DIOPHANTINE EQUATIONS

NAHUM LINHART
NEEL CHATTOPADHYAY

1. **Abstract**

In this paper, we aim to discuss Diophantine equations: equations that express a specific natural number. This paper will primarily focus on one profound Diophantine equation: The Sum of Two Squares. We shall discuss a brief history of Diophantine equations and methods that mathematicians have utilized in the past to solve such problems. We will build towards Pierre de Fermat's theorem of the sum of two squares, which discusses only prime natural numbers, and expand to a generalization for all natural numbers. We aim to discuss and prove the question of what natural numbers can be expressed as a sum of two integer squares.

2. **Introduction**

The earliest, most natural mathematical concepts involve counting and the presentation of numbers in terms of other numbers. Flipping through historic mathematics texts, one easily sees that ever since the conception of geometry, mathematicians have concerned themselves with the question of which numbers can be presented in a specific arithmetic sense. A simple example is the set of integer squares: those numbers n that can be written as x^2 with x an integer. Such a problem setup, where integers are the only legal inputs and/or outputs, is referred to as a Diophantine equation.

Definition 2.1. [3] A Diophantine equation is a polynomial with integral coefficients where integer solutions are only of concern

The first studies of Diophantine equations date back to the third century with Diophantus of Alexandria, hence the name. Solutions to Diophantine equations have dominated advancements in algebra over the centuries. Namely, one is typically concerned with the existence of solutions and a generating expression for all such solutions.

One might ask whether there exists a universal algorithm that deduces whether any Diophantine equation has solutions (in the integers). This problem is David Hilbert's famous "tenth problem" which was solved by Yuri Matiyasevich in 1970. Matiyasevich's theorem states that the set of all Diophantine equations that have a solution in the non-negative integers is not recursive and that no such algorithm exists [2].

Since no general solution or algorithm exists to solve Diophantine equations, one must leverage the unique structure of the problem to solve it. Consider the classical example of the Pythagorean triples, integers a, b, and c that satisfy $c^2 = a^2 + b^2$. The Greeks developed an algorithm to find Pythagorean triples with all integer solutions, called the generating equations.

Proposition 2.2 (Euclid's Generating Functions [8])**.** *Let r and s be integers satisfying the following:*

(1) $0 < r < s$
(2) $\gcd r, s = 1$
(3) $s \not\equiv r \mod 2$.

Then $a = r^2 - s^2$, $b = 2rs$, and $c = r^2 + s^2$ satisfy $a^2 + b^2 = c^2$.

Example 2.3. Lets take $(r, s) = (3, 2)$. Then

$$a = 3^2 - 2^2 = 5$$
$$b = 2 \cdot 3 \cdot 2 = 12$$
$$c = 3^2 + 2^2 = 13,$$

and we can compute that indeed

$$5^2 + 12^2 = 25 + 144 = 169 = 13^2.$$

Uniqueness of solutions is also of concern, i.e. how many distinct n-tuples $(x_1, \ldots, x_n)$ are valid solutions to the equation $z = f(x_1, \ldots, x_n)$.

The main concerns of this paper are early modern results from Pierre de Fermat. Fermat made astonishing discoveries in number theory (including parts of what would later become finite group theory) and proposed two theorems that made significant contributions to the advancement of solving presentation problems. These two theorems are the sum of two squares theorem and the famous Fermat's Last Theorem.

Theorem 2.4 (Sum of Two Squares Theorem [7])**.** *Let p be a prime and x and y be integers satisfying $p = x^2 + y^2$. Then $p = 2$ or $p \equiv 1 \mod 4$.*

Example 2.5. The number 5 satisfies gives empirical evidence for this theorem, as $5 = 1^2 + 2^2$ and $5 \equiv 1 \mod 4$.

This theorem states that for a prime to be written as a sum of two squares, it must be congruent to 1 modulo 4 (or equal to 2), so no primes congruent to 3 modulo 4 are not the sums of two squares. We will prove this and related results in a bit.

The following historic result was only recently proven using methods beyond the scope of this paper.

Theorem 2.6 (Fermat's Last Theorem [4]). *The Diophantine equation $a^n + b^n = c^n$ has no integer solutions for natural number $n > 2$.*

Consider the equation $n = x^2 + y^2$. If we admit numbers x and y from the complex numbers then any $n \neq 0$ can be written this way. However, if we restrict to the case when x and y are integers, this problem becomes more complicated and requires a finer analysis of details and residues. In general, all Diophantine equations have complex solutions, but this is quite uninteresting.

3. **Sums of Two Squares**

3.1. **Primes.** In this section, we will prove the sum of two squares theorem for primes. First, we will give a few definitions in modular arithmetic, a set of foundational ideas that will allow us to properly partition the primes.

Definition 3.1. [5] Let $n \in \mathbb{Z}$. We say that $a \equiv b \mod n$ if a and b have the same remainder r on division by n, where r is an element of the residue system $\mathbb{Z}/n\mathbb{Z} := \{0, 1...n-1\}$.

Example 3.2. We can write 13 as $(4 \cdot 3) + 1$, so we say $13 \equiv 1 \mod 4$

Proof of Theorem 1.4. We recall $\{0, 1, 2, 3\}$ is a complete residue system of $\mathbb{Z}/4\mathbb{Z}$. Note, we are only considering primes expressed as a sum of two squares, and thus we have to consider the set $(\mathbb{Z}/4\mathbb{Z})^2$, where the residue system is reduced once more:

$$\begin{aligned} 0^2 &\equiv 0 \text{ mod } 4 \\ 1^2 &\equiv 1 \text{ mod } 4 \\ 2^2 &\equiv 0 \text{ mod } 4 \\ 3^2 &\equiv 1 \text{ mod } 4. \end{aligned}$$

Thus, the residue system of $(\mathbb{Z}/4\mathbb{Z})^2$ is {0,1}. Yet again, we are only considering the primes written as a sum of two squares, and so we consider all elements of $(\mathbb{Z}/4\mathbb{Z})^2 + (\mathbb{Z}/4\mathbb{Z})^2$:

$$\begin{aligned} 0+0 &\equiv 0 \bmod 4 \\ 1+0 &\equiv 1 \bmod 4 \\ 1+1 &\equiv 2 \bmod 4 \end{aligned}$$

Therefore, the set {0,1,2} expresses the possibilities for which a number can be expressed as a sum of two squares. No prime greater than 2 is congruent to 0 or 2 modulo 4, so we have our result. □

3.2. **Sum of Two Squares (Generalized).** We have proved that a prime p is either 2 or congruent to 1 mod 4 for it to be expressed as a sum of two squares. We will now pose the question for all natural numbers. We earlier discussed that the set {0,1,2} expresses the possibilities of a natural number to be expressed as a sum of two squares mod 4. We now pose the question: can we express a natural number n in terms of it's prime factors? Firstly, we must define the terms group, monoid, ring, and Euclidean domain [1] to properly prove the Sum of Two Squares by utilizing the Gaussian Integers.

Definition 3.3. A group $(G, *)$ is a set G and a binary operator $*$ that must satisfy:

(1) Closure: $a * b \in G$ for all $a, b \in G$.
(2) Associativity: $a * (b * c) = (a * b) * c$ for all $a, b, c \in G$.
(3) Identity: there exists $e \in G$ such that $e * a = a * e = a$ for every $a \in G$.
(4) Invertibility: for every $a \in G$ there exists $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.

Proposition 3.4. $(\mathbb{Z}, +)$ *is a group.*

Proof. Obviously, $a + b \in \mathbb{Z}$ for all $a, b \in \mathbb{Z}$, and we know integer addition is associative. We take $e = 0$ as our identity and the inverses become simple: $a^{-1} := -a$ such that $a + (-a) = -a + a = 0$. □

A group where every element commutes ($a * b = b * a$ for all $a, b \in G$) is called *abelian.* The aforementioned group $(\mathbb{Z}, +)$ is abelian.

Definition 3.5. A monoid $(S, \cdot)$ is a set S under a binary operation $\cdot$ satisfying the properties of closure, associativity, and identity, but not necessarily invertibility.

We may now combine these two structures into the main tools of the paper.

Definition 3.6. A ring $(R, +, \cdot)$ is a set R and two binary operations, $+$ and $\cdot$, that satisfy:

(1) $(R, +)$ is an abelian group.
(2) $(R, \cdot)$ is a monoid.
(3) Distributivity: $r \cdot (s + t) = r \cdot s + r \cdot t$ and $(s + t) \cdot r = s \cdot r + t \cdot r$ for all $r, s, t \in R$

Similar to the notion of a group, if all elements commute under the operator $\cdot$, we call R a *commutative ring.*

Proposition 3.7. $(\mathbb{Z}, +, \cdot)$ *is a commutative ring.*

Proof. We have already shown that $(\mathbb{Z}, +)$ is an abelian group. That $(\mathbb{Z}, \cdot)$ is a monoid is also very clear, and we know that we can distribute multiplication over addition in the integers, so we are done. □

Definition 3.8. A ring $(R, +, \cdot)$ is a Euclidean domain if there exists a Euclidean function $N : R \to \mathbb{N} \cup \{0\}$ that gives meaning to the Euclidean algorithm and division theorems.

For every nonzero $\alpha, \beta \in R$ there exist $\xi, \eta \in R$ such that $\alpha = \beta\xi + \eta$ and $N(\eta) < N(\beta)$.

Proposition 3.9. *The ring* $(\mathbb{Z}, +, \cdot)$ *is a Euclidean Domain.*

Proof. The Euclidean function for the integers is merely taking the absolute value of the integer. In other words, $\mathrm{N}(a) = |a|$ for a an integer. We note obviously the integers give meaning to the Euclidean algorithm and division theorems, and thus the ring $(\mathbb{Z}, +, \cdot)$ is a Euclidean Domain. □

Definition 3.10. For an element u in a ring to be a unit, there must also exist a u^-1 such that, $uu^{-1} = 1$, the multiplicative identity.

Definition 3.11. An irreducible element α is one such that if $\beta | \alpha$ and $N(\beta) < N(\alpha)$, then β is a unit.

Lemma 3.12. *A prime element in an Euclidean Domain is the same as an irreducible element.*

The Gaussian integers are a Euclidean Domain under the Euclidean Function, the Norm, in which elements of the Gaussian integers map to the natural numbers. We shall take an element of the ring z, for which it can be expressed as $z = a + bi$, where a and b are integers, and $i = \sqrt{-1}$. For z to be mapped to the natural numbers, we must take the Euclidean function to be $\mathrm{N}(z) = z\bar{z}$ where $\bar{z}$ is the complex conjugate ($\bar{z} = a - bi$).

Lemma 3.13. *Let $z \in \mathbb{Z}[i]$. The set N(z) expresses the set of natural numbers that can be expressed as a sum of two squares.*

Proof. For $z = a + bi$, observe the result of $\mathrm{N}(z)$

$$\begin{gathered}(a+bi)(a-bi) = \\ a^2 - abi + abi - bi^2 = \\ a^2 - (-b^2) = \\ a^2 + b^2\end{gathered}$$

□

We note by **Lemma 3.13**, that for a natural number n to be expressed as a sum of two squares, it must be the Norm of some element in the Gaussian integers.

In order to progress further, we must discuss the prime factorization of the composite numbers that can be written as a sum of two squares by first prime factorizing them in both the integer primes and Gaussian primes.

Lemma 3.14. *We propose the Norm is multiplicative.*

$$N(xy) = N(x) \cdot N(y).$$

If n is composite, we can prime factorize it into it's prime factors, denoted: $(p_1^{k_1})(p_2^{k_2})...(p_n^{k_n})$.

By utilizing the Norm's multiplicative property, we can rewrite this expression in terms of the Norm of elements $z_p \in \mathbb{Z}[i]$.

$$\begin{gathered}n = (p_1^{k_1})(p_2^{k_2})...(p_n^{k_n}) \\ N(z) = N(z_1^{k_1})N(z_2^{k_2})...N(z_n^{k_n})\end{gathered}$$

We note all prime factors of n are the Norm of some element $z_p \in \mathbb{Z}[i]$. By **Lemma 3.13**, if the prime p is the Norm of some element in the Gaussian Integers, it can be expressed as a sum of two squares. By **Theorem 2.4**, if a prime p can be expressed as a sum of two squares, it must be 2 or congruent to 1 mod 4. Thus, all prime factors of n must be powers of 2 or congruent to 1 mod 4.

And so we can finally state that for a natural number n to be expressed as a sum of two squares, $n = 2^k T$, where k is a non-negative integer, and $T \equiv 1 \bmod 4$.

However, we must account for the other prime factors that are simplified in $(\mathbb{Z}/4\mathbb{Z})^2$. For which 3 is not fully accounted for. By **Theorem**

1.4, a prime factor of n cannot be congruent to 3 mod 4. However, we propose that prime factors congruent to 3 mod 4, raised to even powers are viable prime factors.

$$3^x \equiv 3 \bmod 4, \text{ for } x \equiv 1 \bmod 2.$$
$$3^1 \equiv 3 \bmod 4$$
$$3^y \equiv 1 \bmod 4, \text{ for } y \equiv 0 \bmod 2.$$
$$3^2 \equiv 1 \bmod 4$$

Since the prime factors congruent to 3 mod 4 raised to even powers are congruent to 1 mod 4, they are acceptable prime factors and thus can also be expressed as sums of two squares.

Example 3.15. 6 cannot be expressed as a sum of two squares, but 18 can.

$$6 = 2^1 \cdot 3^1$$
$$6 \neq a^2 + b^2$$
$$18 = 2^1 \cdot 3^2$$
$$18 = 9^2 + 9^2$$

Utilizing the prime factorization of n in the integers, and the Norm's multiplicative property, we can finally give an appropriate expression for n in terms of it's prime factors.

$$\text{For } n = a^2 + b^2, \{a, b, \in \mathbb{Z}\}$$
$$n = 2^k PQ$$
$$n \in \mathbb{N}$$
$$k \in \mathbb{Z}$$
$$P = \textstyle\prod_{p|n,}\ p \equiv 1 \bmod 4$$
$$Q = \textstyle\prod_{p|n} (p \equiv 3 \bmod 4)^s\ \{2|s\}$$

Example 3.16. Let's put this into practice with an element from the Gaussian integers and use the Euclidean Function to map it to the natural numbers. We will then prime factorize its value when mapped using the formula given. We shall use the element $15 + 13i$. Taking the norm of $15 + 13i$ we can determine that the natural number counterpart is 394.

$$(15 + 13i)(15 - 13i) =$$
$$15^2 + 13^2 =$$
$$394$$

Now, let's prime factorize 394, a sum of two squares. 394 can be factored into 2 and 197, which are both primes. $2 = 2^1$, so the value of k is 1. $197 \equiv 1 \bmod 4$, so the value of P is 197. There is no prime factor of

394 congruent to 3 mod 4, so we can treat Q as 1. Plugging this into the formula, we get:

$$n = (2^1)(197)$$
$$n = 394$$

This example is quite trivial, but it gives us a good idea of how this works in practice.

Now briefly we will discuss some other methods to solve Diophantine equations. For the sum of two squares problem, we can take a more abstract approach, by posing questions initially as $x^2 \equiv -1 \bmod p$. As we stated earlier in the residue of $(\mathbb{Z}/4\mathbb{Z})^2$, we can prove this is only true when $p \equiv 1 \bmod 4$. Now this is one way to approach such a problem, and we took a similar approach through our investigation of the residue of $\mathrm{N}(z) = z\bar{z}$.

Now for other Diophantine equations, these methods may or may not work. If such equations involve a quadratic expression, then these methods might work, but you must be clever about designing your Euclidean domain. For example, another Euclidean domain the Eisenstein integers ($\mathbb{Z}[\omega]$), are used in an approach to prove Fermat's Last Theorem in the case of $n = 3$. However, these approaches frequently don't work, but there are techniques, although slightly more advanced, that are commonly used. These include utilizing the discriminant and stereographic projection, which are great tools we didn't primarily showcase in our proofs for other Diophantine equations.

3.3. **Fermat's Last Theorem.** We will close with a brief history of Fermat's Last Theorem (recall **Theorem 1.6**), arguably the most famous Diophantine equation, and one of the most notable equations in Number Theory. Introduced in 1637 by French mathematician Pierre de Fermat, this problem has lots of history surrounding it. During his time, Fermat claimed to have devised a proof for his theorem, yet no proof was ever published or discovered. Although his proof for the general case of $n > 2$ was never published, he proved another theorem essentially proving the case of $n = 4$. Even after Fermat's passing in 1665, mathematicians still held an interest in this mysterious problem, one of the most notable being Leonhard Euler. The case of $n = 3$ was eventually proven by Euler, utilizing some of Fermat's methods. Later on, he also proved the same result by using some other algebraic techniques (with some gaps). However, even after the proof of the case for $n = 3$, mathematicians were stuck for centuries to prove the general case of $n > 2$. The man to finally overcome this barrier was Andrew Wiles, an English mathematician. Wiles found a correlation between Fermat's Last Theorem and the Taniyama–Shimura conjecture, seemingly two extremely different fields of mathematics. Even though both problems were seemingly "unprovable", after a long 6 years, he proved the general case of Fermat's Last Theorem in 1993. This proof had a small error, but with the help of his former student, Richard Taylor, Wiles worked out an accurate proof, published in 1995. Wiles's proof gained incredible popularity, and he was crowned with numerous awards for his genius proof of the 300-year-old problem [4].

3.4. **Real World Applications.** Although Diophantine equations are incredibly important in mathematical fields, especially Number Theory, they also have incredible usages in other fields, notably chemistry. In chemistry, linear Diophantine equations are commonly used when balancing tediously long chemical reactions. Using the process of Diophantine equations and applying laws of conservation of mass, chemical reactions can be treated as mathematical equations by associating chemical elements with prime numbers. In practice, each chemical compound is broken into its chemical components - just as integers can be factorized into its prime factors. We use this relationship to express each compound mathematically, where we can easily compute each integer coefficient utilizing systems of Diophantine equations. We shall give an example below to find the integer coefficients of the chemical reaction:

$$a\mathrm{KNO_3} + b\mathrm{S} + c\mathrm{C} \to d\mathrm{K_2S} + e\mathrm{N_2} + f\mathrm{CO_2}$$

Firstly, we must associate each chemical element with a correlating prime number (K = 67, N = 17, O = 19, S = 47, C = 13).

Since chemical reactions and prime factorizations utilize different operations, we must make the following correlations to derive a mathematical expression:

If there are different chemicals added together in a compound → unique correlating prime numbers are multiplied together.

If there are multiples of the same element in a compound → they are correlating powers of primes.

After applying these rules, we end with a mathematical expression of the chemical reaction.

$(67 \cdot 17 \cdot (19)^3)^a \cdot 47^b \cdot 13^c = ((67^2) \cdot 47)^d \cdot (17^2)^e \cdot (13 \cdot (19^2))^f$

We can derive a system of linear Diophantine equations by utilizing the prime factorization on both sides of the equation.

$(a = 2d,\ a = 2e,\ 3a = 2f,\ b = d,\ c = f)$

After using some basic algebra we find the solution to this system of equations, which are of the following form in terms of a variable j.

$(a = 2j,\ b = j,\ c = 3j,\ d = j,\ e = j,\ f = 3j)$

Since we are only interested in the simplest of integer solutions, we can take $j = 1$, and we end with our resulting balanced chemical equation:

$$2KNO_3 + S + 3C \rightarrow K_2S + N_2 + CO_2$$

This example may seem quite simple, but when working with extremely long chemical reactions these processes are very tedious by hand. By utilizing this formula, alongside some simple computing, we can efficiently balance these chemical equations.[6].

References

[1] G. H. Hardy, E. M. Wright *An Introduction to the Theory of Numbers* Oxford 1954

[2] Yuri V. Matiyasevich *Hilbert's tenth problem* Foundations of Computing Series. MIT Press, Cambridge, MA, 1993

[3] *Diophantine equations* Encyclopedia of Mathematics, EMS Press, 2001

[4] Britannica, T. Editors of Encyclopedia. *"Fermat's last theorem."* Encyclopedia Britannica, April 25, 2024. https://www.britannica.com/science/Fermats-last-theorem.

[5] P. Keef, D. Guichard *Introduction to Higher Mathematics* Department of Mathematics Whitman College 2023

[6] L. Walsh *Chemical Equations and Diophantine Equations* The Reinsurance Actuary 2016

[7] *Sum of Squares Theorems* Brilliant.org https://brilliant.org/wiki/fermats-sum-of-two-squares-theorem/

[8] Bill Richardson *Pythagorean Triples* Wichita State University

Massachusetts Institute of Technology, 77 Massachusetts Avenue, Cambridge, MA 02139