Representations of Integers as Sums of Two, Three, and Four Squares

Miran Deniz

July 12

Working Draft (July 12): This version was submitted to meet the initial course deadline. Sections 3.3, 3.4, and 4 are currently being expanded. A finalized version will be uploaded within 48 hours.

Abstract

Which integers can be written as the sum of two, three, or four squares? This classical question has driven centuries of mathematical development. In this expository paper, we explore both the existence of these representations and the methods used to count them. We begin by detailing how the method of descent can be used to prove Lagrange's Four-Square Theorem. However, because the product of two sums of three squares is not necessarily a sum of three square, descent arguments fail in this case. To bypass this problem, we present a modern geometric proof of Legendre's Three-Square Theorem using Minkowski's Convex Body Theorem. We then use Legendre's Theorem to directly prove Gauss's "Eureka" Theorem. Concluding the paper, we turn our attention from whether a representation exists to exactly how many ways it can be done. We outline Jacobi's divisor formulas for the two- and four-square problems, discuss why the three-square case is difficult, and highlight how modular forms help modern mathematicians solve this counting problem in general.

1 Introduction

The problem of representing integers as sums of squares was first studied by the ancient Greek mathematician Diophantus.[1] However, the modern study of these representations began in 1621, when Claude Gaspard Bachet published a Latin translation of Diophantus's surviving text, *Arithmetica*. In his translation, Bachet conjectured that every natural number could be written as the sum of four integer squares.

A few decades later, Pierre de Fermat systematically categorized these representations. In a 1640 letter to Marin Mersenne, Fermat stated his Two-Square Theorem: an odd prime p can be written as the sum of two squares if and only if $p \equiv 1 \pmod 4$. In other

[1] The historical details in this introduction about Bachet, Fermat, Euler, Lagrange, Legendre, Gauss, and Dirichlet are primarily drawn from [Wei84, Chapters II–IV].

writings, Fermat noted that numbers of the form $8n + 7$ cannot be written as the sum of three squares, and asserted that Bachet's four-square conjecture was true. Fermat claimed to have proofs for all of these statements, though he never published them.

Fermat's statements remained unproven for over a century until Leonhard Euler took up the subject. In the 1740s, Euler published the first complete proof of the Two-Square Theorem. To solve it, he formalized a technique known as the method of descent.

Later in his life, Euler attempted to apply this same descent technique to Bachet's four-square conjecture. He successfully proved several necessary lemmas, but could not complete the final step of the descent argument. Joseph-Louis Lagrange finally closed the gap in 1770, heavily relying on Euler's foundational work to prove the Four-Square Theorem. Shortly afterward, Euler refined Lagrange's proof into the elegant descent argument that we will use in this paper.

Surprisingly, the Three-Square Theorem was much more difficult to prove. Unlike sums of two or four squares, sums of three squares do not have an algebraic identity that provides multiplicativity; the product of two integers that are sums of three squares is not necessarily a sum of three squares (for example, $3 = 1^2 + 1^2 + 1^2$ and $5 = 2^2 + 1^2 + 0^2$, but their product 15 requires four squares since $15 \equiv 7 \pmod 8$, which, as Fermat noted, prevents it from being a sum of three squares). Because Euler's descent method relies on this algebraic identity, the technique fails completely when applied to three squares.

Forced to abandon descent entirely, Adrien-Marie Legendre published a proof in 1798 using early ideas from the theory of quadratic forms. However, his proof contained a significant gap: his argument assumed a property of primes in arithmetic progressions that remained unproven at the time. Shortly after, in 1801, Carl Friedrich Gauss bypassed Legendre's incomplete method and gave the first complete proof of the Three-Square Theorem using his formalization of ternary quadratic forms. It was not until 1837 that Peter Gustav Lejeune Dirichlet proved his theorem on arithmetic progressions, which finally closed the gap in Legendre's original argument.

While Gauss's 1801 proof resolved the three-square problem, his methods required heavy algebraic machinery. Over a century later, in 1957, N. C. Ankeny published an elegant proof of Legendre's Theorem [Ank57] using Minkowski's Geometry of Numbers, building on earlier ideas by H. Davenport.

To simplify our discussion, we define the following terminology: throughout this paper, we will say an integer n is k-representable if it can be written as the sum of k integer squares.

Throughout this paper, we assume the reader is familiar with basic modular arithmetic and quadratic residues. Later, in Section 3, we will rely on Dirichlet's Theorem on Primes in Arithmetic Progressions, Minkowski's Convex Body Theorem, and the Law of Quadratic Reciprocity, which we will state without proof.

The structure of this paper is as follows. In Section 2, we present the classical proof of Lagrange's Theorem using Euler's method of descent. In Section 3, we present Ankeny's modern, geometric proof of Legendre's Theorem. We then use Legendre's Theorem to prove two famous corollaries: Gauss's "Eureka" Theorem and an alternative proof of Lagrange's Theorem. Finally, in Section 4, we move beyond the existence of these sums to briefly discuss formulas that count in how many ways a given integer can be written as a sum of squares.

Before starting with four squares, we conclude this introduction with a brief review of the descent method Euler used to prove the Two-Square Theorem. We outline his argument here because the method of descent he developed provides the same logical

structure we will use to prove Lagrange's Four-Square Theorem in Section 2. Moreover, the Two-Square Theorem is needed to finish Ankeny's proof in Section 3.

Euler's Descent for Two Squares

Theorem 1.1 (The Sum of Two Squares Theorem)**.** *A natural number n is 2-representable if and only if every prime factor p such that $p \equiv 3 \pmod 4$ has an even exponent in the prime factorization of n.*

This theorem relies on the Brahmagupta-Fibonacci Identity:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2.$$

This identity shows that the product of two 2-representable numbers is also 2-representable. Because of this, proving the theorem reduces to showing that 2 and any prime $p \equiv 1 \pmod 4$ are 2-representable.

To prove this for $p \equiv 1 \pmod 4$, Euler used the method of descent. First, he found a 2-representable multiple of p. Because p is of the form $4k + 1$, there exists an integer x such that $x^2 \equiv -1 \pmod p$, which implies that

$$x^2 + 1^2 = mp$$

for some positive integer m. By bounding x, it is easy to show that $0 < m < p$.

Next, Euler showed that if we have a multiple $mp = x_1^2 + x_2^2$ with $m > 1$, we can reduce the bases x_1 and x_2 modulo m to get remainders between $-m/2$ and $m/2$. The sum of the squares of these remainders gives a new multiple nm:

$$y_1^2 + y_2^2 = nm, \quad \text{where } 0 < n < m.$$

Multiplying mp and nm, and using the Brahmagupta-Fibonacci Identity produces a sum of two squares equal to m^2np. By analyzing the terms in modulo m, we see that both bases in this new sum are multiples of m. Dividing the entire equation by m^2 gives a smaller 2-representable multiple np. By the Well-Ordering Principle, this descent must eventually reach 1. This proves $1 \cdot p = p$ is 2-representable.

With this logical structure established, we now move on to four squares.

2 Lagrange's Four-Square Theorem

Theorem 2.1 (Lagrange's Four-Square Theorem)**.** *Every natural number $n \in \mathbb{N}$ is 4-representable.*

We can manually verify this for small numbers (e.g., $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 0^2 + 1^2 + 0^2$). To prove this holds for all natural numbers, our strategy will closely mirror Euler's descent method outlined in the Introduction, following the exposition given by Ireland and Rosen [IR90, Chapter 17]. First, we will establish multiplicativity to reduce the problem to prime numbers. Next, we will find a 4-representable multiple of p, say mp, such that $0 < m < p$. Finally, we will construct a descent argument to reduce the multiple m until $m = 1$.

We begin by proving multiplicativity. Recall that the Brahmagupta-Fibonacci Identity reduced the two-square problem to primes. To apply the same reduction to four

squares, we need a four-square equivalent to show that the product of two 4-representable numbers is also 4-representable. Constructing such an identity from scratch requires algebraic cleverness, but verifying it is straightforward.

Lemma 2.2 (Euler's Four-Square Identity)**.** *If two natural numbers n, m are 4-representable then nm is also 4-representable.*

Proof. Let $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $m = y_1^2 + y_2^2 + y_3^2 + y_4^2$ where $x_i, y_i \in \mathbb{Z}$ for each i. By algebraic manipulation we get:

$$\begin{aligned} nm &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Thus, we see that nm is 4-representable.

□

With Euler's Four-Square Identity established, by straightforward induction, any finite product of 4-representable numbers is 4-representable. Therefore, it is now sufficient for us to prove that every prime number is 4-representable.

Proposition 2.3. *Any prime number p is 4-representable.*

We will prove this proposition in two parts, corresponding to the next two subsections.

2.1 Finding a 4-Representable Multiple

We have already shown that 2 is 4-representable, so assume that $p > 2$. To prove Proposition 2.3, we first find a multiple of p, say mp, that is 4-representable. We do this with the following lemmas.

Lemma 2.4. *For any prime $p > 2$, let $S = \{x^2 : x \in \{0, 1, \ldots, \frac{p-1}{2}\}\}$ be the set of squares in $\mathbb{Z}/p\mathbb{Z}$. Then $|S| = \frac{p+1}{2}$.*

Proof. Assume for the sake of contradiction that $x^2 \equiv y^2 \pmod{p}$ for distinct $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$. This rearranges to $(x - y)(x + y) \equiv 0 \pmod{p}$, which implies $p \mid (x - y)(x + y)$. By Euclid's Lemma, we must have either $p \mid (x - y)$ or $p \mid (x + y)$.

Since x and y are distinct elements in $\{0, 1, \ldots, \frac{p-1}{2}\}$, their difference satisfies $-\frac{p-1}{2} \leq x - y \leq \frac{p-1}{2}$. The only multiple of p in this range is 0, which would mean $x = y$, contradicting that they are distinct. Thus, the first case, $p \mid (x - y)$, is impossible.

Similarly, because x and y are distinct and less than or equal to $\frac{p-1}{2}$, their sum satisfies $0 < (x+y) \leq p-1$. Since this range contains no multiple of p, the second case, $p \mid (x+y)$, is also impossible.

Since both cases lead to a contradiction, our assumption is false. Thus, it is impossible for distinct $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$ to have $x^2 \equiv y^2 \pmod{p}$. This means each element $x \in \{0, 1, \ldots, \frac{p-1}{2}\}$ produces a distinct square, implying $|S| = \frac{p+1}{2}$.

□

Now that we know exactly how many distinct squares exist modulo p, we can use the Pigeonhole Principle to guarantee an intersection between two sets, which gives our desired multiple.

Lemma 2.5. *For any prime $p > 2$ there exist integers x and y such that $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.*

Proof. Consider the set of squares in $\mathbb{Z}/p\mathbb{Z}$ defined as $S = \{x^2 : x \in \{0, 1, \ldots, \frac{p-1}{2}\}\}$ and the set $R = \{-x^2 - 1 : x \in \{0, 1, \ldots, \frac{p-1}{2}\}\}$. By Lemma 2.4 we have $|S| = |R| = \frac{p+1}{2}$. Since $|S| + |R| > p$, by the Pigeonhole Principle there exists $s \in S$ and $r \in R$ such that $s \equiv r \pmod{p}$.

Let $s = x^2$ and $r = -y^2 - 1$ for some $x, y \in \{0, 1, \ldots, \frac{p-1}{2}\}$. We have $x^2 \equiv -y^2 - 1 \pmod{p}$, which we rearrange to get $x^2 + y^2 + 1 \equiv 0 \pmod{p}$. Thus, for any prime $p > 2$ there exist x and y such that $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.

□

By Lemma 2.5, since $x^2 + y^2 + 1 \equiv 0 \pmod{p}$, there exists an integer $m \in \mathbb{Z}$ such that $mp = x^2 + y^2 + 1^2 + 0^2$. Notice that $x^2 + y^2 + 1 > 0$, so we have $m > 0$. Moreover, $x, y \leq \frac{p-1}{2} < \frac{p}{2}$, so $x^2 + y^2 + 1 < \frac{p^2}{4} + \frac{p^2}{4} + 1 < p^2$. Therefore, $mp < p^2$ which implies $m < p$.

We have successfully shown that there exists a multiple mp (with $0 < m < p$) that is 4-representable.

2.2 The Descent Argument

Now that we have bounded a 4-representable multiple of p, our next step is to use a descent argument. We will show that if $m > 1$ then we can find a strictly smaller positive multiple that is also 4-representable, eventually forcing $1 \cdot p$ to be 4-representable.

Lemma 2.6. *Suppose for a prime p there exists an integer $1 < m < p$ such that mp is 4-representable. Then there exists an integer $0 < n < m$ such that np is 4-representable.*

Proof. Write

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{1}$$

for $1 < m < p$. For each i define an integer y_i such that $y_i \equiv x_i \pmod{m}$ and $\frac{-m}{2} < y_i \leq \frac{m}{2}$. Notice that

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}.$$

Hence for some integer $n \geq 0$, we have

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = nm. \tag{2}$$

Since $y_i^2 \leq \frac{m^2}{4}$ for each i, we have $nm \leq m^2$, which implies $n \leq m$.

Notice that $n \neq 0$, otherwise we would have $y_i^2 = 0$ for each i, meaning $x_i \equiv 0 \pmod{m}$. But this implies $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m^2}$. This means $m^2 \mid mp$ forcing $m \mid p$, which is impossible since $1 < m < p$.

Similarly, notice that $n \neq m$. If m is odd, then $\frac{m}{2}$ is not an integer, meaning the strict inequality $y_i^2 < \frac{m^2}{4}$ holds for all i. This implies $nm = y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\left(\frac{m^2}{4}\right) = m^2$, giving $n < m$. If m is even and $n = m$, then we must have $y_i^2 = \frac{m^2}{4}$ for each i, meaning $y_i = \frac{m}{2}$. Since $x_i \equiv y_i \pmod{m}$, this implies $x_i \equiv \frac{m}{2} \pmod{m}$. Squaring this gives $x_i^2 \equiv \frac{m^2}{4} \pmod{m^2}$. Summing all four terms yields $mp = x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4\left(\frac{m^2}{4}\right) \equiv 0 \pmod{m^2}$. As before, this implies $m \mid p$, a contradiction. Therefore, $0 < n < m$.

Multiplying (1) and (2), and applying Euler's Four-Square Identity (Lemma 2.2), we get:

$$\begin{aligned} m^2np &= (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) \\ &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &\quad + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &\quad + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

Recall that $y_i \equiv x_i \pmod{m}$. Substituting this into the terms of the expansion, we see that all bases are multiples of m. For example, the second base modulo m becomes:

$$x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 \pmod{m}.$$

By the same argument the third and fourth bases are multiples of m. The first base is also a multiple of m, because by (1) $x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m}$.

Therefore, we can divide the entire equation by m^2:

$$\begin{aligned} np &= \left(\frac{x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4}{m}\right)^2 \\ &\quad + \left(\frac{x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3}{m}\right)^2 \\ &\quad + \left(\frac{x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4}{m}\right)^2 \\ &\quad + \left(\frac{x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2}{m}\right)^2. \end{aligned}$$

Since every fraction in this equation is an integer, we have successfully proved that np is 4-representable. Because $0 < n < m$, this completes the proof.

□

Next we apply this descent argument to the multiple we have found in Subsection 2.1 to finalize the proof of Proposition 2.3.

Proof of Proposition 2.3. Let M be the set of all natural numbers m such that mp is 4-representable. By the discussion following Lemma 2.5, we know that there exists some $m \in M$ such that $0 < m < p$. Therefore, M is non-empty. By the Well-Ordering Principle M must contain a minimal element, which we will call m_0. Because $m_0 \in M$, m_0p is 4-representable, and $m_0 \leq m < p$.

We claim that $m_0 = 1$. Assume for the sake of contradiction that $m_0 > 1$. Then we would have $p > m_0 > 1$ and m_0p 4-representable. Applying Lemma 2.6, there exists a natural number $0 < n < m_0$ such that np is also 4-representable. This means $n \in M$. But $n < m_0$. This contradicts the minimality of m_0. Therefore, our assumption is false, meaning $m_0 = 1$. Because $1 \in M$, we conclude that $1 \cdot p = p$ is 4-representable.

□

Now that we have proved that all prime numbers are 4-representable, Theorem 2.1 follows straightforwardly from Lemma 2.2.

Proof of Theorem 2.1. Let $n \in \mathbb{N}$. If $n = 1$ we have already shown that it is 4-representable. For $n > 1$, by the Fundamental Theorem of Arithmetic, n has a prime factorization:

$$n = p_1 p_2 \dots p_k.$$

By Proposition 2.3, every prime p_i in this factorization is 4-representable. By the discussion following Euler's Four-Square Identity, a finite product of 4-representable numbers is 4-representable. Thus, n is 4-representable.

□

3 Legendre's Three-Square Theorem

After proving Lagrange's Theorem using Euler's method of descent, we now turn to Legendre's Three-Square Theorem. The descent strategy we used in Section 2 relied heavily on Euler's Four-Square Identity (Lemma 2.2). This identity provided multiplicativity, which allowed us to reduce the problem to primes and execute the descent step. However, as we mentioned in the Introduction, sums of three squares do not have a similar algebraic identity. The product of two 3-representable numbers is not necessarily 3-representable. Recall our earlier example: 3 and 5 are both sums of three squares, but their product 15 requires four. Because we don't have multiplicativity, we can neither reduce the problem to primes nor construct a descent argument. Consequently, the algebraic approach we used for two and four squares fails.

To solve this problem, we need a different approach. In this section, we present N. C. Ankeny's proof of Legendre's Three-Square Theorem [Ank57], which relies on geometry of numbers, specifically Minkowski's Convex Body Theorem.

This section is structured as follows. First, we state Legendre's Theorem and prove the simpler non-representability condition (Part 1) in Subsection 3.1. In Subsection 3.2, we introduce the machinery required for Part 2, which we then use to prove the specific case of $n \equiv 3 \pmod 8$ in Subsection 3.3. In Subsection 3.4, we explain the strategy to extend this proof to all other valid residues. Finally, in Subsection 3.5, we use Legendre's Theorem to prove two famous corollaries: an alternative proof of Lagrange's Theorem and Gauss's "Eureka" Theorem.

Theorem 3.1 (Legendre's Three-Square Theorem)**.** *Let n be a natural number.*

(1) If there exist non-negative integers a and b such that $n = 4^a(8b + 7)$, then n is not 3-representable.

(2) If n cannot be written in the form $4^a(8b + 7)$ for any non-negative integers a and b, then n is 3-representable.

3.1 Proof of Part (1)

The proof of Part (1) of Theorem 3.1 is straightforward. We use induction on a. We first prove the base case $a = 0$ (the numbers of the form $8b+7$) and then use the inductive step to show that for all non-negative a any number of the form $4^a(8b+7)$ is not representable.

Proof of Theorem 3.1, Part (1). Consider the base case $a = 0$, where $n = 4^0(8b + 7) = 8b + 7$ for a non-negative integer b. This means we have $n \equiv 7 \pmod 8$. Notice that the

set of squares modulo 8 is $S = \{x^2 \pmod 8 : x \in \mathbb{Z}\} = \{0, 1, 4\}$. Therefore, there do not exist any $p, r, s \in S$ such that $p + r + s \equiv 7 \pmod 8$. Thus, n is not representable.

Next, we proceed by induction. Assume that for some fixed $a \geq 0$, no natural number of the form $4^a(8b + 7)$ is representable. We will show that any natural number of the form $4^{a+1}(8b + 7)$ is also not representable. We proceed by contradiction.

Suppose for the sake of contradiction that there exists a representable natural number m of the form $m = 4^{a+1}(8b+7)$. Let $m = x_1^2+x_2^2+x_3^2$ for $x_1, x_2, x_3 \in \mathbb{Z}$. Since $a+1 \geq 1$, m is divisible by 4. Notice that the set of squares modulo 4 is $\{x^2 \pmod 4 : x \in \mathbb{Z}\} = \{0, 1\}$. Therefore, the only way to satisfy $m \equiv x_1^2 + x_2^2 + x_3^2 \equiv 0 \pmod 4$ is if $x_i^2 \equiv 0 \pmod 4$ for each term. This implies that $x_i \equiv 0 \pmod 2$, meaning $2 \mid x_i$. Dividing our equation for m by 4 we get:

$$\frac{m}{4} = \left(\frac{x_1}{2}\right)^2 + \left(\frac{x_2}{2}\right)^2 + \left(\frac{x_3}{2}\right)^2$$

where each term on the right-hand side is an integer square since each x_i is divisible by 2. Hence, $\frac{m}{4}$ is representable. But since $\frac{m}{4} = 4^a(8b+7)$, this implies that a number of the form $4^a(8b + 7)$ is representable, contradicting our inductive hypothesis. Thus, our initial assumption is wrong, which means m is not representable.

□

Next, we present a clever proof of Part (2) of Theorem 3.1 due to N. C. Ankeny, which makes use of earlier ideas by H. Davenport. We first introduce the necessary background machinery.

3.2 Machinery for the Proof of Part (2)

The proof of Part (2) of Theorem 3.1 requires several results from number theory and the geometry of numbers. We begin with a result about the existence of primes in specific arithmetic progressions.

3.2.1 Primes in Arithmetic Progressions

Theorem 3.2 (Dirichlet's Theorem on Primes in Arithmetic Progressions)**.** *Let a and d be natural numbers such that $\gcd(a, d) = 1$. There exist infinitely many primes p such that $p \equiv a \pmod d$.*

We will use this theorem combined with Chinese Remainder Theorem to show that there exists a prime q that satisfies a system of congruences. Next, we define several geometric concepts and state Minkowski's Theorem.

Definition 3.3. A point $P = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ is an *integer lattice point* if $x_i \in \mathbb{Z}$ for all i.

Definition 3.4. A region $K \subseteq \mathbb{R}^n$ is *bounded* if it can be entirely enclosed within some sphere of finite radius.

Definition 3.5. A region $K \subseteq \mathbb{R}^n$ is *convex* if for any two points $P, Q \in K$, the line segment PQ is contained in K.

Definition 3.6. A region $K \subseteq \mathbb{R}^n$ is *centrally symmetric about the origin* if whenever $P = (x_1, x_2, \ldots, x_n)$ is in K, its reflection $-P = (-x_1, -x_2, \ldots, -x_n)$ is also in K.

Theorem 3.7 (Minkowski's Convex Body Theorem)**.** *Let $K \subseteq \mathbb{R}^n$ be a bounded, convex region that is centrally symmetric about the origin. If the volume of K is greater than 2^n, then K contains at least one integer lattice point other than the origin.*

In our proof we will apply Minkowski's Theorem in three-dimensional space ($n = 3$), which requires a region of volume greater than $2^3 = 8$. The region we construct will be an ellipsoid. To calculate the ellipsoid's volume we rely on the volume of a sphere, $V = \frac{4}{3}\pi r^3$, and two geometric principles.

Lemma 3.8 (Scaling and Cavalieri's Principle)**.** *Let K be a three-dimensional region.*

1. ***Scaling:*** *If K is stretched along one of its coordinate axes by a positive factor c, the total volume of the region is multiplied by c.*
2. ***Shearing (Cavalieri's Principle):*** *If K is sheared meaning its cross-sections are shifted parallel to a fixed plane by an amount proportional to their distance from that plane, the total volume of the region remains unchanged.*

To build geometric intuition for how we will calculate the volume of our region, Figure 1 presents a 2D visualization of these two transformations.

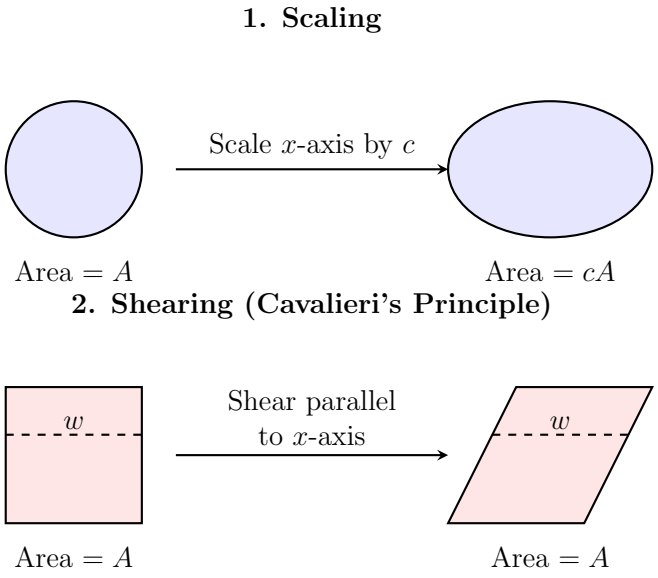

Figure 1: A 2D visualization of scaling and shearing. Scaling multiplies the area by the stretch factor. Shearing parallel to an axis shifts cross-sections without changing their width w, leaving the total area invariant.

Notice that in two dimensions, stretching a shape along an axis multiplies its area by the stretch factor, while shearing a shape parallel to an axis does not change its area at all. This is because shearing merely slides the horizontal cross-sections (of width w) left or right without altering their lengths. Since the total area is essentially the sum of these slices, the area remains exactly A. Cavalieri's Principle guarantees that this geometric logic directly extends to three dimensions: stretching a volume scales it, and shearing a volume leaves it invariant.

Later in the proof, we will encounter an inequality of the form $R^2 + S^2 + T^2 < 2m$. If we treat R, S, and T as standard perpendicular axes, this region is simply a sphere of

radius $\sqrt{2m}$. However, R, S, and T will be defined as scaled and sheared combinations of our actual variables x, y, and z. Applying Lemma 3.8 will allow us to start with the volume of the sphere and track how the volume changes as we revert back to (x, y, z)-space to find the volume of the resulting ellipsoid.

Finally, we establish the properties of the Legendre and Jacobi symbols, which provide an algebraic method to determine if a number is a quadratic residue.

Definition 3.9 (Legendre Symbol)**.** Let p be an odd prime and let a be an integer. The Legendre symbol $\left(\frac{a}{p}\right)$ is defined as:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } p \nmid a \text{ and there exists an integer } x \text{ such that } a \equiv x^2 \pmod{p} \\ -1 & \text{if } p \nmid a \text{ and there is no such integer } x \\ 0 & \text{if } p \mid a. \end{cases}$$

Definition 3.10 (Jacobi Symbol)**.** Let m be a positive odd integer with prime factorization $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ where each p_i is an odd prime. The Jacobi symbol $\left(\frac{a}{m}\right)$ is defined as the product of the Legendre symbols of the primes in the prime factorization:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

The Jacobi symbol generalizes Legendre symbol to composite numbers. But it needs to be used with caution. If p is an odd prime and $\left(\frac{a}{p}\right) = 1$ then a is a quadratic residue modulo p. However, if m is composite $\left(\frac{a}{m}\right) = 1$ does not guarantee that the congruence $x^2 \equiv a \pmod{m}$ has a solution.

Example 3.11. Consider $a = 2$ and $m = 15$. Using the definition of the Jacobi symbol:

$$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$$

However, the set of squares modulo 15 is $\{x^2 \pmod{15} : x \in \mathbb{Z}\} = \{0, 1, 4, 6, 9, 10\}$. Since 2 is not in this set, there is no integer x such that $x^2 \equiv 2 \pmod{15}$.

In the proof, we will rely heavily on the properties of the Jacobi symbol. Because the Jacobi symbol is a product of Legendre symbols, it inherits some useful properties. Firstly, Jacobi symbol is multiplicative in both the numerator and denominator.

Proposition 3.12 (Multiplicativity of the Jacobi Symbol)**.** *Let m and n be positive odd integers, and let a and b be integers. Then:*

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) \quad \textit{and} \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$

Next, we need rules to evaluate the Jacobi symbol for specific values, particularly -1 and 2.

Theorem 3.13 (The Supplements to Quadratic Reciprocity)**.** *Let m be a positive odd integer.*

1. ***First Supplement:***
$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$$
This implies that $\left(\frac{-1}{m}\right) = 1$ *if and only if* $m \equiv 1 \pmod 4$.

2. ***Second Supplement:***
$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$$
This implies that $\left(\frac{2}{m}\right) = 1$ *if and only if* $m \equiv 1$ *or* $7 \pmod 8$.

Finally, we state a powerful symmetry law known as the Law of Quadratic Reciprocity.

Theorem 3.14 (Law of Quadratic Reciprocity for Jacobi Symbols)**.** *Let* m *and* n *be relatively prime positive odd integers. Then:*
$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}$$

In other words, $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$ *unless both* $m \equiv 3 \pmod 4$ *and* $n \equiv 3 \pmod 4$*, in which case* $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

3.3 Proof of Part (2)

Next, we move on to the proof of Part (2) Theorem 3.1. Recall that the Part (2) of this theorem states that every natural number n not of the form $4^a(8b+7)$ is representable as a sum of three squares. We first consider the case where n is square free, and then use a simple lemma to show that it works for all n not of the form $4^a(8b+7)$.

Proposition 3.15. *Let* n *be a natural number not of the form* $4^a(8b+7)$*. Let* n *have the prime factorization* $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$ *where each exponent* $e_i \leq 1$*. Then* n *is representable as a sum of three squares.*

To prove Proposition 3.15 we first consider the case where $n \equiv 3 \pmod 8$. The proofs for other residues modulo 8 follow a similar argument which we will show later on. We first begin by doing the number theory setup to prepare us for the later parts of the proof. We have two lemmas.

Lemma 3.16. *Let* m *be a square-free positive integer such that* $m \equiv 3 \pmod 8$*. Let* m *have the prime factorization* $m = p_1p_2\dots p_k$*. There exists a prime* q *such that:* $q \equiv 1 \pmod 4$ *and* $\left(\frac{-2q}{p_j}\right) = 1$ *for all prime divisors* p_j *of* m.

We use Dirichlet's Theorem on Primes in Arithmetic Progressions and the Chinese Remainder Theorem to prove this lemma.

Proof. Let $m = p_1p_2\dots p_k$. We want a prime q satisfying $q \equiv 1 \pmod 4$ and $\left(\frac{-2q}{p_j}\right) = 1$. Because the Legendre symbol is multiplicative, we have $\left(\frac{q}{p_j}\right) = \left(\frac{-2}{p_j}\right)$. For each p_j, by Lemma 2.4, there exists $\frac{p_j+1}{2}$ quadratic residues $\pmod{p_j}$. Hence, we can find a non-zero residue $a_j \pmod{p_j}$ such that $\left(\frac{a_j}{p_j}\right) = \left(\frac{-2}{p_j}\right)$.

We set up the following system of congruences:

$$\begin{aligned} q &\equiv 1 \pmod 4 \\ q &\equiv a_j \pmod{p_j} \quad \text{for } j = 1, 2, \ldots, k \end{aligned}$$

Since m is odd, 4 and all p_j are pairwise coprime. By the Chinese Remainder Theorem, there is a unique solution $q \equiv A \pmod{4m}$. Since $A \equiv 1 \pmod 4$ and $A \equiv a_j \not\equiv 0 \pmod{p_j}$, it follows that $\gcd(A, 4m) = 1$. By Dirichlet's Theorem on Primes in Arithmetic Progressions, there exist infinitely many primes satisfying $q \equiv A \pmod{4m}$. Thus, there exists a prime q such that $q \equiv 1 \pmod 4$ and $\left(\frac{-2q}{p_j}\right) = 1$ for all prime divisors.

□

Lemma 3.17. *Let $m \equiv 3 \pmod 8$ be a square free positive integer with the prime factorization $m = p_1 p_2 \ldots p_k$. If there exists a prime q such that $q \equiv 1 \pmod 4$ and $\left(\frac{-2q}{p_j}\right) = 1$ for all prime divisors p_j of m, then there exists integers b, h such that $b^2 - 4qh = -m$.*

To prove this, we evaluate the Jacobi symbol $\left(\frac{-m}{q}\right)$ and use Law of Quadratic Reciprocity.

Proof. Consider the Jacobi symbol $\left(\frac{-m}{q}\right)$. By the complete multiplicativity of the Jacobi symbol and the Law of Quadratic Reciprocity:

$$\begin{aligned} 1 &= \prod_{j=1}^{k} \left(\frac{-2q}{p_j}\right) = \prod_{j=1}^{k} \left(\frac{-2}{p_j}\right)\left(\frac{q}{p_j}\right) \\ &= \left(\frac{-2}{m}\right) \prod_{j=1}^{k} \left(\frac{q}{p_j}\right) \\ &= \left(\frac{-2}{m}\right)\left(\frac{m}{q}\right) \quad (\text{since } q \equiv 1 \pmod 4, \text{ by Theorem 3.14 we get } \left(\frac{q}{m}\right) = \left(\frac{m}{q}\right)) \\ &= \left(\frac{-2}{m}\right)\left(\frac{-m}{q}\right) \quad (\text{since } q \equiv 1 \pmod 4, \ \left(\frac{-1}{q}\right) = 1) \end{aligned}$$

Because $m \equiv 3 \pmod 8$, we know $\left(\frac{-2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right) = (-1)(-1) = 1$. Substituting this into our equation gives $1 = \left(\frac{-m}{q}\right)$.

Therefore, $-m$ is a quadratic residue $\pmod q$. So, there exists an integer b such that $b^2 \equiv -m \pmod q$. Since q is odd, if b is even we can replace it with $b + q$, hence we can assume that b is odd. This congruence implies there exists an integer h_1 such that:

$$b^2 - qh_1 = -m$$

We examine this equation modulo 4. Since b is odd, $b^2 \equiv 1 \pmod 4$. We chose $q \equiv 1 \pmod 4$, and we are given $m \equiv 3 \pmod 8$, meaning $-m \equiv 5 \equiv 1 \pmod 4$. Substituting these into the equation gives $1 - 1 \cdot h_1 \equiv 1 \pmod 4$, which forces $h_1 \equiv 0 \pmod 4$. Therefore, $h_1 = 4h$ for some integer h, yielding $b^2 - 4qh = -m$.

□

Finally, by definition, $\left(\frac{-2q}{p_j}\right) = 1$, which means $-2q$ is a quadratic residue for every prime factor of m. This means $(-2q)^{-1} \equiv -\frac{1}{2q}$ is also a quadratic residue for every prime factor of m. By the Chinese Remainder Theorem, we can construct an integer t such that $t^2 \equiv -\frac{1}{2q} \pmod{p_j}$ for all j, which implies $t^2 \equiv -\frac{1}{2q} \pmod{m}$.

Next, we set up a geometric construction to be able to apply Theorem 3.7.

Lemma 3.18. *Let m, q, b, h, and t be defined as in the previous lemmas. There exist integers x_1, y_1, z_1, not all zero, such that if we define:*

$$R_1 = 2tqx_1 + tby_1 + mz_1$$
$$S_1 = \sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1$$
$$T_1 = \frac{\sqrt{m}}{\sqrt{2q}}y_1$$

then $R_1^2 + S_1^2 + T_1^2 < 2m$.

Proof. Consider the region in (R, S, T)-space defined by $R^2 + S^2 + T^2 < 2m$. This is simply a sphere centered at the origin with radius $\sqrt{2m}$. The volume of this sphere is:

$$V_{RST} = \frac{4}{3}\pi(\sqrt{2m})^3 = \frac{4}{3}\pi(2m)^{3/2}$$

We want to find the volume of this region when mapped back to our integer variables in (x_1, y_1, z_1)-space. To do this we can use Lemma 3.8 to track how the volume changes step-by-step from (x_1, y_1, z_1) to (R, S, T).

1. **The T-axis:** Notice that $T = \frac{\sqrt{m}}{\sqrt{2q}}y_1$. This transformation simply scales the y_1-axis by a factor of $\frac{\sqrt{m}}{\sqrt{2q}}$.

2. **The S-axis:** Notice that $S = \sqrt{2q}x_1 + \frac{b}{\sqrt{2q}}y_1$. This transformation scales the x_1-axis by $\sqrt{2q}$. The addition of the y_1 term simply shears the space. By Cavalieri's Principle, shearing parallel to an axis does not change the volume.

3. **The R-axis:** Notice that $R = mz_1 + tby_1 + 2tqx_1$. This scales the z_1-axis by a factor of m. The addition of the x_1 and y_1 terms is another shear, which again does not affect the volume.

By multiplying these three scaling factors together, we find the total scaling factor from (x_1, y_1, z_1)-space to (R, S, T)-space is:

$$\text{Scale Factor} = \left(\frac{\sqrt{m}}{\sqrt{2q}}\right) \cdot (\sqrt{2q}) \cdot (m) = m^{3/2}$$

Since moving from (x_1, y_1, z_1) to (R, S, T) multiplies the volume by $m^{3/2}$, we can find the volume of the region in our original (x_1, y_1, z_1)-space by dividing the sphere's volume by $m^{3/2}$:

$$V_{xyz} = \frac{\frac{4}{3}\pi(2m)^{3/2}}{m^{3/2}} = \frac{4}{3}\pi 2^{3/2} = \frac{8\sqrt{2}\pi}{3}$$

Because $\sqrt{2} \approx 1.414$ and $\pi \approx 3.141$, we can verify that:

$$V_{xyz} = \frac{8\sqrt{2}\pi}{3} \approx 11.84 > 8$$

The region is bounded, convex (as it is an ellipsoid), centrally symmetric, and has a volume strictly greater than $8 = 2^3$. Therefore, by Minkowski's Convex Body Theorem (Theorem 3.7), there exists at least one non-zero integer lattice point (x_1, y_1, z_1) inside this region. This lattice point satisfies $R_1^2 + S_1^2 + T_1^2 < 2m$. □

Draft Note: *The remainder of this proof is currently being typed up. The finalized version will conclude the geometric argument mapping the lattice point back to the original congruences.*

3.4 Proof for Other Residues

Draft Note: *This subsection is currently in progress. The final version will detail how Ankeny extends the geometric proof from $n \equiv 3 \pmod 8$ to the other allowed residues modulo 8.*

3.5 Corollaries of Legendre's Theorem

Legendre's Three-Square Theorem is a very powerful tool. In this section, we will use it to directly prove two famous results in number theory: Lagrange's Four-Square Theorem which we proved in Section 2 and Gauss's Eureka Theorem.

3.5.1 Another Proof of Lagrange's Theorem

Historically, Lagrange proved his Theorem three decades before Legendre proved the Three-Square Theorem. But, once Legendre's Theorem is established, Lagrange's Theorem follows as a simple corollary. Recall Lagrange's Four-Square Theorem.

Theorem 3.19 (Lagrange's Four-Square Theorem)**.** *Every natural number $n \in \mathbb{N}$ is representable as a sum of four squares.*

Proof. Let n be a natural number. We split the proof into two cases based on whether n satisfies the condition in Legendre's Theorem (Theorem 3.1).

Case 1: n is not of the form $4^a(8b + 7)$.
By Legendre's Theorem, n can be written as a sum of three squares. Thus, $n = x^2+y^2+z^2$ for some integers x, y, z. We can simply add 0^2 to represent n as a sum of four squares:

$$n = x^2 + y^2 + z^2 + 0^2$$

Case 2: n is of the form $4^a(8b + 7)$ for some integers $a, b \geq 0$.

We can rewrite n by splitting the odd factor:

$$n = 4^a(8b + 6 + 1) = 4^a(8b + 6) + 4^a = 2^{2a+1}(4b + 3) + (2^a)^2$$

Let $m = 2^{2a+1}(4b+3)$. We claim that m is not of the form $4^k(8c+7)$. For any number of the form $4^k(8c + 7)$, the highest power of 2 dividing it is exactly 2^{2k}, which has an

even exponent. However, the highest power of 2 dividing m is 2^{2a+1}, which has an odd exponent. Therefore, m cannot be of the form $4^k(8c+7)$.

By Legendre's Theorem m is representable as a sum of three squares. Say $m = x_1^2 + x_2^2 + x_3^2$. By Substituting this back into our equation for n we get

$$n = m + (2^a)^2 = x_1^2 + x_2^2 + x_3^2 + (2^a)^2$$

Thus, n is representable as a sum of four squares.

□

3.5.2 Gauss's Eureka Theorem

A triangular number represents the number of dots needed to form an equilateral triangle. Triangular numbers are of the form $T_k = \frac{k(k+1)}{2}$ for some integer $k \geq 0$. In 1796, Carl Friedrich Gauss wrote in his diary: *"EUREKA! num* $= \Delta + \Delta + \Delta$*"*, meaning he had discovered that every integer is the sum of at most three triangular numbers. This can be shown as a corollary of Legendre's Theorem.

Theorem 3.20 (Gauss's Eureka Theorem)**.** *Every natural number $n \in \mathbb{N}$ can be represented as the sum of three triangular numbers.*

Proof. Let n be a natural number. We wish to find non-negative integers x, y, z such that:

$$n = \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2}$$

Multiplying the entire equation by 8 and adding 3 we get:

$$8n + 3 = 4x^2 + 4x + 1 + 4y^2 + 4y + 1 + 4z^2 + 4z + 1$$
$$8n + 3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2$$

Therefore, proving that n is the sum of three triangular numbers is equivalent to proving that $8n + 3$ is the sum of three odd squares.

First, observe that any number of the form $4^a(8b+7)$ is either $\equiv 7 \pmod 8$ (if $a = 0$) or $\equiv 0 \pmod 4$ (if $a \geq 1$). Since $8n+3 \equiv 3 \pmod 8$, it cannot be of the form $4^a(8b+7)$. By Legendre's Theorem, there exist integers A, B, C such that:

$$8n + 3 = A^2 + B^2 + C^2$$

Next, we must show that A, B, and C are odd. The set of squares modulo 8 is $\{x^2 \pmod 8 : x \in \mathbb{Z}\} = \{0, 1, 4\}$. The only way to choose three numbers from $\{0, 1, 4\}$ that sum to $3 \pmod 8$ is $1 + 1 + 1$. Thus, we must have:

$$A^2 \equiv B^2 \equiv C^2 \equiv 1 \pmod 8$$

This implies that A, B, and C are odd integers.

Since they are odd, we can write $|A| = 2x + 1$, $|B| = 2y + 1$, and $|C| = 2z + 1$ for some non-negative integers x, y, z. Substituting these back gives:

$$8n + 3 = (2x+1)^2 + (2y+1)^2 + (2z+1)^2$$

Expanding the squares, subtracting 3, and dividing by 8 reverses our initial algebra, resulting in $n = T_x + T_y + T_z$. Thus, n is the sum of three triangular numbers.

□

4 Number of Representations

Draft Note: This section is currently being expanded. The final paper will conclude with a deeper discussion on why the number of representations for three-squares lacks the simple divisor formulas of the two- and four-square cases, and will briefly mention how modern mathematicians use modular forms to resolve this.

Throughout this paper, we have focused on the *existence* of representations. We proved that certain numbers can or cannot be written as sums of two, three, or four squares. A natural evolution of this problem is to ask for the exact *quantity* of such representations.

Let $r_k(n)$ denote the number of ways to write an integer n as the sum of k squares. In this counting function, both the order of the terms and the signs of the bases matter. For example, $1^2 + 0^2$ and $0^2 + 1^2$ are considered distinct representations, as are $1^2 + 0^2$ and $(-1)^2 + 0^2$.

4.1 Sums of Two and Four Squares

The formulas for $r_2(n)$ and $r_4(n)$ were both discovered by Carl Gustav Jacob Jacobi in the 19th century. They are famously elegant, relying only on the divisors of n.

For the sum of two squares, we define two simple divisor counting functions: let $d_1(n)$ be the number of divisors d of n such that $d \equiv 1 \pmod 4$, and let $d_3(n)$ be the number of divisors such that $d \equiv 3 \pmod 4$.

Theorem 4.1 (Jacobi's Two-Square Formula)**.** *For any natural number $n \in \mathbb{N}$, the number of ways to represent n as a sum of two squares is given by:*

$$r_2(n) = 4(d_1(n) - d_3(n))$$

For example, if $n = 5$, the divisors are 1 and 5. Both are congruent to 1 (mod 4). Thus, $d_1(5) = 2$ and $d_3(5) = 0$, giving $r_2(5) = 4(2 - 0) = 8$. These 8 representations correspond to the permutations and signs of $(\pm 2)^2 + (\pm 1)^2$ and $(\pm 1)^2 + (\pm 2)^2$.

The underlying mechanism that makes Theorem 4.1 possible is the arithmetic of the Gaussian integers, $\mathbb{Z}[i]$. Because the norm of a Gaussian integer is exactly $a^2 + b^2$, representing n as two squares is equivalent to factoring n in the ring $\mathbb{Z}[i]$. The formula arises directly from tracking how prime numbers split or remain prime when lifted into the complex plane.

An equally beautiful formula exists for the sum of four squares.

Theorem 4.2 (Jacobi's Four-Square Formula)**.** *For any natural number $n \geq 1$, the number of ways to represent n as a sum of four squares is given by:*

$$r_4(n) = 8 \sum_{\substack{d \mid n \\ 4 \nmid d}} d$$

This formula states that to find $r_4(n)$, we sum all the divisors of n that are not multiples of 4, and multiply by 8. For instance, if $n = 2$, the divisors are 1 and 2. Neither

is a multiple of 4. Their sum is 3, so $r_4(2) = 8(3) = 24$. This matches the 24 permutations and sign combinations of $(\pm 1)^2 + (\pm 1)^2 + 0^2 + 0^2$.

Just as the two-square formula is powered by the complex numbers, the four-square formula is powered by quaternions. By studying prime factorization within a specific ring of quaternions (known as the Hurwitz quaternions), mathematicians can count representations in four dimensions using the multiplicativity of the quaternion norm.

Both $r_2(n)$ and $r_4(n)$ possess clean, closed-form divisor formulas because they correspond to 2-dimensional and 4-dimensional algebraic systems that possess a multiplicative norm. However, as we move to three squares, this algebraic convenience completely vanishes.

Acknowledgments

The author would like to thank Akrit Ray and Simon Rubinstein-Salzedo for guidance during the preparation of this paper. The author is also grateful to the students of the Euler Circle Independent Research and Paper Writing class for their helpful feedback and engaging discussions throughout the program.

References

[Ank57] N. C. Ankeny. Sums of three squares. *Proceedings of the American Mathematical Society*, 8(2):316–319, 1957.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, second edition, 1990.

[Wei84] André Weil. *Number Theory: An approach through history from Hammurapi to Legendre*. Birkhäuser, 1984.