SUM OF TWO SQUARES (E228)

ARYAN DALAL, RITHWIK SHARMA

Abstract. In this paper, we will explore one of the several works of Leonhard Euler and discuss some interesting approaches employed by him to study and understand the nature of sum of two squares. We will furthermore show that any prime of the form $p = 4k + 1$ and $p = 4k + 3$ is a sum of two squares and not a sum of two squares respectively utilizing Algebraic Number Theory through both Euler and Fermat's work.

1. Introduction

Sum of two squares is one of several interesting Diophantine problems, that which was explored by Euler in his E228 Paper. However, since Euler's work, considerable development within the area of diophantine analysis involving sum of two squares has been put forth by Pierre de Fermat some of which will be discussed in this paper in reference to Euler's proofs.

Interestingly, when exploring sum of two squares of the form, $x^2 + y^2$ or $xx + yy$, it turns out that working with prime numbers would be easier as there's a distinct pattern that can be noticed. Consider the following table:

n	Prime	Sum of Two Squares
1		$1 = 0^2 + 1^2$
2	Yes	$2 = 1^2 + 1^2$
3	Yes	Not a Sum of Two Squares
4		$4 = 2^2 + 0^2$
5	Yes	$5 = 2^2 + 1^2$
6		Not a Sum of Two Squares
7	Yes	Not a Sum of Two Squares
8		$8 = 2^2 + 2^2$
9		$9 = 3^2 + 0^2$
10		$10 = 3^2 + 1^2$
11	Yes	Not a Sum of Two Squares
12		Not a Sum of Two Squares
13	Yes	$13 = 3^2 + 2^2$

We can continue this table for all n, however, we notice two patterns: Any prime

$p = 4k+1$ is a sum of two squares while any prime $p = 4k+3$ is not a sum of two squares.

Euler also showed that at least up to 200, the multitude of numbers which are not sums of two squares is in fact greater than the multitude of which are sums of two squares. This will be key in some of the propositions that he later lays and in the extension through Fermat's work.

We note that propositions and proofs explored in this paper have been written by Euler and Fermat respectively. This paper will simply explore these propositions and proofs, expanding on their implications and extending on the idea of Sum of Two Squares.

Let's first begin with a few definitions.

Definition 1.1. For $a, b \in \mathbb{Z}$, a is considered a **divisor** of b if there exists an integer x such that $ax = b$. b is then divisible by a, denoted, $a|b$ and refer to b as a multiple of a.

Definition 1.2. A positive integer p is **prime** if p has no proper divisors. If $p \in \mathbb{Z}^+$, then the primes $p_1, p_2, \ldots, p_{k-1}, p_k$ satisfy $p_1 \times p_2 \times \cdots \times p_{k-1} \times p_k$ where the product $p_1 \times p_2 \times \cdots \times p_{k-1} \times p_k$ is the prime factorization of p.

Definition 1.3. If the only common divisors of a and b are units, then $a, b \in \mathbb{Z}$ are **relatively prime**.

Definition 1.4. Consider $1|a$,$-1|a$ or $a|a$ and $-a|a$ where $a \in \mathbb{Z}$. $-1, 1, a, -a$ are the trivial divisors of a where -1 and 1 are units. Any other divisors are referred to as proper divisors.

Definition 1.5. Given $a, b \in \mathbb{Z}$, we define the **greatest common divisor** function, gcd, of a and b, denoted as $\gcd(a, b)$ as some positive integer c such that $c|a$ and $c|b$. As well as for all d such that $d|a$, $d|b$ and $d|c$. This also includes the largest such positive integer.

We will make more definitions as we continue.

Euler noted several interesting observations on his work on Sum of Two Squares that which are shared below:

He noticed that since each square number is either even, in which case it would be divisible by 4 and contained in the form $4a$, or odd, in which it case it would be contained in the form $8b + 1$, where each number formed from two squares will be:

1. A sum of two even squares and will be of the form $4a + 4b$, suggesting that it will be divisible by 4

2. The sum of two squares, one odd and one even, $4a + 8b + 1$, will be contained in the form $4a + 1$, and thus, will exceed a multiple of 4 by one
3. The sum of two odd squares will be of the form $8a+1+8b+1 = 8a+8b+2$ and will be contained in the form $8a + 2$ suggesting that it will exceed a multiple of eight by two.

As such, it can be concluded that since all odd numbers will either exceed a multiple of four by one or are one less than a multiple of four, following the forms of $4n + 1$ and $4n - 1$ respectively, then no odd numbers of the form $4n - 1$ can be sums of two squares. This implies that all numbers contained within the form of $4n - 1$ are therefore not part of the group of numbers that which follow the sums of two squares as does of the form $4n + 1$.

We can then also comment upon the unequal even numbers, that is, they either ecessed a multiple of eight by two or are two less than a multiple of eight and follow the form, $8n + 2$ and $8n - 2$ respectively. Therefore, no number of the form $8n - 2$ can form sums of two squares and will therefore not be part of the group of numbers that can form a sum of two squares such as of the form $8n + 2$.

But while we have established that numbers of the form $4n + 1$ and $8n + 2$, *in general* form sums of two squares, there are plenty that don't follow this establishment such as 21, 33,57, 69 and more.

Lemma 1.1. If a number p is a sum of two squares, then the numbers $4p$, $9p$, $16p$, and, in general, nnp will be sums of two squares.

This was shown by Euler as he considered that since $p = a^2+b^2$, then, $4p = 4a^2+4b^2$, $9p = 9a^2 + 9b^2$, $16p = 16a^2 + 16b^2$, and as such, $n^2p^2 = n^2a^2 + n^2b^2$, which are similarly sums of two squares.

Lemma 1.2. If a number p is a sum of two squares, then so will be $2p$ and, in general, $2n^2p$ will be q sum of two squares.

Euler showed that if we let $p = a^2 + b^2$; we will have $2p = 2a^2 + 2b^2$. But since $2a^2+2b^2 = (a + b)^2+(a - b)^2$, therefore, $2p = (a + b)^2+(a - b)^2$, and therefore also the sum of two squares. This allowed him to conclude that $2n^2p = n^2 (a + b)^2+n^2 (a - b)^2$

Lemma 1.3. If the even number $2p$ is a sum of two squares, then half of it, p, will also be a sum of two squares.

Euler showed this by letting $2p = a^2 + b^2$; where both the numbers a and b will be even and odd. This suggests, that both $(a + b)/2$ and $(a - b)/2$, in either cause, will be integers. As such, it can then be expressed that $a^2+b^2 = 2 ((a + b) /2)^2+2 ((a - b) /2)$

and, by substitutiong, would yield, $p = \left((a+b)/2\right)^2 + \left((a-b)/2\right)^2$

Using this information, we will now begin with a few theorems.

Theorem 1.4. If p and q are two numbers, each of which is the sum of two squares, then their product pq will also be the sum of two squares.

Proof. Let $p = a^2 + b^2$ and $q = c^2 + d^2$

$$pq = \left(a^2 + b^2\right)\left(c^2 + d^2\right) \implies a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2$$

This can be expressed as

$$pq = a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2$$

Which simplifies to,

$$pq = (ac + bd)^2 + (ad - bc)^2$$

This shows that the product pq will be a sum of two squares. ■

2. Proposition 1

Euler now lays the first of his seven propositions with regards to the sum of two squares,

Proposition 2.1. If the product pq is a sum of two squares and one factor p is a prime number and similarly a sum of two squares, then the other factor q will also be a sum of two squares.

Proof. Let $pq = a^2 + b^2$ and $p = c^2 + d^2$. Since p is a prime number, the numbers c and d will be prime between themselves. Therefore, $q = \dfrac{a^2 + b^2}{c^2 + d^2}$, suggesting that q is an integer and the term $a^2 + b^2$ will be divisible by $c^2 + d^2$ or rather, $c^2 + d^2 | a^2 + b^2$.

$$cc\left(a^2 + b^2\right) = a^2c^2 + b^2c^2$$

This too will be divisible by $c^2 + d^2$, and since the number,

$$aa\left(c^2 + d^2\right) = a^2c^2 + a^2d^2$$

is also divisible by $c^2 + d^2$, it is necessary for the difference of these numbers,

$$a^2c^2 + b^2c^2 - a^2c^2 - a^2d^2 = b^2c^2 - a^2d^2$$

to be divisible by $c^2 + d^2$. But since $c^2 + d^2$ is a prime number, with $b^2c^2 - a^2d^2$ having factors $bc + ad$ and $bc - ad$, of these two, is going to be divisible by $c^2 + d^2$.

Let $bc \pm ad = mc^2 + md^2$, then,

$$b = mc + x \qquad \text{and} \qquad a = \pm md + y$$

where x and y are either positive or negative integers. When substituting these values for b and a, the equation $bc \pm ad = mc^2 + md^2$ will take on the form:

$mc^2 + cx + md^2 \pm dy = mc^2 + md^2$ or $cx \pm dy = 0$.

We can then conclude that $\frac{x}{y} = \mp\frac{d}{c}$ and since d and c are prime between themselves, $x = nd$ and $y = \mp nc$, through which, we obtain $a = \pm md \mp nc$ and $b = mc + nd$ where a and b ought to have values such that the number $pq = a^2 + b^2$ is divisible by the prime number $p = c^2 + d^2$.

Substituting thoe values,

$$pq = m^2d^2 - 2mncd + n^2c^2 + m^2c^2 + 2mncd + n^2d^2$$

or $pq = (m^2 + n^2)(c^2 + d^2)$. But since $p = c^2 + d^2$, we will have have $q = m^2 + n^2$; and since the product pq is the sum of two squares with one factor p prime and similarly a sum of two squares $c^2 + d^2$, it follows that the other factor q will also be a sum of two squares. ■

Corollary 2.1. If the sum of two squares is divisible by a prime number which itself is sum of two squares, the quotient resulting from the division will also be a sum of two squares. So if the sum of two squares is divisible by some number from these prime numbers 2, 5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, etc., the quotient will always be a sum of two squares.

Example 2.1. Let's consider the number 125 which can be written as $10^2 + 5^2$ or $10 \cdot 10 + 5 \cdot 5$. This is divisible by the prime number 5 which, in turn, is the sum of two squares, $2^2 + 1^2$ or $2 \cdot 2 + 1 \cdot 1$. Then the quotient, $125/5 = 25$ is also a sum of two squares where $25 = 4^2 + 3^2 = 4 \cdot 4 + 3 \cdot 3$.

Corollary 2.2. If the letters α, β, γ, δ, etc. denote such prime numbers which are sums of two squares, it is evident from this that if the product αq is a sum of two squares, then the factor q will also be a sum of two squares.

Example 2.2. Consider $\alpha = 13$ that's also a prime. This is also a sum of two squares expressed as $13 = 3^2 + 2^2 = 3 \cdot 3 + 2 \cdot 2$. Consider another number $q = 17 = 4^2 + 1^2 = 4 \cdot 4 + 1 \cdot 1$. Then the product $\alpha q = 13 \cdot 17 = 221$ which is a sum of two squares as it can be written as $10^2 + 11^2 = 10 \cdot 10 + 11 \cdot 11$.

Corollary 2.3. It is easily obtained later on that if the product $\alpha\beta q$ is a sum of two squares, the factor q will also be a sum of two squares. Indeed, because $\alpha\beta q$ is a sum of two squares, by the corollary above, βq will also be a sum of two squares; and by the same reaasoning, q, will also be a sum of two squares.

Example 2.3. Consider the product $\alpha\beta q = 1105$ which is taken as $\alpha = 13$, $\beta = 17$ and $q = 5$. This is a sum of two squares in exactly 4 ways, one of which is, $31^2 + 12^2 = 31 \cdot 31 + 12 \cdot 12$. By the corollary, the product βq is also a sum of two squares which is $17 \times 5 = 85$. This is in fact a sum of two squares as 85 can be rewritten as $9^2 + 2^2 = 9 \cdot 9 + 2 \cdot 2$.

Corollary 2.4. It is evident that if the product $\alpha\beta\gamma\delta\epsilon q$ is a sum of two squares, then the factor q is also a sum of two squares; hence if the product pq is a sum of two squares, and the factor p is a product of however many prime numbers, each of which is a sum of two squares, then the other factor q will also be a sum of two squares.

3. Proposition 2

Euler makes another proposition,

Proposition 3.1. If the product pq is a sum of two squares but its factor q is not a sum of two squares, then the other factor p, if it is a prime number, will not be a sum of two squares, but if however it is not prime, it will certainly have at least one prime factor which is not a sum of two squares.

Proof. Since the factor p is either a prime number or composite, each case must be analyzed separately.

Let p be a prime number, if it was a sum of two squares, the factor q would also be a sum of two squares, which is false according to the hypothesis. This follows that the factor p is in fact not a sum of two squares.

Let p be a composite number, as established earlier, if the prime factors of p are sums of squares, then the factor q will also have its prime factors as sums of squares.

Thus, it can be concluded that since q is not a sum of two squares, not all factors of p are soms of two squares either. ■

Corollary 3.1. The the product pq is a sum of two squares, but one of its factors q cannot be expressed as two squares, then the other factor p is either itself not a sum of two squares or will have at least one prime factor which cannot be expressed as two squares.

Example 3.1. Let's consider the case of $pq = 45$. If we let $p = 3$, then $q = 15$. q has a factor 3 which itself cannot be expressed as a sum of two squares.

Corollary 3.2. It can't be consluded that the other factor p is not a sum of two squares. It hasn't yet been established in the case when$p$ is a composute number, since p can have a factor which can't be written as the sum of two squares eventhough p itself is a sum of two squares.

Corollary 3.3. If p is a sum of two squares, then it has not just one but at least two prime factors which cannot be written as the sum of two squares.

4. Proposition 3

We will now explore another proposition made by Euler. The proof of this proposition shows that the other part $c^2 + d^2$, a sum of two squares, is divisible by p in a similar way that $a^2 + b^2$ is divisible by p. He also shows that neither of the formulas in the sum of squares $c^2 + d^2$ exceed the square p^2, and thus, the sum of tqo squares $c^2 + d^2$ will be produced that is not greater than $\frac{1}{2}p^2$ but is still divisible by p.

Proposition 4.1. If the sum of two square primes between themselves, $a^2 + b^2$, is divisible by a prime number p, a sum of two other squares, $c^2 + d^2$ can always be generated which is divisible by that same number p so that the sum $c^2 + d^2$ is not greater than $\frac{1}{2}p^2$

Proof. Let the sum of two squares, prime, between themselves $a^2 + b^2$ be divisible by the number p.

Let a and b be numbers of any size.

Since neither a nor b is divisible by p, the numbers a and b can be expressed as $a = mp \pm c$ and $b = np \pm d$, such that m and n are selected where c and d don't exceed the value of $\frac{1}{2}p$.

As such,

$$a^2 + b^2 = m^2p^2 \pm 2mcp + c^2 + n^2p^2 \pm 2ndp + d^2$$

However, since this whole expression is divisible by p as established in the proposition, and the terms,

$$m^2p^2 \pm 2mcp + n^2p^2 \pm 2ndp$$

contain the factor p, making it divisible, that suggests that $c^2 + d^2$ is also divisible by p, which is a sum of two squares.

However, since the roots c and d don't exceed $\frac{1}{2}p$ as stated earlier, neither of the formulas in the sum of squares $c^2 + d^2$ will exceed p^2, and thus, the sum of two squares $c^2 + d^2$ can be produced that is not greater than $\frac{1}{2}p^2$, which is still divisible by p. ■

Corollary 4.1. If there is no sum of two squares, prime between themselves, divisible by p, and doesn't exceed $\frac{1}{2}p^2$, then there is num of two squares prime between themselves which is divisible by the number p.

Corollary 4.2. If there is num of squares prime between themselves, less than $\frac{1}{2} \times 9 = \frac{9}{2}$, and divisible by 3, then it clearly follows that there is no sum of two squares prime between themselves which is divisible by 3. And in a similar way by the number 7, since there is no sum of two squares less than $\frac{1}{2} \times 7^2 = \frac{49}{2}$, and divisible by 7, it follows that certainly neither among larger numbers is there a sum of two squares prime between themselves which is divisible by 7.

In the above propositions, we show a glimpse of some of Euler's findings and his work on the Sum of Two Squares. Euler proposed four more propositions, that which we won't explore in this paper, but it sets the precedence that there was certainly a lot of math to explore in the Sum of Two Squares. We will now extend the sum of two squares through some of Fermat's work.

5. Extensions

Proposition 5.1. If $n \equiv 3 \pmod 4$, then n is not a sum of two squares.

Lemma 5.1. For a prime $p \equiv 1 \pmod 4$, there exists $x \in \mathbb{Z}$ such that $p \mid (x^2 + 1)$ (Fermat's Lemma)

Essentially, what we are trying to establish here is that Fermat asserts that a specific form of sum of two squares is divisible by p. Why is this significant? In short, its relevance pertains to how Gaussian integers work, that is, $x^2 + 1$ is reducible over $\mathbb{C}$ where, $(x^2 + 1) = (x + i)(x - i)$. From this, we can ascertain that $p \mid (x + i)$ and $p \mid (x - i)$ based on Euclid's Lemma.

However, it must also be considered that in the Quotient field $\mathbb{Q}[i]$, the element $(x + i)/p = \frac{x}{p} + \frac{1}{p}i$ where $1/p$ is $\notin \mathbb{Z}$. That would suggest p is in fact not irreducible therefore, factorizing as,

$$p = (a + bi)(c + di)$$

with $1 < N(a + bi), N(c + di)$. This also suggests that,

$$p = N(a + bi) = (a + bi)(a - bi) = a^2 + b^2$$

where $N(p) = p^2$. This also further develops the idea that $c + di = a - bi$ where a prime p is irreducible must split into a product of two conjugate irreducible elements over the field $\mathbb{Z}[i]$.

Proposition 5.2. If p is a prime, then $p \mid (p - 1)! + 1$. (Wilson's Theorem)

Proof. We see that,

$$(p - 1)! \equiv -1 \pmod p$$

Alternatively, we can multiply all the non-zero elements of the finite field $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$,, getting -1.

We can show this for $p = 2$ where $2 = (2 - 1)! + 1$, thus, we can assume with fair certainty that p is an odd prime.

Consider the map ι: $\mathbb{F}_p^\times \to \mathbb{F}_p^\times$ given by $x \mapsto x^{-1}$. This map is a bijection, that is, every element has a unique inverse.

Furthermore, the "fixed points" of the map ι are those elements $x = \iota(x)$ which is equal to their own inverse, that is, $x = x^{-1}$, which can be rewritten as $x^2 = 1$ with the solutions, $x = \pm 1$.

This also suggests that the polynomial $x^2 - 1$ can have at most two roots in the field $\mathbb{F}_p^\times$, implying that every element different from ±1 in $\mathbb{F}_p^\times$ is distinct from its inverse. Thus, when we multiply out the non-zero elements of $\mathbb{F}_p^\times$, we get,

$$1 \cdot -1 \cdot \left(x_1 \cdot x_1^{-1}\right) \cdots \left(x_{\frac{p-3}{2}} \cdot x_{\frac{p-3}{2}}^{-1}\right)$$

All the elements apart from ±1 can in fact be paired with their distinct and unique multiplicative inverse, making the product -1 clear. ■

This can further be explored through Wilson's theorem to prove Fermat's lemma which eventually leads to Fermat's Two Squares Theorem. The proof utilized the idea of **reduced residue system** and eventually yields the theorem:

Theorem 5.2. A prime p is a sum of two integer squares if and only $p = 2$ or $p = 4k + 1$. (Fermat's Two Squares Theorem)

6. Conclusion

The Sum of Two Squares is a vast area of Mathematics that which has been explored by both Euler and Fermat. Euler's work through his seven propositions shows the vastness of the underlying math within where he analyzed several patterns, drawing multiple corollaries. Similarly, the discovery of which primes are sums of two squares was primarily led by Fermat through his theorem.

This paper could only explore three of the seven propositions that Euler laid out in his paper E228 and the development towards Fermat's Theorem, however, we expand on several examples showing Euler's Corollaries while exploring his work including explanation and its implications through several examples.

7. Note

As stated earlier in the Introduction, propositions and proofs explored in this paper have been written by Euler and Fermat respectively. This paper has simply explored these propositions and proofs, expanding on their implications and extending on the idea of Sum of Two Squares.

References

[1] *4400twosquares.pdf*. URL: `http://alpha.math.uga.edu/~pete/4400twosquares.pdf` (visited on 07/28/2023).

[2] *Bhaskar.pdf*. URL: `https://math.uchicago.edu/~may/VIGRE/VIGRE2008/REUPapers/Bhaskar.pdf` (visited on 07/28/2023).

[3] Leonhard Euler. "On numbers which are the sum of two squares, E228en". In: (). (Visited on 07/28/2023).

Euler Circle, Mountain View, CA 94040
Email address: aryandalal06@gmail.com, rithwik.sharma18185@gmail.com