HIGH SCHOOL EDITION
Journal of Student Research
Volume 12 Issue 4 (2023)

Proof of Sum of Two Squares Theorem Using Gaussian Integers

Ayush Jain[1] and Joy Hamlin[#]

[1]The Shri Ram School Aravali, India
[#]Advisor

ABSTRACT

I provide a proof of Fermat's Sum of Two Squares theorem using Gaussian Integers. The theorem characterizes the integers that can be represented as a sum of two integer squares: $n = a^2 + b^2$ for some $n, a, b \in Z$.

Introduction

Fermat wrote an elaborate article on the statement that every prime p of the form 4n+1 is the sum of two squares. This was published in the 17th century, but Fermat's initial proof was incomplete. Euler completed the proof using infinite descent almost 100 years later. Towards the end of the 19th century, Dedekind was the first to provide a simpler proof using Gaussian integers [4]. Recently, this theorem has been extended to characterize all integers, not just primes, that can be written as a sum of two squares. [1], [3] provides proof of this extended theorem using Thu's Lemma and Fermat's Little Theorem. This paper uses Gaussian integers to prove the extended theorem[1], which is stated below.

Theorem 1 (Sum of two squares theorem). A number n can be expressed as a sum of two squares $a^2 + b^2$, where $a, b \in Z$, if and only if all prime factors of n that are congruent to 3 modulo 4 have even powers in its prime factorization.

In simpler terms, if a prime factor of n is of the form 4k + 3 and occurs with an odd power in the prime factorization of n, then n cannot be written as a sum of two squares. For instance, the number 27 with prime factorization 3^3 cannot be expressed as a sum of two squares because its prime factor 3, which is congruent to 3 modulo 4, has an odd power. In contrast, 36 with prime factorization $2^2 \cdot 3^2$ can be represented as a sum of two squares, $6^2 + 0^2$, because it has only one prime factor 3 that is congruent to 3 modulo 4, and this prime factor has an even power.

Another example illustrating the theorem is 877149, which has prime factorization $7^2 \cdot 13 \cdot 17 \cdot 3^4$. This number can be expressed as a sum of two squares, namely $315^2 + 882^2$, because both prime factors 7 and 3 that are congruent to 3 modulo 4 have even powers in its prime factorization.

Gaussian Integers

Gaussian integers were introduced by Gauss in 1832. Since the norm of a Gaussian integer is a sum of two squares, the theory of Gaussian integers is closely related to the sum of two squares theorem, which makes the proof easier. We state important definitions and related theorems of Gaussian integers below. For a detailed exposition on Gaussian integers, see Conrad [2].

Definition 1. The set of Gaussian integers is denoted by G and defined as $G = a + bi : a, b \in Z, i^2 = -1$.

Definition 2. The conjugate of a Gaussian integer $z = a + bi$ is defined as another Gaussian integer $\bar{z} = a - bi$.

[1] I do not claim that this is the only paper that uses Gaussian Integers to prove extended theorem, but I provide a simpler approach that only requires the existence of Gaussian primes.

Definition 3. The norm function $D : G \to Z$ of a Gaussian integer is defined as the product of the number and its conjugate, i.e., $D(z) = z\bar{z} = a^2 + b^2$, which is a sum of two squares. The norm also has a multiplicative property: $D(z_1 z_2) = D(z_1)D(z_2)$,where $z_1, z_2 \in G$.

The fact that a Gaussian integer multiplied by its conjugate results in a sum of two squares is a pivotal element of our proof of the "sum of two squares" theorem.

Definition 4. An element of G with norm 1 is called a unit of G, and the complete set of units of G is $1, -1, i, -i$.

G follows a divisibility rule defined by the following theorem:

Theorem 2. A Gaussian integer z = a + bi is divisible by an ordinary integer c ∈ Z if and only if c|a and c|b in Z. This also implies that if z is divisible by c then $\bar{z}$ is also divisible by c.

G contains irreducible elements which are analog of prime number in the Integer domain. The irreducible elements follow property similar to that of prime integers. Two important properties which we will use in our proof are stated below without the proof.

Definition 5. An element p ∈ G is irreducible if and only if whenever it is represented in the form p = a.b where a,b ∈ G, then at-least one of a or b is a unit.

Theorem 3. If an element p ∈ G is irreducible then p|a · b implies p|a or p|b.

Theorem 4 (Unique factorization). Any z ∈ G can be factorized into a unique (up to multiplication by units) product of irreducible elements in G.

The above theorems assert that the fundamental theorem of arithmetic can also be applied to the domain of Gaussian integers.

Preliminary Results

Before proving our main theorem, we require several intermediate results, which we provide in the following lemmas.

Lemma 1 (Unique multiplicative inverse in Zp). If p is a prime then there exists a unique inverse x for each $a \in 1,2, \dots, p-1$ such that $ax \equiv 1(\mathrm{mod} p)$

Proof. Consider any $a \in 1,2, \dots, p-1$. Since p is a prime, we have $\gcd(a, p) = 1$. By using Bezout's identity, we can write the following Diophantine equation for some $x, y \in Z$.

$$ax + py = 1$$

$$ax \equiv 1(\mathrm{mod}\ p)$$

This implies that there exists an x such that $ax \equiv 1(\mathrm{mod}\ p)$. Next, we prove that the inverse is unique. Suppose not, so that there are two distinct integers $x, y \in 1,2, \dots, p-1$ such that $ax \equiv 1(\mathrm{mod}\ p)$ and $ay \equiv 1(\mathrm{mod}\ p)$.This implies

$$a(x-y) \equiv 0(\mathrm{mod}\ p)$$

Since x and y are distinct integers in $\{1,2.., p-1\}$, $(x-y) \neq pk$ for some $k \in Z$, which implies

$$a \equiv 0(\mathrm{mod}\ p)$$

This contradicts $\gcd(a, p) = 1$. Therefore, the inverse of each $a \in 1,2, \dots, p-1$ is unique. □

Lemma 2 (Wilson's Theorem). $(p-1)! \equiv -1 (\mathrm{mod}\ p)$ for any prime number p.

Proof. By Lemma 1, each of the numbers in the set $1,2, \dots, p-1$ has a unique inverse modulo p. Furthermore, 1 and p−1 are their own inverses since

$$1.1 \equiv 1(\mathrm{mod}\ p) \text{ and } (p-1)^2 \equiv p^2 - 2p + 1 \equiv 1(\mathrm{mod}\ p).$$

Thus, we can write:

$$(p-1)! = 1.2.3 \dots (p-2).(p-1) = 1.(p-1)[2.3 \dots (p-2)]$$

Since 1 and $p-1$ are their own inverses, all numbers in $2,3, \dots, p-2$ must have inverses within the same set, and these inverses are unique. Therefore,

$$2.3 \dots (p-2) \equiv 1(\mathrm{mod}\ p)$$

Hence,

$$(p-1)! \equiv 1.(p-1).1(\mathrm{mod}\ p)$$

$$(p-1)! \equiv -1(\mathrm{mod}\ p)$$

□

Lemma 3. If a prime p is congruent to 1 (mod 4) then there exists some $x \in N$ such that $x^2 \equiv -1$ (mod p).

Proof. Since $p = 4k + 1$ for some $k \in N$, we have $\frac{p-1}{2} = 2k$, which is an even number. We also know that

$$a \equiv a - p(\mathrm{mod}\ p)$$

Therefore, we can write:

$$\frac{p+1}{2} \dots (p-2)(p-1) \equiv -\frac{p-1}{2} \dots -2.-1 \equiv (-1)^{2k} 1.2 \dots \frac{p-1}{2} \equiv (\frac{p-1}{2})!(\mod p)$$

which implies

$$(p-1)! \equiv \left[1.2 \dots \frac{p-1}{2}\right]\left[\frac{p+1}{2} \dots (p-2)(p-1)\right] \equiv \left(\frac{p-1}{2}!\right)^2(\mod p)$$

By Wilson's theorem (Lemma 2), we know that

$$(p-1)! \equiv \left(\frac{p-1}{2}!\right)^2 \equiv 1(\mod p)$$

Since $\frac{p-1}{2}!$ "exists", x also exists such that $x^2 \equiv -1(\mathrm{mod}\ p)$. □

Lemma 4. If a prime p is congruent to 1 (mod 4) then p is reducible, meaning it can be factorized into two factors $x, y \in G$, none of them is a unit.

Proof. Suppose that prime p is congruent to 1 (mod 4). By Lemma 3 there exists some $x \in Z$ such that $p | x^2 + 1 \Rightarrow p | (x + i)(x - i)$.

If $p | (x + i)$ then $x + i = pk$ for some $k \in G$. Let $k = a + bi$ for some $a,b \in Z$. Hence,

$x + i = p\,a + p\,b\,i \Rightarrow pb = 1$

This leads to a contradiction as p is prime and b is an integer, so $p\,b \neq 1$. Hence $p \dagger x + i$. Similarly, we can show $p \dagger x - i$. If p does not divide either of the factors $x + i$ or $x - i$ but divides the product, $(x + i)(x - i)$, then p is not a prime element in G and hence p is reducible (from theorem 3).

Lemma 5. A prime p that is congruent to 1 (mod 4) can be expressed as a sum of two squares.

Proof. We know from Lemma 4 that such prime p is reducible, and hence p can be factorized into two non unit Gaussian integers x,y ∈ G. Using the properties of norm function

$$D(p) = D(xy) = D(x).D(y)$$

Since p is a prime integer, $D(p) = p^2$. Therefore,

$$D(x).D(y) = p^2$$

Since p^2 has only three integer factors $1, p, p^2$ and $D(x) \neq 1, D(y) \neq 1$. This implies:

$D(x) = D(y) = p$
. If $x = a + bi$ then
$p = D(x) = a^2 + b^2$

□

Lemma 6 (Brahmagupta-Fibonacci identity). Let p and q be two positive integers that can be written as a sum of two squares then their product can also be written as a sum of two squares.

Proof. Let $p = x^2 + y^2$ and $q = u^2 + v^2$ where $x, y, u, b \in Z$. Then p q can be written as

$$p\,q = (x^2 + y^2)(u^2 + v^2) = x^2\,u^2 + x^2v^2 + y^2u^2 + y^2v^2$$

$$= (x^2u^2 \pm 2xyuv + y^2v^2) + (x^2v^2 \mp 2xyuv + y^2u^2)$$

$$pq = (xu \pm yv)^2 + (xv \mp yu)^2$$

Since $xu \pm yv$ and $xv \pm yu$ are integers, pq is a sum of two squares. □

Lemma 7. The only way a Gaussian integer $z = a + ib$ with $b \neq 0$ can be transformed into a non-zero ordinary integer is through multiplication by a multiple of its conjugate.

Proof. Let's say that the Gaussian integer is a + bi where $b \neq 0$. If we represent this number graphically, then the line passing through a + bi and the original makes an angle $\alpha = \tan^{-1}(\frac{b}{a}) \neq 0$.

Since a regular integer will have angle 0 from the x-axis, and the angles add during multiplication in the domain of G, we need to multiply a + bi with another number say c + di such that

$$\tan^{-1}(\frac{d}{c}) = -\alpha = -\tan^{-1}(\frac{b}{a})$$

The above equation is only satisfied if $ad + bc = 0$ which means $c + di = k(a - bi)$ for some $k \neq 0, k \in Z$. □

Lemma 8. A prime q such that $q \equiv 3 (\mathrm{mod}\ 4)$ is irreducible.

Proof. Suppose q is reducible. Since q is a prime integer and reducible, it must be the product of two conjugates (from Lemma 7). q also does not have another integer factor because q is prime. Therefore, we can write:

$$q = (a + ib)(a - ib) = a^2 + b^2 \text{ where } a, b \in Z$$

Since $a^2 \pmod 4 \in \{0,1\}$ and $b^2 \pmod 4 \in \{0,1\}$, $a^2 + b^2 \pmod 4 \in \{0,1,2\}$. Therefore, a sum of two squares number can't be congruent to 3 (mod 4), which is a contradiction. Hence q is irreducible. □

Proof of Sum of Two Squares Theorem

a) First, we prove the necessary condition. Let's suppose that each prime factor $q \equiv 3(mod\ 4)$ occurs to an even power in the prime factorization of *n*. We can represent *n* in terms of its prime factors as follows:

$$2^k \prod_{p\equiv 1\ (mod\ 4)} p_i^{r_i} \prod_{q\equiv 3\ (mod\ 4)} q_j^{s_j}$$

We know that $2 = 1^2 + 1^2$ is a sum of two squares, all p_i's are a sum of two squares from Lemma 5, and we can add 0^2 to represent each q_j with even power as a sum of two squares by adding 0^2. Therefore, using Lemma 6, their product *n* is a sum of two squares.

b) Next, we will prove the converse. Let's suppose that $n = a^2 + b^2$. We can represent *n* in terms of its prime factors as follows:

$$n = 2^k \prod_{p\equiv 1\ (mod\ 4)} p_i^{r_i} \prod_{q\equiv 3\ (mod\ 4)} q_j^{s_j} = a^2 + b^2$$

Since 2^k and $p_i^{r_i}$ for all *i* are sums of two squares, their product is also a sum of two squares by Lemma 5. Let this product be α. Thus, we have:

$$n = \alpha \prod_{q\equiv 3\ (mod\ 4)} q_j^{s_j} = a^2 + b^2$$

Consider any *j*. Using division algorithm, $q_j | a^2 + b^2 \Rightarrow q_j | (a + bi)(a - bi)$. Since q_j is irreducible (from Lemma 8), q_j must divide either $a + bi$ *or* $a - bi$ (from Theorem 3). Without the loss of generality, let's assume q_j divides $a + bi$ and the maximum power of q_j that divides $a + bi$ is *k* i.e. $q_j^k | a + bi$.

By Theorem 2, if $q_j^k | a + bi$, then $q_j^k | a - bi$. Next, we show that *k* is the maximum power of q_j that divides $a - bi$. Suppose not and $q_j^m | a - bi$ where $m > k$. Again, from Theorem 2, if $q_j^m | a - bi$ then $q_j^m | a + bi$, which is a contradiction that *k* is the maximum power of q_j that divides $a + bi$. Thus, the power of q_j that divides each of $a + bi$ and $a - bi$ must be equal to *k* and hence the power of q_j that divide $(a + bi)(a - bi)$ is $s_j = 2k$. Hence, s_j is even, and this is true for all *j*. In other words, each prime factor $q \equiv 3(\ mod\ 4)$ occurs to an even power.

Looking Ahead

After identifying the number that can be represented as a sum of two squares, the next important question is how we can identify the corresponding components of the two squares. In other words, what are the solutions to the Diophantine equation $n = a^2 + b^2$?

Acknowledgments

I would like to thank my advisor for the valuable insight provided to me on this topic.

References

[1] J. Bhaskar. Sum of two squares. *REU Papers*, 2008. URL https://math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf.

[2] K. Conrad. The gaussian integers. URL https://kconrad.math.uconn.edu/blurbs/ugradnumthy/Zinotes.pdf.

[3] C. Londahl. Lecture on sums of squares. 2011. URL https://carllondahl.files.wordpress.com/2011/05/sumsofsquares1.pdf.

[4] J. Stillwell. *Introduction to Theory of Algebraic Integers by Richard Dedekind*. Cambridge Mathematical Library, Cambridge University Press, 1996.