ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 39, Number 4, 2009

A FEW REMARKS ON CONGRUENT NUMBERS

TERUTAKE ABE, ASHVIN RAJAN AND FRANÇOIS RAMAROSON

Dedicated to Professor Takashi Ono

ABSTRACT. Adapting an argument by Nigel Boston, we provide a new elementary proof of a theorem due to J.S. Chahal which asserts that every residue class $a \pmod 8$ for which $\gcd(a,8)$ is square-free contains an infinite set of congruent numbers. We then establish the following stronger result. Fix a positive integer q, an integer a such that $\gcd(a,q)$ is square-free, and a real number θ such that $0 < \theta < \pi$, for which $\cos\theta$ is a rational number. Then the number of integers in the interval $[1,n]$ that are θ-congruent numbers belonging to the residue class $a \pmod q$ is at least $\mathcal{O}(\sqrt{n})$.

1. Introduction. Fix a real number θ such that $0 < \theta < \pi$, for which $\cos\theta = s/r$, where r and s are relatively prime integers with $r > 0$. Write $\alpha_\theta = \sqrt{r^2 - s^2}$. A square-free integer n is a *θ-congruent number* if $n\alpha_\theta$ is the area of a rational triangle one of whose angles is θ. (A *rational triangle* is a triangle whose three sides all have rational lengths.) We call $(\pi/2)$-congruent numbers "congruent numbers."

Our inspiration was the following pretty density argument, proposed by Nigel Boston. For an odd, positive, square-free integer n, the triple $(n-2, n, n+2)$ must be relatively prime in pairs, and hence if the three positive integers n and $n \pm 2$ are all square-free, then so is $2n(n^2-4)$, which is the area of the rational right triangle whose sides make up the integral triple $(n^2-4, 4n, n^2+4)$. Thus, to prove that the set of congruent numbers is infinite, it suffices to prove that all three entries in triples $(n-2, n, n+2)$ are square-free infinitely often. If there were at most a finite number of such triples in which all three entries were square-free, then the natural density of the positive odd square-free integers *amongst all the positive odd integers* can be no more than $2/3$. However, as is well-known, this density is $8/\pi^2$. And since $8/\pi^2 > 2/3$, the set of (even) congruent numbers must be infinite.

2000 AMS *Mathematics subject classification.* Primary 11A05, 11B05,11E76, 11H46, Secondary 11G05, 11B25.
Keywords and phrases. Congruent numbers, density, binary forms.
Received by the editors on February 19, 2007.

DOI:10.1216/RMJ-2009-39-4-1083

For positive integral q, a residue class $a \pmod{q}$ is *permissible* if $\gcd(a, q)$ is square-free. We modify Boston's argument to re-prove a theorem due to Chahal [**3**], which states that each permissible residue class modulo 8 contains an infinite set of congruent numbers. Chahal's theorem was extended by Bennett [**1**], who proved that for an arbitrary positive integer q, every permissible residue class $a \pmod{q}$ contains an infinite set of congruent numbers. Fujiwara [**4**] has also refined Chahal's theorem, proving that for any θ with $0 < \theta < \pi$, where $\cos\theta$ is a rational number, every permissible residue class modulo 8 contains an infinite set of θ-congruent numbers.

We generalize these theorems of Bennett and Fujiwara, via asymptotic estimates for the distribution of square-free values of binary forms proved by Stewart and Top [**8**], and establish that for an arbitrary integer $q \geq 1$ and θ such that $0 < \theta < \pi$, with $\cos\theta$ rational, the number of integers in the interval $[1, x]$ that are θ-congruent numbers belonging to each permissible residue class $a \pmod{q}$ is at least $\mathcal{O}(\sqrt{x})$.

2. Density arguments and Chahal's theorem. The *natural density of a set* S of positive integers is $\delta(S) = \lim_{n\to\infty}(|S \cap [1, n]|/n)$, and if C is a second subset of positive integers containing S, the *relative natural density of* S in C is $\delta_C(S) = \lim_{n\to\infty}(|S \cap [1, n]|/|C \cap [1, n]|)$. Landau [**6**] proved that the relative natural density $\delta_{a,q}$ of square-free integers in a residue class $a \pmod{q}$ where $\gcd(a, q)$ is square-free, is

$$\delta_{a,q} = B \cdot \frac{6}{\pi^2} \cdot \prod_{p|q,\ p\text{: prime}} \left(p^2/(p^2-1)\right), \text{ where}$$
$$B = \varphi(q)/[\gcd(a, q) \cdot \varphi(q/\gcd(a, q))].$$

We see that the relative density of the square-free integers amongst the integers in each permissible residue class modulo 8 is $8/\pi^2$. This enables us to prove the following theorem.

Theorem 2.1 [**3**]. *Every permissible residue class modulo* 8 *contains an infinite set of congruent numbers.*

Proof. Consider the triple $(n-8, n, n+8)$ where n is odd. Since these three entries are relatively prime in pairs, if all three are square-free, then so is $2n(n^2-64)$, which, being the area of the rational right triangle with sides

$$\left(\frac{n^2-64}{2}, 8n, \frac{n^2+64}{2}\right),$$

is a congruent number. If the three entries in $(n-8, n, n+8)$ were all square-free only finitely often, then the density of the square-free integers in the congruence class $n \pmod 8$ could be at most $2/3$. However, since this density is $8/\pi^2$, there must be an infinite set of triples with all three entries square-free. Choosing $n \equiv 1 \pmod 8$ (or $3 \pmod 8$) yields an infinite set of congruent numbers in the residue class $2 \pmod 8$ (or $6 \pmod 8$). To treat the odd residue classes modulo 8, we work with $n(n^2-16)$ which is the area of the right triangle with sides

$$\left(\frac{n^2-16}{2}, 4n, \frac{n^2+16}{2}\right).$$

Landau's density estimate modulo 4 enables one to conclude immediately that there are infinite sets of triples $(n-4, n, n+4)$ whose entries are all square-free, in each of the residue classes 1 and $3 \pmod 4$. Let $T_{1,4}$ be the set of all positive integers $n \equiv 1 \pmod 4$ for which the entries of $(n-4, n, n+4)$ are all square-free. Then the intersection of $T_{1,4}$ with each of the two residue classes 1 and $5 \pmod 8$ is infinite. For if, to the contrary, $T_{1,4}$ contained only finitely many n with $n \equiv 1 \pmod 8$, then there is a positive integer A, so that if $n > A$ and $n \equiv 1 \pmod 8$ then at most two of $(n-4, n, n+4)$ are square-free. This certainly implies that for each n with $n > A$ and $n \equiv 1 \pmod{16}$, at most three of $(n-4, n, n+4, n+8)$ are square-free. Let X be the set of all integers in the residue class 1 modulo 4 which are greater than A, and let S be the set of all square-free integers in X. Then $\delta(S)$ must be $\delta_{1,4}/4 = 2/\pi^2$. On the other hand, since $\delta(X) = 1/4$,

$$\begin{aligned}\delta(S) &= \lim_{N\to\infty} \frac{|S \cap [1, N]|}{N} \\ &= \lim_{N\to\infty} \frac{|S \cap [1, N]|}{|X \cap [1, N]|} \cdot \frac{1}{4} \leq \frac{3}{4} \cdot \frac{1}{4} < \frac{2}{\pi^2}.\end{aligned}$$

So, there must be an infinite set of triples $(n-4, n, n+4)$ where $n \equiv 1 \pmod 8$, with all three entries square-free. Each such triple gives the square-free congruent number $n(n^2-16) \equiv 1 \pmod 8$. Repeating the argument with $n \equiv 5 \pmod 8$ yields an infinite set of congruent numbers in the residue class 5 (mod 8), and replacing $T_{1,4}$ by $T_{3,4}$ and choosing $n \equiv 3$ or $7 \pmod 8$ produces infinite sets of congruent numbers belonging to the residue classes 3 or 7 (mod 8), respectively. □

3. Congruent numbers as values of binary quartic forms. To prove a general result, and recover the theorems of Bennett and Fujiwara as special cases, we view θ-congruent numbers as square-free values of binary quartic forms. So, fix a real θ where $0 < \theta < \pi$, with $\cos\theta = s/r$ where r and s are relatively prime integers and $r > 0$. Kan [**5**] has proved that a square-free natural number n is a θ-congruent number if and only if n is the square-free part of the value of the binary form

$$G(X, Y) = XY(X + Y)(2rX + (r - s)Y)$$

at integral X and Y. The following very powerful theorem by Stewart and Top [**8**] gives asymptotic estimates for the distribution of square-free values of binary forms. We state a version that applies to our situation.

Let $Q \geq 1$, U and V be integers, and let

$$F(X, Y) = a_d X^d + a_{d-1} X^{d-1} Y + \cdots + a_0 Y^d$$

be a homogenous binary form of degree $d > 2$ with integral coefficients. Assume that $F(X, Y) > 0$ if X and Y are positive. Let $R_2(x)$ denote the number of square-free integers $t \in [1, x]$ for which there exist $u \equiv U \pmod Q$ and $v \equiv V \pmod Q$ such that $F(u, v) = t$.

Theorem 3.1 [**8**]. *If there is a pair of integers $(u, v) \equiv (U, V) \pmod Q$ such that $F(u, v)$ is square-free, the degree of the largest irreducible factor of F over $\mathbf{Q}$ is less than 6, and the discriminant of $F(X, Y)$ is nonzero, then there are positive real numbers c and C (which depend on Q and F) such that if $x > c$, then $R_2(x) > Cx^{2/d}$.*

Theorem 3.2. *Assume that for $0 < \theta < \pi$, $\cos\theta = s/r$, where $r > 0$, and $\gcd(s, r) = 1$. Fix a positive integer q. Then every permissible residue class $a \pmod q$ contains an infinite set of θ-congruent numbers. More precisely, there is a positive constant C, depending on*

θ and q, such that for a sufficiently large positive integer n, the number of integers in the interval $[1, n]$ that are θ-congruent numbers in the residue class $a \pmod q$ is at least $C\sqrt{n}$.

Proof. In Theorem 3.1, set $Q = q$, and consider the binary quartic form

$$G(X,Y) = XY(X+Y)(2rX + (r-s)Y).$$

Let $r = r_1 l$, where r_1 is the largest factor of r that is relatively prime with q. Set $X = u$ and $Y = 2q^2 lv$. Then

$$\begin{aligned} G(X,Y) &= XY(X+Y)(2rX + (r-s)Y) \\ &= 4q^2 l^2 uv\left(u + 2q^2 lv\right)\left(r_1 u + (r-s)q^2 v\right). \end{aligned}$$

So, square-free values of $G(X,Y)$, for $X = u$ and $Y = 2q^2 lv$, are square-free values of

$$F(u,v) = uv\left(u + 2q^2 lv\right)\left(r_1 u + (r-s)q^2 v\right),$$

and these square-free values are θ-congruent numbers. Since $\gcd(q, r_1) = 1$, there exists a t_1 such that $t_1 r_1 \equiv 1 \pmod q$. Let $U = 1$ and $V = at_1$ (with $\gcd(a,q)$ square-free). If $(u,v) \equiv (1, at_1) \pmod q$, then $F(u,v) \equiv a \pmod q)$. To see that $F(u,v)$ achieves square-free values infinitely often for $(u,v) \equiv (1, at_1) \pmod q$, we consider the cubic polynomial $f(x) = F(1, at_1 + qx)$, which is the product of three linear factors with positive integral coefficients, such that no two factors are proportional to each other. Elementary arguments verify that $f(x) \equiv 0$ $(\text{mod } p)^2)$ has fewer than p^2 solutions for every prime number p. A theorem by Shapiro ([**7**, Theorem 4.2]) then allows us to conclude that the set of positive integers x for which $f(x)$ is square-free has positive density. This proves that the number of square-free values of $F(u,v)$ in the residue class $a \pmod q$ is infinite. Thus, this residue class contains an infinite set of θ-congruent numbers.

Moreover, every irreducible factor of the form F, being linear, is of degree less than 6, the discriminant of F is easily seen to be nonzero, and the argument above shows that there is at least one (in fact infinitely many) $(u,v) \equiv (1, at_1) \pmod q$ for which $F(u,v)$ is square-free. Thus, the assumptions of Theorem 3.1 are satisfied, and we can now conclude that there exist positive constants c and C such that for real numbers $x > c$, $R_2(x) > C\sqrt{x}$. This immediately implies that the number of integers in the interval $[1, n]$ that are θ-congruent numbers belonging to the residue class $a \pmod q$ is at least $\mathcal{O}(\sqrt{n})$. $\square$

Finally, we remark in closing that, in Theorem 3.2, specializing to $\theta = \pi/2$ one obtains Bennett's theorem, while setting $q = 8$ yields Fujiwara's theorem.

Acknowledgments. The third author would like to thank Howard University for providing him a sabbatical leave of absence for the spring semester in the academic year 2006–2007 during which this work was completed.

REFERENCES

1. M.A. Bennett, *Lucas' pyramid problem revisited*, Acta Arith. **105** (2002), 341–347.

2. N. Boston, *Infinitely many congruent numbers*, Internet posting.

3. J.S. Chahal, *On an identity of Desboves*, Proc. Japan Acad. Math. Sci. **60** (1984), 105–108.

4. M. Fujiwara, *θ-congruent numbers*, Number Theory, K. Györy, A. Pethö and V. Sós, eds., de Gruyter, 1997, Berlin.

5. M. Kan, *θ-congruent numbers and elliptic curves*, Acta Arith. **54** (2000), 153–160.

6. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig, 1953.

7. H. Shapiro, *Powerfree integers represented by linear forms*, Duke Math. J. **16** (1949), 601–607.

8. C.L. Stewart and J. Top, *On ranks of twists of elliptic curves and power-free values of binary forms*, J. Amer. Math. Soc. **8** (1995), 943–973.

Department of Mathematical and Physical Sciences, Texas A&M International University, Laredo, Texas, 78041
Email address: tabe@tamiu.edu

3935 Cloverhill Road, Baltimore, MD 21218
Email address: ashvinrj@aol.com

Department of Mathematics, Howard University, Washington, DC 20059
Email address: framaroson@howard.edu