THE REPRESENTATION OF INTEGERS BY THREE POSITIVE SQUARES

E. GROSSWALD, A. CALLOWAY AND J. CALLOWAY

1. The representation of an integer n as sums of a fixed number s of squares has been studied extensively. In counting the number $r_s(n)$ of these representations, i.e. the number of solutions of the diophantine equation

$$\sum_{i=1}^{s} x_i^2 = n \tag{1}$$

in integers x_i, solutions are considered distinct, if they differ by the order, or by the sign of any x_i. The following results are classical:

Necessary and sufficient conditions that (1) should have solutions are:

for $s=1$, that n should be a square;

for $s=2$, that the highest power at which any prime $p\equiv 3 \pmod 4$ divides n should be even (possibly zero);

for $s=3$, that n should not belong to the set M_4 of integers of the form $n=4^a n_1$, $n_1\equiv 7 \pmod 8$, with integral $a\geqq 0$;

for $s=4$, (1) has solutions for every n.

In these statements as also in the papers of Lehmer [**10**] and Chakrabarti [**2**], no distinction is made between representations involving zeros and those by positive squares. The problem of characterizing and counting the integers $n\leqq x$, having representations by s positive squares has been investigated for various values of s by Descartes [**3**, p. 256, 337–338], Dubois [**5**] and G. Pall [**11**] (see also [**4**, especially vol. 2]). The results may be summarized in the following

THEOREM A (G. PALL [**11**]). *Denote by B the set of integers* (1, 2, 4, 5, 7, 10, 13). *For $s\geqq 6$, every integer n can be represented as a sum of s positive squares, except* $1, 2, \cdots, s-1$ *and $s+b$, with $b\in B$. For $s=5$ the same statement holds, with $b\in\{B, 28\}$. For $s=4$ the statement holds, with $b\in\{B, 25, 37\}$, except for $n=4^a n_1$ with $n_1\in\{2, 6, 14\}$.*

For $s=1$ the situation is obvious, and for $s=2$ it follows easily that every n is a sum of two positive squares, if and only if $n=4^a n_1 n_2^2$, with

Received by the editors February 11, 1957 and, in revised form, March 27, 1958 and September 11, 1958.

integral $a \geqq 0$, $n_1 > 1$ and where $n_1 = \prod_i p_i^{\alpha_i}$, $p_i \equiv 1 \pmod 4$, $n_2 = \prod_j q_j^{\beta_j}$, $q_j \equiv 3 \pmod 4$, with p_i, q_j primes.

2. No similar complete results seem to be known for $s=3$. As partial results one has the following two theorems:

THEOREM B (HURWITZ [8]). *The set N_1 of integers n that are squares but not sums of three positive squares consists precisely of $n=4^a$ and $n=25.4^a$.*

THEOREM C (G. PALL [11]).[1] *Every integer $n \notin M_4$ and containing an odd square factor larger than one is a sum of three positive squares, unless $n=4^a \cdot 25$.*

It is the purpose of this paper to prove the following

THEOREM. *There exists a finite set S of m integers, such that every integer n is a sum of three positive squares, unless $n \in M_4 \cup M$, with M_4 defined above and M consisting of the integers $n=4^a n_1$, $n_1 \in S$. If N stands for the set of integers that are sums of three positive squares and $N(x)$ is the number of integers in N not exceeding x, then*

$$N(x) = \frac{5x}{6} - \left(m - \frac{7}{8}\right) f \log x + a - R \tag{2}$$

with $f = (\log 4)^{-1}$, $\cdot a = 7/6 + f(\sum_{n \in S} \log n - (7/8) \log 7)$ and $0 < R < f \log x/7 + m + 2$.

3. PROOF OF THE THEOREM.[2] Let N_i $(i=1, 2)$ stand for the set of integers that are sums of i, but not of three positive squares and set $N_i(x) = \sum_{n \leqq x} 1$, with the summations extended over N_i. Let also $N_{12}(x) = \sum_{n \leqq x} 1$ with $n \in N_1 \cap N_2$ and $M_4(x) = \sum_{n \leqq x} 1$, $n \in M_4$. Every $n \notin M_4$ belongs either to N, or to $N_1 \cup N_2$. N_1 is known by Theorem B so that only N_2 remains to be determined, in order to complete the characterization of N.

If $n = 4^a n_1$, $n_1 \not\equiv 0 \pmod 4$ and $n \in N_2$, then $n_1 \in N_2$ and conversely. Hence, it is sufficient to determine the set $T \subset N_2$ of integers $n \in N_2$, $n \not\equiv 0 \pmod 4$. By Theorem C, if $n \in T$, then either $n=25$, or else n cannot contain the square of any odd prime; hence it is square free. Consequently, if any prime $q \equiv 3 \pmod 4$ would divide n, $q^2 \nmid n$, and, hence, by a classical result $r_2(n)=0$, so that $n \notin N_2$, contradicting

[1] This result follows also from [1].

[2] The authors gratefully acknowledge valuable suggestions of a referee, in particular the use of Siegel's rather than Tatuzawa's theorem in the present proof. Also the correction of many minor and of at least one serious error are due to the exceptional attention of a referee.

$n \in T \subset N_2$. All intgers of T, except $n=25$, are therefore of the form $n=\prod_i p_i$, with $p_i \not\equiv 3 \pmod 4$, $p_i \neq p_j$ for $i \neq j$ and $n \equiv 1$, 2 or 5 (mod 8); and T contains all such integers that are sums of two, but not of three positive integers. We show now that the set of these integers is finite.

As $n=a^2+b^2+0=b^2+0+a^2=0+a^2+b^2$ are counted as three distinct representations of n in $r_3(n)$,

$$r_3(n) \geqq 3r_2(n) \tag{3}$$

holds for any n, and n has a representation by three positive squares if, and only if, the inequality in (3) is strict. In order to show that this is always the case for sufficiently large square free $n \equiv 1, 2$ or 5 (mod 8) we observe that (see [1]) for any n, $r_3(n)=\sum_{d^2|n} R_3(n/d^2)$ with $R_3(n)=(G_n/\pi)n^{1/2}L(1, \chi)$. Here G_n depends only on the residue class (mod 8) of n, and

$$L(1,\chi) = \sum_{v=1}^{\infty} \frac{(-k/v)}{v}, \text{ with } k = 4n.$$

For square free $n=1$, 2 or 5 (mod 8), $r_3(n)=R_3(n)$ and $G_n=24$, so that $r_3(n)=(24/\pi)n^{1/2}L(1, \chi)$. Also, if $n \in T$, $n=2^b n_1$ ($b=0$, 1), then $r_2(n)=4\tau(n_1) \leqq 4\tau(n)$, where $\tau(n)$ stands for the number of divisors of n. The strict inequality in (3) is now a consequence of

$$\frac{24}{\pi} n^{1/2}L(1,\chi) > 12\tau(n) \text{ or } \tau(n)\frac{1}{L(1,\chi)} < \frac{2}{\pi} n^{1/2},$$

which holds for sufficiently large n because for any $\epsilon > 0$, $\tau(n)=O(n^\epsilon)$ (see [**7**, Theorem 315]) and $1/L(1, \chi)=O(k^\epsilon)=O(n^\epsilon)$, by Siegel's theorem (see [**12** or **6**]).

This finishes the proof that there are only finitely many, say t integers in T. The integers n of N_2 are precisely those of the form $n=4^a n_1$, $n_1 \in T$ and, in order to obtain M, one only has to adjoin to them the elements of N_1, not already in N_2; these are the integers $n=4^a$, as follows from theorem B. This finishes the proof of the first part of the theorem, with $S=\{1, T\}$ and $m=t+1$.

4. In order to prove (2), one observes that

$$N(x) = [x] - M_4(x) - N_1(x) - N_2(x) + N_{12}(x), \tag{4}$$

the square bracket denoting the greatest integer function. Following Landau [**2**, vol. 2, p. 644]

$$M_4(x) = \frac{x}{6} - \frac{x}{24\cdot 4^z} - \frac{7}{8}(z+1) + \theta_1(z+1)$$

with

$$z = [f \log (x/7)] = f \log (x/7) - 1 + \theta_2,$$
$$f = (\log 4)^{-1} \quad \text{and} \quad 0 < \theta_i \leqq 1 \qquad (i = 1, 2).$$

Hence, $M_4(x) = x/6 + (\theta_1 - 7/8)f \log (x/7) - (7/6)4^{-\theta_2} - (7/8)\theta_2 + \theta_1\theta_2$. Similarly, by Theorem B, $N_1(x) - N_{12}(x) = f \log x + \theta_3$, $0 < \theta_3 \leqq 1$. Finally, for given $n \not\equiv 0 \pmod 4$, the number of integers $4^a n \leqq x$ is $[f \log (x/n)] + 1$; hence,

$$N_2(x) = \sum_{n \in T; n \leqq x} \{[f \log (x/n)] + 1\} = t \cdot f \cdot \log x - f \sum_{n \in T} \log n + t\theta_4,$$
$$0 < \theta_4 \leqq 1.$$

Replacing in (4) $[x]$ by $x - 1 + \theta_5$ and $M_4(x)$, $N_1(x) - N_{12}(x)$ and $N_2(x)$ by their values, setting $m = t + 1$ and observing that in the last summation $n \in T$, may be replaced by $n \in S$, one obtains (2) with $R = \theta_1 f \log x/7 + \theta_1\theta_2 - (7/8)\theta_2 - (7/6)4^{-\theta_2} + \theta_3 + (m-1)\theta_4 - \theta_5 + 13/6$, $0 < \theta_i \leqq 1$ $(i = 1, 2, \cdots, 5)$. For $x \to \infty$, R is dominated by its first term; hence, R is maximum for $\theta_1 = \theta_3 = \theta_4 = 1$, $\theta_5 = 0$. An elementary consideration shows that now R increases with θ_2; setting $\theta_1 = \theta_2 = \theta_3 = \theta_4 = 1$, $\theta_5 = 0$ one obtains $R = f \log x/7 + m + 2$. Similarly, one shows that $R = 0$ is the least possible value for R, attained for $\theta_1 = \theta_3 = \theta_4 = 0$, $\theta_2 = \theta_5 = 1$. In order to complete the proof of the theorem it is sufficient to observe that R cannot take its extreme values, because $\theta_i \neq 0$.

5. By direct computation one finds that the integers 1, 2, 5, 10, 13, 25, 37, 58, 85 and 130 belong to S, and up to 2000 no further integers of S are found. This suggests (see [**10**]) the

CONJECTURE. $S = \{1, 2, 5, 10, 13, 25, 37, 58, 85, 130\}$. From this conjecture would follow that $m = 10$ and (2) could be sharpened to read:

$$N(x) = \frac{5}{6} x - \frac{73}{8} f \log x + a - R$$

with $f = (\log 4)^{-1}$, $a = 19.68 \cdots$ and $\theta < R < 12 + f \log x/7$.

BIBLIOGRAPHY

1. P. T. Bateman, *Representations of a number as a sum of squares*, Trans. Amer. Math. Soc. vol. 71 (1951) pp. 70–101.

2. M. C. Chakrabarti, *On the limit points of a function connected with the three-square problem*, Bull. Calcutta Math. Soc. vol. 32 (1940) pp. 1–6.

3. R. Descartes, *Oeuvres*, vol. 2, Paris, Cerf, 1898.

4. L. E. Dickson, *History of the theory of numbers*, New York, Chelsea Publishing Company, 1952.

5. E. Dubouis, L'Interm. des Math. vol. 18 (1911) pp. 55–56, 224–225.

6. T. Esterman, *On Dirichlet's L-functions*, J. London Math. Soc. vol. 23 (1948) pp. 275–279.

7. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 3d ed., Oxford, The Clarendon Press, 1954.

8. A. Hurwitz, *Problems*, L'Interm. des Math. vol. 14 (1907) p. 107, Math. Werke vol. 2, p. 751.

9. E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2d ed., New York, Chelsea Publishing Company, 1953.

10. D. H. Lehmer, *On the partition of numbers into squares*, Amer. Math. Monthly vol. 55 (1948) pp. 476–481.

11. G. Pall, *On sums of squares*, Amer. Math. Monthly vol. 40 (1933) pp. 10–18.

12. C. L. Siegel, *Ueber die Classenzahl quadratischer Zahlkoerper*, Acta Arithmtica vol. 1 (1936) pp. 83–86.

Carleton College and
University of Pennsylvania