American Journal of Mathematics and Statistics 2026, 15(1): 1-2
DOI: 10.5923/j.ajms.20261501.01

A Note on the Hypotenuse of a Pythagorean Triple

Qingquan Wu

West Texas A&M University, College of Engineering, 2501 4th Ave, Canyon, TX 79016, USA

Abstract This note highlights the mathematical and pedagogical significance of the classical result: a positive integer c is the hypotenuse of a Pythagorean triple if and only if it has at least one prime divisor congruent to 1 (mod 4). While often overlooked in favor of more constructive results about generating triples, this theorem offers deep insight into the interplay between geometry, arithmetic, and algebra. We emphasize its elementary formulation, surprising power, and role as a gateway to advanced ideas—without relying on any proof details.

Keywords Pythagorean triples, Hypotenuse, Gaussian integers

1. Introduction

Let c be a positive integer. What is a complete characterization of c being the hypotenuse of a Pythagorean triple (an all-integer right triangle)? It is known that c must have at least one prime divisor congruent to 1 modulo 4; see, for example, [3]. However, proofs that c cannot be the hypotenuse of a Pythagorean triple without such divisors often rely on properties of the sum of squares function, which are not easily accessible; see, for example, [1], pages 140–142.

In this paper, we provide an elementary proof using properties of the Gaussian integers $Z[i]$.

Theorem 1. *A positive integer c is the hypotenuse of a Pythagorean triple if and only if c has at least one prime divisor congruent to 1 modulo 4.*

The proof combines elementary number theory with a few basic facts about the Gaussian integers $Z[i]$, such as the factorization of rational primes in this ring. No deeper tools from algebraic number theory—such as ideals in general quadratic fields or group theory—are required. This limited use of algebraic methods keeps the argument accessible while still revealing a deep connection between classical Diophan-tine equations and arithmetic in $Z[i]$.

2. Preliminaries

A Pythagorean triple is a tuple (a, b, c) of positive integers satisfying $a^2 + b^2 = c^2$, where c is the hypotenuse and a, b are the legs. If a, b, c have no common positive divisor other than 1, the triple is primitive. For any positive integer a, there exist primitive Pythagorean triples with a as a leg. However, a positive integer c is the hypotenuse of a primitive Pythagorean triple if and only if each of its prime factors is congruent to 1 modulo 4, in which case the number of such triples is 2^k, where k is the number of distinct prime factors of c; see [5], which uses some group theory.

To prove our main result in an elementary way, we need the following results from number theory.

Theorem 2. *Let (a, b, c) be a primitive Pythagorean triple with a odd. Then there exists a unique pair of coprime positive integers $m > n > 0$, one of which is even, such that $a = m^2 - n^2$, $b = 2mn$, and $c = m^2 + n^2$.*

Proof. See Section 8.1 of [4].

Proposition 3. *If a prime number $p \equiv 1 \pmod 4$, then there exists integers m and n such that $p = m^2 + n^2$.*

Proof. See Proposition 8.3.1, page 95 of [2]. Alternatively, it is a consequence of Proposition 4 below.

Proposition 4. *In the ring of Gaussian integers $Z[i]$, the factorization of a rational prime p is determined by its residue modulo 4:*

1. *(p) is a product of two distinct prime ideals in $Z[i]$ if $p \equiv 1 \pmod 4$.*
2. *(p) is a prime ideal in $Z[i]$ if $p \equiv 3 \pmod 4$.*
3. *$(2) = (1 + i)^2$.*

Proof. See Propositions 13.1.3 and 13.1.4, page 190 of [2], with $d = -1$.

Proposition 5. *$Z[i]$ is a unique factorization domain with units $\{\pm 1, \pm i\}$.*

Proof. See Proposition 1.4.1, page 12 of [2].

3. Proof of the Main Theorem

We now prove Theorem 1.

Proof. **Necessity.** Assume c has at least one prime divisor $p \equiv 1 \pmod 4$. By Proposition 3, we have $p = m^2 + n^2$ for some positive integers m,n. Since p is odd, $m \neq n$. Without loss of generality, assume $m > n > 0$. Then $(m^2 - n^2, 2mn, m^2 + n^2) = (m^2 - n^2, 2mn, p)$ is a Pythagorean triple. If $c = pk$, then $(k(m^2 - n^2), k(2mn), kp) = (k(m^2 - n^2), k(2mn), c)$ is a

* Corresponding author:
qwu@wtamu.edu (Qingquan Wu)
Received: Feb. 26, 2026; Accepted: Mar. 12, 2026; Published: Apr. 10, 2026
Published online at http://journal.sapub.org/ajms

Pythagorean triple with c as the hypotenuse.

Sufficiency. Assume, by way of contradiction, that (a, b, c) is a Pythagorean triple, but c has no prime divisors congruent to 1 modulo 4. Without loss of generality, we may assume (a, b, c) is primitive, since a non-primitive triples (ka, kb, kc) without prime divisors congruent to 1 modulo 4 implies the same property for the induced primitive Pythagorean triple (a, b, c). Switching a and b if necessary, we may assume a is odd. By Theorem 2, there exist coprime positive integers $m > n > 0$, one of which is even, such that $c = m^2 + n^2$.

By our assumption, the factorization of c is

$$c = 2^t \prod_j p_j^{e_j},$$

where $p_j \equiv 3 \pmod 4$ are prime numbers and $t \geq 0$. By Proposition 4, the factorization of c in the ring of Gaussian integers $\mathrm{Z}[i]$ is:

$$(c) = (1+i)^{2t} \prod_j p_j^{e_j} \tag{1}$$

On the other hand, we have $c = m^2 + n^2 = (m + ni)(m - ni)$. By Proposition 5, $\mathrm{Z}[i]$ is a unique factorization domain, we may write

$$m + ni = u(1+i)^s \prod_j p_j^{f_j}$$

by (1), where $u \in \{\pm 1, \pm i\}$ is a unit in $\mathrm{Z}[i]$, and s, f_j are non-negative integers. Denote the rational integer $\prod_j p_j^{f_j} \in \mathrm{Z}$ by A.

As a complex number, $1 + i$ has argument $\pi/4$. Thus, $(1 + i)^s$ has argument $s\pi/4$. The arguments of u and A are integer multiples of $\pi/2$. Hence, the argument of $m + ni$ is an integer multiple of $\pi/4$. Let it be $k\pi/4$ for some integer $k \geq 0$.

However, this leads to a contradiction. Indeed, we have

$$\begin{cases} n = 0 & \text{if } k \equiv 0 \text{ or } 4 \pmod 8, \\ m = n & \text{if } k \equiv 1 \text{ or } 5 \pmod 8, \\ m = 0 & \text{if } k \equiv 2 \text{ or } 6 \pmod 8, \\ m = -n & \text{if } k \equiv 3 \text{ or } 7 \pmod 8. \end{cases}$$

None of these cases are possible since $m > n > 0$.

REFERENCES

[1] Beiler, A. H. (1966). *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains*. New York: Dover.

[2] Ireland, K., & Rosen, M. (1990). *A Classical Introduction to Modern Number Theory* (2nd ed.). Springer-Verlag.

[3] Online Platform. https://math.stackexchange.com/questions/1461202.

[4] Ore, O. (1948). *Number Theory and Its History*. McGraw-Hill.

[5] Yekutieli, A. (2023). Pythagorean triples, complex numbers, abelian groups and prime numbers. *Amer. Math. Monthly*. 130: 321–334.