Fermat's Last Theorem: A Historical and Mathematical Overview

Ijtihed Kilani

Abstract

This paper offers a comprehensive examination of Fermat's Last Theorem, a statement in number theory that captivated mathematicians for over 350 years until its proof by Andrew Wiles in 1994. Beginning with historical context surrounding Pierre de Fermat and the theorem's formulation, the paper meticulously reviews the mathematical foundations underlying the theorem, including Diophantine equations, modular forms, and elliptic curves. Special attention is given to Wiles' groundbreaking use of the Taniyama-Shimura-Weil conjecture and Ribet's theorem to provide a complete proof, including the resolution of an initial flaw in the proof. Furthermore, the paper explores the theorem's far-reaching implications in number theory, algebraic geometry, cryptography, and computer science. The study reveals that Fermat's Last Theorem is not just an isolated mathematical problem but a testament to the depth, beauty, and interconnectedness of mathematics, with broad impact across various scientific disciplines.

1 Introduction

Fermat's Last Theorem, a statement in number theory that was first formulated by Pierre de Fermat in 1637 [36], has been one of the most celebrated and studied theorems in the history of mathematics. The theorem asserts that there are no three positive integers a, b, c that can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2 [10]. While the theorem may appear simple and straightforward, its proof eluded mathematicians for more than 350 years, making it one of the most enduring challenges in the field [7].

The theorem has been a focal point of research in number theory, inspiring a multitude of mathematical techniques and theorems [15]. It has connections to modular forms, elliptic curves, and algebraic equations, among other areas [12]. The monumental proof by British mathematician Andrew Wiles in 1994 not only resolved this longstanding problem but also introduced groundbreaking techniques and methods that have had far-reaching implications in various branches of mathematics and computer science [46].

This paper aims to provide a comprehensive overview of Fermat's Last Theorem, delving into its history, the formal statement of the theorem, the intricacies

of its proof, and its modern-day implications [6]. We will explore the role of modular forms, elliptic curves, and Ribet's theorem in the proof, as well as the theorem's applications in cryptography and other areas of mathematics [43].

The journey through Fermat's Last Theorem is not just a tale of a mathematical problem solved; it is a testament to the depth, beauty, and interconnectedness of mathematics [37]. As we navigate through the complexities of the theorem and its proof, we will gain insights into the rich tapestry of modern mathematics [27].

2 Historical Context

2.1 The Life of Pierre de Fermat

Pierre de Fermat was born between October 31 and December 6, 1607, in Beaumont-de-Lomagne, France. His father, Dominique Fermat, was a wealthy leather merchant and served as one of the four consuls of Beaumont-de-Lomagne [26, 8]. Pierre had one brother and two sisters and was almost certainly brought up in the town of his birth [26].

Fermat attended the University of Orléans, where he received a bachelor's degree in civil law in 1626 [8]. He then moved to Bordeaux, where he began his first serious mathematical researches. In Bordeaux, he was in contact with mathematicians like Beaugrand and Étienne d'Espagnet, with whom he shared mathematical interests [26].

In 1630, Fermat bought the office of a councilor at the Parliament of Toulouse, one of the High Courts of Judicature in France [8]. He held this office for the rest of his life, and it entitled him to change his name from Pierre Fermat to Pierre de Fermat [26].

Fermat is best known for his Last Theorem, which he described in a note in the margin of his copy of Diophantus' "Arithmetica" [8]. The theorem states that no three positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2 [19].

Despite his significant contributions to mathematics, much of Fermat's work was not published during his lifetime. He often communicated his findings in letters to other mathematicians like Blaise Pascal and Marin Mersenne, leaving it to future generations to rediscover and formally prove many of his theories [26, 19].

Fermat's work laid the foundation for the development of several areas of mathematics, and his methods and theorems continue to be studied and applied in various scientific disciplines today [8, 19].

2.2 The Birth of the Theorem

Fermat's Last Theorem was first formulated by Pierre de Fermat in 1637. The theorem was introduced in a rather unusual manner; Fermat wrote it as a marginal note in his copy of the book "Arithmetica" by Diophantus [29]. The

note was written in Latin and stated that he had discovered "a truly marvelous proof of this proposition which this margin is too narrow to contain" [16].

The theorem itself is a statement in number theory that asserts that no three positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2. The theorem was not published in any of Fermat's works, and it was only after his death that his son, Samuel, found the famous marginal note while going through his father's papers [29].

The lack of a proof for the theorem and the intriguing note left by Fermat led to much speculation and effort to prove it, marking the beginning of a journey that would span more than three and a half centuries. Despite the absence of a formal proof, the theorem captivated the imagination of mathematicians and amateurs alike, inspiring a plethora of proofs for specific cases and laying the groundwork for future research in number theory [16].

Fermat himself only proved the case for $n = 4$, and it was Euler who first extended the proof to $n = 3$. However, a general proof eluded mathematicians until Andrew Wiles provided one in 1994, thereby resolving one of the most famous problems in the history of mathematics [29, 16].

2.3 Early Attempts and Partial Proofs

Fermat's Last Theorem, originally stated by Pierre de Fermat in 1637, remained unproven for more than three centuries. During this period, various mathematicians made significant contributions by proving the theorem for specific exponents. One of the earliest proofs was provided by Fermat himself for the case $n = 4$, using a method known as infinite descent [21].

In the 19th century, Sophie Germain made substantial contributions by innovating an approach that was relevant to an entire class of primes. Her work laid the foundation for future mathematicians to extend the proof to cover all regular primes [40].

Ernst Kummer further extended this work in the mid-19th century, proving the theorem for all regular primes. This left irregular primes to be analyzed individually. Over time, mathematicians were able to extend the proof to cover all prime exponents up to four million [8].

Further advancements were made in the 20th century, particularly around 1955, when Japanese mathematicians Goro Shimura and Yutaka Taniyama suspected a link between elliptic curves and modular forms. This eventually led to Andrew Wiles providing the first complete proof of the theorem in 1995 [26].

For those interested in a more in-depth study, H.M. Edwards' "Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory" is a recommended read [40].

2.4 Taniyama-Shimura-Weil Conjecture

The Taniyama-Shimura-Weil Conjecture, now formally proven and referred to as the Modularity Theorem, was a groundbreaking hypothesis in the realm of number theory and algebraic geometry. The conjecture asserts that every elliptic

curve E over the field of rational numbers $\mathbb{Q}$ can be parameterized by modular forms. Mathematically, an elliptic curve E over $\mathbb{Q}$ is defined by the equation

$$y^2 = x^3 + Ax + B,$$

where $A, B \in \mathbb{Q}$ [25].

The conjecture was initially met with skepticism and was considered a part of what mathematicians colloquially termed "moonshine mathematics." However, it gained significant attention when Andrew Wiles recognized its deep connection to Fermat's Last Theorem, which can be expressed as

$$a^n + b^n \neq c^n \quad \text{for } n > 2, a, b, c \in \mathbb{Z}^+.$$

Wiles hypothesized that if the Taniyama-Shimura-Weil Conjecture could be proven true for a specific class of semistable elliptic curves, then Fermat's Last Theorem would follow as a corollary [47].

Wiles dedicated several years to this complex problem, often working in isolation. His work involved intricate mathematical objects like modular forms, which can be represented as complex functions $f(z)$ satisfying

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z),$$

where $a, b, c, d \in \mathbb{Z}$ and k is the weight of the modular form [47].

Ultimately, Wiles succeeded in proving the conjecture for a specific class of elliptic curves, thereby providing the first complete proof of Fermat's Last Theorem. His work not only resolved a centuries-old problem but also validated the Taniyama-Shimura-Weil Conjecture for semistable elliptic curves [25, 47].

2.5 Andrew Wiles and the Final Proof

Andrew Wiles, a British mathematician, achieved a monumental milestone in the history of mathematics by proving Fermat's Last Theorem in 1994 [25, 3]. His proof was the culmination of a seven-year solitary endeavor, during which he worked in secrecy in his attic [25].

Wiles's approach to the proof was groundbreaking. He utilized the Shimura-Taniyama-Weil Conjecture, which posits a deep connection between elliptic curves and modular forms [35]. The conjecture was initially considered almost impossible to prove with the existing mathematical knowledge. Wiles's proof not only confirmed the conjecture for semistable elliptic curves but also, as a corollary, established the truth of Fermat's Last Theorem. Mathematically, this can be expressed as:

$$a^n + b^n \neq c^n \quad \text{for } n > 2, a, b, c \in \mathbb{Z}^+$$

His proof employed sophisticated techniques from algebraic geometry and number theory, including the use of modular lifting theorems and deformation rings [35].

However, the journey was not without hurdles. After his initial announcement in 1993, a gap was discovered in the proof. With the help of his former student, Richard Taylor, Wiles was able to correct the error within a year [25].

Wiles's proof had a profound impact on number theory and opened new avenues for research. His work was recognized with numerous honors, including the Abel Prize, often considered the "Nobel Prize of Mathematics" [25].

3 Mathematical Foundations

3.1 Basic Number Theory

Number theory, a branch of pure mathematics, is devoted to the study of integers and more generally to objects built out of them. One of the central concepts in number theory is that of a *prime number*. A prime number is an integer greater than 1 that has no positive divisors other than 1 and itself. The Fundamental Theorem of Arithmetic states that every integer greater than 1 is either a prime number or can be uniquely factored into prime numbers [16].

$$n = p_1^{e_1} \times p_2^{e_2} \times \ldots \times p_k^{e_k} \tag{1}$$

where $p_1, p_2, \ldots, p_k$ are prime numbers and $e_1, e_2, \ldots, e_k$ are their respective exponents.

Another important concept is that of *modular arithmetic*. In modular arithmetic, numbers "wrap around" upon reaching a certain value, known as the modulus. The notation $a \equiv b \mod m$ means that a and b leave the same remainder when divided by m.

$$a \equiv b \mod m \iff m \mid (a - b) \tag{2}$$

Fermat's Little Theorem is often used in number theory and is particularly relevant to the proof of Fermat's Last Theorem. It states that if p is a prime number, then for any integer a such that $0 < a < p$,

$$a^{p-1} \equiv 1 \mod p \tag{3}$$

These concepts are foundational in understanding the proof of Fermat's Last Theorem, as they are extensively used in the proof's modular forms and elliptic curves [45].

3.2 Algebraic Equations

Diophantine equations, named after the ancient Greek mathematician Diophantus, are polynomial equations for which integer solutions are sought. These equations play a crucial role in number theory and are intimately connected to Fermat's Last Theorem [28, 9].

One of the most famous Diophantine equations is the Pythagorean equation $a^2 + b^2 = c^2$, which has an infinite number of integer solutions. However,

Fermat's equation $x^n + y^n = z^n$ for $n > 2$ has no integer solutions, which is the essence of Fermat's Last Theorem.

The study of Diophantine equations has led to various techniques and theorems that are instrumental in understanding the properties of numbers. For example, the Modular Arithmetic method is often employed to find the integer solutions of these equations [23].

Elliptic curves, a special class of Diophantine equations, have been instrumental in the proof of Fermat's Last Theorem. These curves are defined by equations of the form $y^2 = x^3 + ax + b$, and their properties have been extensively studied in the context of the theorem.

In summary, Diophantine equations serve as the algebraic foundation upon which the complexities of Fermat's Last Theorem are built. Their study has not only provided insights into the theorem itself but has also enriched the field of number theory as a whole.

3.3 Modular Forms

Modular forms are complex analytic functions defined on the upper half-plane, satisfying specific transformation properties under the action of the modular group. Mathematically, a modular form f of weight k for the modular group Γ is a function that satisfies:

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.

Andrew Wiles utilized modular forms to prove Fermat's Last Theorem by establishing a connection between elliptic curves and modular forms, known as the Modularity Theorem. This theorem states that every elliptic curve over the rational numbers is modular, meaning it can be associated with a unique modular form [38]. The Modularity Theorem was the cornerstone of Wiles's proof, as it allowed him to transfer the problem from the realm of elliptic curves to the well-understood theory of modular forms.

Further, modular forms have applications beyond Fermat's Last Theorem, including in string theory and the sphere packing problem [5]. The study of modular forms continues to be an active area of research, contributing to various fields of mathematics and theoretical physics.

3.4 Elliptic Curves

Elliptic curves are algebraic structures that have found applications in various branches of mathematics and computer science, including number theory and cryptography [34]. In the context of Fermat's Last Theorem, they play a pivotal role, particularly through their deep connection with modular forms [11].

An elliptic curve E over the field of rational numbers $\mathbb{Q}$ is defined by a cubic equation of the form $y^2 = x^3 + Ax + B$, where $A, B \in \mathbb{Q}$ and the discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$ to ensure the curve is non-singular [17].

The set of rational points on an elliptic curve, denoted $E(\mathbb{Q})$, forms an abelian group. The point at infinity serves as the identity element of this group. The structure of this group has been a subject of extensive study in number theory [34].

The Taniyama-Shimura-Weil conjecture, which was ultimately proved by Andrew Wiles, posits that every elliptic curve over $\mathbb{Q}$ is modular [47]. This means that there exists a modular form that corresponds to each elliptic curve, and the Fourier coefficients of this modular form encode information about the curve's rational points [11].

Wiles' proof of Fermat's Last Theorem hinged on this modularity property. He showed that if there existed a counterexample to Fermat's Last Theorem, it would lead to the construction of a non-modular elliptic curve, thereby contradicting the Taniyama-Shimura-Weil conjecture [47].

The study of elliptic curves and their properties has far-reaching implications. Their role in the proof of Fermat's Last Theorem serves as a testament to the interconnectedness of various mathematical disciplines [34].

4 The Statement of the Theorem

4.1 Formal Statement

Fermat's Last Theorem, one of the most famous theorems in the history of mathematics, posits that no three positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2. This conjecture was first scribbled by Pierre de Fermat in the margin of his copy of an ancient Greek text, "Arithmetica," in 1637. Fermat added that he had discovered "a truly marvelous proof of this proposition which this margin is too narrow to contain" [14, 32].

4.1.1 Special Cases and Generalizations

Over the centuries, the theorem has been proven for specific cases. Euler proved the theorem for $n = 3$, and Fermat himself had proven the case for $n = 4$. These special cases were solved using methods from elementary number theory [39, 2]. However, the general case eluded mathematicians for more than 350 years, becoming one of the most enduring challenges in the field.

4.1.2 Modern Formulations

In modern terms, the theorem is often stated using the language of algebraic number theory and modular forms. These mathematical structures were instrumental in Andrew Wiles' groundbreaking proof of the theorem in 1994. Wiles' proof utilized modular forms to establish a link between elliptic curves and

modular forms, thereby proving the Taniyama-Shimura-Weil [33] conjecture for semistable elliptic curves, which in turn proved Fermat's Last Theorem.

4.1.3 Impact and Relevance

The proof of Fermat's Last Theorem had far-reaching implications, not just in number theory but also in other areas of mathematics and cryptography [39, 2]. Its proof marked a significant milestone, resolving a problem that had been open for more than three centuries and demonstrating the depth and interconnectedness of modern mathematics.

5 The Proof

5.1 Modular Elliptic Curves

Modular elliptic curves are central to the proof of Fermat's Last Theorem. Andrew Wiles, in collaboration with Richard Taylor, proved that every semistable elliptic curve over the rational numbers is modular [22]. This monumental result confirmed the Shimura-Taniyama-Weil conjecture for semistable elliptic curves, which in turn implied Fermat's Last Theorem.

5.1.1 Wiles-Taylor Method

Wiles and Taylor's method involved a deep understanding of the modularity of elliptic curves. They utilized modular forms to construct a proof that was both intricate and elegant. The proof also made use of deformation theory and Hecke algebras [4]. The key equation that Wiles used can be represented as follows:

$$E : y^2 = x^3 + Ax + B \tag{4}$$

where E is an elliptic curve, and A and B are coefficients that satisfy $4A^3 + 27B^2 \neq 0$.

5.1.2 Implications for Number Theory

The proof had far-reaching implications, not just for Fermat's Last Theorem but also for number theory at large. It led to advancements in the understanding of elliptic curves and modular forms, and even had implications for Euclid's Infinitude of Primes [42]. One of the key equations that emerged from this work is:

$$L(E, s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \tag{5}$$

where $L(E, s)$ is the L-series associated with the elliptic curve E, N is the conductor, and a_p are Fourier coefficients [22].

5.2 The Role of Ribet's Theorem

5.2.1 Introduction and Historical Context

Ribet's theorem, originally known as the epsilon conjecture, is a cornerstone in number theory that links modular forms with Galois representations. Proposed by Jean-Pierre Serre and proven by Ken Ribet, this theorem was a pivotal step towards proving Fermat's Last Theorem (FLT) [30].

5.2.2 Mathematical Statement

The theorem can be mathematically stated as follows: Let f be a weight 2 newform on $\Gamma_0(qN)$ with an absolutely irreducible 2-dimensional mod p Galois representation $\rho_{f,p}$. Then, there exists a weight 2 newform g such that $\rho_{f,p} \simeq \rho_{g,p}$ [41]. In equation form, this can be represented as:

$$\rho_{f,p} \simeq \rho_{g,p} \tag{6}$$

5.2.3 Implications for Fermat's Last Theorem

Ribet's theorem implies that if an elliptic curve E has certain properties, then that curve cannot be modular. This was crucial for FLT, as it showed that a counterexample to FLT would create a curve that would not be modular [30]. Mathematically, if E is a counterexample to FLT, then:

$$E \ncong \text{Modular Curve} \tag{7}$$

5.2.4 Level Lowering

The theorem also discusses the concept of level lowering, stating that an elliptic curve of a certain conductor N does not guarantee the existence of another elliptic curve with rational Fourier coefficients [41]. This can be expressed as:

$$N(E) \neq N(E') \tag{8}$$

5.2.5 Contribution to Taniyama-Shimura-Weil Conjecture

Ribet's theorem proved that the Taniyama-Shimura-Weil conjecture implies FLT, thereby setting the stage for Andrew Wiles to prove FLT [30]. This relationship can be expressed as:

$$\text{Taniyama-Shimura-Weil Conjecture} \Rightarrow \text{FLT} \tag{9}$$

5.3 The Flaw and the Fix

In June 1993, Andrew Wiles initially announced his proof of Fermat's Last Theorem. However, a gap was discovered in the proof in September of the same year. The gap was related to the identification of a deformation ring with a Hecke algebra, a crucial step now referred to as an $R = T$ theorem.

5.3.1 The Gap

The gap in the original proof was in the part where Wiles tried to show that certain modular forms are also Galois representations. Mathematically, this can be represented as:

$$\phi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{C}) \tag{10}$$

where ϕ is a Galois representation. Wiles' original argument failed to establish this isomorphism for all cases.

5.3.2 The Fix

Wiles, along with his former student Richard Taylor, managed to fix the gap by incorporating additional techniques from algebraic geometry. They introduced a new tool, now known as the Taylor-Wiles method, to establish the $R = T$ theorem. The corrected proof can be summarized in the equation:

$$R \cong T \tag{11}$$

where R is the universal deformation ring and T is the Hecke algebra. This identification was crucial for the modularity lifting theorem, which was the cornerstone of Wiles' proof.

5.3.3 Impact

The method of identifying a deformation ring with a Hecke algebra has had a profound impact on algebraic number theory and has been generalized in various ways. The corrected proof was finally published in 1995, solidifying Wiles' monumental achievement.

6 Implications and Applications

6.1 Cryptography

Number theory is the backbone of modern cryptography, providing the mathematical underpinnings for many cryptographic algorithms. One of the most prominent examples is the RSA algorithm, which is widely used for secure data transmission and digital signatures [24].

6.1.1 RSA Algorithm

The RSA algorithm, named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman, is an asymmetric cryptographic algorithm that uses two different keys: a public key for encryption and a private key for decryption [31].

Mathematical Foundations: The RSA algorithm relies on the mathematical properties of prime numbers and their role in modular arithmetic. Specifically, it uses Euler's totient function $\phi(n)$, which is defined as the number of integers less than n that are coprime to n.

Key Generation:

1. Select two large prime numbers p and q.
2. Compute $n = p \times q$.
3. Compute $\phi(n) = (p-1) \times (q-1)$.
4. Choose an integer e such that $1 < e < \phi(n)$ and $\gcd(e, \phi(n)) = 1$. The pair (e, n) serves as the public key.
5. Compute d as $d \equiv e^{-1} \mod \phi(n)$. The pair (d, n) serves as the private key.

Encryption: Given a plaintext message m, the ciphertext c is computed using the public key as follows:

$$c \equiv m^e \mod n$$

Decryption: The decrypted message m is recovered using the private key as follows:

$$m \equiv c^d \mod n$$

The security of RSA is based on the computational difficulty of the integer factorization problem. Specifically, given n, it is computationally infeasible to find p and q in polynomial time [1].

Example: Let's consider a simple example to illustrate the RSA algorithm. Suppose $p = 53$ and $q = 59$, then $n = 3127$ and $\phi(n) = 3016$. Let $e = 3$ and $d = 2011$. To encrypt a message $m = 89$, we compute $c = 89^3 \mod 3127 = 1394$. To decrypt, we compute $m = 1394^{2011} \mod 3127 = 89$.

Applications in Modern Cryptography: RSA is widely used in various forms of secure data transmission, digital signatures, and secure key exchange. Its security and efficiency make it a standard choice in industry applications [24].

6.2 Other Areas of Mathematics

The proof of Fermat's Last Theorem has had a profound impact on various other areas of mathematics. Its techniques and results have found applications in several domains.

6.2.1 Algebraic Geometry

The proof introduced new methods in algebraic geometry, particularly through the use of elliptic curves. For example, the Weierstrass equation for elliptic curves is given by:

$$y^2 = x^3 + ax + b$$

This equation is central to the study of elliptic curves and has applications in coding theory [34].

6.2.2 Representation Theory

The Taniyama-Shimura-Weil conjecture, which was proven for semistable elliptic curves, has implications in representation theory. Specifically, it relates to the Langlands program, which aims to establish connections between Galois groups and automorphic forms [18].

6.2.3 Topology

The proof also has implications in topology, particularly in the study of 3-manifolds. The geometrization conjecture, which classifies all 3-manifolds, can be formulated using techniques similar to those used in the proof [44].

6.2.4 Number Theory

Beyond Fermat's Last Theorem itself, the proof has enriched the field of number theory, particularly in the study of Diophantine equations. For example, the equation $x^n + y^n = z^n$ can be generalized to other forms of Diophantine equations [13].

6.2.5 Computational Mathematics

The algorithms and techniques used in the proof have found applications in computational mathematics, particularly in the area of integer factorization and primality testing. For example, the AKS primality test is given by:

$$(a - b)^n \equiv a^n - b^n \mod n$$

This equation is used to test the primality of numbers [20].

7 Conclusion

The journey through the proof of Fermat's Last Theorem has been a monumental one, traversing various mathematical landscapes from modular forms to elliptic curves, and from algebraic equations to cryptography. This paper has aimed to provide a comprehensive overview of the theorem's history, its formal statement, and its modern implications.

The theorem, which posits that no three positive integers a, b, c can satisfy the equation $a^n + b^n = c^n$ for any integer $n > 2$, has been a cornerstone in the field of number theory. Its proof by Andrew Wiles in 1994 was a watershed moment, not just for the theorem itself but for mathematics as a whole. The proof utilized groundbreaking techniques in modular forms and elliptic curves, encapsulated by the equation $E : y^2 = x^3 + Ax + B$, where E is an elliptic curve.

The role of Ribet's theorem in setting the stage for Wiles cannot be overstated. Ribet's theorem, mathematically expressed as $\rho_{f,p} \simeq \rho_{g,p}$, provided

the crucial link between modular forms and Galois representations, thereby implying that a counterexample to Fermat's Last Theorem would contradict the Taniyama-Shimura-Weil conjecture.

The proof also had its share of drama, with a gap identified in the original proof. This gap was later fixed by Wiles and his former student Richard Taylor, using the equation $R \simeq T$, where R is the universal deformation ring and T is the Hecke algebra.

Beyond the theorem itself, the techniques used in its proof have found applications in various other areas of mathematics and computer science. In cryptography, for instance, the RSA algorithm relies heavily on number theory and modular arithmetic, expressed through Euler's totient function $\phi(n)$.

In summary, the proof of Fermat's Last Theorem serves as a testament to the interconnectedness of various mathematical disciplines. It not only resolved a centuries-old problem but also enriched our understanding of number theory, algebraic geometry, and even cryptography. As we continue to explore these mathematical landscapes, the theorem will undoubtedly continue to serve as a beacon, guiding us through the complexities and wonders of the mathematical world.

References

[1] Rsa algorithm in cryptography - geeksforgeeks.

[2] Oxford Academic. Fermat's last theorem: basic tools. *Bulletin of the London Mathematical Society*, 2015.

[3] Scientific American. Are mathematicians finally satisfied with andrew wiles's proof of ... *Scientific American*, 1999.

[4] Scientific American. Are mathematicians finally satisfied with andrew wiles's proof of ... *Scientific American*, 1999.

[5] arXiv. Lectures on modular forms and strings. *arXiv.org*, 2022.

[6] Avner Ash and Robert Gross. *Fearless Symmetry: Exposing the Hidden Patterns of Numbers*. Princeton University Press, 2006.

[7] E. T. Bell. *The Last Problem*. Mathematical Association of America, 1961.

[8] Encyclopedia Britannica. Pierre de fermat | biography & facts. *Encyclopedia Britannica*, 2023.

[9] Cambridge. On a few diophantine equations related to fermat's last theorem. *Canadian Mathematical Bulletin*, 2023.

[10] John Coates. Fermat's last theorem: A theorem's journey from obscurity to prominence. *Notices of the AMS*, 42:330–337, 1995.

[11] Gary Cornell and Joseph H. Silverman. *Modular Forms and Fermat's Last Theorem*. Springer, 1997.

[12] Gary Cornell, Joseph H. Silverman, and Glenn Stevens. Modular forms and fermat's last theorem. *Springer*, 1997.

[13] Henri Darmon. Diophantine equations and fermat's last theorem. *McGill University*, 2023.

[14] Christian Elsholtz. Fermat's last theorem implies euclid's infinitude of primes. *Tandfonline*, 2021.

[15] Catherine Goldstein. The history of fermat's last theorem. *Science in Context*, 15:485–506, 2002.

[16] Jeremy Gray. Fermat's last theorem. *SpringerLink*, 2023.

[17] Erwin Kreyszig. *Advanced Engineering Mathematics*. Wiley, 2010.

[18] Robert Langlands. The langlands program. *Notices of the AMS*, 2007.

[19] Michael S. Mahoney. The mathematical career of pierre de fermat, 1601-1665. *Project MUSE*, 2023.

[20] Nitin Saxena Manindra Agrawal, Neeraj Kayal. Primes is in p. *Annals of Mathematics*, 2002.

[21] Nikos Mantzakouras. Proof of fermat's last theorem (using 7 methods) - general solution for diophantine equation of degree n, with number of variables d. 06 2020.

[22] MIT Mathematics. 26 fermat's last theorem. *MIT Mathematics*, 2017.

[23] McGill. Infinite sums, diophantine equations and fermat's last theorem. *McGill*, 2023.

[24] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[25] Nature. The mathematician who proved why hippos waddle. *Nature*, 2016.

[26] J. J. O'Connor and E. F. Robertson. Pierre de fermat - biography. *MacTutor History of Mathematics*, 2023.

[27] Piergiorgio Odifreddi. *The Mathematical Century: The 30 Greatest Problems of the Last 100 Years*. Princeton University Press, 2004.

[28] ResearchGate. Diophantine equations and fermat's last theorem. *ResearchGate*, 2023.

[29] Paulo Ribenboim. The early history of fermat's last theorem. *SpringerLink*, 2023.

[30] Kenneth Ribet. From the taniyama-shimura conjecture to fermat's last theorem. *Annales de la faculté des sciences de Toulouse Sér. 5*, pages 116–139, 1990.

[31] Abhishek Saini and Dr Vandana. A study on modified rsa algorithm in network security. 4:1461–1465, 04 2022.

[32] ScienceDirect. Fermat's last theorem - an overview. *ScienceDirect Topics*, 2023.

[33] ScienceDirect. Fermat's last theorem, schur's theorem (in ramsey theory), and the ... *ScienceDirect*, 2023.

[34] Joseph H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, 2009.

[35] Ranber Singh. A marvelous simple proof of fermat's last theorem discovered. 04 2017.

[36] Simon Singh. *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathematical Problem*. Walker, 1997.

[37] Simon Singh. *The Proof of Fermat's Last Theorem*. Fourth Estate, 2002.

[38] American Mathematical Society. Modular forms and fermat's last theorem 1. history. *AMS Bulletin*, 1999.

[39] SpringerLink. Fermat's last theorem. *SpringerLink*, 2023.

[40] Math StackExchange. Proof of fermats last theorem for given exponent. *Math StackExchange*, 2023.

[41] Lenny Taelman. A herbrand-ribet theorem for function fields. *Inventiones Mathematicae - INVENT MATH*, 188, 04 2011.

[42] TandF. Fermat's last theorem implies euclid's infinitude of primes. *Taylor and Francis Online*, 2021.

[43] John Tate. Applications of fermat's last theorem. *Proceedings of the International Congress of Mathematicians*, 1:163–172, 1998.

[44] William P. Thurston. Three-dimensional geometry and topology. *Princeton University Press*, 1997.

[45] Unknown. Fermat's last theorem implies euclid's infinitude of primes. *Taylor & Francis Online*, 2021.

[46] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 142:443–551, 1995.

[47] Andrew Wiles. Modular elliptic curves and fermat's last theorem. *Annals of Mathematics*, 1995.