The representation function for sums of three squares along arithmetic progressions

By Paul POLLACK

Department of Mathematics, University of Georgia, Boyd Graduate Studies Research Center, Athens, Georgia 30602, USA

(Communicated by Kenji FUKAYA, M.J.A., Sept. 12, 2016)

Abstract: For positive integers n, let $r(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2+y^2+z^2 = n\}$. Let g be a positive integer, and let $A \bmod M$ be any congruence class containing a squarefree integer. We show that there are infinitely many squarefree positive integers $n \equiv A \bmod M$ for which g divides $r(n)$. This generalizes a result of Cho.

Key words: Class number; imaginary quadratic field; three squares.

1. Introduction. For each positive integer n, let $r(n)$ denote the number of ways of writing n as a sum of three squares, i.e., $r(n) = \#\{(x,y,z) \in \mathbf{Z}^3 : x^2+y^2+z^2 = n\}$. Recently, Cho established the following result concerning values of $r(n)$ divisible by a fixed integer [2, Theorem 2].

Theorem A. *Let g be a positive integer.*

(a) *There are infinitely many squarefree $n \equiv 1 \bmod 4$ for which $12g \mid r(n)$.*
(b) *If g is odd, then there are infinitely many squarefree $n \equiv 2 \bmod 4$ for which $12g \mid r(n)$.*
(c) *If g is odd, then there are infinitely many squarefree $n \equiv 3 \bmod 8$ for which $24g \mid r(n)$.*

In this note, we strengthen Theorem A by proving a divisibility result valid not only for the progressions $1, 2 \bmod 4$ and $3 \bmod 8$, but for any progression $A \bmod M$ compatible with the squarefree condition. Moreover, in every case we guarantee divisibility by an arbitrary positive integer g.

Theorem 1. *Let g be a positive integer. Let $A \bmod M$ be any congruence class containing a squarefree integer. There are infinitely many squarefree $n \equiv A \bmod M$ for which $g \mid r(n)$.*

Corollary 2. *Let g be a positive integer. Let $A \bmod M$ be a congruence class containing a squarefree integer, and suppose that $A \bmod M$ is not entirely contained in the residue class $7 \bmod 8$. There are infinitely many squarefree $n \equiv A \bmod M$ with $r(n)$ a nonzero multiple of g.*

Remark 3. It is well-known that the progression $A \bmod M$ contains at least one squarefree integer precisely when $\gcd(A, M)$ is squarefree, in which case a positive proportion of the positive integers $n \equiv A \bmod M$ are squarefree. See, for instance, §2 of Pappalardi's survey [9].

2. Proof of Theorem 1 and Corollary 2.

2.1. Sketch. We require two auxiliary results. The first is essentially due to Gauss [4, Art. 291] (cf. [5, Chapter 4]). In what follows, we write $h(d)$ for the class number of the quadratic field $\mathbf{Q}(\sqrt{d})$.

Proposition 4. *Let n be a squarefree integer with $n > 3$.*

(a) *If $n \equiv 1, 2 \bmod 4$, then $r(n) = 12h(-n)$.*
(b) *If $n \equiv 3 \bmod 8$, then $r(n) = 24h(-n)$.*
(c) *If $n \equiv 7 \bmod 8$, then $r(n) = 0$.*

At the heart of the proof of Theorem 1 is a divisibility result for class numbers of imaginary quadratic fields (compare with [2, Theorem 1]).

Proposition 5. *Let g be a positive integer. Let $A \bmod M$ be a congruence class containing a squarefree integer. There are infinitely many positive squarefree integers $d \equiv A \bmod M$ for which the class group of $\mathbf{Q}(\sqrt{-d})$ contains an element of order g.*

Proof of Theorem 1. Suppose $d > 3$ is squarefree with $d \equiv A \bmod M$ and with the class group of $\mathbf{Q}(\sqrt{-d})$ containing an element of order g. Then g divides $h(-d)$, which in turn divides $r(d)$ by Proposition 4. By Proposition 5, there are infinitely many of these d, and Theorem 1 follows. □

Proof of Corollary 2. We claim we can find an arithmetic progression contained in the intersection of the progression $A \bmod M$ and one of the progressions $1, 2, 3, 5, 6 \bmod 8$, and containing a

2010 Mathematics Subject Classification. Primary 11R29, 11R11; Secondary 11E25.

doi: 10.3792/pjaa.92.96

squarefree integer. Keeping in mind Proposition 4, the corollary then follows from Theorem 1.

Let A_0 be a squarefree integer from the residue class $A \bmod M$. Suppose first that $A_0 \not\equiv 7 \bmod 8$. In this case $A_0 \bmod 8M$ is the desired progression. Suppose now that $A_0 \equiv 7 \bmod 8$. Then $8 \nmid M$, so that $\mathrm{lcm}[4, M] \equiv 4 \bmod 8$. Then $A_0 + \mathrm{lcm}[4, M] \equiv 3 \bmod 8$ and $\gcd(A_0 + \mathrm{lcm}[4, M], 8M)$ is squarefree. So (keeping in mind Remark 3) the residue class $A_0 + \mathrm{lcm}[4, M] \bmod 8M$ has the desired properties. $\square$

The remainder of this note is devoted to a proof of Proposition 5.

2.2. Proof of Proposition 5. To construct our imaginary quadratic fields, we employ a lemma appearing in work of Soundararajan [10, Proposition 1] (compare with earlier results of Nagel [8, Sätze IV, V], Humbert [6, Théorème 1], and Ankeny and Chowla [1, Theorem 1]).

Lemma 6. *Let $g \geq 3$ be an integer. Suppose $d \geq 63$ is a squarefree integer satisfying*

$$t^2 d = m^g - n^2, \tag{1}$$

where t, m, n are positive integers with $\gcd(m, 2n) = 1$ and $m^g < (d+1)^2$. Then the class group of $\mathbf{Q}(\sqrt{-d})$ contains an element of order g.

We will also use the following elementary result concerning gth power residues. Below, we write $\nu_p(g)$ for the p-adic valuation of the integer g.

Lemma 7. *Let g be a positive integer. If p is an odd prime, then every integer $n \equiv 1 \bmod p^{\nu_p(g)+1}$ is a gth power in the ring $\mathbf{Z}_p$ of p-adic integers. The same holds if $p = 2$ under the stronger hypothesis that $n \equiv 1 \bmod p^{\nu_p(g)+2}$.*

Proof. This follows from the fact that the usual binomial expansion for $(1+x)^{1/g}$ converges p-adically for $|x|_p \leq p^{-\nu_p(g)-1}$ when p is odd, and for $|x|_p \leq p^{-\nu_p(g)-2}$ when $p = 2$ (see, for instance, [3, Corollary 4.2.16, p. 216]). $\square$

Proof of Proposition 5. The case $g = 1$ is trivial. Suppose $g = 2$. By genus theory, $h(-d)$ is odd for a positive squarefree number $d > 2$ if and only if d is a prime with $d \equiv 3 \bmod 4$. Since the primes have asymptotic density 0, it follows that the conclusion of Proposition 5 holds for asymptotically 100% of squarefree $d \equiv A \bmod M$. Henceforth, we assume that $g \geq 3$. Let A_0 be a squarefree integer with $A_0 \equiv A \bmod M$. By replacing A with A_0 and M by $4M^2$, we can assume that M is even, squarefull, and that no integer congruent to $A \bmod M$ is divisible by the square of a prime dividing M. Set

$$t = 2 \prod_{p \mid M} p^{\nu_p(g)+1}.$$

We fix an integer m_0 satisfying

$$m_0^g \equiv 1 + t^2 A \bmod Mt^2.$$

Such an m_0 exists, since $1 + t^2 A$ is a gth power in $\mathbf{Z}_p$ for every prime $p \mid Mt^2$, by Lemma 7. If $n \equiv 1 \bmod Mt^2$, and $m \equiv m_0 \bmod Mt^2$, then $m^g - n^2 \equiv t^2 A \bmod Mt^2$, so that $t^2 \mid m^g - n^2$, and

$$d := \frac{m^g - n^2}{t^2} \equiv A \bmod M. \tag{2}$$

We now impose further conditions on m and n in order to apply Lemma 6.

Let x be a large real number. Here "large" always means "sufficiently large, in a way that can be made to depend only on the fixed parameters A, M, and g." Note that $\gcd(m_0, Mt^2) = 1$; thus, by the prime number theorem for progressions, we may choose a prime $m \equiv m_0 \bmod Mt^2$ with $\frac{1}{2}x < m^g \leq x$. With $X := \sqrt{m^g/2}$, we look for integers $n \in [1, X]$ with $n \equiv 1 \bmod Mt^2$, $\gcd(m, n) = 1$ and with d, as defined in (2), squarefree. For any such n,

$$x > d = \frac{m^g - n^2}{t^2} \geq \frac{1}{2}\frac{m^g}{t^2} > \frac{1}{4}\frac{x}{t^2},$$

and hence d certainly exceeds 63 for large x. Also, for large x,

$$(d+1)^2 > \frac{1}{16}\frac{x^2}{t^4} > x \geq m^g.$$

Thus, Lemma 6 applies, and each such n gives rise to a squarefree $d \equiv A \bmod M$ with the class group of $\mathbf{Q}(\sqrt{-d})$ having an element of order g.

The number of n as above is at least $\sum_1 - \sum_2 - \sum_3$, where

$$\sum\nolimits_1 = \sum_{\substack{n \leq X \\ n \equiv 1 \bmod Mt^2}} 1,$$

$$\sum\nolimits_2 = \sum_{\substack{n \leq X \\ n \equiv 1 \bmod Mt^2 \\ m \mid n}} 1,$$

$$\sum\nolimits_3 = \sum_{\substack{n \leq X \\ n \equiv 1 \bmod Mt^2 \\ \gcd(n,m)=1 \\ d \text{ not squarefree}}} 1.$$

Clearly, $\sum_1 \geq \frac{X}{Mt^2} - 1 > 0.9\,\frac{X}{Mt^2}$, while $\sum_2 \leq \frac{X}{Mmt^2} + 1 < 0.1\,\frac{X}{Mt^2}$ (for large x). Now suppose n is counted in $\sum_3$, and that the prime p is such that $p^2 \mid d$. Then $n^2 \equiv m^g \bmod p^2$. Since $\gcd(m,n)=1$, we have $p \nmid m$. Thus, the congruence $n^2 \equiv m^g \bmod p^2$ puts n in one of two residue classes modulo p^2. We also know that $p \nmid M$; indeed, $d \equiv A \bmod M$ and no integer from the residue class $A \bmod M$ is divisible by the square of a prime dividing M. Since $n \equiv 1 \bmod Mt^2$ and $\gcd(Mt^2, p^2)=1$, we see that n is in one of two residue classes modulo Mt^2p^2. So for a given p, the number of corresponding $n \le X$ is at most $\frac{2X}{Mt^2p^2}+1$. Finally, we bound $\sum_3$ by summing on possible primes p. Note that p is odd (since M is even) and that $p^2 \le m^g/t^2 < m^g/2 = X^2$. Thus,

$$\sum\nolimits_3 \le \sum_{2<p\le X}\left(\frac{2X}{Mt^2p^2}+1\right) < \frac{X}{Mt^2}\sum_{p>2}\frac{2}{p^2}+\pi(X).$$

Since

$$\sum_{p>2}\frac{2}{p^2} < \frac{2}{9}+2\sum_{j\ge5}\frac{1}{j^2} < \frac{2}{9}+2\sum_{j\ge5}\int_{j-1}^{j}\frac{dt}{t^2} < 0.73$$

and $\pi(X) < 0.01\,\frac{X}{Mt^2}$ for large x (as the primes have density 0), we have $\sum_3 < \frac{3}{4}\frac{X}{Mt^2}$. Collecting our estimates, we see that the number of suitable n is bounded below by

$$0.05\,\frac{X}{Mt^2} > \frac{0.025}{Mt^2}\cdot x^{1/2}.$$

Since distinct n give rise to distinct d, this is also a lower bound on the number of $d \le x$ satisfying the conclusion of Proposition 5. Since this lower bound tends to infinity with x, the full collection of d satisfying the conclusion of Proposition 5 must be an infinite set. □

Remark 8. We have stated Proposition 5 in a qualitative form, but the result actually established is quantitative. Namely, for fixed A, M, and g, the number of $d \le x$ satisfying the conclusion of Proposition 5 is $\gg x^{1/2}$, for all large x. Here (and in the next paragraph) the notation suppresses the dependence of implied constants on A, M, and g.

Without aiming for the sharpest possible lower bound, we now describe how to do slightly better with little effort. Suppose $g \ge 3$. At the moment where we choose m in the above proof, we can instead consider running the argument for all of the $\asymp x^{1/g}/\log x$ possible choices of m. We find that if x is large, we produce $\gg x^{1/2+1/g}/\log x$ values of $d \le x$; the only problem is that distinct m may yield the same values of d. By an argument of Murty [7, bottom of p. 235], each pair of distinct m results in an overlap of only $x^{o(1)}$ values of d (as $x \to \infty$). Hence, the total overlap is accounted for by subtracting a term of size $x^{2/g+o(1)}$. Since $x^{2/g+o(1)}$ is of smaller order than $x^{1/2+1/g}/\log x$, we deduce that there are $\gg x^{1/2+1/g}/\log x$ values of $d \le x$ satisfying the conclusion of Proposition 5.

3. Conclusion. We finish this note by remarking that Proposition 5 yields a short, conceptually simple proof of the following theorem of Yamamoto [12, Theorem 1]:

Theorem 9. *Let g be a positive integer. Let $p_1,\dots,p_k$ be distinct primes, and for each $1 \le i \le k$, let $\epsilon_i \in \{-1,0,1\}$. There are infinitely many negative fundamental discriminants D with the class group of $\mathbf{Q}(\sqrt{D})$ containing an element of order g and with $(\frac{D}{p_i}) = \epsilon_i$ for all $1 \le i \le k$.*

Proof. It is well-known that there are infinitely many fundamental discriminants D_0 satisfying $(\frac{D_0}{p_i}) = \epsilon_i$ for all $1 \le i \le k$. In fact, a positive proportion of all fundamental discriminants have this property; for rather far-reaching generalizations of these facts, see [11]. Fix any such D_0. Observe that if D is any fundamental discriminant with $D \equiv D_0 \bmod 4\prod_{i=1}^{k} p_i$, then $(\frac{D}{p_i}) = \epsilon_i$ for all $1 \le i \le k$.

Suppose that 4 divides D_0. Apply Proposition 5 to the progression $-D_0/4 \bmod 4\prod_{i=1}^{k} p_i$, which contains the squarefree integer $-D_0/4$. If d is as in the conclusion of the Proposition, then $-d \equiv D_0/4 \equiv 2,3 \bmod 4$ and so $\mathbf{Q}(\sqrt{-d})$ has discriminant $D := -4d$. Then $D \equiv D_0 \bmod 4\prod_{i=1}^{k} p_i$. Moreover, $\mathbf{Q}(\sqrt{D}) = \mathbf{Q}(\sqrt{-d})$, and the class group has an element of order g. This completes the proof of Theorem 9 in the case when $4 \mid D_0$.

When $D_0 \equiv 1 \bmod 4$, we argue analogously, this time applying Proposition 5 to the progression $-D_0 \bmod 4\prod_{i=1}^{k} p_i$. □

Acknowledgments. The author is supported by NSF award DMS-1402268. He thanks Prof. Carl Pomerance for suggesting the statement of Corollary 2.

References

[1] N. C. Ankeny and S. Chowla, On the divisibility of the class number of quadratic fields, Pacific J. Math. **5** (1955), 321–324.
[2] P. J. Cho, Sum of three squares and class numbers of imaginary quadratic fields, Proc. Japan Acad. Ser. A Math. Sci. **87** (2011), no. 6, 91–94.
[3] H. Cohen, *Number theory. Vol. I*, Graduate Texts

in Mathematics, 239, Springer, New York, 2007.

[4] C. F. Gauss, *Disquisitiones arithmeticae*, translated and with a preface by Arthur A. Clarke, Springer, New York, 1986.

[5] E. Grosswald, *Representations of integers as sums of squares*, Springer, New York, 1985.

[6] P. Humbert, Sur les nombres de classes de certains corps quadratiques, Comment. Math. Helv. **12** (1940), 233–245.

[7] M. R. Murty, Exponents of class groups of quadratic fields, in *Topics in number theory* (*University Park, PA, 1997*), 229–239, Math. Appl., 467, Kluwer Acad. Publ., Dordrecht, 1999.

[8] T. Nagel, Über die Klassenzahl imaginär-quadratischer Zahlkörper, Abh. Math. Sem. Univ. Hamburg **1** (1922), no. 1, 140–150.

[9] F. Pappalardi, A survey on k-freeness, in *Number theory*, Ramanujan Math. Soc. Lect. Notes Ser., 1, Ramanujan Math. Soc., Mysore, 2005, pp. 71–88.

[10] K. Soundararajan, Divisibility of class numbers of imaginary quadratic fields, J. London Math. Soc. (2) **61** (2000), no. 3, 681–690.

[11] M. M. Wood, On the probabilities of local behaviors in abelian field extensions, Compos. Math. **146** (2010), no. 1, 102–128.

[12] Y. Yamamoto, On unramified Galois extensions of quadratic number fields, Osaka J. Math. **7** (1970), 57–76.