Sum of Two Squares

Number Theory

Nahum Linhart, Neel Chattopadhyay

May 19, 2024

Abstract

Many know of equations such as the Pythagorean triples, where $a^2 + b^2 = c^2$, but what if we set more restrictions? How do the results differ and how do we solve such proposed equations?

Diophantine equation

Polynomials with integral coefficients in which only integer solutions are of interest

In this presentation, we will discuss one of these **"Diophantine equations"**, the Sum of Two Squares, which poses the question of which natural numbers can be expressed as a sum of two integer squares.

Question

What primes can be written as a sum of two integer squares?

In other words, for which $p \in \mathbb{P}$ do there exist $a, b \in \mathbb{Z}$ such that $p = a^2 + b^2$?

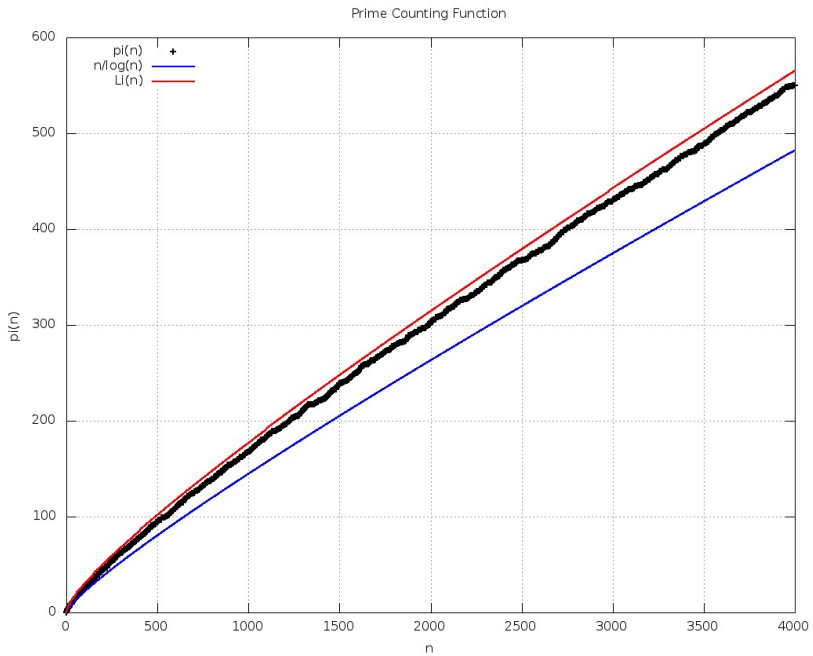

Figure: Prime Distribution Graph

Does there exist an obvious pattern?

Let's venture empirically and look at the integers $1 - 10$

$$1 = 1^2 + 0^2$$

$$2 = 1^2 + 1^2$$

No solution exists for 3

$$4 = 2^2 + 0^2$$

$$5 = 2^2 + 1^2$$

No solution exists for 6

No solution exists for 7

$$8 = 2^2 + 2^2$$

$$9 = 3^2 + 0^2$$

$$10 = 3^2 + 1^2$$

Pattern: No

Figure: Diophantus of Alexandria

- No observable pattern
- Most Diophantine equations cannot be solved based on pure observation
- Diophantine equations have infinite solutions if admitting elements $\in \mathbb{C}$

Modular Arithmetic

The *integers modulo 4* ($\mathbb{Z}/4\mathbb{Z}$) is an easy way to classify all integers.

The set $\mathbb{Z}/4\mathbb{Z}$

For any positive integers a and $b \neq 0$ there exist integers q and r such that

$$a = bq + r,$$

and where $0 \leq r < b$. If $b = 4$ then $r \in \{0, 1, 2, 3\} := \mathbb{Z}/4\mathbb{Z}$

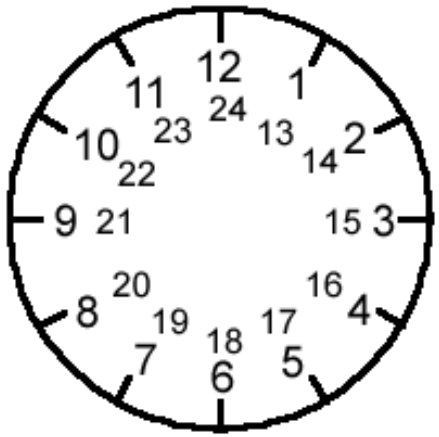

Figure: Clock Display

Modular Arithmetic cont'd

The *squares modulo 4* $(\mathbb{Z}/4\mathbb{Z})^2$ are the $a \in \mathbb{Z}/4\mathbb{Z}$ for which there is an integer x such that $a \equiv x^2 \mod 4$.

Check for yourselves that the only ones are 0 and 1!

The *sums of two squares modulo 4* is denoted $(\mathbb{Z}/4\mathbb{Z})^2 + (\mathbb{Z}/4\mathbb{Z})^2$. The elements of this set are:

$$0 \equiv 0^2 + 0^2 \mod 4$$
$$1 \equiv 0^2 + 1^2 \mod 4$$
$$2 \equiv 1^2 + 1^2 \mod 4$$

Sum of Two Squares Theorem I

Albert Girard

Pierre de Fermat

General version using modulus

An integer a is the sum of two squares if and only if a is congruent to $0, 1$, or 2 modulo 4.

But the primes are much more restrictive.

Sum of Two Squares (Primes)

A prime p is the sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.

Restatement of Question

What if we expand this question to all natural numbers, and not just primes? Can we get a statement in terms of the prime factorization?

Sum of Two Squares Solution

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

Definitions

To answer this, we must consider the *ring of Gaussian integers* $\mathbb{Z}[i]$.
Let's first start with some definitions:

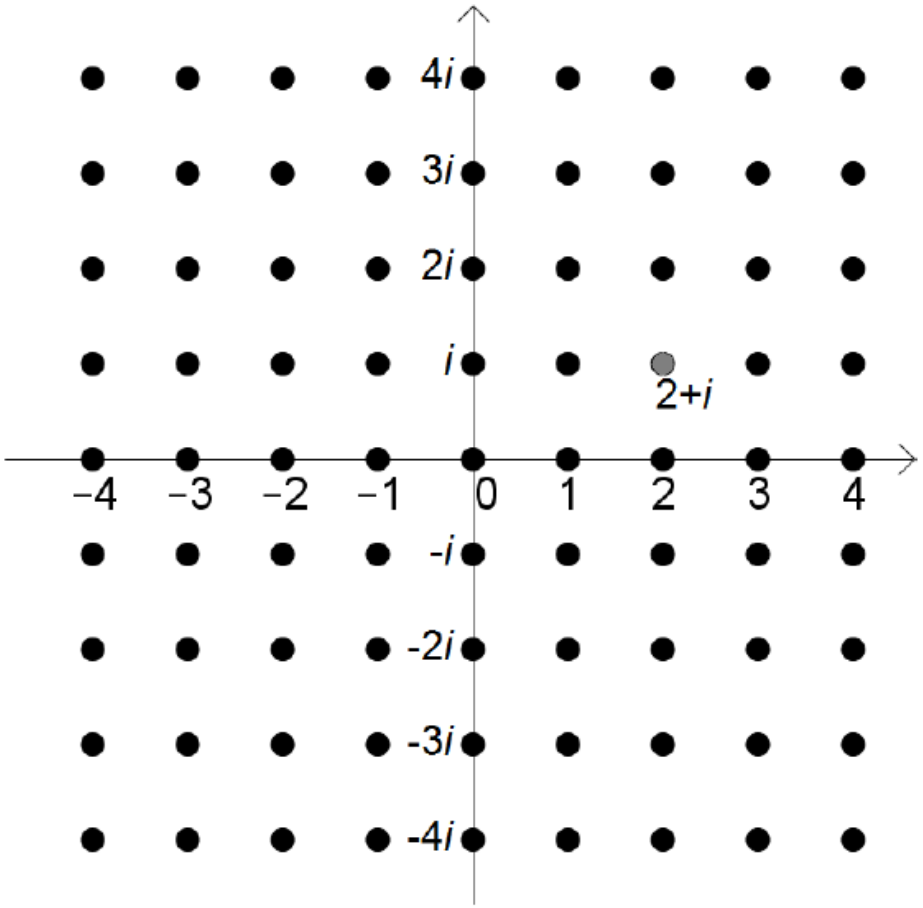

Figure: Gaussian Integer Graph

Definitions

Group

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 $a + a^{-1} = a^{-1} + a = e$.

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

Example

The Integers are an abelian group under addition, $(\mathbb{Z}, +)$

Definitions

Monoid

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

Example

The integers are a monoid under multiplication, $(\mathbb{Z}, \times)$

Ring

A ring $(R, +, \times)$ is a set R and two binary operations, $+$ and $\times$, that satisfy:

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

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

Example

The integers are a ring under addition and multiplication, $(\mathbb{Z}, +, \times)$

Definitions

Euclidean Domain

A ring $(R, +, \times)$ 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, i.e. for every nonzero $\alpha, \beta \in R$ there exist $\gamma, \delta \in R$ such that

$$\alpha = \beta\gamma + \delta$$

and $N(\delta) < N(\beta)$.

Example

The integers are mapped to the natural numbers by the Euclidean function: $\mathrm{N}(t) = |t|$.

Gaussian Integers

The Gaussian integers ($\mathbb{Z}[i]$) are an Euclidean Domain under the Euclidean Function, the Norm, in which $\mathbb{Z}[i] \mapsto \mathbb{N}$. An element of the ring, z, can be expressed as

$$z = a + bi, \text{ where } a, b \in \mathbb{Z}, i = \sqrt{-1}.$$

$N(z) = (z\bar{z})$ where $\bar{z}$ is the complex conjugate of z ($\bar{z} = a - bi$).

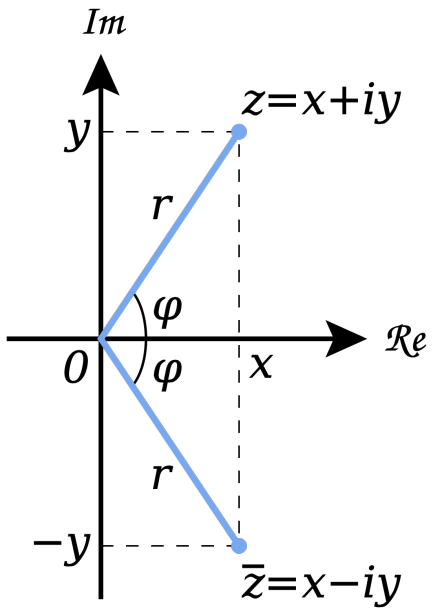

Figure: Complex Conjugate

Gaussian Integers

We notice that z becomes a sum of two integer squares when mapped to the natural numbers by the Norm.

$$(a+bi)(a-bi) =$$
$$a^2 - abi + abi - bi^2 =$$
$$a^2 - (-b^2) =$$
$$a^2 + b^2$$

Note

Note for the rest of this proof,

$$z = a + bi\{z \in \mathbb{Z}[i]\},$$
$$N(z) = n = a^2 + b^2, \{a, b \in \mathbb{Z}, n \in \mathbb{N}\}.$$

Sum of Two Squares...

Lemma

The Norm is multiplicative:

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

If n is **NOT** prime, we can prime factorize the natural number n into $(p_1^{k_1})(p_2^{k_2})...(p_n^{k_n})$
Using our multiplicative Norm, we can relate the prime factors of n to other elements $\in \mathbb{Z}[i]$

$$n = (p_1^{k_1})(p_2^{k_2})...(p_n^{k_n})$$
$$N(z) = N(r_1^{k_1})N(r_2^{k_2})...N(r_n^{k_n})$$

Sum of Two Squares Cont...

- Each prime factor p is the Norm of some other element $r \in \mathbb{Z}[i]$.
- The Norm of Gaussian Integers displays the set of numbers that can be expressed as a sum of two squares
- The prime factors must be within that set

Recall our theorem for primes:

Sum of Two Squares (Primes)

A prime p is the sum of two squares if and only if $p = 2$ or $p \equiv 1 \mod 4$.

Each prime factor p of n must be 2 or congruent to 1 mod 4.

What about 3?

While finding the residue set $(\mathbb{Z}/4\mathbb{Z})^2$, our other possible prime factor 3 is simplified

If a prime factor p is congruent to 3 mod 4, it must be raised to an even power.

$$3^1 = 3 \equiv 3 \bmod 4$$
$$3^2 = 9 \equiv 1 \bmod 4$$

Sum of Two Squares Solution

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

Thank you for listening!