J. Math. Anal. Appl. 462 (2018) 407–427

Contents lists available at ScienceDirect

Journal of Mathematical Analysis and Applications

www.elsevier.com/locate/jmaa

A parametrization of θ-congruent numbers with many prime factors and with prescribed prime factors ☆

Bo-Hae Im *, Hansol Kim

Department of Mathematical Sciences, KAIST, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, South Korea

ARTICLE INFO

Article history:
Received 14 August 2017
Available online 6 February 2018
Submitted by B. Bongiorno

Keywords:
Elliptic curve
Congruent number
θ-congruent number

ABSTRACT

Let θ be a real number such that $0 < \theta < \pi$ and $\cos\theta \in \mathbb{Q}$. For each positive integer n, we give a parametrization $S_n(\alpha)$ whose square-free part $N_n(\alpha)$ for each negative integer α is a θ-congruent number with many prime factors including any given primes (especially, at least n prime factors that are guaranteed to appear) by showing the positivity of the rank of the corresponding θ-congruent number elliptic curve over $\mathbb{Q}$. Especially, we show that if a given odd prime $p > 2n$ is near $2n$, then p appears as a factor of $N_n(\alpha)$ very often as α varies all over negative integers by proving that the probability of the set of all negative integers α such that p divides $N_n(\alpha)$ is $\frac{2n+1}{p+1}$.

1. Introduction

A congruent number is a square-free positive integer that is the area of a right triangle with rational sides. The classification of congruent numbers called *the congruent number problem* has been an open question. Tunnell [14] has given some criteria for non-congruent numbers, which are implied by the non-vanishing of the Fourier coefficients of some modular forms of weight 3/2, and Heegner [6], Birch [1] and Monsky [11] have proved that for each $i = 3, 5, 7$, if q_i denotes a prime such that $q_i \equiv i \pmod 8$, then

$$q_5,\ q_7,\ 2q_3,\ 2q_7,\ q_3q_7,\ q_3q_5,\ 2q_3q_5 \text{ and } 2q_5q_7$$

are congruent numbers. Recently Tian [13] has proved that for each positive integer k, there are infinitely many congruent numbers with k prime factors. More precisely, it has been proved in [13] that for a given $e \in \{3, 5, 7\}$, if $p_0 \equiv e \pmod 8$ and $p_i \equiv 1 \pmod 8$ for $i = 1, \ldots, k-1$ and the imaginary quadratic field $\mathbb{Q}(\sqrt{-n})$ where $n = p_0p_1 \cdots p_{k-1}$ has no ideal classes of exact order 4, then n is a congruent number.

☆ This work is supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (NRF-2017R1A2B4002619).

* Corresponding author.
E-mail addresses: bhim@kaist.ac.kr (B.-H. Im), jawlang@kaist.ac.kr (H. Kim).

https://doi.org/10.1016/j.jmaa.2018.01.068
0022-247X/

As a generalization of a congruent number, we recall the definition of a θ-congruent number where $\cos\theta$ is a rational number.

Definition 1.1. For a real number θ such that $0 < \theta < \pi$ and $\cos\theta = \frac{s}{r}$ with $r, s \in \mathbb{Z}$ and $r > 0$, a square-free positive integer n is *a θ-congruent number* if $n\sqrt{r^2 - s^2}$ is the area of a triangle with rational sides and angle θ. A $\frac{\pi}{2}$-congruent number (i.e. $r = 1$, and $s = 0$) is *a congruent number.*

It has been known that there is an equivalent condition between θ-congruent numbers n and the positive rank of the elliptic curves E_n defined as follows.

Theorem 1.2. *([2],[4]) For $n \neq 1, 2, 3, 6$, n is a θ-congruent number if and only if $E_n : y^2 = x(x + (r + s)n)(x - (r - s)n)$ has positive rank over $\mathbb{Q}$. In particular, if $r = 1$ and $s = 0$, then n is a congruent number if and only if the rank of $E_n(\mathbb{Q})$ is positive.*

For $\cos\theta = \frac{s}{r}$, an elliptic curve E_n defined in Theorem 1.2 is called *a θ-congruent number elliptic curve.*

In [7], the first author has given a parametrization of θ-congruent numbers and their distribution as follows.

Theorem 1.3. *[7, Corollary 15] Let $\cos\theta = \frac{s}{r}$ with $\gcd(r, s) = 1$ and let $d = \gcd(r - s, r + s)$ and write $r + s = \ell d$ and $r - s = -kd$ and let ℓ' be the square-free part of ℓ. Then for each of infinitely many integers $t \in \mathbb{Z}$ such that $t > \frac{\ell - k}{\ell}$ and $\gcd(t - 1, k) = 1$, the square-free parts of the values of dS_t where*

$$S_t := -\ell'(\ell t + k)(\ell t + k - \ell)(\ell(k - \ell)t + k^2 - k\ell + \ell^2)$$

are distinct θ-congruent numbers, and if we let $S'_t = \begin{cases} dS_t, & \text{if } d = 2 \text{ and } d \nmid \ell', \\ S_t/d, & \text{otherwise,} \end{cases}$ then for sufficiently large N,

$$\#\{t \in [1, N] \mid S'_t \text{ is a } \theta\text{-congruent number}\} = cN + \mathcal{O}(N^{2/3+\epsilon}),$$

where $c > 0$ and ϵ is an arbitrary small positive number, if this number is non-zero.

Our main results in this paper are Theorem 2.4, Proposition 3.2 and Theorem 3.3. We have been motivated by Tian's result [13] on congruent numbers mentioned earlier and the first named author's result in Theorem 1.3, and by extending them to θ-congruent numbers, for each positive integer n, we give a parametrization $S_n(t) \in \mathbb{Z}[t]$ given in (1) whose square-free parts $N_n(\alpha)$ for all negative integers α are θ-congruent numbers with many prime factors, especially, at least n prime factors that are guaranteed to appear as proved in Theorem 2.4. This new parametrization $N_n(\alpha)$ gives θ-congruent numbers for every negative integer α while the parametrization S_t in Theorem 1.3 has restriction that $t - 1$ and k are relatively prime as well as t is bounded below. The idea of the construction of this parametrization is to have many linear factors which are relatively prime and whose integral values are not perfect squares so that we get distinct prime factors from the square-free part of their products, and to get positive rank of the corresponding θ-congruent number elliptic curve.

The main idea of the construction of our parametrization $S_n(t)$ given in (1) over $\mathbb{Z}$ is to find $a(t), b(t) \in \mathbb{Z}[t]$ such that $x + (r + s)S_n(t) = x + kdS_n(t) = a(t)b(t)$ and $x - (r - s)S_n(t) = x + \ell dS_n(t) = \frac{x}{a(t)} \cdot b(t)$. Then, for x which is a multiple $a(t)c(t)$ of $a(t)$ and $y = a(t)b(t)c(t)$, (x, y) is a point of the elliptic curve $E_{S_n(t)} : y^2 = x(x + (r + s)S_n(t))(x - (r - s)S_n(t))$ and $S_n(t)$ is a multiple of $b(t)$. Moreover, we can choose them so that $b(t)$ has enough number of linear factors $L_i(t)$ in t with the properties that the product of two consecutive linear factors satisfies that $L_{2i-1}(t)L_{2i}(t) \equiv 3 \pmod 4$ for every $t \in \mathbb{Z}$, and $L_{2i-1}(t)L_{2i}(t)$