Gaussian Numbers and Further Sums of Squares

Matteo Melis (40324932)

Contents

February 28, 2025

1 Introduction

Gaussian numbers are integers expressible as sums of two squares ($a^2 + b^2 : a, b \in \mathbb{Z}$). They are foundational objects in number theory, deeply intertwined with classical questions about prime factorisation. These numbers, which arise as the *norms* of Gaussian integers (complex numbers of the form $a + bi$ where $a, b \in \mathbb{Z}$), provide a critical bridge between algebraic structures and arithmetic results.

Central to this study are the Gaussian integers themselves, which form a Euclidean domain. Their rich structure, encompassing unique prime factorisation, the Euclidean algorithm, and norms that map to Gaussian numbers, enables precise characterisations of primes representable as sums of two squares. By leveraging these tools, the work not only recovers classical results like Fermat's theorem on two squares but also extends to higher-dimensional analogues, such as Lagrange's four-square theorem.

We begin by defining some pre-requisite and foundational properties of the Gaussian numbers, and tying them into the algebraic framework of Gaussian integers through its norm function.

2 Properties of Gaussian Numbers

Definition 2.1. A natural number n is called a **Gaussian number** if $n = m^2 + k^2$ for some $m, k \in \mathbb{Z}$.

Theorem 2.2. The product of two Gaussian numbers is itself a Gaussian number.

Proof. Let $n = a^2 + b^2$ and $m = c^2 + d^2$ be Gaussian numbers, with $a, b, c, d \in \mathbb{Z}$. Then:

$$\begin{aligned} nm &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= ((ac)^2 + 2abcd + (bd)^2) + ((ad)^2 - 2abcd + (bc)^2) \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

Since $a, b, c, d \in \mathbb{Z}$, we have that $ac + bd$, $ad - bc \in \mathbb{Z}$ and hence nm is a Gaussian number. □

Definition 2.3. The **Gaussian integers** are the set

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}, \text{where } i^2 = -1, \tag{1}$$

of complex numbers whose real and imaginary parts are both integers.

Remark 2.4. Since the Gaussian integers are closed under addition and multiplication, they form a commutative ring, which is a subring of the field of complex numbers. It is thus an integral domain.

Definition 2.5. The **norm** of a Gaussian integer is its product with its conjugate. That is, we can define the norm function $N : \mathbb{Z}[i] \to \mathbb{N}$ by:

$$N(a + bi) = a^2 + b^2, \tag{2}$$

for some $a, b \in \mathbb{Z}$.

Remark 2.6. Note that the norm is multiplicative, meaning that for any $z_1, z_2 \in \mathbb{Z}[i]$, we have:

$$N(z_1 z_2) = N(z_1)N(z_2). \tag{3}$$

Remark 2.7. The norm of a Gaussian integer is simply the sum of two (integer) squares. Meaning, it takes the precise form of a Gaussian number.

Corollary 2.8. The only Gaussian integers that are invertible in $\mathbb{Z}[i]$ are ± 1 and $\pm i$.

Proof. It is easy to see that ± 1 and $\pm i$ have inverses in $\mathbb{Z}[i]$: The elements 1 and -1 are their own inverses. The elements i and $-i$ satisfy $i \cdot (-i) = 1$, so they are inverses of each other.
For the converse direction, suppose $\alpha \in \mathbb{Z}[i]$ is invertible. Then there exists some $\beta \in \mathbb{Z}[i]$ such that

$$\alpha\beta = 1 \iff N(\alpha)N(\beta) = 1. \tag{4}$$

Since the norm of any Gaussian integer is a non-negative integer, we must have

$$N(\alpha) = 1 \iff a^2 + b^2 = 1. \tag{5}$$

Thus, we need to solve $a^2 + b^2 = 1$. The integer solutions to this equation give us the four values $\alpha = \pm 1, \pm i$ as required. □

Remark 2.9. Invertible elements are called *units*. The units of $\mathbb{Z}$ are ± 1. From our previous theorem we know the units of $\mathbb{Z}[i]$ are ± 1 and $\pm i$. Knowing a Gaussian integer up to the multiplication by a unit is analogous to knowing an integer up to its sign.

3 Gaussian Integers as a Euclidean domain

The existence of a *Euclidean function* on $\mathbb{Z}[i]$ facilitates a well-defined *division algorithm*, demonstrating that $\mathbb{Z}[i]$ inherits many algebraic properties akin to the ring of ordinary integers $\mathbb{Z}$. Specifically, the norm function $N(a + bi) = a^2 + b^2$ serves as a Euclidean function, enabling the application of the *Euclidean algorithm* to compute greatest common divisors within $\mathbb{Z}[i]$.

This Euclidean structure implies that $\mathbb{Z}[i]$ is a *Principal Ideal Domain (PID)*, where every ideal is generated by a single element. Moreover, since every *PID* is also a *Unique factorisation Domain (UFD)*, this establishes that every non-zero, non-unit element in $\mathbb{Z}[i]$ can be factored uniquely into a product of *Gaussian primes*, up to units and the order of factors.

Consequently, *Gaussian primes* exhibit properties analogous to ordinary primes in $\mathbb{Z}$, bolstering the utility of $\mathbb{Z}[i]$ in various aspects of *algebraic number theory* and *Diophantine analysis*. The following begins to explore some of these features, and aims to motivate the relevance of $\mathbb{Z}[i]$ in this area.

Definition 3.1. An **integral domain** is a commutative ring $R \neq \{0\}$ with the property that

$$xy = 0 \implies x = 0 \text{ or } y = 0 \quad (x, y \in R).$$

An element $x \in R$ such that $xy = 0$ or $yx = 0$ for some $y \neq 0$ is called a **zero divisor**. Therefore, an integral domain is a commutative ring without non-zero zero divisors.

Definition 3.2. Let R be an integral domain. A **Euclidean function** is a function $\varphi : R\backslash\{0\} \to \mathbb{N}$ such that for any $x, d \in R$, with $d \neq 0$, there exist some $q, r \in R$ such that

$$x = qd + r \quad \text{and either} \quad r = 0 \quad \text{or} \quad \varphi(r) < \varphi(d).$$

If a Euclidean function exists, we say R is a **Euclidean domain**.

Remark 3.3. From definition 3.1, it is clear that any field is an integral domain. But indeed, any (unital) subring of a field is an integral domain. This tells us that $\mathbb{Z}[i] < \mathbb{C}$ is an integral domain. We now use this fact to show the Gaussian integers form a Euclidean domain.

Lemma 3.4. The Gaussian integers $\mathbb{Z}[i]$ with the field norm

$$N : \mathbb{Z}[i] \to \mathbb{N} \text{ defined by } N(a+bi) = a^2 + b^2, \text{ where } a, b \in \mathbb{Z}, \tag{6}$$

is a Euclidean domain.

Proof. Let $\alpha, \beta \in \mathbb{Z}[i]$ with $\beta \neq 0$, meaning $\alpha = a + bi$ and $\beta = c + di$. Then put $\frac{\alpha}{\beta} = r + si$ with $r, s \in \mathbb{Q}$. We let p be the closest integer to r and q be the closest integer to s, so that both, $|r - p| \leq \frac{1}{2}, |s - q| \leq \frac{1}{2}$. Now let $\phi = \alpha - (p + qi)\beta$, which is a Gaussian integer since $\alpha - (p+qi)\beta = a+bi-(p+qi)(c+di)$ with $a, b, c, d, p, q \in \mathbb{Z}$ as well as their sums and products. Then we have that:

$$\begin{aligned} N(\phi) &= N(\alpha - (p+qi))\beta = N(\alpha/\beta - (p+qi))N(\beta) \\ &= ((r-p)^2 + (s-q)^2)N(\beta) = \frac{1}{2}N(\beta) < N(\beta), \end{aligned}$$

and so we have the division algorithm. [1] □

We now examine classic results concerning Euclidean Domains, PIDs, and UFDs, which are paramount to establishing the foundational algebraic structures that underpin much of commutative algebra and number theory. They will naturally also serve as backing to our final conclusions regarding the Gaussian and ordinary integers.

Definition 3.5. If R is a commutative ring, the ideal

$$aR = \{ax : x \in R\},$$

is called the **principal ideal** generated by a. We often write (a) for aR. In general, if $a_1, \ldots, a_k \in R$ then the ideal $(a_1, \ldots, a_k)$ is defined by

$$(a_1, \ldots, a_k) = a_1R + \cdots + a_kR = \{a_1x_1 + \cdots + a_kx_k : x_1, \ldots, x_k \in R\}.$$

This is the ideal generated by $a_1, \ldots, a_k$. We say that an ideal I is **finitely generated** if $I = (a_1, \ldots, a_k)$ for some $a_1, \ldots, a_k \in R$.

Definition 3.6. A **principal ideal domain** (PID) is an integral domain in which every ideal is principal.

Theorem 3.7. Any Euclidean domain R is a principle ideal domain

Proof. Let φ be a Euclidean function for R. Let $I \triangleleft R$ be a non-zero ideal. Let d be an element of $I \setminus \{0\}$ minimising $\varphi(d)$. We claim $I = (d)$. Since $d \in I$, clearly $(d) \subseteq I$. Let $x \in I$. Then $x = qd + r$ for some $q, r \in R$ such that $r = 0$ or $\varphi(r) < \varphi(d)$. Since $x, d \in I$ and I is an ideal, it follows that $r = x - qd \in I$. By the minimality of $\varphi(d)$, it follows that $r = 0$. Thus $x = qd \in (d)$. Hence $I = (d)$. [2] □

Definition 3.8. An integral domain R is a **unique factorisation domain** (UFD) if

1. every non-zero non-unit can be written as a product of irreducible elements,
2. if $p_1...p_m = q_1...q_n$ with $p_1, ..., p_m, q_1, ..., q_n$ irreducible then $m = n$ and the lists can be recorded so that p_i and q_i are associates for each $i = 1, ..., n$.

Theorem 3.9. Let R be a principal ideal domain. Then R is a unique factorisation domain.

Proof. We have two things to show:

1. Every non-zero non-unit can be written as a product of irreducibles.

2. If $p_1 \cdots p_m = q_1 \cdots q_n$, then $m = n$ and the q_j's can be reordered so that p_i is an associate of q_i for each $i = 1, \ldots, n$.

(1) Suppose $x \in R$ is a non-zero non-unit which is *not* a product of irreducible elements. In particular, x is not itself irreducible, so $x = x_1 y_1$ where $x_1, y_1 \in R$ are non-zero non-units. Since x is not a product of irreducibles, either x_1 or y_1 (or both) is not a product of irreducibles. Suppose without loss of generality x_1 is not a product of irreducibles. Then by the same argument $x_1 = x_2 y_2$ where $x_2, y_2 \in R$ are non-zero non-units and x_2 is not a product of irreducibles.

If we continue in this way, we obtain an infinite sequence $x_1, x_2, \ldots$ such that x_{n+1} is a proper divisor of x_n for each $n \geq 1$, in contradiction with the fact that any sequence of principal ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ in a PID is eventually constant. Thus, every non-zero non-unit can be written as a product of irreducibles.

(2) Suppose $p_1 \cdots p_m = q_1 \cdots q_n$ with p_i and q_j irreducible. Then p_1 divides $q_1 \cdots q_n$. Since irreducibles are prime, p_1 divides some q_j. By reordering, we may assume p_1 divides q_1. Since q_1 is irreducible, this implies p_1 and q_1 are associates. We can cancel p_1 and q_1 from both sides and repeat the argument to show $m = n$ and each p_i is an associate of a q_i. [2] □

Useful Result: We know from Lemma 3.4 that the Gaussian integers $\mathbb{Z}[i]$ form a *Euclidean domain*, implying that every ideal in $\mathbb{Z}[i]$ is principal and so $\mathbb{Z}[i]$ is a PID and by extension a UFD.

Remark 3.10. Since $\mathbb{Z}[i]$ is UFD, this guarantees that prime factorisation in $\mathbb{Z}[i]$ is unique up to multiplication by units $\{\pm 1, \pm i\}$. Just as in $\mathbb{Z}$, where every integer can be expressed uniquely as a product of primes, every non-zero, non-unit Gaussian integer can be factored uniquely into a product of Gaussian primes. This parallel ensures that Gaussian primes serve as a natural extension of the concept of primes in $\mathbb{Z}$, maintaining the fundamental arithmetic structure of unique factorisation within the extended domain of complex integers.

Example 3.11. Lets look at 5, a prime in $\mathbb{Z}$ but not in $\mathbb{Z}[i]$. It's factorisation is $5 = (2+i)(2-i)$. Checking its factors are irreducible in $\mathbb{Z}[i]$:

$$N(2+i) = 2^2 + 1^2 = 5 \implies N(2-i) = 5.$$

Hence, 5 has a unique factorisation in $\mathbb{Z}[i]$, up to units. An alternative factorisation is:

$$5 = (-i)(-2+i)(-i)(-2-i) = (-i)(2-i)(i)(2+i).$$

$\pm i$ are units, therefore factorisation remains unique up to unit multiplication. Note here the analogy to prime factorisation over $\mathbb{Z}$ — each unique factorisation is comprised of products of primes over the Gaussian integers (Gaussian primes).

Remark 3.12. This example highlights how the concept of primality adapts in the Gaussian integers, demonstrating that elements considered prime in $\mathbb{Z}$ may factorise further in $\mathbb{Z}[i]$. Nevertheless, the preservation of unique factorisation up to units confirms that Gaussian primes maintain an essential analogue to ordinary primes in ensuring the arithmetic structure of $\mathbb{Z}[i]$. This analogy is particularly useful in number theory, as it allows the application of prime-based arguments from $\mathbb{Z}$ to $\mathbb{Z}[i]$, enabling proofs of classical results such as Fermat's Two-Square Theorem.

4 The Euclidean Algorithm in $\mathbb{Z}[i]$

While the ring of integers $\mathbb{Z}$ enjoys a well-defined notion of division with remainder through the division algorithm, extending this concept to the Gaussian integers $\mathbb{Z}[i]$ requires a more nuanced approach. Unlike $\mathbb{Z}$, where every division of integers produces a quotient and a remainder within

clear bounds, the complex nature of $\mathbb{Z}[i]$ means that exact division is not always possible in the same way.

The Euclidean Algorithm provides a powerful framework to overcome this limitation by offering a method to approximate division. Through iterative application of the division algorithm adapted to $\mathbb{Z}[i]$, we can vitally compute the greatest common divisor (gcd) of Gaussian integers. This process introduces a division-like structure, allowing us to determine when two elements are relatively prime and enabling the construction of linear combinations via Bézout's identity.

We begin by defining some well known concepts over the integers, namely, greatest common divisors and relative primality, but over the Gaussian integers instead.

Definition 4.1. For non-zero α and β in $\mathbb{Z}[i]$, a **greatest common divisor** of α and β is a common divisor with maximal norm.

Remark 4.2. Notice how this is somewhat analogous to the usual definition in $\mathbb{Z}$, however we are not strictly constrained to a specific number. Since, for any d, a greatest common divisor of α and β, we know that its unit multiples: $-d, id,$ and $-id$, are too greatest common divisors of α and β. For now we can speak about the concept of *a* greatest common divisor, but not *the* greatest common divisor when working with $\mathbb{Z}[i]$. However, later in this section we show that, for any d, a greatest common divisor of α and β, the set of unit multiples of d are in fact the only greatest common divisors of α and β. A similar result would fall in $\mathbb{Z}$ if the greatest common divisor was defined as a common divisor with largest absolute value, instead of being the largest positive common divisor. We are left with a looser definition of greatest common divisors only up to a unit multiple in $Z[i]$ as we don't currently have an analogue for positivity here.

Definition 4.3. For any α, $\beta \in \mathbb{Z}[i]$ such that they only have unit factors in common, we say they are **relatively prime**.

Theorem 4.4. (Euclidean Algorithm in $\mathbb{Z}[i]$)
In $\mathbb{Z}[i]$, the Euclidean Algorithm is outlined by the following procedure. Let $\alpha, \beta \in \mathbb{Z}[i]$ be non-zero. Recursively apply the division algorithm, starting with this pair, and make the divisor and remainder in one equation the new dividend and divisor in the next, provided the remainder is not zero:

$$\begin{aligned}
\alpha &= \beta\gamma_1 + \rho_1, \ N(\rho_1) < N(\beta) \\
\beta &= \rho_1\gamma_2 + \rho_2, \ N(\rho_2) < N(\rho_1) \\
\rho_1 &= \rho_2\gamma_3 + \rho_3, \ N(\rho_3) < N(\rho_2) \\
&\vdots
\end{aligned}$$

The last non-zero remainder is divisible by all common divisors of α and β, and is itself a common divisor, so it is a great common divisor of α and β. [3]

Proof. Omitted. Identical to the usual proof of Euclid's algorithm in $\mathbb{Z}$. □

Example 4.5. Take $\alpha, \beta \in \mathbb{Z}[i]$ such that

$$\alpha = 11 + 26i, \quad \beta = 38 + 27i. \tag{7}$$

Then we apply the algorithm as follows:

$$\begin{aligned}(11+26i) &= (38+27i)(1+0i)+(-27-i)\\ (38+27i) &= (-27-i)(-1-i)+(12-i)\\ (-27-i) &= (12-i)(-2+0i)+(-3-3i)\\ (12-i) &= (-3-3i)(-2+2i)-i\\ (-3-3i) &= (-i)(3-3i)+0i.\end{aligned}$$

The last non-zero remainder is $-i$. Recall that a greatest common divisor in $\mathbb{Z}[i]$ is only unique up to multiplication by a unit $(\pm 1, \pm i)$, meaning an equivalent greatest common divisor is i. Notice α and β only have unit factors in common, hence α and β are relatively prime (associates).

Remark 4.6. Notice from the above example that, unlike Euclidean's algorithm over $\mathbb{Z}$, two Gaussian integers that are relatively prime do not necessarily obtain 1 as the last non-zero remainder. Rather, we just obtain some unit.

Example 4.7. Consider a counter example, where the greatest common divisor is not a unit. Let $\alpha = 11+3i$ and $\beta = 1+8i$. Then

$$\begin{aligned}11+3i &= (1+8i)(1-i)+2-4i\\ 1+8i &= (2-4i)(-1+i)-1+2i\\ 2-4i &= (-1+2i)(-2)+0,\end{aligned}$$

so a greatest common divisor of α and β is $-1+2i$.
Notice, we could proceed in a different way in the second equation, and get a different last non-zero remainder:

$$\begin{aligned}11+3i &= (1+8i)(1-i)+2-4i\\ 1+8i &= (2-4i)(-2+i)+1-2i\\ 2-4i &= (1-2i)(2)+0.\end{aligned}$$

Therefore $1-2i$ is also a greatest common divisor. Our two different answers are not inconsistent, since, a greatest common divisor is defined at best only up to a unit multiple anyway, and $-1+2i$ and $1-2i$ are unit multiples of each other: $-1+2i = (-1)(1-2i)$. We do note however that here, α and β are not relatively prime since they have a non-unit greatest common divisor.

Corollary 4.8. For non-zero α and β in $\mathbb{Z}[i]$, let d be a greatest common divisor produced by Euclid's algorithm. Any greatest common divisor of α and β is a unit multiple of d.

Proof. Let d' be a greatest common divisor of α and β. From the proof of Euclid's algorithm, d' divides d (because d' is a common divisor). Write $d = d'\gamma$, so

$$N(d) = N(d')N(\gamma) \geq N(d').$$

Since d' is a greatest common divisor, its norm is maximal among the norms of common divisors, so the inequality $N(d) \geq N(d')$ must be an equality. That implies $N(\gamma) = 1$, so $\gamma = \pm 1$ or $\pm i$. Thus, d and d' are unit multiples of each other. □

Theorem 4.9. (Bézout's Theorem in $\mathbb{Z}[i]$).
Let d be any greatest common divisor of two non-zero Gaussian integers α and β. Then $d = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$.

Proof. Let $\alpha, \beta \in \mathbb{Z}[i]$ be non-zero Gaussian integers. First, we notice being able to write d as a combination of a and b is unaffected by unit multiplication. Thus, by Corollary 4.8, we only need to give a proof of any d a greatest common divisor coming from the Euclidean algorithm.

To prove that a greatest common divisor, $d = \gcd(\alpha, \beta)$, can be expressed as $d = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$, we carry out a proof by induction with respect to the norm of one of the Gaussian integers, take $N(\beta)$.

Base case: Consider $\beta \mid \alpha$, then $\gcd(\alpha, \beta) = \beta$. Meaning, we have the trivial case of:

$$\beta = \alpha \cdot 0 + \beta \cdot 1, \tag{8}$$

satisfying $d = \alpha x + \beta y$ with $x = 0, y = 1$. Therefore, base case holds.

For our inductive hypothesis, assume Bezout's identity holds for any pair $(\gamma, \delta) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$, with $N(\delta) < N(\beta)$. That is, there exists $x', y' \in \mathbb{Z}[i]$ such that:

$$\gcd(\gamma, \delta) = \gamma x' + \delta y'. \tag{9}$$

To prove our inductive step, consider dividing α by β to obtain:

$$\alpha = \beta\gamma + \rho \text{ where } N(\rho) < N(\beta), \tag{10}$$

for some quotient $\gamma \in \mathbb{Z}[i]$ and some remainder $\rho \in \mathbb{Z}[i]$. By the Euclidean algorithm:

$$\gcd(\alpha, \beta) = \gcd(\beta, \rho). \tag{11}$$

Since $N(\rho) < N(\beta)$, by the inductive hypothesis, there exist $x', y' \in \mathbb{Z}[i]$ such that:

$$\gcd(\beta, \rho) = \beta x' + \rho y'. \tag{12}$$

Substituting $\rho = \alpha - \beta\gamma$ from Eq. (10) into our previous result Eq. (12), we obtain:

$$\gcd(\beta, \rho) = \beta x' + (\alpha - \beta\gamma)y' \iff \gcd(\alpha, \beta) = \beta(x' - \gamma y') + \alpha y'.$$

Setting $y = x - \gamma y'$ and $x = y'$, we conclude:

$$d = \alpha x + \beta y. \tag{13}$$

□

Lemma 4.10. The non-zero Gaussian integers α and β are relatively prime if and only if we can write

$$\alpha x + \beta y = 1, \text{ for some } x, y \in \mathbb{Z}[i]. \tag{14}$$

Proof. If α and β are relatively prime, then 1 is a greatest common divisor of α and β, so $1 = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$ by Bezout's Theorem. Conversely, if $1 = \alpha x + \beta y$ for some $x, y \in \mathbb{Z}[i]$, then any common divisor of α and β is a divisor of 1, and thus is a unit. That says α and β are relatively prime. [3] □

Example 4.11. Consider our previous Example 5.5, we confirmed that $\alpha = 11 + 26i, \quad \beta = 38 + 27i$ are relatively prime. Reversing our calculations from the Euclidean Algorithm, we can express $-i$ as a combination of α and β:

$$\begin{aligned} -i &= (12 - i) - (-3 - 3i)(-2 + 2i) \\ &= (12 - i) - ((-27 - i) + 2(12 - i))(-2 + 2i) \\ &= \beta(5 - 4i) + (\alpha - \beta)(11 - i) \\ &= \alpha(11 - i) - \beta(6 + 3i). \end{aligned}$$

Finally, to write this combination in terms of 1, instead of $-i$, we simply multiply by i:

$$\alpha(1+11i)+\beta(-3+6i)=1. \tag{15}$$

5 Prime Factorisation of Gaussian Numbers

With a view to examining how the prime factorisation of a number is related to its Gaussian decomposability, we will lean on a few key theorems from number theory. These centre on determining when numbers can be written as a sum of two squares.

In particular, we will rely on *Fermat's Two-Square Theorem*, which provides necessary and sufficient conditions for a prime number to be expressed as a sum of two squares. We will also utilise the characterisation of composite numbers as sums of two squares, which states that a number can be expressed in this form if and only if every prime factor congruent to 3 (mod 4) appears with an even exponent in its prime factorisation.

This result follows from the properties of prime representations in the ring of *Gaussian integers* $\mathbb{Z}[i]$, explored in previous sections. By leveraging these results, we will establish a systematic method to determine whether a given number is a Gaussian number based solely on its prime factorisation.

Theorem 5.1. No prime p of the form $4k+3$, $k\in\mathbb{N}$ is a sum of two squares.

Proof. Working modulo 4, we have $a\equiv 0,1,2,\text{or } 3$, for all $a\in\mathbb{Z}$. Thus, $a^2\equiv 0 \pmod 4$ or $a^2\equiv 1 \pmod 4$. Then for arbitrary $a,b\in\mathbb{Z}$:

$$a^2+b^2\equiv 0,1,\text{or } 2 \pmod 4. \tag{16}$$

Noticing that $p\equiv 3 \pmod 4$, we see that $p=a^2+b^2$ is impossible. □

Lemma 5.2. Let $p\equiv 1 \pmod 4$ be an odd prime. Then it is not irreducible in $\mathbb{Z}[i]$.

Proof. Since $p\equiv 1 \pmod 4$, the group $G=(\mathbb{Z}/p\mathbb{Z})^\times$ of units modulo p is a cyclic group of order $p-1$. Because $4\mid(p-1)$, there exists an element $a\in G$ of order 4.
This implies that in $\mathbb{Z}[i]/(p)$, the equation

$$x^2+1=0, \tag{17}$$

has more than two solutions, namely $\pm a$ and $\pm i$. Normally, this equation has at most two solutions ($\pm i$) if p were irreducible and $\mathbb{Z}[i]/(p)$ were an integral domain.

However, since there are more than two solutions, $\mathbb{Z}[i]/(p)$ cannot be an integral domain. An integral domain cannot have zero divisors or excess solutions to a polynomial of degree 2. Since, as shown in Section 3, $\mathbb{Z}[i]$ is a Principal Ideal Domain (PID), an element is irreducible if and only if the quotient by its principal ideal is an integral domain. As $\mathbb{Z}[i]/(p)$ is not an integral domain, p is not irreducible in $\mathbb{Z}[i]$. □

Theorem 5.3. (Fermat's Two-Square Theorem). An odd prime p is expressible as a sum of two squares if and only if $p\equiv 1 \pmod 4$.

Proof. Suppose an odd prime p can be expressed as a sum of two squares, that is, there exists $a,b\in\mathbb{Z}$ such that:

$$p=a^2+b^2. \tag{18}$$

By Theorem 5.1, we know that no prime congruent to 3 (mod 4) can be written as a sum of two squares. Hence, $p\not\equiv 3 \pmod 4$. The only remaining possibility for an odd prime is $p\equiv 1 \pmod 4$.

For the converse, assume that $p \equiv 1 \pmod 4$. Since p is a prime number in $\mathbb{Z}$, we now determine its factorisation in $\mathbb{Z}[i]$. From Lemma 5.2, we know that a prime $p \equiv 1 \pmod 4$ is not irreducible in $\mathbb{Z}[i]$. Instead, it splits into a product of two Gaussian primes:

$$p = \alpha\bar{\alpha}, \tag{19}$$

where $\alpha = a + bi$ and $\bar{\alpha} = a - bi$ for some $a, b \in \mathbb{Z}$. Applying the norm function to both sides:

$$N(p) = N(\alpha\bar{\alpha}). \tag{20}$$

Since $N(\alpha) = a^2 + b^2$ and $N(p) = p^2$, we can use the multiplicativity of the norm to obtain:

$$p^2 = N(\alpha)N(\bar{\alpha}) = (a^2 + b^2)(a^2 + b^2). \tag{21}$$

Since p is prime in $\mathbb{Z}$ and $a, b \in \mathbb{Z}$, it must be that $p = a^2 + b^2$ as required. □

Lemma 5.4. For any odd prime $p \equiv 3 \pmod 4$ such that $p \mid a^2 + b^2$ for some $a, b \in \mathbb{Z}$, then $p \mid a$ and $p \mid b$.

Proof. Let $p \equiv 3 \pmod 4$, such that $p \mid a^2 + b^2$ for some $a, b \in \mathbb{Z}$. Now, assume toward a contradiction that, $p \nmid a$ and $p \nmid b$. We know that since $p \mid a^2 + b^2$, then $p^2 \mid a^2 + b^2$. Since $p \equiv 3 \pmod 4$, $p^2 \equiv 1 \pmod 4$ and 1 is a trivial divisor of every Gaussian number. This implies that:

$$a^2 + b^2 \equiv 0 \pmod p. \tag{22}$$

Rearranging, we get:

$$a^2 \equiv -b^2 \pmod p. \tag{23}$$

Dividing both sides by b^2 (which is possible since p does not divide b), we obtain:

$$(a/b)^2 \equiv -1 \pmod p. \tag{24}$$

Now consider the subgroup $\langle a/b \rangle$ in $\mathbb{Z}_p^*$, the multiplicative group modulo p. We have:

$$\begin{aligned}(a/b)^2 &\equiv -1 \pmod p,\\ (a/b)^3 &\equiv -(a/b) \pmod p,\\ (a/b)^4 &\equiv 1 \pmod p.\end{aligned}$$

Thus, the subgroup generated by a/b has order 4, that is $|\langle a/b \rangle| = 4$. By Lagrange's theorem, the order of every subgroup of $\mathbb{Z}_p^*$ divides the order of $\mathbb{Z}_p^*$, which is $p - 1$. This implies:

$$4 \mid (p - 1). \tag{25}$$

Therefore, we conclude that:

$$p - 1 = 4k, \text{ for some } k \in \mathbb{Z}, \tag{26}$$

which implies:

$$p = 4k + 1 \iff p \equiv 1 \pmod 4. \tag{27}$$

But this contradicts our assumption that $p \equiv 3 \pmod 4$. □

Theorem 5.5. A natural number n is expressible as a sum of two squares if and only if every prime $p \equiv 3 \pmod 4$ in its prime factorisation appears with an even exponent.

Proof. We first prove the forward implication: if $n = a^2 + b^2$, then any prime factor $p \equiv 3 \pmod 4$ must have an even exponent. We achieve this through induction with respect to our exponent e.

For the base case let $e = 0$, e is of course even and p does not appear in the prime factorisation, hence our statement holds. Our inductive hypothesis assumes that for any $e \leq k$, $k \in \mathbb{N}$, e is even.

For our inductive step, take $e = k + 1$. Meaning we have:

$$a^2 + b^2 = m \cdot p^{k+1}, \text{ where } a, b \in \mathbb{Z} \text{ and } m = \prod_{p \text{ prime}} p^{e_p}. \tag{28}$$

From Lemma 5.4, we know that $p \mid a^2 + b^2$ implies $p \mid a$ and $p \mid b$. Additionally, $p^2 \mid a^2 + b^2$. That is, we can write:

$$a^2 + b^2 = p^2((a_1)^2 + (b_1)^2), \text{ where } a_1, b_1 \in \mathbb{Z}. \tag{29}$$

Subbing this into our equation for prime factorisation we get:

$$p^2(a_1^2 + b_1^2) = m \cdot p^{k+1}. \tag{30}$$

Hence $k + 1 \geq 2$ and we can divide both sides by p^2 to obtain:

$$a_1^2 + b_1^2 = m \cdot p^{k-1}, \tag{31}$$

By our inductive hypothesis, $k - 1$ is even. Therefore $e = k + 1$ is also even as required.

Next, we prove the converse: if every prime $p \equiv 3 \pmod 4$ appears with an even exponent, then n is a sum of two squares. Write:

$$n = 2^a \cdot p_1^{2e_1} \cdot p_2^{2e_2} \cdots p_k^{2e_k} \cdot q_1^{f_1} \cdots q_m^{f_m}, \tag{32}$$

where:

- Each $p_i \equiv 3 \pmod 4$ appears with an *even exponent* $2e_i$.
- Each $q_j \equiv 1 \pmod 4$ appears with any exponent f_j.

for $i, j \in \mathbb{N}$, where $1 \leq i \leq k$ and $1 \leq j \leq m$.

Since each $p_i^{2e_i}$ is itself a perfect square, it does not affect the sum-of-squares property when multiplied with other terms.

By Fermat's Two-Square Theorem, each $q_j \equiv 1 \pmod 4$ can be written as a sum of two squares, and we have already shown that the product of two such numbers is again a sum of two squares.

Finally, 2^a is also always expressible as a sum of two squares (as $2 = 1^2 + 1^2$ and squaring preserves this form), it follows that n can be written as a sum of two squares. □

Example 5.6. Consider the following example with:

$$n = 2^3 \cdot 5^3 \cdot 7^2 = 49,000.$$

Since n meets all the conditions of Theorem 5.5, it is indeed a Gaussian number. We can explicitly represent 49,000 as a sum of two squares by recursively applying the multiplicative property established in the proof of Theorem 2.2:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2. \tag{33}$$

Notice that $2^3 = 8 = 2^2 + 2^2$ and $5^3 = 125 = 11^2 + 2^2$. Thus, applying the identity to 2^3 and 5^3 we obtain:

$$ac - bd = 2 \cdot 11 - 2 \cdot 2 = 18, \quad ad + bc = 2 \cdot 2 + 2 \cdot 11 = 26.$$

Combine this result with $7^2 = 7^2 + 0^2$ and applying the property once more gives:

$$ac - bd = 18 \cdot 7 - 26 \cdot 0 = 126, \quad ad + bc = 18 \cdot 0 + 26 \cdot 7 = 182.$$

Altogether we have that, $(18^2 + 26^2) \cdot (7^2 + 0^2) = 49,000 = 126^2 + 182^2$ as needed.

Example 5.7. Consider a basic counter example with:

$$n = 3 \cdot 5^2 = 75.$$

Note that, the prime factor 3 of n does not satisfy the conditions for a prime factor $q \equiv 3 \pmod 4$ as it appears with exponent 1 (which is odd). Thus, by Theorem 5.5, $n = 75$ is not Gaussian number and it can be seen that there is no representation of 75 as the sum of two squares.

6 Sums of more than 2 squares

The question of how many squares are needed to represent a natural number can be viewed as a special case of *Waring's problem* [4], which asks whether every natural number can be expressed as a sum of a fixed number of k-th powers of natural numbers. While Waring's problem extends to all powers $k \geq 1$, our focus here first is on the case of squares. As demonstrated in the above example, there exist positive integers that are not Gaussian numbers, meaning they cannot be written as a sum of two squares. This naturally leads to a broader line of questioning: if a number is not expressible as the sum of *two* squares, how many squares are needed? Can every $n \in \mathbb{Z}^+$ be written as the sum of three squares? If not, what about four?

Intuitively, allowing more squares should reduce the number of exceptions. With the goal of reaching a point where no numbers are excluded, we seek to clarify the existence of cases where three squares are insufficient and determine whether four squares always suffice.

The study of sums of squares is an area of interest in number theory, leading to fundamental results such as Legendre's Three-Square Theorem and Lagrange's Four-Square Theorem. In this section, we explore these theorems, their proofs, and their implications.

Theorem 6.1 (Legendre's Three-Square Theorem)**.** No positive integer of the form:

$$4^n(8m + 7), \quad n, m \in \mathbb{Z}, \tag{34}$$

can be represented as the sum of three squares.

Proof. First, we show that $8m + 7$ cannot be represented as the sum of three squares.
Take $a \in \mathbb{Z}$, then $a^2 \equiv 0, 1,$ or $4 \pmod 8$. So for any $a, b, c \in \mathbb{Z}$ it follows that:

$$a^2 + b^2 + c^2 \equiv 0, 1, 2, 3, 4, 5, \text{or } 6 \pmod 8. \tag{35}$$

Therefore, since $8m + 7 \equiv 7 \pmod 8$, the equation:

$$a^2 + b^2 + c^2 \equiv 8m + 7, \tag{36}$$

is impossible. This term cannot be represented as a sum of three squares.

Next, suppose towards a contradiction that:

$$4^n(8m + 7) = a^2 + b^2 + c^2, \tag{37}$$

where we require $n \geq 1$, since the case $n = 0$ has already been addressed. Since the left-hand side is divisible by 4, it follows that each $a, b, c \in \mathbb{Z}$ must necessarily be even, owing to the fact that the sum of 3 numbers is only even if all three are even themselves - and any even square is

the result of an even number being squared. By setting $a = 2a_1, b = 2b_1, c = 2c_1$, factoring out 4 on the right-hand side and dividing through, we obtain:

$$4^{n-1}(8m + 7) = a_1^2 + b_1^2 + c_1^2. \tag{38}$$

If $n - 1 \geq 1$, the same logic is repeated as many times as necessary until $8m + 7$ is represented by the sum of three squares, when $n - 1 = 0$. Since this is guaranteed to happen eventually, the supposition is contradicted, which completes the proof. □

Since this result shows that some numbers cannot be expressed as the sum of three squares, we now extend our investigation to the sum of four squares. The following useful lemma can be verified algebraically, but the expansion (while straightforward) is cumbersome and lengthy – hence only the equality is given in its proof.

Lemma 6.2 (Euler's 4-Square Identity)**.** [5] If $m, n \in \mathbb{Z}$ are each the sum of four squares, then mn is likewise so representable.

Proof. If $m = a^2 + b^2 + c^2 + d^2$ and $n = e^2 + f^2 + g^2 + h^2$ for $a, b, c, d, e, f, g \in \mathbb{Z}$, then:

$$\begin{aligned} mn &= (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \\ &= (ae + bf + cg + dh)^2 \\ &\quad + (af - be + ch - dg)^2 \\ &\quad + (ag - bh - ce + df)^2 \\ &\quad + (ah + bg - cf - de)^2. \end{aligned}$$

□

The next lemma is key for verifying a subsequent corollary which in turn will assist in proving the flagship theorem.

Lemma 6.3. If p is an odd prime, then the congruence

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}, \tag{39}$$

has a solution x_0, y_0 where $0 \leq x_0 \leq (p - 1)/2$ and $0 \leq y_0 \leq (p - 1)/2$.

Proof. Consider the two sets:

$$S_1 = \left\{ 1 + 0^2, 1 + 1^2, 1 + 2^2, \ldots, 1 + \left(\frac{p-1}{2}\right)^2 \right\}$$
$$S_2 = \left\{ -0^2, -1^2, -2^2, \ldots, -\left(\frac{p-1}{2}\right)^2 \right\}.$$

No two elements of S_1 are congruent modulo p, since if

$$1 + x_1^2 \equiv 1 + x_2^2 \pmod{p}, \tag{40}$$

then we must have one of two cases $x_1 \equiv x_2 \pmod{p}$ or $x_1 \equiv -x_2 \pmod{p}$. Upon examination though, the latter is not possible since $0 < x_1 + x_2 < p$ (except when $x_1 = x_2 = 0$, which does not concern this case of distinct elements). Then we must have $x_1 = x_2$.By similar logic, no two elements of S_2 are congruent modulo p.

In total, S_1 and S_2 contain $2(1 + \frac{p-1}{2}) = p + 1$ integers. The *Pigeonhole Principle*, a standard combinatorial observation, states that: if n objects are placed in m pigeonholes and $n > m$,

then some pigeonhole will contain at least two objects. By this principle, some element of S_1 must be congruent to some element of S_2. This assertion can be equally represented in saying that there exist x_0, y_0 such that:

$$1 + x_0^2 \equiv -y_0^2 \pmod{p}, \tag{41}$$

where $0 \leq x_0 \leq (p-1)/2$ and $0 \leq y_0 \leq (p-1)/2$. □

Corollary 6.4. Let p be an odd prime. Then there exists an integer $k < p$ such that kp is the sum of four squares.

Proof. As stated by the previous lemma, we can find $x_0, y_0 \in \mathbb{Z}$,

$$0 \leq x_0 < \frac{p}{2}, \quad 0 \leq y_0 < \frac{p}{2}, \tag{42}$$

such that

$$x_0^2 + y_0^2 + 1^2 + 0^2 = kp, \tag{43}$$

for an appropriate k. Using the bounds on x_0 and y_0, we have that

$$kp = x_0^2 + y_0^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2. \tag{44}$$

Since $p \neq 0$, we cancel and obtain that $k < p$. □

Theorem 6.5. Any prime p can be written as the sum of four squares.

Proof. First examining $p = 2$, we see that $2 = 1^2 + 1^2 + 0^2 + 0^2$. So now we need only focus on odd primes.
Let k be the smallest positive integer such that kp equals the sum of four squares, say

$$kp = x^2 + y^2 + z^2 + w^2. \tag{45}$$

The previous corollary insists that $k < p$. **Claim:** $k = 1$.
Indeed, first we guarantee that k has odd parity: Assume towards a contradiction that k is even. Then x, y, z and w are sure to be all even; or all odd; or two are even and two are odd. In any such case, WLOG we may rearrange as such:

$$x \equiv y \pmod{2} \quad \text{and} \quad z \equiv w \pmod{2}. \tag{46}$$

Now, define new variables by halving the sums and differences of the original variables:

$$a = \frac{x-y}{2}, \quad b = \frac{x+y}{2}, \quad c = \frac{z-w}{2}, \quad d = \frac{z+w}{2}. \tag{47}$$

Since x, y, z, and w share the same parity, a, b, c, and d are guaranteed to be integers. The original sum of squares can now be expressed as:

$$x^2 + y^2 + z^2 + w^2 = 2(a^2 + b^2 + c^2 + d^2). \tag{48}$$

Substituting this back into the sum of squares for kp, we obtain:

$$kp = x^2 + y^2 + z^2 + w^2 = 2(a^2 + b^2 + c^2 + d^2). \tag{49}$$

By dividing by 2, we derive the final equality:

$$\frac{kp}{2} = a^2 + b^2 + c^2 + d^2. \tag{50}$$

Expressing this in terms of our defined variables, we achieve the equation:

$$\frac{kp}{2} = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2. \tag{51}$$

This transformation shows that if k were even, then $\frac{k}{2} \cdot p$ could also be represented as a sum of four squares, contradicting the minimality of k assumed previously. Therefore, we conclude that k must be odd.

Now assume that $k \neq 1$. As an odd integer, we have that $k \geq 3$. Thus, it is possible to choose $e, f, g, h \in \mathbb{Z}$ such that:

$$e \equiv x \pmod{k}, \quad f \equiv y \pmod{k}, \quad g \equiv z \pmod{k}, \quad h \equiv w \pmod{k}; \tag{52}$$

and

$$|e| < \frac{k}{2}, \quad |f| < \frac{k}{2}, \quad |g| < \frac{k}{2}, \quad |h| < \frac{k}{2}, \tag{53}$$

by recalling that every integer can be represented modulo k by a unique integer in the interval $\left(-\frac{k}{2}, \frac{k}{2}\right)$. Then we have that

$$\begin{aligned} e^2 + f^2 + g^2 + h^2 = x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k} \\ \implies e^2 + f^2 + g^2 + h^2 = nk, \end{aligned}$$

for some $n \in \mathbb{Z}_{\geq 0}$. The inequalities involving e, f, g, h ensure that

$$0 \leq nk = e^2 + f^2 + g^2 + h^2 < 4\left(\frac{k^2}{4}\right) = k^2. \tag{54}$$

Now certainly $n \neq 0$ since this would imply that $e = f = g = h = 0$ and, in turn, that $k \mid x, y, z, w$. Then $k^2 \mid kp$ or $k \mid p$, which is not possible given that $1 < k < p$. We conclude from $nk < k^2$ that $n < k$ and hence that $0 < n < k$. Together, we have that:

$$k^2np = (kp)(kn) = (x^2 + y^2 + z^2 + w^2)(e^2 + f^2 + g^2 + h^2). \tag{55}$$

By the Euler's 4-Square identity concerning the products of four-square numbers, we can now write

$$k^2np = r^2 + t^2 + s^2 + u^2, \tag{56}$$

where

$$\begin{aligned} r &= xe + yf + zg + wh \\ s &= xf + ye + zh + wg \\ t &= xg + yh + ze + wf \\ u &= xh + yg + zf + we. \end{aligned}$$

We note here that each of r, s, t, u have k as a factor, by the definition of e, f, g, h (e.g. $xe = e^2$ etc.). Hence, $r \equiv s \equiv t \equiv u \equiv 0 \pmod{k}$ and we rearrange to reach the equation

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2, \tag{57}$$

with $r/k, s/k, t/k, u/k \in \mathbb{Z}$. Once again, we have contradicted the assumption that k is the smallest positive integer giving rise to kp being the sum of four squares. So it is guaranteed that

$k = 1$, and the result. □

Theorem 6.6 (Lagrange's Four-Square Theorem)**.** Any $n \in \mathbb{Z}^+$ can be written as the sum of four squares, some of which may be zero.

Proof. Starting with $1 \in \mathbb{Z}^+$, we have $1 = 1^2 + 0^2 + 0^2 + 0^2$ which clearly satisfies the property. So now assume that $n > 1$ and decompose it into its prime factors. That is $n = p_1 \cdot p_2 \cdots p_m$ where $p_1, \ldots, p_m$ are not necessarily distinct. By the previous theorem each of these primes can be be written as a sum of four squares, and we deploy Euler's 4-Square Identity to insist that the product of any two of these primes is also the sum of four squares. One can use the same logic to extend the pattern to any finite number of prime factors that n might have. Doing so $m - 1$ times will procure the pertinent representation. This completes the proof of this flagship theorem. □

Example 6.7. By the previous theorem, we can write $513 = 3^3 \cdot 19$ as the sum of four squares. We lean on Euler's 4-Square Identity to do so:

$$\begin{aligned}
513 &= 3^2 \cdot 3 \cdot 19 \\
&= 3^2(1^2 + 1^2 + 1^2 + 0^2)(4^2 + 1^2 + 1^2 + 1^2) \\
&= 3^2[(4 + 1 + 1 + 0)^2 + (1 - 4 + 1 - 0)^2 + (1 - 1 - 4 + 0)^2 + (1 + 1 - 1 - 0)^2] \\
&= 3^2[6^2 + 2^2 + 4^2 + 1^2] \\
&= 18^2 + 6^2 + 12^2 + 3^2.
\end{aligned}$$

Evidently, the identities and theorems discussed in this section offer a systematic and efficient method for expressing numbers as the sum of four squares.

7 Conclusions and Further Work

This report demonstrates that the Gaussian integers $\mathbb{Z}[i]$ provide a powerful algebraic framework for resolving classical number-theoretic questions, particularly those involving Gaussian numbers (sums of squares). By establishing $\mathbb{Z}[i]$ as a Euclidean domain, we derived its unique prime factorisation property and applied the Euclidean algorithm to classify primes expressible as sums of two squares. These results not only recover Fermat's theorem on two squares but also reveal the deep interplay between algebraic structures and arithmetic ideas.

Extending to sums of more than two squares, the project underscores how algebraic insights complement combinatorial and number-theoretic methods, exemplified by Lagrange's four-square theorem. The limitations of $\mathbb{Z}[i]$ in addressing higher-dimensional sums further highlight the necessity of alternative structures, such as quaternions for four squares. Looking towards further research, here are some topic of interest that we didn't get to explore in this report:

Asymptotic Distribution of Gaussian Numbers. This is analogous to the prime number theorem which states that prime numbers are distributed as follows:

$$\pi(N) \sim \frac{N}{\log(N)}, \tag{58}$$

where $\pi(N)$ is the prime-counting function (the number of primes less than or equal to N). In a similar light, we believe it can be shown that Gaussian Numbers are distributed as follows:

$$\gamma(N) \sim C\frac{N}{\sqrt{\log(N)}}, \tag{59}$$

where $\gamma(N)$ denotes the count of natural numbers $s \leq N$ such that $s = a^2 + b^2$ for $a, b \in \mathbb{Z}$ and C is a density constant. This allows us to merge algebraic insights (e.g. unique factorisation in $\mathbb{Z}[i]$), and move from qualitative results of number representations to quantitative ones: how many representations are there. This synergy not only solves classical problems but also opens doors to modern questions in arithmetic geometry and mathematical physics.

Matrix Representations as Sums of Squares. The classical problem of expressing integers as sums of squares invites a compelling generalisation to matrix theory. Within the ring $\mathcal{M}_2(\mathbb{Z})$ of 2×2 integer matrices - can every matrix in these rings be decomposed into a finite sum of squares of other matrices? One could then further their research and look towards $\mathcal{M}_n(\mathbb{Z})$ for $n \geq 2$, seeking analogues of foundational results such as *Lagrange's Four-Square Theorem* in matrix rings.

Waring's Problem. First proposed by the British mathematician Edward Waring (1736-1798), this problem explores a central challenge in additive number theory: Given a positive integer k, does there exist a minimal integer $g(k)$ such that *every* natural number n can be expressed as the sum of at most $g(k)$ non-negative k-th powers? [4] While classical results resolve this for specific cases - such as $k = 2$, where Lagrange's theorem guarantees $g(2) = 4$, the broader question for arbitrary k remains a topic of inquiry. Progress hinges on leveraging algebraic frameworks, such as Gaussian integers or their generalisations, to uncover patterns in higher-power representations. Extending these methods beyond squares (e.g., to cubes or quartics) poses unresolved theoretical and computational challenges, inviting novel approaches at the intersection of number theory and abstract algebra.

References

[1] Erik Landin. Gaussian Integers and Related Topics, 2021. Accessed: Feb 11, 2025 Viewable here.

[2] David Barnes. MTH3012 Algebra Notes, 2025. Lecture Notes.

[3] Keith Conrad. Notes on *Z[i]*: The Gaussian Integers, 2021. Accessed: February 15, 2025 Viewable here.

[4] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers - Chapter 20 : The Representation of a Number by two or Four Squares.* Oxford University Press, 6th edition, 2008.

[5] David M. Burton. *Elementary Number Theory - Chapter 13: Representations of Integers as Sums of Squares.* McGraw-Hill, 6th edition, 2006.