Proceedings of the 2nd International Conference on Mathematical Physics and Computational Simulation
DOI: 10.54254/2753-8818/41/20240576

The sum of four squares: An exploration of Lagrange's theorem and its legacy in number theory

Yifan Cheng

United International College, Zhuhai, 519000, China

r130033004@mail.uic.edu.cn

Abstract. Lagrange's Four-square Theorem is a fundamental principle in number theory, which states that every positive integer can be expressed as the sum of four squares. The theorem was first conjectured by the Greek mathematician Diophantus of Alexandria in the 3rd century CE. It was later proved by Pierre de Fermat in the 17th century, and the first published proof was attributed to Joseph-Louis Lagrange in 1770. This paper presents a comprehensive account of the four-square theorem in number theory, which focuses on finding integer solutions to polynomial equations. The theorem has significantly advanced the study of Diophantine equations. It traces Lagrange's Four-square Theorem from its conjectural origins to its emergence as a cornerstone of contemporary mathematical research. This paper reviews the proof of the theorem and its implications, as well as its connection to modern research and applications, highlighting its timeless relevance in mathematics. In addition, the paper reaffirms the extensive influence of the theorem on the advancement of Diophantine equations and its ongoing significance in elucidating the enigmas of number theory. This enhances our comprehension of the theorem's position in the wider story of mathematical progress, confirming its significance in both historical and contemporary contexts.

Keywords: Lagrange's Four-Square Theorem, Diophantine Equations, Computational Number Theory, Quantum Computing

1. Introduction

The study of numbers and their properties is a fundamental aspect of mathematical inquiry, with the representation of numbers as sums of squares occupying a pivotal role throughout history. This fascination spans from the Pythagorean triples rooted in ancient geometry to the sophisticated realms of modern number theory. Positioned at the confluence of historical curiosity and contemporary mathematical rigor, this paper aims to explore the representation of integers as sums of squares, a question that has intrigued mathematicians for centuries [1]. The foundation of modern number theory, enriched by resources like NRICH and Silverman's "A Friendly Introduction to Number Theory" [2] [3], builds upon these ancient questions, showing their relevance in today's mathematical challenges. By delving into the historical evolution of this problem, from the early explorations by Pythagoras and Diophantus to the groundbreaking proofs by Fermat, Euler, and Lagrange, it uncovers the mathematical underpinnings and implications of such representations. Combined with a comprehensive review of the historical literature tracing the development of sums of squares in number theory and an analysis of contemporary mathematical texts and papers demonstrating current research and methods in the field,

DOI: 10.54254/2753-8818/41/20240576

this paper bridges the gap between historical insights and modern mathematical advances, providing a holistic view of the subject matter.

2. Historical Background

The journey to express numbers as the sum of squares begins with Diophantus of Alexandria in the 3rd century (Diophantus of Alexandria, 3rd century CE) [4,5], whose work "Arithmetica" laid early foundations for algebra and introduced the concept of Diophantine equations—seeking integer solutions for equations. Diophantus's insights into equations involving squares paved the way for future mathematical breakthroughs. The narrative advanced significantly with Pierre de Fermat in the 17th century. Fermat proposed that every prime number of the form 4n+1 could be uniquely expressed as the sum of two squares. This proposition, known as Fermat's theorem on sums of two squares, opened new vistas in understanding the nature of numbers. The story took a monumental leap with Joseph-Louis Lagrange in the 18th century, who proved that every positive integer could be represented as the sum of four squares. Lagrange's proof not only underscored the significance of sums of squares within number theory but also highlighted the analytical techniques' prowess in addressing mathematical challenges.

Leonhard Euler contributed further by developing the Euler four-square identity, enhancing the mathematical framework for analyzing sums of squares. Similarly, Adrien-Marie Legendre's work, including his three-square theorem, deepened the understanding of numbers' representation as squares, particularly in relation to prime numbers. These milestones by Diophantus, Fermat, Lagrange, Euler, and Legendre have fundamentally shaped the study of number theory, especially concerning the intriguing challenge of expressing numbers as the sum of squares. Their collective work underscores the mathematical field's depth, interconnectedness, and the ongoing quest to unravel the complexities of integers.

3. Mathematical Foundations

In number theory, there are several basic concepts and notations pivotal for understanding theorems such as the Lagrange's four-square theorem [1][4], including:

- Integers ($\mathbb{Z}$): The set of whole numbers including positive, negative numbers, and zero.
- Prime numbers: Natural numbers greater than 1 that have no positive divisors other than 1 and themselves.
- Squares: Numbers that are the product of an integer with itself. For example, $4 = 2^2$ is a square.
- Sum of squares: An expression that represents a number as the sum of the squares of integers.

Lagrange's Four-Square Theorem states that every positive integer can be expressed as the sum of four squares of integers. Formally, for any positive integer n, there exist integers a, b, c and d such that:

$$n = a^2 + b^2 + c^2 + d^2 \tag{1}$$

- Euler's Four-Square Identity: According to the Figure 1, this identity shows how the product of two sums of four squares is itself a sum of four squares. Specifically, if we have two numbers expressed as the sum of four squares:

$$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \tag{2}$$

DOI: 10.54254/2753-8818/41/20240576

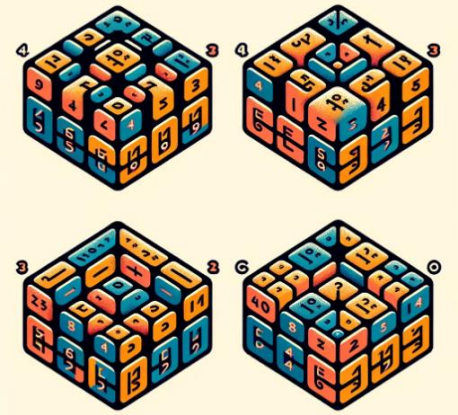

Figure 1. The visualization of Euler's Four-Square Identity

Euler's identity allows us to express this product again as a single sum of four squares, an essential concept for proving that the set of numbers expressible as the sum of four squares is closed under multiplication [6]. This principle is further elucidated in texts such as Silverman's introduction to number theory, offering a gateway to understanding complex mathematical structures [3]. Understanding these concepts and their interrelations not only facilitates the comprehension of the theorem's proofs but also illustrates the elegance and depth of mathematical structures dealing with integers and their properties.

4. Proof of Theorem

Lagrange's original proof of the four-square theorem was presented in a simplified manner, leveraging earlier works by mathematicians like Fermat [5] and Euler [6]. A detailed step-by-step simplification of Lagrange's proof would require a deep dive into complex number theory, the essence of his approach was to show that every positive integer can be broken down into a sum of four squares, leveraging earlier works by mathematicians like Fermat. Lagrange's proof is notable for its methodical approach, showing that if the theorem holds for certain types of numbers, it must then hold for all positive integers. One key aspect of his proof involved demonstrating that if two numbers can be expressed as the sum of four squares, then their product can also be expressed in the same form. This foundational concept is crucial for understanding the theorem's proof and its significance.

4.1. Alternative Proofs and Generalizations

The aim of this chapter is to examine alternative proofs and generalizations of the original theories or conclusions. This not only demonstrates the diversity and flexibility of the original ideas but also provides new perspectives and possibilities for further research and application.

4.1.1. Infinite Descent. Fermat famously used the method of infinite descent to prove various propositions, which consisted of assuming there is a smallest counterexample to a proposition and then showing that a smaller one exists, leading to a contradiction. Though not directly applied to the original four-square theorem, this method has influenced proofs in related areas.

4.1.2. Hurwitz Quaternions. A more modern approach to understanding sums of squares involves the algebra of Hurwitz quaternions, which are complex number systems that extend real numbers. These quaternions provide a powerful framework for generalizing and proving the sums of squares theorems, illustrating the deep connections between number theory and algebra.

4.2. Computational Methods in Proofs

With the advent of computers, computational methods have become invaluable in exploring the realms of number theory, including proofs related to the four-square theorem. Computers empower

DOI: 10.54254/2753-8818/41/20240576

mathematicians to validate hypotheses on large datasets, identify patterns, and even provide proofs for specific cases that would be unmanageable manually. These methods have not only confirmed the vast applicability of the theorem but also opened new avenues for its exploration and application.

4.3. Applications and Implications.

The four-square theorem finds applications across various domains of mathematics and science, demonstrating its fundamental nature:

4.3.1. Cryptography. In cryptographic systems, particularly those based on lattice problems and quadratic forms, the ability to represent numbers as sums of squares has implications for encryption algorithms and security protocols [7].

4.3.2. Coding Theory. The theorem's concepts are applied in coding theory, where sums of squares are related to error-detecting and error-correcting codes, crucial for data transmission and storage.

4.3.3. Quantum Computing. In quantum computing, the mathematical structures underlying the four-square theorem can influence algorithms and the development of quantum error correction.

The four-square theorem, with its rich history and wide applicability, continues to be a subject of fascination and study within the mathematical community. Its enduring legacy underscores the timeless nature of mathematical inquiry and its relevance to both foundational research and practical applications.

5. Contemporary Perspectives

In the realm of number theory, researchers often focus on advancing the understanding of the four-square theorem. And recent developments may include efforts to generalize the theorem to other number systems or to explore its connections to other area of mathematics. Additionally, researchers might be working on computational approaches to efficiently find representations of numbers as sums of squares or investigating specific open problems and conjectures related to the theorem. Nonetheless, this paper can lead to an understanding of the focus of the research community and the types of developments that are likely to occur. The advent of powerful computational tools, as detailed by Crandall and Pomerance in "Prime Numbers: A Computational Perspective," allows researchers to test hypotheses related to the four-square theorem on a scale not previously possible, verifying the theorem for very large numbers and exploring its implications in computational complexity and algorithmic number theory [8].

5.1. Recent Generalizations and Computational Approaches

Recent generalizations include extending the four-square theorem to more complex structures, such as higher-dimensional lattices or other algebraic systems. Mathematicians are also interested in similar representations for other forms, like cubes or higher powers, and the conditions under which similar theorems hold. These explorations are supported by advancements in computational number theory, which Silverman and Crandall with Pomerance discuss in their respective works [3,8].

- Generalizations: Research might explore extending the four-square theorem to more complex structures, such as higher-dimensional lattices or other algebraic systems. Mathematicians are also interested in similar representations for other forms, like cubes or higher powers, and the conditions under which similar theorems hold.
- Computational Number Theory: The advent of powerful computational tools allows researchers to test hypotheses related to the four-square theorem on a scale not previously possible. This includes verifying the theorem for very large numbers or exploring its implications in computational complexity and algorithmic number theory.

5.2. Open Problems and Conjectures:

- Density and Distribution: Questions about the density and distribution of the representations of numbers as the sum of squares, and how these properties might influence other areas of number

DOI: 10.54254/2753-8818/41/20240576

theory and combinatorics.

- Connections to Other Fields: Exploring deeper connections between the four-square theorem and other mathematical fields, such as elliptic curves, modular forms, and cryptographic algorithms, may yield new insights and open problems.

6. Discussion

The Four-square Theorem, proven by Joseph-Louis Lagrange in 1770, stands as a monumental testament to the beauty and depth of number theory. This theorem, demonstrating that every positive integer can be represented as the sum of four squares, resolved a long-standing question and catalyzed a new era of mathematical exploration. Its simplicity belies the profound implications it has for number theory and beyond, having inspired countless mathematicians to delve into the properties of numbers, leading to the emergence of new branches within mathematics and a deeper understanding of existing ones. ThisStewart and Tall's "Algebraic Number Theory and Fermat's Last Theorem" and Weil's historical approach in "Number Theory: An Approach Through History from Hammurapi to Legendre" provide context for the theorem's impact beyond its initial proofs, demonstrating its foundational role in algebraic number theory and its historical significance [9]. Meanwhile, Conway and Smith's exploration of "On Quaternions and Octonions" illuminates the deep connections between the theorem and algebra, highlighting the quaternion algebra's role in generalizing and proving sums of squares theorems [10].

7. Conclusion

This paper has sought to illuminate these facets, presenting a comprehensive review of the theorem's historical development, its pivotal role in advancing number theory, and the myriad ways it continues to influence modern mathematical research. By highlighting the theorem's ongoing relevance and potential for future discoveries, it underscores the dynamic nature of mathematics, where ancient questions give rise to contemporary challenges and innovations. In conclusion, the four-square theorem remains a cornerstone of mathematical inquiry, a source of inspiration for both theoretical exploration and practical application. Looking ahead, it is clear that the theorem not only constitutes a significant chapter in the history of mathematics but also serves as a springboard for future generations of mathematicians to explore the endless mysteries of numbers. This work provides a deeper understanding of the theorem's place in mathematical thought, reaffirming its timeless significance and the endless curiosity it inspires

References

[1] Lagrange, J. L. (1770). Demonstration d'un théorème d'arithmétique. Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin.
[2] Silverman, J. H. (2020). A friendly introduction to number theory. Brown University.
[3] Stewart, I., & Tall, D. (1979). Algebraic number theory and Fermat's last theorem. Cambridge, MA: Cambridge University Press.
[4] Fermat, P. de (1670). Observationes ad Diophantum [Marginal notes to Diophantus].
[5] Diophantus of Alexandria. (3rd century CE). Arithmetica
[6] NRICH. (n.d.). An introduction to number theory. Retrieved from https://nrich.maths.org/numbertheory
[7] Euler, L. (1772). De compositione numerorum ex quattuor quadratis [On the composition of numbers from four squares]. Novi Commentarii Academiae Scientiarum Petropolitanae, 16, 64-93.
[8] Conway, J. H., & Smith, D. A. (2003). On quaternions and octonions. Wellesley, MA: A K Peters/CRC Press.
[9] Weil, A. (1798). Number theory: An approach through history from Hammurapi to Legendre. Paris, France: Springer.
[10] Crandall, R., & Pomerance, C. (2005). Prime numbers: A computational perspective. New York, NY: Springer.