Scientific Research Publishing

Advances in Pure Mathematics, 2026, 16(9), 678-681
https://www.scirp.org/journal/apm
ISSN Online: 2160-0384
ISSN Print: 2160-0368

Elaborating the Condition in Fermat's Two Square Theorem

Nianrui Lin

Department of Systems Engineering, City University of Hong Kong, Hong Kong, China
Email: nianrui.lin@my.cityu.edu.hk

How to cite this paper: Lin, N.R. (2026) Elaborating the Condition in Fermat's Two Square Theorem. *Advances in Pure Mathematics*, **16**, 678-681.
https://doi.org/10.4236/apm.2026.169033

Received: August 21, 2026
Accepted: September 17, 2026
Published: September 20, 2026

Abstract

It is a well-known result that prime numbers congruent to 1 modulo 4 are representable as a sum of two squares. A recent article shows that the number of representations can imply the primality of square-free integers congruent to 1 modulo 4. However, the authors did not clarify the distinctness of the construction of representations in the proof of the main theorem. We provide a complementary proof to clarify this construction and also present an alternative proof based on Jacobi's two square theorem.

Keywords

Fermat's Two Square Theorem, Primality, Sum of Two Squares

1. Introduction

Fermat's two square theorem states that an odd prime p can be represented as a sum of two squares if and only if $p \equiv 1 \pmod 4$ [1]. However, this classical theorem only reveals the property of representability as a sum of two squares for primes congruent to 1 modulo 4, while little attention has been paid to the complete picture: using the number of such representations to detect primality for a general positive integer congruent to 1 modulo 4.

The recent article [2] presents a criterion for testing the primality of square-free positive integers congruent to 1 modulo 4, based on the uniqueness of representations as a sum of two squares. It goes beyond Fermat's theorem and establishes a two-way connection between uniqueness of representation as a sum of two squares and primality. Modern primality tests include the deterministic, polynomial-time AKS algorithm [3] and the probabilistic Miller-Rabin test [4] [5], whose error probability can be reduced through repeated rounds. Unlike these computational algorithms, the theorem in [2] connects primality to the uniqueness of

representation as a sum of two squares.

Unfortunately, the proof of the main theorem relies on the implicit assumption that the constructed representations are pairwise distinct, but a justification was not provided.

In this paper, we further clarify the counting step in the proof of the main theorem in [2], showing that the representations generated in Step 2 of Section 3 are pairwise distinct up to order and signs.

2. Two Supplementary Proofs of the Theorem

We first recall the main theorem of [2].

Two integer pairs are regarded as equivalent if one can be obtained from the other by changing order and signs independently. The representation of an integer a as a sum of two squares is considered unique if all integer solutions of $a = c^2 + d^2$ form exactly one equivalence class under this relation.

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

The authors of [2] prove the theorem by offering the following method to construct 2^{k-1} candidate representations as a sum of two squares for $a = p_1 p_2 \cdots p_k$. Since such a representation exists, every prime factor congruent to 3 modulo 4 must occur with an even exponent. Combined with the fact that a is square-free, p_j's are all distinct primes congruent to 1 modulo 4.

The first factor p_1 has a representation $p_1 = x_1^2 + y_1^2$ by Fermat's two square theorem.

Assume that p_j has a representation $p_j = x_j^2 + y_j^2$, where $x_j, y_j > 0$, and a representation $A^2 + B^2$ of $p_1 \cdots p_{j-1}$ has already been obtained. The Brahmagupta-Fibonacci Identity gives two representations for $p_1 \cdots p_j$:

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

After incorporating all k factors, this process generates 2^{k-1} candidate representations.

In [2], these 2^{k-1} candidate representations are regarded as pairwise distinct up to order and signs in the proof of the main theorem, but this does not immediately follow. We now provide two ways to justify this counting step.

The first is to justify that the candidate representations are pairwise distinct up to order and signs by the following lemma.

Lemma The 2^{k-1} candidate representations as a sum of two squares are pairwise distinct, where we consider two representations the same if they differ only in the order of the summands or in signs.

Proof:

We prove the lemma by induction. The first prime factor p_1 has a unique representation class by Fermat's Theorem. Suppose that $p_1 \cdots p_{j-1}$ has 2^{j-2} distinct representation classes (A, B). Using the construction in [2], we obtain 2^{j-1}

representations of $p_1 \cdots p_{j-1} p_j = \left(A^2 + B^2\right)\left(x_j^2 + y_j^2\right)$. We show that each of these 2^{j-1} representations (s,t) is generated uniquely from a pair (A,B) along with one of the two Brahmagupta-Fibonacci identities.

Any representation (A,B) of $p_1 \cdots p_{j-1}$ that generates representation (s,t) of $p_1 \cdots p_j$ must satisfy

$$s = Ay_j + Bx_j,\ t = \left|Ax_j - By_j\right|$$

or

$$s = \left|Ay_j - Bx_j\right|,\ t = Ax_j + By_j.$$

By solving four linear systems arising from the sign choices in the absolute values, we obtain the following two possible solutions of (A,B) (the remaining two candidates have non-positive components and are discarded):

$$(A,B) = \left(\frac{y_j s + x_j t}{p_j}, \frac{\left|x_j s - y_j t\right|}{p_j}\right), \left(\frac{\left|y_j s - x_j t\right|}{p_j}, \frac{x_j s + y_j t}{p_j}\right).$$

If both of the solutions for A and B are feasible, then p_j divides both s and t. Hence p_j^2 divides $s^2 + t^2 = p_1 \cdots p_{j-1} p_j$, which forces p_j to divide $p_1 \cdots p_{j-1}$, contradicting that the prime factors $p_1, p_2, \cdots, p_j$ are distinct. Therefore, (s,t) is generated in exactly one way. Hence each induction step doubles the number of distinct representation classes. This proves the lemma. ▪

The lemma justifies the distinctness, up to order and signs, of the representations generated by the iterative construction in [2]. Therefore, at least 2^{k-1} representations are found by this construction. From this, unique representation as a sum of two squares leads to primality.

Another direct way is to prove the main theorem of [2] without the construction. In fact, we can get the number of representations from Jacobi's two square theorem [6] [7]. Jacobi's theorem states that the number of integer solutions $(x,y) \in \mathbb{Z}^2$ of $a = x^2 + y^2$ is $4\left(d_1(a) - d_3(a)\right)$, where $d_1(a)$ and $d_3(a)$ denote the numbers of positive divisors of a congruent to 1 and 3 (mod 4) respectively. As demonstrated in Step 1 of [2], the integer $a = p_1 p_2 \cdots p_k$ in the main theorem has only distinct prime factors congruent to 1 modulo 4. Therefore, the number of such solutions is

$$4\left(d_1(a) - d_3(a)\right) = 4 \times \left(2^k - 0\right) = 2^{k+2}.$$

On the other hand, if the representation of a as a sum of two squares is unique, then it has exactly eight integer solutions (x,y), since neither coordinate can be zero when a is square-free, and their absolute values cannot be equal when a is odd. Thus, $2^{k+2} = 8$ leads to $k = 1$. This proves the theorem.

3. Conclusion

We justify that the representations constructed in the proof of [2] are pairwise distinct, and we also provide an alternative proof based on Jacobi's two square theorem. The main contribution of [2], together with the supplementary proofs

presented in this paper, is to extend the scope of Fermat's two square theorem by developing the representability of integers as sums of two squares from a property of primes into a criterion for primality testing.

Acknowledgements

The author thanks Way Kuo for insightful discussions. This research is supported by City University of Hong Kong project No. 9610556.

Conflicts of Interest

The author declares 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. https://doi.org/10.2307/2323918

[2] 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

[3] Agrawal, M., Kayal, N. and Saxena, N. (2004) Primes Is in P. *Annals of Mathematics*, **160**, 781-793. https://doi.org/10.4007/annals.2004.160.781

[4] Miller, G.L. (1975) Riemann's Hypothesis and Tests for Primality. *Proceedings of 7th Annual ACM Symposium on Theory of Computing—STOC* '75, Albuquerque, 5-7 May 1975, 234-239. https://doi.org/10.1145/800116.803773

[5] Rabin, M.O. (1980) Probabilistic Algorithm for Testing Primality. *Journal of Number Theory*, **12**, 128-138. https://doi.org/10.1016/0022-314x(80)90084-0

[6] 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

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