)n = 4u^3(u-2v), \quad -(r-s)n = 4v^3(v-2u), \quad 2rn = 4(u-v)^3(u+v), \quad (u,v)=1, \quad u > 2v > 0.$$

We claim here that $n=2$ or 6 in our case. In fact, let p be an odd prime dividing u, then p does not divide n. Namely, $(u,n)=1$ or 2. Similarly $(v,n)=1$ or 2. n must be even since, otherwise 2 divides r and s. Putting $n=2m$, m is obviously odd. m divides both $u-2v$ and $v-2u$, thus dividing $3(u-v)$. It is easy to see that m does not divide $u-v$. Consequently $m=1$ or 3 and $n=2$ or 6 as claimed.

Therefore we have

- $n=2, \ r+s = 2u^3(u-2v), \ r = (u-v)^3(u+v)$ or
- $n=6, \ r+s = \frac{2}{3}u^3(u-2v), \ r = \frac{1}{3}(u-v)^3(u+v)$.

These respectively correspond to (ii) or (iv) of (II) in Th.2. (q.e.d.)

3 Proofs of Theorem 3 and Theorem 4

We need the following lemma of Kan for the proofs.

Lemma 3 ([1], [2]) *A square free natural number n is θ-congruent if and only if there exist natural numbers (p,q) with $(p,q)=1$ such that n =square free part of $pq(p+q)(2rq+p(r-s))$.*

(Remark) It turns out, by examining the proof of the lemma, that r and s need not be coprime, and p and q neither, in lemma 3.

Proof of Theorem 3. Let θ be as in Th.3 and m be any natural number. As is usual, $\cos\theta = \dfrac{s}{r}$, $r > |s|$, $(r,s)=1$. Let c be an integer $0 < c \le m$. Let q be a positive integer defined by $q = cm^2(r-s)$ and p be a prime defined by $p = 1+tq$, where t is to be determined later. We note that p and q are coprime. Let n be a natural number defined by

$$n = \frac{pq(p+q)(2rq+p(r-s))}{m^2(r-s)^2}.$$

By lemma 3, though n may not be square free, n is still a θ-congruent number. Moreover, by substitution, we can easily show that

$$n = c(1+tq)(1+tq+cm^2(r-s))(2rcm^2+1+tq) \equiv c \pmod{m}.$$

Owing to Dirichlet's theorem on primes in arithmetic progressions, there exist infinitely many integers t that make our p primes. Since these primes p, as long as $p > 2r$, obviously divide n, we have infinitely many θ-congruent numbers n such that $n \equiv c \,(\mathrm{mod}\, m)$. This completes our proof. (q.e.d.)

Proof of Theorem 4. By Dirichlet's pigeon hole principle, there exist infinitely many integers $a, b > 0$ such that $|\frac{3-\cos\theta}{2n} - \frac{b}{a}| < \frac{1}{a^2}$. Here we put $r = ab+1$. Obviously $r > 0$ and

$$|\frac{3-\cos\theta}{2n} - \frac{b^2}{r}| \leq |\frac{3-\cos\theta}{2n} - \frac{b}{a}| + |\frac{b}{a} - \frac{b^2}{ab+1}| < \frac{1}{a^2} + \frac{b}{a(ab+1)} = \frac{1}{ab+1}(\frac{2b}{a} + \frac{1}{a^2}).$$

For any $\epsilon > 0$, $\frac{b}{a} + \frac{1}{2a^2} < \frac{3-\cos\theta+\epsilon}{2n}$ for all sufficiently large a. Therefore

$$|\frac{3-\cos\theta}{2n} - \frac{b^2}{r}| < \frac{3-\cos\theta+\epsilon}{nr}.$$

Now define s by $s = 3r - 2nb^2$. Here we claim that $r > |s|$ and n is $\theta_{r,s}$-congruent. In fact, from above inequality,

$$|r(3-\cos\theta) - 2nb^2| < 2(3-\cos\theta+\epsilon) < 8.$$

Therefore, for large r, we have

$$-r < r\cos\theta - 8 < 3r - 2nb^2 < r\cos\theta + 8 < r.$$

Hence $r > |s|$. Put $p = r$ and $q = nb^2 - r$ in lemma 3. Then it is easy to see that

$$pq(p+q)(2rq + p(r-s)) = 4np^2q^2b^2.$$

Considering the remark after lemma 3, n is $\theta_{r,s}$-congruent. On the other hand,

$$|\cos\theta_{r,s} - \cos\theta| = |\frac{s}{r} - \cos\theta| = |\frac{3r-2nb^2}{r} - \cos\theta| = 2n|\frac{3-\cos\theta}{2n} - \frac{b^2}{r}| < 2n\frac{3-\cos\theta+\epsilon}{nr} < \frac{8}{r}.$$

Using mean value theorem, putting $\theta_{r,s} - \theta = \alpha$ for brevity,

$$\cos\theta_{r,s} - \cos\theta = -\alpha\sin(\theta + t\alpha) \text{ for some } 0 < t < 1. \qquad (*)$$

Again, by mean value theorem

$$\sin(\theta + t\alpha) = \sin\theta + t\alpha\cos(\theta + t't\alpha) \text{ for some } 0 < t' < 1.$$

As r tends to ∞, from the above inequality, $\cos\theta - \cos\theta_{r,s}$ tends to 0. This in turn implies $\theta_{r,s} - \theta = \alpha$ tends to 0. Thus $|t\alpha\cos(\theta + t't\alpha)|$ tends to 0 and therefore, for any $\epsilon' > 0$, we have for large r, $|\sin(\theta + t\alpha)| > (1-\epsilon')\sin\theta$. Consequently by $(*)$, $|\cos\theta_{r,s} - \cos\theta| > (1-\epsilon')|\theta_{r,s} - \theta|\sin\theta$ and hence, by $(*)$ again $\frac{8}{r(1-\epsilon')\sin\theta} > |\theta_{r,s} - \theta|$. Therefore we obtained the inequality in Th.4.

It only remains to prove $(r, s) = 1$. Let d be the greatest common divisor of r and s. Then obviously $d = (r, s) = (r, 2n)$ by our choice of r and s. That is to say, d is a divisor of $2n$. For those infinitely many r and s chosen above, we put $r' = \frac{r}{d}$ and $s' = \frac{s}{d}$. Then we have still infinitely many r' and s' with $(r', s') = 1$ such that r' and s' satisfy all the conditions in Th.4. (q.e.d.)

References

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

[2] Kan, M., *θ-congruent numbers and elliptic curves*, Acta Arithmetica, XCIV.**2**, 2000, 153–160.

[3] Hibino, T. and Kan, M., *θ-congruent numbers and Heegner points*, to appear in Archiv der mathematik.

[4] Knapp, A.W., Elliptic curves, Princeton University Press, Princeton, 1993.

[5] Koblitz, N., Introduction to elliptic curves and modular forms, Springer Verlag, New York-Berlin-Heidelberg, 1984.

[6] Silverman, J.H., The arithmetic of elliptic curves, Springer Verlag, New York-Berlin-Heidelberg, 1986.

[7] Tunnel, J.B., *A classical Diophantine problem and modular forms of weights* $\frac{3}{2}$, Invent. math. **72**, 1983, 323–334.