NOTES

When Is n^2 a Sum of k Squares?

TODD G. WILL
University of Wisconsin–La Crosse
La Crosse, WI 54601
will.todd@uwlax.edu

The square 169 can be written as a sum of two squares $5^2 + 12^2$, as a sum of three squares $3^2 + 4^2 + 12^2$, as a sum of four squares $1^2 + 2^2 + 8^2 + 10^2$, as a sum of five squares $1^2 + 2^2 + 2^2 + 4^2 + 12^2$, and so on for quite a long while. In fact, Jackson, et al. [**5**] note that 169 can be written as a sum of k positive squares for all k from 1 to 155 and first fails as a sum of length 156. The authors go on to ask whether there is any limit to such a string of sums. Specifically, for every positive integer b is there an integer n which can be written as a sum of k positive squares for all k from 1 to b? We assemble a collection of results, most of which have been known for quite some time, to answer this question and, in fact, to specify all possible lengths for sums of squares equal to a given square.

This investigation began when I read a manuscript in which the author proved that a certain combinatorially defined integer $c(k)$ could be written as a sum of k positive integer squares. Although the proof technique was interesting, I wondered if it wouldn't be more surprising to find that a sufficiently large integer *couldn't* be written as a sum of k squares. For that reason, in what follows we address the possible lengths for sums of squares equal to a given integer which may or may not be a square.

Sums of 5 or more positive squares Dickson [**1**] credits Dubouis with publishing the following theorem in 1911. An integer $n \geq 34$ can be written as a sum of k positive squares for all k satisfying $5 \leq k \leq n$ except for $k = n - 13$, $n - 10$, $n - 7$, $n - 5$, $n - 4$, $n - 2$, $n - 1$. Writing 20 years later, Pall [**7**] laments over having duplicated Dubouis' work before noticing the report of it but resists presenting his own proof. Writing over 75 years later still, I suspect that both Dubouis' and Pall's proofs resembled the following.

First we show that no integer n can be written as a sum of k positive squares for $k \in \{n - 13, n - 10, n - 7, n - 5, n - 4, n - 2, n - 1\}$. To see this note that the sum of k positive squares $n = s_1^2 + \cdots + s_k^2$ can be obtained from the sum of n ones by repeatedly replacing s_i^2 of the ones with the single square s_i^2. This replacement reduces the number of summands by $s_i^2 - 1$. For example, replacing four ones, $1 + 1 + 1 + 1$, with a single square 2^2 reduces the number of summands by 3. A replacement of 3^2 ones reduces the number of summands by 8 and larger squares reduce the number of summands by at least 15. A quick check shows that the count of n summands in the sum of all ones cannot be reduced by any of the amounts 1, 2, 4, 5, 7, 10, 13 using reductions of 3 and 8.

We now use induction to show that n can be written as sums of the specified lengths, securing the base case of $n = 34$ with a hand check. For $n > 34$ we add 1^2 to each of

Math. Mag. **83** (2010) 210–213. doi:10.4169/002557010X494850. © Mathematical Association of America

the sums of squares equal to $n-1$ given by the induction hypothesis. This gives all of the required lengths of sums for n except for a length 5 sum.

The proof is completed by showing that all $n > 34$ can be written as a sum of 5 positive squares. A computer check (an additional hand check for Pall and Dubouis) verifies this for $34 < n \leq 169$. For $n > 169$ we use Lagrange's theorem, which states that every positive integer can be written as a sum of four or fewer positive squares. For $n > 169$, use Lagrange's theorem to write $n - 169$ as a sum of 1, 2, 3 or 4 positive squares. Then add the appropriate representation of 169 as the sum of 4, 3, 2, or 1 positive squares to obtain five positive squares summing to n.

So, except for lengths of 2, 3, and 4, this result specifies all possible lengths for sums of squares equal to a given square. In addition the result greatly simplifies the question in Jackson, et al., since if a square n can be written as a sum of 2, 3, and 4 positive squares then n can be written as a sum of k positive squares for all $1 \leq k \leq n - 14$.

Sums of two positive squares There seems to be some disagreement about when an integer can be written as a sum of two positive squares. In the 1959 article [**3**] the condition is stated that the integer must have the form $4^a n_1 n_2^2$, with integral $a \geq 0$, $n_1 > 1$, the prime factors of n_1 congruent to 1 mod 4 and the prime factors of n_2 congruent to 3 mod 4. In the 2006 book [**6**] the condition is the same except that 4^a is replaced with 2^e, with e a nonnegative integer. In both sources the claims are said to follow easily from previous results, but proofs are not given. However, neither of these conditions include $18 = 2 \times 3^2 = 3^2 + 3^2$ since 18 has no $4k+1$ prime factor. More generally the conditions exclude the numbers $n = m^2 + m^2$ where m has no $4k+1$ prime. Perhaps the authors meant to describe conditions in which n could be written as a sum of two distinct positive squares.

In any case, the correct statement is that a positive integer n can be written as the sum of two positive squares if and only if either n is twice a square or n has at least one $4k+1$ prime factor and all of its $4k+3$ prime factors appear to even powers.

This fact follows easily from the much deeper theory for computing $r_k(n)$ which is defined to be the number of ways of writing n as a sum of k integer squares. In computing $r_k(n)$ the squares of both positive and negative integers as well as 0^2 are allowed and permutations of addends are counted as distinct sums. So, for example $r_2(9) = 4$ since $9 = 0^2 + (\pm 3)^2 = (\pm 3)^2 + 0^2$ are the four ways to express 9 as the sum of two integer squares.

Let $n = 2^k \prod p_i^{a_i} \prod q_j^{b_j}$ be the prime factorization of n with the p_i and q_j being the primes congruent to 1 and 3 mod 4, respectively. Gauss showed that if any of the b_j are odd then $r_2(n) = 0$ and otherwise $r_2(n) = 4\prod(1 + a_i)$. So for example, since $n = 9$ has no $4k+3$ primes to an odd power, and all $4k+1$ primes occur to the zero power, $r_2(9) = 4(1+0) = 4$ as counted above.

Now assume that $n = a^2 + b^2$ is the sum of two positive squares. Either n is twice a square or $a \neq b$ in which case $n = (\pm a)^2 + (\pm b)^2 = (\pm b)^2 + (\pm a)^2$ shows that $r_2(n) \geq 8$. From this it follows that all $4k+3$ primes appear to even powers and there is at least one $4k+1$ prime. Conversely, if $n = 2k^2$, then clearly n is the sum of two nonzero squares. If, on the other hand, all $4k+3$ primes appear to even power and there is at least one $4k+1$ prime, then $r_2(n) \geq 8$. Since at most 4 of these sums can use 0^2, there must be a sum with two positive squares.

Sums of three positive squares When an integer can be written as a sum of three positive squares has not quite been pinned down. Legendre showed that numbers of the form $4^h(8k+7)$ are those which cannot be written as the sum of three *or fewer* positive squares. But this left open the set of numbers which cannot be written as a sum of three positive squares but can be written as a sum of one or two. In 1959 Grosswald,

et al., [**3**] proved that there exists a finite set of integers S such that n is not the sum of three positive squares if and only if $n = 4^h q$ where $q = 7 \bmod 8$ or q is an element of the finite set S. They conjectured that $S = \{1, 2, 5, 10, 13, 25, 37, 58, 85, 130\}$ but their proof showed only that the set S is finite.

Despite this disappointment, it is known which *squares* are sums of three positive squares. Hurwitz [**4**] proved that with the exception of $(2^k)^2$ and $(5 \times 2^k)^2$, every positive square can be written as a sum of three positive squares. Fraser and Gordon later gave an elementary proof of this fact in [**2**].

As a digression, note that Hurwitz's result shows that the set S contains no squares other than 1 and 25. So, in considering whether there might be additional numbers in S, we need only consider nonsquares. If n is not a square, then for $n = a^2 + b^2$ neither a nor b are zero and so the orderings in the three sums $0^2 + a^2 + b^2$, $a^2 + 0^2 + b^2$, $a^2 + b^2 + 0^2$ are distinct. If n cannot be written as a sum of three positive squares, then all sums of three squares equal to n must have one of these three forms. Thus if n is not a square, then n cannot be written as a sum of three positive squares if and only if $r_3(n) = 3r_2(n)$. In three hours, a laptop search using Mathematica's built-in SquaresR function verified that the conjectured values for S are correct for $n \leq 5 \times 10^6$.

Sums of four positive squares In [**6**], Pall is credited with showing that n can be written as a sum of four positive squares if and only if n is not one of $\{1, 3, 5, 9, 11, 17, 29, 41\}$ or of the form 2×4^k, 6×4^k, 14×4^k. In a footnote of the cited work [**7**], Pall says that "the reader will have no difficulty in proving [this result] by using the following classical result, which was first stated by Fermat, and was first proved by Legendre in 1798. A positive integer is a sum of three [or fewer positive] squares if and only if it is not of the form $4^h(8k + 7)$". With such a challenge I picked up my pen and searched for the proof. Minutes ticked away to hours with my ego sinking all the while. I eventually did hit upon the following proof similar to the one I later found in [**8**].

First note that $4^h(8k + 7) = 0, 4, 7 \bmod 8$. If $n = 2, 3, 4, 6, 7 \bmod 8$, then $n - 13^2 = 1, 2, 3, 5, 6 \bmod 8$ and so $n - 13^2$ is not of the form $4^h(8k + 7)$. Thus for $n > 13^2$, Legendre's results shows that $n - 13^2$ can be written as a sum of three or fewer positive squares. Augment this sum with the appropriate choice from among $13^2 = 5^2 + 12^2 = 3^2 + 4^2 + 12^2$ to obtain four positive squares summing to n. For $n \leq 13^2$, a computer check finds that $\{2, 3, 6, 11, 14\}$ are the only integers in these congruence classes which cannot be written as a sum of four positive squares.

If $n = 1, 5 \bmod 8$, then $n - 26^2 = 5, 1 \bmod 8$. So for $n > 26^2$, $n - 26^2$ can be written as a sum of three positive squares. Augment this sum with the appropriate choice from among $26^2 = 10^2 + 24^2 = 6^2 + 8^2 + 24^2$ to obtain four positive squares summing to n. For $n \leq 26^2$, a computer check finds that $\{1, 5, 9, 17, 29, 41\}$ are the only integers in these congruence classes which cannot be written as a sum of four positive squares.

If $n = 0 \bmod 8$, consideration mod 8 shows that n is a sum of four positive squares if and only if $n/4$ is. Repeated applications of this observation allows n to be written as $4^a 2j$ where $2j \neq 0 \bmod 8$ and n is a sum of four positive squares if and only if $2j$ is. Previous cases show that $2j \neq 0 \bmod 8$ is not a sum of four positive squares only for $2j = 2, 6, 14$.

Conclusion What, then, are the possible lengths for sums of squares equal to a given positive square?

The possible lengths of 5 and higher are specified by Dubouis' result for squares 36 and above. A direct check shows that the same result holds for 16 and 25 and that the possible sum lengths for 9 are 1, 3, 6, 9. Since a square cannot also be twice a square,

the squares which can be written as a sum of two positive squares are those with a prime factor congruent to 1 mod 4. We see that among positive squares, $(2^k)^2$ and $(5 \times 2^k)^2$ are the only ones which cannot be written as a sum of three positive squares and that 1 and 9 are the only ones which cannot be written as a sum of four positive squares.

Combining these conditions, we learn that with the exception of $(5 \times 2^k)^2$, a square can be written as sums of 2, 3, and 4 positive squares if and only if it has at least one prime factor congruent to 1 mod 4. Moreover such a square n can be written as a sum of k positive squares for all k from 1 to $n - 14$.

The first few squares meeting the combined conditions are 169, 225, 289, 625, 676, 841, 900. Going out a little farther we find $n = 1\,000\,002\,000\,001 = (101 \times 9901)^2$ with 101 being a prime congruent to 1 mod 4. So this square can be written as a sum of k positive squares for all k from 1 to 1 000 001 999 987, making 169's run of 155 look not so special after all.

REFERENCES

1. Leonard Eugene Dickson, *History of the Theory of Numbers, Vol. II: Diophantine Analysis*, Dover, New York, 2005.
2. Owen Fraser and Basil Gordon, On representing a square as the sum of three squares, *Amer. Math. Monthly* **76** (1969) 922–923. doi:10.2307/2317949
3. E. Grosswald, A. Calloway, and J. Calloway, The representation of integers by three positive squares, *Proc. Amer. Math. Soc.* **10** (1959) 451–455. doi:10.2307/2032865
4. Adolf Hurwitz, *Mathematische Werke. Bd. II: Zahlentheorie, Algebra und Geometrie*, Birkhäuser Verlag, Basel, 1963.
5. Kelly Jackson, Francis Masat, and Robert Mitchell, Extensions of a sums-of-squares problem, *Math. Mag.* **66** (1993) 41–43.
6. Carlos J. Moreno and Samuel S. Wagstaff, Jr., *Sums of Squares of Integers*, Chapman & Hall/CRC, Boca Raton, FL, 2006.
7. Gordon Pall, On sums of squares, *Amer. Math. Monthly* **40** (1933) 10–18. doi:10.2307/2301257
8. Don Redmond, *Number Theory: An Introduction*, Marcel Dekker, New York, 1996.

Summary This note shows that with the exception of $(5 \times 2^k)^2$, an integer square can be written as sums of 2, 3, and 4 positive squares if and only if it has at least one prime factor congruent to 1 mod 4. Moreover such a square n can be written as a sum of k positive squares for all k from 1 to $n - 14$. The question of when a non-square can be written as a sum of k positive squares is also examined.

How Fast Will We Lose?

RON HIRSHON
College of Staten Island
Staten Island, NY 10314
rhirshon@aol.com

Two players X and Y play a gambling game. They start with bankrolls of x and y dollars respectively, where x and y are positive integers and $(x, y) \neq (1, 1)$. They repeatedly flip a coin, which may be a fair or unfair coin. When heads appears, X wins and receives one dollar from Y; when tails appears, X loses and pays one dollar to Y.

Math. Mag. **83** (2010) 213–218. doi:10.4169/002557010X494869. © Mathematical Association of America