Congruent numbers with many prime factors

Ye Tian[1]

Morningside Center of Mathematics, Academy of Mathematics and Systems Science, Chinese Academy of Sciences, Beijing 100190, China

Edited† by S. T. Yau, Harvard University, Cambridge, MA, and approved October 30, 2012 (received for review September 28, 2012)

Mohammed Ben Alhocain, in an Arab manuscript of the 10th century, stated that the principal object of the theory of rational right triangles is to find a square that when increased or diminished by a certain number, *m* becomes a square [Dickson LE (1971) *History of the Theory of Numbers* (Chelsea, New York), Vol 2, Chap 16]. In modern language, this object is to find a rational point of infinite order on the elliptic curve $my^2 = x^3 - x$. Heegner constructed such rational points in the case that *m* are primes congruent to 5,7 modulo 8 or twice primes congruent to 3 modulo 8 [Monsky P (1990) *Math Z* 204:45–68]. We extend Heegner's result to integers m with many prime divisors and give a sketch in this report. The full details of all the proofs will be given in ref. 1 [Tian Y (2012) Congruent Numbers and Heegner Points, arXiv:1210.8231].

Gross-Zagier formula | modular curve | genus theory

A positive integer is called a congruent number if it is the area of a right-angled triangle, all of whose sides have rational length. The problem of determining which positive integers are congruent is buried in antiquity (ref. 2, chap. 16) with it long being known that the numbers 5, 6, and 7 are congruent. Fermat proved that 1 is not a congruent number, and similar arguments show that 2 and 3 are not congruent numbers. No algorithm has ever been proven for infallibly deciding whether a given integer $n \geq 1$ is congruent, the reason being that an integer $n \geq 1$ is congruent if and only if there exists a point (x,y), with x and y rational numbers and $y \neq 0$, on the elliptic curve $\mathrm{E}^{(n)}$: $y^2 = x^3 - n^2x$. Moreover, assuming n to be square-free, a classical calculation of root numbers shows that the complex L-function of this curve has zero of odd order at the center of its critical strip precisely when n lies in one of the residue classes of 5, 6, and 7 modulo (mod) 8. Thus, in particular, the unproven conjecture of Birch and Swinnerton-Dyer (3, 4) predicts that every positive integer lying in the residue classes of 5, 6, and 7 mod 8 should be a congruent number. The aim of this paper is to prove the following partial results in this direction.

Theorem 1. *For any given integer $k \geq 0$, there are infinitely many square-free congruent numbers with exactly $k+1$ odd prime divisors in each residue class of 5, 6, 7 mod 8.*

Theorem 1 follows from the following result by Remark 2 below. For any abelian group A and an integer $d \geq 1$, we write $A[d]$ for the Kernel of the multiplication by d on A.

Theorem 2. *Let $k \geq 0$ be an integer and $n = p_0p_1 \cdots p_k$ a product of distinct odd primes with $p_i \equiv 1 \bmod 8$ for $1 \leq i \leq k$. Let $m = n$ or $2n$ such that $m \equiv 5, 6,$ or $7 \bmod 8$. Then m is a congruent number provided that the ideal class group $\mathcal{A}$ of the field $K = \mathbb{Q}(\sqrt{-2n})$ satisfies the condition*

$$\dim_{\mathbb{F}_2}(\mathcal{A}[4]/\mathcal{A}[2]) = \begin{cases} 0, & \text{if } n \equiv \pm 3 \bmod 8, \\ 1, & \text{otherwise.} \end{cases} \qquad [1]$$

Remark 1: The above result when $k = 0$ is due to Heegner (5), and completed by Birch (6), Stephens (7), and Monsky (8); and that when $k = 1$ is due to Monsky (8) and Gross (9). Actually Heegner is the first mathematician who found a method to construct fairly general solutions to cubic Diophantine equations (5). The method of this paper is based on Heegner's construction.

Remark 2: The kernel $\mathcal{A}[2]$ and the image $2\mathcal{A}$ of the multiplication by 2 on $\mathcal{A}$ are characterized by Gauss' genus theory. Note that the multiplication by 2 induces an isomorphism $\mathcal{A}[4]/\mathcal{A}[2] \overset{\times 2}{\simeq} \mathcal{A}[2] \cap 2\mathcal{A}$. By Gauss' genus theory, Condition **1** is equivalent in that there are exactly an odd number of spanning subtrees in the graph whose vertices are $p_0, \cdots, p_k$ and whose edges are those p_ip_j, $i \neq j$, with the quadratic residue symbol $\left(\frac{p_i}{p_j}\right) = -1$. It is then clear that *Theorem 1* follows from *Theorem 2*.

The congruent number problem is not only to determine whether a given integer m is congruent, but also to construct infinite order points on the elliptic curve $E^{(m)} : my^2 = x^3 - x$ for congruent m.

Let $X_0(32)$ be the modular curve defined over $\mathbb{Q}$ for the congruent subgroup $\Gamma_0(32)$, which is a genus 1 curve, and the cusp ∞ is rational so that $E' := (X_0(32), \infty)$ is an elliptic curve over $\mathbb{Q}$. It is known that E' has Weierstrass equation $y^2 = x^3 + 4x$. Let E be the elliptic curve $y^2 = x^3 - x$ and let $f : X_0(32) \to E$ be a modular parametrization of degree 2 mapping ∞ to 0, i.e., it is a degree 2 isogeny from E' to E.

Let $n = p_0p_1 \cdots p_k$ be a product of distinct odd primes with $p_1, \cdots, p_k \equiv 1 \bmod 8$. Let $m = n$ or $2n$ such that $m \equiv 5, 6$ or $7 \bmod 8$. Let H be the Hilbert class field of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-2n})$. Let $m^* = (-1)^{(n-1)/2}m$ so that $K(\sqrt{m^*}) \subset H$ and let $E(\mathbb{Q}(\sqrt{m^*}))^-$ be the group of points $x \in E(\mathbb{Q}(\sqrt{m^*}))$ such that $\sigma x = -x$ where σ is the nontrivial element in the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt{m^*})/\mathbb{Q})$. Then $E(\mathbb{Q}(\sqrt{m^*}))^- \cong E^{(m)}(\mathbb{Q})$, whose torsion subgroup is $E[2]$. We now construct the so-called Heegner point $y_m \in E(\mathbb{Q}(\sqrt{m^*}))^- \cong E^{(m)}(\mathbb{Q})$, which will be shown to be of infinite order for m satisfying Condition **1** in *Theorem 2*.

1. If $n \equiv 5 \bmod 8$, then $m = m^* = n$. Let $P \in X_0(32)$ be the image of $i\sqrt{2n}/8$ on the upper half plane $\mathcal{H}$ via the complex uniformization $X_0(32) = \Gamma_0(32)\backslash(\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q}))$. It turns out that the point $z := f(P) + (1+\sqrt{2}, 2+\sqrt{2})$ on E is defined over the Hilbert class field H, and that $y_n := \mathrm{Tr}_{H/K(\sqrt{n})}z \in E(\mathbb{Q}(\sqrt{n}))$. Moreover, y_n (resp. $2y_n$) belongs to $E(\mathbb{Q}(\sqrt{n}))^-$ if $k \geq 1$ (resp. $k = 0$).
2. If $n \equiv 3, 7 \bmod 8$, then $m^* = -m$. Let $P \in X_0(32)$ be the image of $(i\sqrt{2n}+2)/8$ via the complex uniformization and let $z := f(P) + (1+\sqrt{2}, 2+\sqrt{2})$, which turns out to be a point defined over $H(i)$. Identify $\mathcal{A}$ with $G = \mathrm{Gal}(H(i)/K(i))$ and let $\sigma_0 \in \mathrm{Gal}(H(i)/K(i))$ be the element corresponding to the ideal class of $(2, \sqrt{-2n})$. Let χ be the character of G factor through $\mathrm{Gal}(K(i, \sqrt{m^*})/K(i))$, which is nontrivial if $m \neq 2n$. Let $\phi \subset \mathcal{A}$ be a complete representative of $G/\langle\sigma_0\rangle$ and define $y_m := y_{m,\phi} = \sum_{\sigma \in \phi}\chi(\sigma)z^\sigma$.

The following theorem is our main result, from which *Theorem 2* follows.

Author contributions: Y.T. designed research, performed research, and wrote the paper.

The author declares no conflict of interest.

See Commentary on page 21182.

†This Direct Submission article had a prearranged editor.

[1]To whom correspondence should be addressed. E-mail: ytian@math.ac.cn.