Turkish Journal of Analysis and Number Theory, 2026, Vol. 14, No. 1, 1-5
Available online at http://pubs.sciepub.com/tjant/14/1/1
Published by Science and Education Publishing
DOI:10.12691/tjant-14-1-1

A New Approach to the Girard-Fermat's Two Squares Theorem with Some Remarks on Primes' Decomposition as Sums of Squares

Arto Adili[1,*], Adrian Naço[2], Lorena Kelo[1]

[1]Department of Mathematics and Physics, "Fan S. Noli" University, Korçë, Albania
[2]Department of Mathematics Engineering, Polytechnic University, Tirana, Albania
*Corresponding author: aadili@unkorce.edu.al

Received February 14, 2026; Revised March 16, 2026; Accepted March 23, 2026

Abstract A new elementary approach to the Girard-Fermat theorem, generalizing the equality of the sum of squares with the prime to its divisibility by that prime. That reveals some interesting properties of the corresponding decomposition's components.

Keywords: *Girard-Fermat theorem, primitive root, indexes*

Cite This Article: Arto Adili, Adrian Naço, and Lorena Kelo, "A New Approach to the Girard-Fermat's Two Squares Theorem with Some Remarks on Primes' Decomposition as Sums of Squares." *Turkish Journal of Analysis and Number Theory*, vol. 14, no. 1 (2026): 1-5. doi: 10.12691/tjant-14-1-1.

1. Introduction

The issues of the numbers which are sum of two squares has been addressed early. It has been studied the amount of different representations of the same number as a sum of squares, and the conditions that a number has such representations. Some first results, albeit accompanied by uncertainly and inaccuracy, as quoted by Dixon [1] pg. 225, are mentioned by Diofant and Mohammed Ben Alhocain (Arab mathematician in tenth century). The first exact formulations of the existence of such representations are mentioned at [1] pg. 227.

The earliest one is that of Albert Girard (1625) - "a number is a sum of two squares only when: It is a square, it is a prime of the form $4k+1$, it is the product of such numbers, and when it is the double of one of the foregoing". Fermat (1640) wrote that the condition for a number of the form $2a+1$ to be a sum of two squares, the number a must not be odd, and $2a+1$, when divided by the greatest square entering it as a factor, must not be divisible by any prime of the form $4n-1$ (as quoted by [1]). Fermat (quoted by Dickson [1], pg. 228) calls the proposition staying in the core of their formulations: "Every prime number $4n+1$ is a sum of two squares" the "fundamental theorem on right triangles". Dickson himself calls it "Girard theorem".

Generally, the proposition:

Theorem 1.1. An odd prime can be expressed as

$$p = x^2 + y^2,$$

with x and y integers, if and only if $p \equiv 1 (\mathrm{mod}\, 4)$.

is called "*Fermat's theorem on sums of two squares*". The prime numbers for which this is true are called *Pythagorean primes*.

Its proof has a long history too. Fermat asserts (as Dickson [1] quoted at pg. 228) that it has an irrefutable proof, based on the "method of indefinite descent". The first known irrefutable proof is that of Euler (1747, 1749), another one is that of Lagrange (1775), simplified by Gauss. Dedekind has provided two ones, which use the ring of Gaussian integers; are also well known two quite different and almost recent ones by Heath Brown and Zagier [2].

We'll call it "the Girard-Fermat's two-square theorem".

The uniqueness of prime's representation as sum of squares was observed early by Euler, which, for the numbers that appeared in two different ways as sums of squares, offered a factorization method, leading to an factorizing algorithm running in $O(n^{\frac{1}{3}+\varepsilon})$ steps [3].

The following results will be used in our approach to the demonstration of the Girard-Fermat theorem.

Theorem 1.2. [4] If q is a prime number such that $q \mid u^2 + v^2$, then $q = 2$ or $q \equiv 1 (\mathrm{mod}\, 4)$.

Theorem 1.3. [5] Let $f(x)$ be a polynomial with integer coefficients and $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ the canonical factorization of the positive integer n. The number of roots of the equation

$$f(x) \equiv 0 (\mathrm{mod}\, n),$$

equals the product of the roots' numbers of the following equations

$$f(x) \equiv 0 (\mathrm{mod}\, p_1^{\alpha_1}), \dots, f(x) \equiv 0 (\mathrm{mod}\, p_k^{\alpha_k}).$$

2. Some properties of couple (a, b) such a^2+b^2 are multiples of a prime

Let p be a prime of the form $p \equiv 1 (\mathrm{mod}\, 4)$. In this section we find all the pairs of positive integers (a, b), $1 \le a, b \le p-1$, such that $p \mid a^2+b^2$ and some their interesting properties.

We will use the following proposition:

Theorem 2.1. [6] If p is a prime $\equiv 1 (\mathrm{mod}\, 4)$, then for every divisor d of $p-1$ the congruence $x^d \equiv 1 (\mathrm{mod}\, p)$ has d distinct solutions smaller than p.

If the prime p is $\equiv 1 (\mathrm{mod}\, 4)$, then $p = 4k+1$ for some $k \in \mathbb{N}$. So, for the divisor $k = \frac{p-1}{4}$ of $p-1$ theorem 2.1. yields that the congruence $x^k \equiv 1 (\mathrm{mod}\, p)$, has k distinct solution. Let as denote them by $h_1, h_2, \ldots, h_k$. $(*)$

Theorem 2.2. [7] Consider the congruence

$$x^n \equiv h (\mathrm{mod}\, m),$$

for some $h, n, m \in \mathbb{N}$. If g is a primitive root modulo m and $(h, m) = 1$, then the given congruence is equivalent to the congruence

$$n \cdot ind_g x \equiv ind_g h (\mathrm{mod}\, \varphi(m)).$$

This congruence is linear regarding $ind_g x$ and admits solutions if $ind_g h$ is divisible by $d = (n, \varphi(m))$. If this is the case, it has d distinct solutions.

The prime number p has primitive roots, let g be one of them. For each h_i at $(*)$ $i = 1, 2, \ldots k$, let us consider the congruence

$$x^4 \equiv h_i (\mathrm{mod}\, p).$$

These congruences satisfy the conditions of Theorem 2.2., for $(h_i, p) = 1$, $i = 1, 2, \ldots, k$, so they are equivalent to the corresponding

$$4 \cdot ind_g x \equiv ind_g h_i (\mathrm{mod}\, p-1).$$

Necessary and sufficient condition for these linear congruences to admit any solution is that

$$4 = (4, p-1) \text{ devides } s_i = ind_g h_i.$$

g is a primitive root modulo p, so $ord_p g = p-1$. Also, by $s_i = ind_g h_i$ we get

$$h_i \equiv g^{s_i} (\mathrm{mod}\, p).$$

Taking into account that $\forall i = 1, 2, \ldots, k$, $h_i^k \equiv 1 (\mathrm{mod}\, p)$, we have

$$h_i^k \equiv g^{ks_i} \equiv 1 (\mathrm{mod}\, p),$$

which means that

$$p-1 \mid ks_i,$$

being g a primitive root modulo p. This way we have that

$ks_i = l \cdot (p-1) = 4kl$, whereform $s_1 = 4l$, $l \in \mathbb{N}$.

So, even the indexes $ind_g h_i$ must be multiples of 4. Since $\forall i = 1, 2, \ldots, k$, the congruences

$$4 \cdot ind_g x \equiv ind_g h_i (\mathrm{mod}\, p-1)$$

have solutions, then each one of them has 4 distinct ones.

Let us consider the first two positive solutions of each one of the following $\frac{p-1}{4}$ equations:

$$x^4 \equiv h_1 (\mathrm{mod}\, p)$$
$$x^4 \equiv h_2 (\mathrm{mod}\, p)$$
$$\ldots \quad \ldots \quad \ldots$$
$$x^4 \equiv h_k (\mathrm{mod}\, p)$$

All of them are in the set $A = \left\{1, 2, \ldots, \frac{p-1}{2}\right\}$. Taking into account that there are $\frac{p-1}{4}$ such congruences, each one of them having two distinct solutions in the set A, then the numbers

$$1, 2, \ldots, \frac{p-1}{2},$$

can be organized in couples (u, v) such that for each one of them

$$u^4 \equiv v^4 \equiv h_i (\mathrm{mod}\, p), \; i = 1, 2, \ldots, k.$$

For the positive integers u and v we have:

$$p \mid u^4 - v^4 = (u^2+v^2)(u-v)(u+v),$$

wherefrom

$$p \mid u^2+v^2,$$

because $1 < |u-v| < u+v < p$, with u and v such $1 \le u, v \le \frac{p-1}{2}$.

We have proved the following:

Theorem 2.3. For every prime $p \equiv 1 (\mathrm{mod}\, 4)$, the set

$$\left\{1, 2, \ldots, \frac{p-1}{2}\right\},$$

can be divided in $\frac{p-1}{4}$ couples of numbers, the sum of squares of each of them being divisible by the prime p.

Example 2.4. For the prime $p = 29 = 4 \cdot 7 + 1$ we have the following "decompositions" in sums of two squares:

$$1^2+12^2=5\cdot 29 \qquad 6^2+14^2=8\cdot 29$$
$$2^2+5^2=29 \qquad 8^2+9^2=5\cdot 29$$
$$3^2+7^2=2\cdot 29 \qquad 11^2+13^2=10\cdot 29$$
$$4^2+10^2=4\cdot 29$$

So, the numbers $1, 2, \ldots, 14$ are divided in 7 couples, the sum of squares of each one of them is divisible by 29.

In the following, we will can two couples of natural numbers (a, b) and (c, d) congruent modulo n, $n \in \mathbb{N}$, if $a \equiv c \pmod n \wedge b \equiv d \pmod n$ and write

$$(a, b) \equiv (c, d) \pmod n .$$

We put also the following "scalar multiplication" in the set of couples

$$m \cdot (a, b) = (ma, mb) .$$

Definition 2.5. Let p be a prime number. We will call as "a square couple of the prime p" every couple of non-negative integers (a, b) such that $p \mid a^2+b^2$. A square couple (a, b) of p is called a "primitive square couple" if $1 \le a, b \le p-1$.

In the following, we will not make any distinction between the couples (a, b) and (b, a), considering them the same couple.

Theorem 2.6. For every prime $p \equiv 1 \pmod 4$ there are exactly $p-1$ primitive square couples of p, generated by multiplying any arbitrary primitive square couple by elements of a reduced residue system modulo p.

Proof. Since for every $a \in \{1, 2, \ldots, p-1\}$ the congruence

$$x^2 + a^2 \equiv 0 \pmod p ,$$

has exactly two solutions in this set, then for every such a exist exactly two primitive square couples of p which have the number a. But the number of elements of the set $\{1, 2, \ldots, p-1\}$ is $p-1$ and every number $1 \le a \le p-1$ appears twice in these primitive square couples, so there are exactly $p-1$ primitive square couples of the prime p

Let (a, b) be any primitive square couple of the prime p and $A = \{1, 2, \ldots, p-1\}$ the respective reduced residue system. Let us now consider the following $p-1$ primitive square couples:

$$1 \cdot (a, b) = (a, b)$$
$$2 \cdot (a, b) = (2a, 2b)$$
$$\ldots \quad \ldots \quad \ldots$$
$$(p-1) \cdot (a, b) = ((p-1)a, (p-1)b)$$

They are all different from each other. Indeed, if

$$(ua, ub) \equiv (va, vb) \pmod p ,$$

then

$$ua \equiv va \pmod p \wedge ub \equiv vb \pmod p \quad \Rightarrow \quad u = v .$$

Example 2.7. $(2, 3)$ is a primitive square couple of the prime $p = 13$. Using the construction of the proof of theorem 2.6. we get the following list of all primitive square couples of 13:

$$1 \cdot (2, 3) \equiv (2, 3) \qquad 7 \cdot (2, 3) \equiv (1, 8)$$
$$2 \cdot (2, 3) \equiv (4, 6) \qquad 8 \cdot (2, 3) \equiv (3, 11)$$
$$3 \cdot (2, 3) \equiv (6, 9) \qquad 9 \cdot (2, 3) \equiv (5, 1)$$
$$4 \cdot (2, 3) \equiv (8, 12) \qquad 10 \cdot (2, 3) \equiv (7, 4)$$
$$5 \cdot (2, 3) \equiv (10, 2) \qquad 11 \cdot (2, 3) \equiv (9, 7)$$
$$6 \cdot (2, 3) \equiv (12, 5) \qquad 12 \cdot (2, 3) \equiv (11, 10)$$

Corollary 2.8. For every two square couples (a, b) and (c, d) of the prime p, there is a positive integer m such that:

$$m(a, b) \equiv (c, d) \pmod p .$$

Theorem 2.9. If (a, b) and (c, d) are squares couples of the prime p, the for every $l, s \in \mathbb{Z}$,

$$(la + sc, lb + sd)$$

is also a square couple of the prime p.

Proof. Corollary 2.8. yields a positive integer m, such that $m(a, b) \equiv (c, d) \pmod p$, namely

$ma \equiv c \pmod p$ and $mb \equiv d \pmod p$.

Since

$$\begin{aligned}(la+sc)^2 + (lb+sd)^2 &= \\ &= l^2a^2 + s^2c^2 + 2lsac + l^2b^2 + s^2d^2 + 2lsbd = \\ &\equiv l^2(a^2+b^2) + s^2(c^2+d^2) + 2lsm(a^2+b^2) \equiv \\ &\equiv l(l+2sm)(a^2+b^2) + s^2(c^2+d^2) \pmod p,\end{aligned}$$

we have $p \mid (la+sc)^2 + (lb+sd)^2$. So, the couple

$$(la + sc, lb + sd)$$

is a square couple of prime p.

Remark 1. We have these special cases:

- For $l = s = 1$. If (a, b) and (c, d) are square couples of prime p, then $(a+c, b+d)$ is also a square couple of the prime p.
- For $l = -s = 1$. If (a, b) and (c, d) are square couples of prime p, then $(a-c, b-d)$ is also a square couple of the prime p.

Theorem 2.10. Let p be a prime $\equiv 1 \pmod 4$. Then the sums of the components of the $p-1$ primitive square couples of p form a reduced residue system modulo p.

Proof. Firstly, we show that if (a, b) is a primitive square couple of p, then $a + b \not\equiv 0 \pmod p$. Indeed, if

$$a + b \equiv 0 \pmod p ,$$

then $2ab \equiv 0 \pmod p$, consequently $p \mid 2ab$, which is impossible because $1 \le 2, a, b \le p-1$.

Since there are $p-1$ primitive square couples, to prove the theorem it suffices to show that for every two primitive square couples the sums of their components are not congruent modulo p. Suppose that (a,b) and (c,d) are two primitive square couples such that

$$a+b \equiv c+d \pmod p .$$

By Corollary 2.8. exists $m \in \{1, 2, \dots, p-1\}$ such that $ma \equiv c \pmod p$ and $mb \equiv d \pmod p$. So, we have

$$m(a+b) \equiv a+b \pmod p ,$$

which, taking into account that $a+b \not\equiv 0 \pmod p$, means that $m=1$ and (a,b), (c,d) are not different.

3. Proof(s) of Girard-Fermat Theorem

In this section we will present two new proofs of Girard-Fermat Theorem, relying on the results of the section 2.

Theorem 3.1. (Girard-Fermat) Every prime number of the form $4k+1$ can be expressed as a sum of two squares of two natural numbers in only one way.

Proof. Let (a,b) a primitive square couple of the prime p with the least sum of its components, whose existence is provided by Theorem 2.10. We will now prove that $a^2+b^2=p$.

First proof. Let as suppose that $a^2+b^2>p$. Since (a,b) is a primitive square couple, then $a^2+b^2=wp$ for any natural w and by Theorem 1.2. all the divisors of a^2+b^2 are $\equiv 1 \pmod 4$.

By Theorem 1.3. the number wp can be expressed as sum of two squares in at least two ways:

$$wp = a^2+b^2 = c^2+d^2 .$$

Supposing that $a>c$ and $d>b$ we have:

$$a^2-c^2 = d^2-b^2 \Rightarrow (a-c)(a+c) = (d-b)(d+b) .$$

By the supposition $a+b<c+d$, so

$$(a+b)^2 < 2(a^2+b^2) < 2(a+b)^2$$

and, taking into account that $a^2+b^2=c^2+d^2$ we obtain that

$$a+b < c+d < \sqrt{2}(a+b) .$$

We denote by $h=(a+b, c+d)$. We have to prove that $h>2$. If $h=1$ then the equality

$$(a-c)(a+c) = (d-b)(d+b) ,$$

gives

$$a+c \mid d-b \text{ and } d+b \mid a-c ,$$

whereby the contradiction:

$$a+c \le d-b < d+b \le a-c < a+c .$$

If $h>2$, than the couples of numbers a, b and c, d have the same parity, so the halves $\frac{a-c}{2}$, $\frac{a+c}{2}$, $\frac{d-b}{2}$, $\frac{d+b}{2}$, are integers. Similarly, we get that the equalities

$$\left(\frac{a+c}{2}, \frac{d+b}{2}\right)=1 \text{ and } \frac{a+c}{2}\cdot\frac{a-c}{2} = \frac{d-b}{2}\cdot\frac{d+b}{2}$$

yield

$$\frac{a+c}{2} \mid \frac{d-b}{2} \text{ and } \frac{d+b}{2} \mid \frac{a-c}{2} ,$$

whereby the contradiction:

$$\frac{a+c}{2} \le \frac{d-b}{2} < \frac{d+b}{2} \le \frac{a-c}{2} < \frac{a+c}{2} .$$

So, $h>2$ and $\left(\frac{a+c}{h}, \frac{d+b}{h}\right)$ is a primitive square couple whose sum of components is:

$$\frac{a+b+c+d}{h} \le \frac{a+b+c+d}{3} < \frac{a+b+\sqrt{2}(a+b)}{3} < a+b ,$$

which contradicts our supposition $a^2+b^2>p$.

Second proof. Firstly, we see that $(a,b)=1$. Indeed, if $(a,b)=d>1$, then $\left(\frac{a}{d}, \frac{b}{d}\right)$ is also a primitive square couple, because

$$p \mid \frac{1}{d^2}(a^2+b^2) = \left(\frac{a}{d}\right)^2 + \left(\frac{b}{d}\right)^2 \text{ and } 0 < \frac{a}{d}, \frac{b}{d} < p .$$

But the sum of elements of this couple is $\frac{a+b}{d} < a+b$, which is impossible. The positive integer a and b can't be both odd. Indeed, if we get $a>b$, since:

$$p \mid \frac{1}{2}(a^2+b^2) = \left(\frac{a+b}{2}\right)^2 + \left(\frac{a-b}{2}\right)^2$$

and

$$0 < \frac{a-b}{2} < \frac{a+b}{2} < a < p ,$$

the couple $\left(\frac{a+b}{2}, \frac{a-b}{2}\right)$ is a primitive squares couple. So, the sum of elements of this couple is

$$\frac{a+b}{2} + \frac{a-b}{2} = a$$

and $a < a+b$, which is impossible. Also, the positive integers a and b cannot be both even, because $(a,b)=1$. Consequently, a primitive square couple of prime p with the smallest sum of its elements has one component an odd number and the other an even number.

Suppose now that $a^2+b^2>p$. Since $p \mid a^2+b^2$, there is any integer $w>1$ such that $a^2+b^2=wp$. But, from Theorem 1.2. the divisors of w are all $\equiv 1 \pmod 4$. By Theorem 1.3., the number wp can be expressed as sum of two squares in at least two ways:

$$a^2+b^2=c^2+d^2=wp\,.$$

We see that the parities of c and d must be different, because those of a and b are different. Suppose that $a>c$ and $d>b$. Then $(a-c)(a+c)=(d-b)(d+b)$. Since $a+b<c+d$ we have $a-c<d-b$, then

$$a+c>d+b\,.$$

Now, since (a,b) and (c,d) are square couples of the prime p, by Theorem 1.2. we have that:

$$(a-c,d-b)$$

is also a square couple of the prime p. We noticed that the parities of a and b are different and the same holds for c and d, so the components of the couple $(a-c,d-b)$ have the same parity. The following two cases are possible:

Case 1. The numbers $a-c$ and $d-b$ are both odd. Since $a-c<d-b$, there is a square couple

$$(u,v)=\left(\frac{(d-b)-(a-c)}{2},\frac{(d-b)+(a-c)}{2}\right)$$

with sum of its elements $\sum=d-b$. But, since:

$$(a+b)^2>a^2+b^2>d^2$$

then $a+b>d$, wherefrom

$$d-b<d<a+b\,,$$

which contradicts the assumption.

Case 2. The numbers $a-c$ and $d-b$ are both even. The couple

$$\left(\frac{a-c}{2},\frac{d-b}{2}\right)$$

is a square couple and the sum of its elements is

$$\frac{a+d-b-c}{2}\,.$$

But, since $d<d+b<a+c<a+c+3b$ we have:

$$d-b-c<a+2b \;\Rightarrow\; a+d-b-c<2(a+b)$$

$$\Rightarrow\; \frac{a+d-b-c}{2}<a+b$$

which also contradicts the assumption.

References

[1] Dickson, Leonard Eugene (2005) [1920] - History of the theory of numbers. Vol. II: Diophantine analysis, New York: Dover Publications, ISBN 978-0-486-44233-4.

[2] Zagier, D. (1990) A one-sentence proof that every prime p ≡ 1 mod 4 is a sum of two squares, American Mathematical Monthly, 97 (2): 144.

[3] James McKee Turning Euler's factoring method into a factoring algorithm Bull. Lon don Math. Soc. 28 (1996) 351-355.

[4] Sato N.: Art of Problem Solving (Notes on Number Theory for students at the IMO), https:// artofproblemsolving.com/ articles/files/SatoNT.pdf (accessed at February 17, 2019).

[5] Sierpinski W.: Elementary theory of Numbers, North-Holland, PWN-Polish Scientific Publisher.

[6] Adler A., Coury J.E.: The Theory of Numbers, Jones and Barlett Publisher, Boston, London, Singapore, 1995.

[7] Apostol T.M.: Introduction to Analytic Number Theory, Springer-Verlag 1976.

© The Author(s) 2026. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).