Scientific Research Publishing

Advances in Pure Mathematics, 2026, 16(6), 412-415
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

A Sufficient Condition for the Primality of the Sum of Two Squares

Han-Lin Li[1], Shu-Cherng Fang[2], Way Kuo[3*]

[1]Department of Computer Science, City University of Hong Kong, Hong Kong SAR, China
[2]Department of Industrial and Systems Engineering, North Carolina State University, Raleigh, NC, USA
[3]Hong Kong Institute for Advanced Study, City University of Hong Kong, Hong Kong SAR, China
Email: *way@cityu.edu.hk

How to cite this paper: Li, H.-L., Fang, S.-C. and Kuo, W. (2026) A Sufficient Condition for the Primality of the Sum of Two Squares. *Advances in Pure Mathematics*, **16**, 412-415.
https://doi.org/10.4236/apm.2026.166022

Received: May 4, 2026
Accepted: June 8, 2026
Published: June 11, 2026

Abstract

The famous Fermat's Christmas Theorem states that all Pythagorean primes can be expressed as a sum of two squares of integers. This report specifies the conditions that a $(4k+1)$-type integer expressed in a sum of two squares becomes prime.

Keywords

Fermat, Brahmagupta-Fibonacci Identity, Primality

1. Introduction

Legendary mathematician Pierre de Fermat wrote to his friend on December 25, 1640 that any Pythagorean prime can be expressed as the sum of the squares of two integers [1]. This statement is known as Fermat's Christmas Theorem or Fermat's Sum of Two Squares Theorem, one of the most significant propositions in mathematics [2]-[4]. However, it remains largely an open and unsolved problem to find sufficient conditions for the primality of a $(4k+1)$-type of integer to be expressed as a sum of two squares.

Aletheia-Zomlefer [5] states that prime values of quadratic polynomials are conjectural in general. Cox [2] studies to determine which primes can be represented in quadratic forms, indicating that to claim under what conditions a sum of squares will be prime requires analytic conjectures. Iwaniec and Kowalski [6] also emphasize that the general problem of prime values of polynomials, including quadratic cases, remains open.

Pinz [7] indicates that Landau's problem of n^2+1 type is a long-standing challenge. Jacobi [8] [9] demonstrates that if an integer n has every $(4k+3)$-type

prime factor occurring to an even power, then the number of representations of n as a sum of two squares is $4\left(d_1(n)-d_3(n)\right)$, where $d_1(n)$ and $d_3(n)$ denote the numbers of $(4k+1)$-type and $(4k+3)$-type divisors of n; however, Jacobi's theorem does not specify any conditions implying the primality. Jacobi's formula specifies the number of sum-of-squares representations, which is not the focus of this study.

This brief report sets out when a $(4k+1)$-type integer expressed in a sum of two squares becomes prime. Our finding provides a characterization of primes $p \equiv 1 \pmod 4$ in terms of the uniqueness of sum-of-squares representation. This is a rather elegant result.

2. Preliminaries

Before diving into the main theorem and its proof, we recall some of the well-known results as background knowledge.

Fermat's Sum of Two Squares Theorem [4] (Fact 1) states that an odd prime p can be written as a sum of two squares if and only if $p \equiv 1 \pmod 4$. Moreover, when such a representation exists, it is unique up to order and signs.

General Representability [4] (Fact 2) states that a positive integer n can be expressed as a sum of two squares if and only if every prime factor of n that is congruent to 3 (mod 4) appears to an even power.

Brahmagupta-Fibonacci Identity [4] (Fact 3) states that the product of two sums of squares is itself a sum of squares, which may appear in two different expressions:

$$\left(x^2+y^2\right)\left(u^2+v^2\right)=\left(xu-yv\right)^2+\left(xv+yu\right)^2=\left(xu+yv\right)^2+\left(xv-yu\right)^2$$

for real numbers x, y, u, v.

This identity is the engine that generates multiple representations for composite numbers.

3. Main Theorem

Theorem Let a be a square-free positive integer and $a \equiv 1 \pmod 4$. If $a=c^2+d^2$ has a unique representation as the sum of two squares (up to order and signs) for a pair of positive integers c and d, then a is prime.

Proof:

First, notice that if $a=c^2+d^2$ and $g=\gcd(c,d)>1$, then g^2 divides $a=c^2+d^2$. But a is square free, so no perfect square greater than 1 can divide it. Therefore, $g=\gcd(c,d)=1$ holds automatically.

We now take a contrapositive proof: if a satisfies all the given conditions but is composite, then a has more than one distinct representation as a sum of two squares.

(Step 1): Let us determine the prime factors of a.

Suppose a satisfies our hypotheses: $a \equiv 1 \pmod 4$, a is square free, and $a=c^2+d^2$; $c,d \in N_+$ for some integers with $\gcd(c,d)=1$. Since a is square

free (no prime appears more than once), we have the factorization: $a = p_1 p_2 \cdots p_k$ with each p_i being a distinct prime for $i = 1, \cdots, k$.

Let us check what kinds of primes can divide a.

(i) It is easy to see that no prime $p_i \equiv 0 \pmod 4$ or $p_i \equiv 2 \pmod 4$ can divide a. (ii) Since a is expressible as a sum of two squares, Fact 2 tells that any prime $p_i \equiv 3 \pmod 4$ dividing a must appear to be an even power. However, a is square-free, therefore no prime $p_i \equiv 3 \pmod 4$ can divide a at all. Therefore, every prime factor of a must be congruent to 1 (mod 4). In other words,

$$a = p_1 p_2 \cdots p_k$$

where each p_i is a distinct prime with $p_i \equiv 1 \pmod 4$.

(Step 2): Let us count possible sum-of-squares representations of a.

This counting work follows the basics of [2] [4] [7] easily. By Fermat's Two-Square Theorem (Fact 1), each prime $p_i \equiv 1 \pmod 4$ has a unique representation $p_i = x_i^2 + y_i^2;\ x_i, y_i \in N_+$.

When we multiply two sums of squares using the Brahmagupta-Fibonacci identity (Fact 3), we get a binary choice at each step. Specifically, if we have built up a representation for $p_1 \cdots p_{j-1}$, say $p_1 \cdots p_{j-1} = A^2 + B^2$ for some non-zero integers A and B, and incorporate $p_j = x_j^2 + y_j^2$, we then have

$$\left(A^2 + B^2\right)\left(x_j^2 + y_j^2\right) = \left(Ax_j - By_j\right)^2 + \left(Ay_j + Bx_j\right)^2$$

or

$$\left(A^2 + B^2\right)\left(x_j^2 + y_j^2\right) = \left(Ax_j + By_j\right)^2 + \left(Ay_j - Bx_j\right)^2.$$

These two choices yield different representations.

Starting with $p_1 = x_1^2 + y_1^2$ (one representation), at each subsequent prime, we double the number of representations. After incorporating all k primes, we have 2^{k-1} distinct representations. (The factor is 2^{k-1} rather than 2^k because we start with one representation and make $k-1$ binary choices.) ▪

(Step 3): Let us finish the proof of our theorem.

Suppose a satisfies all the hypotheses and has a unique representation as a sum of two squares.

From Step 1, we know $a = p_1 \cdots p_k$ where all $p_i \equiv 1 \pmod 4$ are distinct. Moreover, from Step 2, we know the number of distinct representations is 2^{k-1}.

Since a is assumed to have a unique representation, we have

$$2^{k-1} = 1 \Rightarrow k - 1 = 0 \Rightarrow k = 1.$$

Consequently, a consists of a single prime factor, which means a is prime.

4. Conclusions

The beautiful insight here is that the Brahmagupta-Fibonacci identity acts as a "representation multiplier". Each time we multiply two numbers expressible as sums of squares, we get a choice of how to combine them, which creates additional representations. A prime has exactly one representation, and each additional prime

factor in a square-free product doubles the count. It elaborates classical theorems, including representations by quadratic forms.

The conditions $a \equiv 1 \pmod 4$ and square-free work together to ensure that all prime factors are $\equiv 1 \pmod 4$, which puts in exactly the setting where this counting argument applies cleanly. This theorem gives us a characterization of primes $p \equiv 1 \pmod 4$ in terms of the uniqueness of their sum-of-squares representation, which is a rather elegant result.

Acknowledgements

This research is supported in part by City University of Hong Kong project No. 9610556. We acknowledge Nianrui Lin, an anonymous reviewer, and ChatGPT for providing input to the reference list.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zagier, D. (1990) A One-Sentence Proof That Every Prime $p \equiv 1 \pmod 4$ Is a Sum of Two Squares. *The American Mathematical Monthly*, **97**, 144-144. https://doi.org/10.1080/00029890.1990.11995565

[2] Cox, D. A. (2013) Primes of the Form $x^2 + ny^2$: Fermat, Class Field Theory, and Complex Multiplication. Wiley. https://doi.org/https://doi.org/10.1002/9781118400722

[3] Davenport, H. (2008) The Higher Arithmetic: An Introduction to the Theory of Numbers. 8th Edition, Cambridge University Press. https://doi.org/10.1017/cbo9780511818097

[4] Hardy, G.H. and Wright, E.M. (2008) An Introduction to the Theory of Numbers. Oxford University Press. https://doi.org/10.1093/oso/9780199219858.001.0001

[5] Aletheia-Zomlefer, S.L., Fukshansky, L. and Garcia, S.R. (2020) The Bateman-Horn Conjecture: Heuristic, History, and Applications. *Expositiones Mathematicae*, **38**, 430-479. https://doi.org/10.1016/j.exmath.2019.04.005

[6] Iwaniec, H. and Kowalski, E. (2004) Analytic Number Theory. American Mathematical Society. https://doi.org/10.1090/coll/053

[7] Pintz, J. (2009) Landau's problems on primes. *Journal de théorie des nombres de Bordeaux*, **21**, 357-404. https://doi.org/10.5802/jtnb.676

[8] Hirschhorn, M.D. (1985) A Simple Proof of Jacobi's Two-Square Theorem. *The American Mathematical Monthly*, **92**, 579-580. https://doi.org/10.1080/00029890.1985.11971686

[9] Jacobi, C. (1829) Fundamenta Nova Theoriae Functionum Ellipticarum. Bornträger.