Written Assignment 1
Sum of Two Squares

Elijah Hantman
University of California at Santa Cruz
Santa Cruz, CA 95064 USA

July 17, 2025

Abstract

We discuss when a given positive integer can be expressed as a sum of two squares. For odd primes, this question depends on whether these odd primes are congruent to 1 or 3 modulo 4.

1 Introduction

We say that a positive integer n is a sum of two squares if there exist integers a and b such that $n = a^2 + b^2$. Some positive integers can be expressed as a sum of two squares, but not all integers admit such an expression. For example integer 7 cannot be a sum of two squares as can be easily seen. Some integers admit more than one way to write it as a sum of two squares. For example,

$$745 = 27^2 + 4^2 = 24^2 + 13^2.$$

In this short article, we attempt to characterize those integers which can be written as sum of two squares.

This is a generalization of a theorem by Pierre Fermat which characterizes exactly which odd primes can be represented as the sum of two squares.

2 Basic Properties

First we show that the set of positive integers which are sum of two squares is closed under products. We can use the following formulae.

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= (ac + bd)^2 + (ad - bc)^2 \\ &= (ac - bd)^2 + (ad + bc)^2.\end{aligned}$$

Lemma 2.1. *If m and n are each a sum of two squares, then their product mn is also a sum of two squares.*

Proof.

$$
\begin{aligned}
m &= a^2 + b^2 \tag{1}\\
n &= c^2 + d^2 \tag{2}\\
mn &= (a^2 + b^2)(c^2 + d^2) \tag{3}\\
mn &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \tag{4}\\
mn &= (ac + bd)^2 + (ad - bc)^2 \tag{5}\\
mn &= (ac - bd)^2 + (ad + bc)^2 \tag{6}
\end{aligned}
$$

□

Notice that the above two formululae give two ways to write mn as sums of two squares.

Every integer which is a square, say N^2, is trivially a sum of two squares since $N^2 = N^2 + 0^2$. More generally,

Lemma 2.2. *If m is a sum of two squares, then the integer N^2m is also a sum of two squares.*

Proof.

$$
\begin{aligned}
m &= a^2 + b^2 \tag{7}\\
N^2m &= N^2(a^2 + b^2) \tag{8}\\
&= a^2N^2 + b^2N^2 \tag{9}\\
&= (aN)^2 + (bN)^2 \tag{10}
\end{aligned}
$$

□

Every positive integer n can be written uniquely as $n = N^2m$ where N, m are positive integers and m is square free, that is, in the prime decomposition of m every prime factor of m appears exactly once, to the first power.

In view of previous lemmas, if every prime appearing in m is a sum of two squares, then $n = N^2m$ is also a sum of two squares. Thus, our next question is; which prime is a sum of two squares? The answer, surprisingly, depends on the property of primes $\mod 4$, for odd primes. For the even prime $p = 2$, it is of course a sum of two squares: $2 = 1^2 + 1^2$. To investigate this question, we first prove one general result.

Theorem 2.3. *If a positive integer n is a sum of two squares, then $n \equiv 0, 1, 2 \mod 4$.*

Proof. If a positive integer n is squared there are 4 cases.

Case 1: $n \equiv 0$ modulo 4.

$$
\begin{aligned}
n &= 4k \tag{11}\\
n^2 &= 16k^2 \tag{12}\\
n^2 &= 4(4k^2)n^2 \equiv 0 \tag{13}
\end{aligned}
$$

Case 2: $n \equiv 1$ modulo 4.

$$n = 4k + 1 \tag{14}$$
$$n^2 = 16k^2 + 8k + 1 \tag{15}$$
$$n^2 = 4(4k^2 + 2k) + 1 \tag{16}$$
$$n^2 \equiv 1 \tag{17}$$

Case 3: $n \equiv 2$ modulo 4.

$$n = 4k + 2 \tag{18}$$
$$n^2 = 16k^2 + 16k + 4 \tag{19}$$
$$n^2 = 4(4k^2 + 4k + 1) \tag{20}$$
$$n^2 \equiv 0 \tag{21}$$

Case 4: $n \equiv 3$ modulo 4.

$$n = 4k + 3 \tag{22}$$
$$n^2 = 16k^2 + 24k + 9 \tag{23}$$
$$n^2 = 16k^2 + 24k + 8 + 1 \tag{24}$$
$$n^2 = 4(4k^2 + 6k + 2) + 1 \tag{25}$$
$$n^2 \equiv 1 \tag{26}$$

Now consider the sum of two positive integers.

$$a = 4k + s \tag{27}$$
$$b = 4r + v \tag{28}$$
$$a + b = 4k + 4r + s + v \tag{29}$$
$$a + b = 4(k + r) + s + v \tag{30}$$

We can see the sum is congruent to the sum of s and v modulo 4.

As shown above, the square of a positive integer modulo 4 is congruent to either 0 or 1. This gives 3 possibilities without loss of generality.

Case 1: $a^2 \equiv 0$ and $b^2 \equiv 0$.

$$a^2 + b^2 \equiv 0 + 0 \equiv 0 \tag{31}$$

Case 2: $a^2 \equiv 1$ and $b^2 \equiv 0$.

$$a^2 + b^2 \equiv 1 + 0 \equiv 1 \tag{32}$$
$$a^2 + b^2 \equiv 0 + 1 \equiv 1 \tag{33}$$

Case 3: $a^2 \equiv 1$ and $b^2 \equiv 1$.

$$a^2 + b^2 \equiv 1 + 1 \equiv 2 \tag{34}$$

We can therefore see that the sum of two squares must be congruent to 0, 1 or 2 modulo 4. □

As an immediate consequence, we get the following corollaries.

Corollary 2.4. *If an odd prime p is a sum of two squares, then we have $p \equiv 1 \mod 4$.*

Proof. Assume p is an odd prime and a sum of two squares.

There are three cases, either p modulo 4 is 0, 1, or 2.

If p modulo 4 is 0:

$$p = 4k + 0 \tag{35}$$

$$p = 4k \tag{36}$$

$$4|p \tag{37}$$

Therefore p cannot be prime and thus p modulo 4 cannot be 0.

If p modulo 4 is 2:

$$p = 4k + 2 \tag{38}$$

$$p = 2(k + 1) \tag{39}$$

$$2|p \tag{40}$$

Therefore p cannot be prime and thus cannot be congruent to 2. By process of elimination any odd prime p which is a sum of 2 squares, it must be congruent to 1 modulo 4. □

Corollary 2.5. *If an odd prime p is such that $p \equiv 3 \mod 4$, then p is not a sum of two squares.*

Proof. According to theorem 2.3, all positive integers must be congruent to 0, 1, or 2 modulo 4 if they are the sum of two squares.

All odd primes are positive integers, so if an odd prime is the sum of two squares it must be congruent to 0, 1, or 2 modulo 4. □

The question is which odd prime p such that $p \equiv 1 \mod 4$ can be written as a sum of two squares. This is the content of the famous Fermat's Theorem.

Theorem 2.6 (Fermat). *Every odd prime p such that $p \equiv 1 \mod 4$ is a sum of two squares.*

The proof is not easy, so we do not discuss here. By combining all previous results, we obtain the following characterization on the set of integers which are sum of two squares.

Theorem 2.7. *Let n be a positive integer and write it as $n = N^2m$ where m is square free. If m contains no prime factor of the form $4k + 3$, then n is a sum of two squares.*

Proof. Assume n is a sum of two squares.

Because n is a positive integer we can write it as N^2m where m is a square free number. We know by Lemma 2.2 that if n is a sum of two squares then m must also be a sum of 2 squares.

Since m is a square free number we can write it as the product $\prod m_1m_2m_3$.... However we know from Lemma 2.2 that the product of two numbers is a sum of squares if the terms are sums of squares.

We know that some term m_n is of the form $4k + 3$. This means that m_n is an odd prime of the form $4k + 3$ which means it is congruent to 3 modulo 4. However by Corollary 2.5 we know that all odd primes congruent with 3 modulo 4 cannot be the sum of squares.

Therefore m cannot be a sum of squares, and therefore n cannot be a sum of squares. □

It is known that the above property completely characterizes the set of positive integers which are sum of two squares.

For example, we can write the following integers as sums of two squares in two different ways, as follows.

- $3185 = 5 \cdot 7^2 \cdot 13 = (1^2 + 2^2) \cdot 7^2 \cdot (3^2 + 2^2) = 49^2 + 28^2 = 7^2 + 56^2$
- $48314 = 2 \cdot 7^2 \cdot 17 \cdot 29 = (1^2 + 1^2) \cdot 7^2 \cdot (5^2 + 2^2) \cdot (4^2 + 1^2) = 217^2 + 35^2 = 175^2 + 133^2$.

3 Closing Remarks

While not the most important theorem or property in algebra and mathematics, but it is a very interesting observation and characterization. The sum of two squares answers the question about what integer pythagorean triples exist, and provides a method to construct new pythgorean triples via mutiplication of odd primes.

References

[1] J. Abhau, C.-F. Bödigheimer and R. Ehrenfried, *Homology of the mapping class group* $\Gamma_{2,1}$ *for surfaces of genus 2 with a boundary curve*, arXiv:0712.4254.

[2] M. F. Atiyah, *Topological quantum field theories*, Inst. Hautes Etudes Sci. Publ. Math. No 68 (1988), 175–186.

[3] C.-F. Bödigheimer and U. Tillmann, *Stripping and splitting decorated mapping class groups*, Birkhäuser, Progress in Math. 196(2001), 47–57.

[4] K.S. Brown, *Cohomology of Groups*, Graduate Texs in Mathematics, 87, Springer Verlag, New York (1982).

[5] D. Chataur and L. Menichi, *String topology of classifying spaces*, arXiv:0801.0174.

[6] M. Chas and D. Sullivan, *String topology*, CUNY, to appear in Ann. of Math. (1999). math.GT/9911159

[7] R. Cohen and V. Godin, *A polarized view of string topology*, Topology, geometry and quantum field theory, London Math. Soc. Lecture Note Ser. Vol 308, 127–154. Cambridge Univ. Press, Cambridge, 2004