Characterization of the Positive Integers Represented as a Sum of Two Squares

Storm Frazier

April 24, 2019

Abstract

The purpose of this paper is to explore the characterizations of positive numbers that can be written as the sum of two squares.

Introduction

Given $n \in \mathbb{N}$, we can say that n is a *sum of two squares* if there exists non-negative $x, y \in \mathbb{Z}$ such that $n = x^2 + y^2$. For example 25 is a sum of two squares since,

$$25 = 4^2 + 3^2 = 5^2 + 0^2 = \left(2^2 + 1^2\right)\left(2^2 + 1^2\right) = (4+1)^2 + (2-2)^2$$

The example of 25 gives rise to a few interesting characterizations. Note that 25 has more than one distinct sum of squares representation. Note also that 25 is the product of two sum of squares also. In general, which numbers can be respresented as a sum of two squares? If a number can be represented as a sum of two squares, how many distinct representations does it have? Can the problem be reduced to dealing only with primes? We will start by answering the first question.

Classification

Among all the integers from 1 to 100, the following are not representable as a sum of two squares.

3	6	7	11	12	14	15	19	21	22	23
24	27	28	30	31	33	35	38	39	42	43
44	46	47	48	51	54	55	56	57	59	60
62	63	66	67	69	70	71	75	76	77	78
79	83	84	86	87	88	91	92	93	94	95
96	99									

Compared to the integers that are representable as a sum of two squares.

1	2	4	5	8	9	10	13	16	17	18
20	25	26	29	32	34	36	37	40	41	45
49	50	52	53	58	61	64	65	68	72	73
74	80	81	82	85	89	90	97	98	100	

After a quick investigation, it is clear that there is no set pattern as to which integers have a sum of squares representation, but can we at least narrow down our search?

Theorem 1: Consider $x \in \mathbb{Z}$, then $x^2 \equiv 0\,(mod 4)$ or $x^2 \equiv 1\,(mod 4)$.

Proof: Take $x \in \mathbb{Z}$. Suppose x is even. Then $x = 2n$, where $n \in \mathbb{Z}$. Then, $x^2 = 4n^2 = 4\left(n^2\right) \equiv 0\,(mod 4)$. Suppose x is odd. So $x = 2n+1$, where $n \in \mathbb{Z}$. Then, $x^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 4(n^2+n) + 1 \equiv 1\,(mod 4)$ $\square$

Theorem 2: If $n \equiv 3\,(mod 4)$, then n is not a sum of two squares.

Proof: Take $n \in \mathbb{N}$ such that $n \equiv 3\,(mod 4)$. Recall that $x^2 \equiv 0{,}1\,(mod 4)$ for all integers x. Thus for any two integers a and b, $a^2 + b^2 \equiv 0, 1$, or $2\,(mod 4)$. So $a^2 + b^2 \equiv 3\,(mod 4)$ is impossible. $\square$

Theorem 3: An odd prime number p is a sum of two squares iff $p \equiv 1\,(mod 4)$

Proof: Suppose we have an odd prime $p = x^2 + y^2$ for some non-negative $x, y \in \mathbb{Z}$. By *Theorem* 1, $x^2, y^2 \in \{0, 1\}\,(mod 4)$, thus $p \in \{0, 1, 2\}\,(mod 4)$. Because p is odd, it follows $p \equiv 1\,(mod 4)$. Conversely, suppose $p \equiv 1\,(mod 4)$. Then we have the Legendre symbol $\left(\frac{-1}{p}\right) = 1$. Take $r \in \mathbb{N}$ with $r^2 \equiv -1\,(mod p)$. Define $f(x, y) = x + ry$ and $N = \lfloor \sqrt{p} \rfloor$. Note that

$$N < \sqrt{p} < N + 1,$$

as $\sqrt{p} \notin \mathbb{N}$. Consider all pairs (x, y) with $0 \leq x \leq N$ and $0 \leq y \leq N$. There exist $(N+1)^2 > p$ such pairs. If we then consider the multiset of all $f(x, y)$ for such x, y, then by the Pigeonhole Principle, two such pairs $(x_1, y_1) \neq (x_2, y_2)$ for which $f(x_1, y_1) \equiv f(x_2, y_2)\,(mod p)$. Hence,

$$x_1 + ry_1 \equiv x_2 + ry_2\,(mod p)$$

$$x_1 - x_2 \equiv -r\,(y_1 - y_2)$$

$$a \equiv -rb\,(mod p)\,,$$

where $a = (x_1 - x_2)$ and $b = (y_1 - y_2)$. Hence $a^2 \equiv -b^2\,(mod p)$ since $r^2 \equiv -1\,(mod p)$, giving us $p \mid a^2 + b^2$. But $|a| \leq N$ and $|b| \leq N$, giving
$0 < a^2 + b^2 \leq 2N^2 < 2p$. Thus $a^2 + b^2 = p$. $\square$

Theorem 4: If n, m are positive integers with a sum of two squares representation, then the product nm can be written as a sum of two squares.

Proof: Suppose $n = x^2 + y^2$ and $m = w^2 + z^2$, where $w, x, y, z \in \mathbb{Z}$. Then,

$$nm = \left(x^2 + y^2\right)\left(w^2 + z^2\right)$$

$$= x^2w^2 + x^2z^2 + y^2w^2 + y^2z^2$$

$$= x^2w^2 + x^2z^2 + 2xyzw - 2xyzw + y^2w^2 + y^2z^2$$

$$= \left(x^2w^2 + 2xyzw + y^2z^2\right) + \left(x^2z^2 - 2xyzw + y^2w^2\right)$$

$$= (xw - yz)^2 + (xz + yw)^2$$

$\square$

Theorem 5: If $3 \mid x^2 + y^2$, then $3 \mid x$ and $3 \mid y$.

Proof: By contrapositive. Assume that $3 \nmid x$ or $3 \nmid y$. WOLOG assume x is not divisible by 3. Then, $x = 3k + 1$ or $x = 3k + 2$ for $k \in \mathbb{Z}$. So, $(3k+1)^2 = 9k^2+6k+1 = 3(3k^2+2k)+1 \equiv 1\,(mod 3)$. Similarly, $(3k+2)^2 = 9k^2+12k+4 = 3(3k^2+4k)+4 \equiv 1\,(mod 3)$. Thus, $x^2 \equiv 1\,(mod 3)$ and $y^2 \equiv 0, 1\,(mod 3)$. So $x^2 + y^2 \equiv 1, 2\,(mod 3)$, thus not divisible by 3.□

Theorem 6: If $n \equiv 3\,(mod 9)$ or $n \equiv 6\,(mod 9)$, then n is not the sum of two squares.

Proof: By contradiction. Assume that $n = x^2 + y^2$ and $n \equiv 3, 6\,(mod 9)$. Therefore, $3 \mid n$. So by *Theorem* 5 we have that $3 \mid x$ and $3 \mid y$. Thus $x^2 = (3k)^2 = 9k^2 \equiv 0\,(mod 9)$ and $y^2 = (3l)^2 \equiv 0\,(mod 9)$ for some $k, l \in \mathbb{Z}$. So $x^2 + y^2 \equiv 0\,(mod 9)$. A contradiction to the assumption $n \equiv 3, 6\,(mod 9)$. □

Theorem 7: If n is a positive integer such that every prime factor of n that is congruent to 3 modulo 4 appears with an even power, then n has a sum of two squares representation.

Proof: Suppose $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_0} \dots q_r^{\beta_r}$ where each $p_i \equiv 1\,(mod 4)$ and each $q_j \equiv 3\,(mod 4)$ with β_j even. 2 is clearly a sum of squares, namely $2 = 1^2 + 1^2$. Each p_i is a sum of two squares, thus $p_i^{\alpha_i}$ is also a sum of two squares by *Theorem* 3. Because each β_j is even, can write $\beta_j = 2\beta_j'$. We then have $q_j^{\beta_j} = \left(q_j^{\beta_j'}\right)^2 + 0^2$, so each term can written as the sum of two squares. So together using *Theorem* 4 it follows that the product $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_k^{\alpha_k} q_1^{\beta_0} \dots q_r^{\beta_r}$ is also a sum of two squares. □

Other Properties

Now that we have classified what integers can be represented as a sum of two squares, the next questions might be, are they unique? Given a sum of two squares for an integer, can we produce more, and if we can, how many more? Next we will explore how to find additional representations of an integer. I won't present any new theorems, but instead will give some insight into what methods to use to find additional sum of two squares. The use of Guassian integers will be required.

Suppose we have an integer c with the sum of two squares $a^2 + b^2$. Then writing c as the sum of two squares, $c = a^2 + b^2$, is equivalent to factoring c as $c = (a + bi)(a - bi)$ over the Gaussian integers. So to find all possible factors of c, we just need to solve the problem for each prime factor of c of the form

$4k+1$. Then we combine each factor in each possible way to get all our sums of two squares.

Examples: Suppose $n = 85$, which factors as $5 \cdot 17$. We have $5 = 2^2 + 1^2 = (2+i)(2-i)$, and $17 = 4^2 + 1^2 = (4+i)(4-i)$. We can then write 85 as a sum of two squares using the following method:

- Taking $(2+i)(4+i) = 7+6i$ tells us $85 = 7^2 + 6^2$.
- Taking $(2+i)(4-i) = 9+2i$ tells us $85 = 9^2 + 2^2$.

Note that any other combination is redundant since we are squaring the result. Consider a more complicated example, $n = 1170$, which factors as $2 \cdot 3^2 \cdot 5 \cdot 13$. Note that 3 can not be written as sum of two squares, so must treat 3^2 as $(3+0i)(3-0i)$. Next, $2 = 1^2 + 1^2 = (1+i)(1-i)$. We have $5 = 2^2 + 1^2 = (2+i)(2-i)$. Finally, $13 = 3^2 + 2^2 = (3+2i)(3-2i)$. Consider:

- Taking $(1+i)(3+0i)(2+i)(3+2i) = -21+27i$ tells us $1170 = 21^2 + 27^2$.
- Taking $(1+i)(3+0i)(2+i)(3-2i) = 33+9i$ tells us $1170 = 33^2 + 9^2$.

Again note that any other combination yields the same results. The difficulty in finding a sum of two squares lies in the factoring.

References

[1] Hardy, Wright. An Introduction to the Theory of Numbers. Oxford. 1954.

[2] K. Rosen. Elementary Number Theory and Its Applications. Addison-Wesley Publishing Co. 1993.

[3] P. Shiu, Euler's contribution to number theory, Math. Gazette 91 (2007), 453–461.

[4] Underwood, Dudley (1978). Elementary Number Theory (2 ed.). W.H. Freeman and Company. pg. 136-140.

[5] https://www.maths.ed.ac.uk/~chris/NTh/Ch6_Sum2sq_Ch7_Fermat_descent.pdf

[6] https://math.stackexchange.com/questions/2294749/finding-other-representations-for-a-sum-of-two-squares