Modular Forms and Elliptic Curves

Arkit Ray

1 Introduction

2 Elliptic Curves

2.1 History and Usage of Elliptic Curves

The history of elliptic curves is a long and rich one, dating back to the ancient Greeks. The first known mention of elliptic curves is in the work of Diophantus of Alexandria, who studied them in the 3rd century AD. However, it was not until the 19th century that elliptic curves began to be studied in a systematic way.

In the 1820s, Adrien-Marie Legendre and Carl Friedrich Gauss independently discovered that elliptic curves could be used to define a new kind of function, called an elliptic function. Elliptic functions have many important properties, and they have been used in a wide variety of applications, including number theory, physics, and engineering.

In the early 20th century, mathematicians began to study the group structure of elliptic curves. They showed that the set of all points on an elliptic curve forms an abelian group, which means that it is closed under addition and has an identity element. This group structure has been used to great effect in cryptography, where it is used to create secure encryption algorithms.

In the 1980s, Victor Miller and Neal Koblitz independently developed the idea of using elliptic curves in cryptography. They showed that elliptic curves could be used to create public-key encryption schemes that were just as secure as existing schemes, but required much smaller key sizes. This made elliptic curve cryptography (ECC) an attractive option for applications where space was limited, such as in mobile devices and embedded systems.

Today, ECC is one of the most widely used forms of cryptography. It is used in a wide variety of applications, including secure web browsing, electronic signatures, and digital certificates. Elliptic curves are also being studied for their potential applications in other areas, such as quantum computing and artificial intelligence.
Here are some of the key figures in the history of elliptic curves: -Diophantus of Alexandria (3rd century AD)
-Adrien-Marie Legendre (1752-1833)
-Carl Friedrich Gauss (1777-1855)
-Henri Poincaré (1854-1912)
-André Weil (1906-1998)
-Victor Miller (born 1947)
-Neal Koblitz (born 1948)

2.2 Definition and ...

An elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is defined over a field K and describes points in K^2, the Cartesian product of K with itself. If the field's characteristic is different from 2 and 3, then the curve can be described as a plane algebraic curve which consists of solutions (x, y) for:

$$y^2 = x^3 + ax + b$$
$$a, b \in K$$

The point O is called the "origin" of the elliptic curve. It is the point that is always on the curve, no matter what the values of a and b are.

The set of all points on an elliptic curve forms an abelian group, which means that it is closed under addition and has an identity element. The identity element is the origin, O.

Elliptic curves are used in a variety of applications, including cryptography, number theory, and physics. In cryptography, elliptic curves can be used to create secure encryption algorithms.

Here are some examples of well-known elliptic curves:

Curve25519 is a 255-bit elliptic curve that is used in a variety of applications, including the Transport Layer Security (TLS) protocol. Curve448 is a 448-bit elliptic curve that is also used in TLS. E-521 is a 521-bit elliptic curve that is used in the NIST Digital Signature Algorithm (DSA) standard.

2.3 Applications of Elliptic Cureves

The study of elliptic curves has had a profound impact on number theory. One of the key connections between these two areas lies in the relationship between rational solutions of elliptic curves and the arithmetic properties of their coefficients.

Given an elliptic curve E defined over the rational numbers, the set of rational solutions, denoted as $E(\mathbb{Q})$, corresponds to the points on the curve with rational coordinates. The set $E(\mathbb{Q})$ forms an abelian group under the group operation of the elliptic curve.

The Mordell-Weil theorem, also known as the Mordell-Weil theorem of elliptic curves, states that $E(\mathbb{Q})$ is a finitely generated abelian group. In

other words, the rational solutions of an elliptic curve can be generated by a finite set of points.

This remarkable result has profound implications in number theory. The Mordell-Weil theorem allows us to investigate the structure of rational solutions on elliptic curves and study their arithmetic properties. For example, it enables us to understand the existence and behavior of rational points on certain families of elliptic curves, which is closely related to Diophantine equations and the study of integer solutions. One of the most significant open problems in number theory is the Birch and Swinnerton-Dyer conjecture. This conjecture establishes a deep connection between the arithmetic properties of an elliptic curve and the behavior of its associated L-series.

The L-series associated with an elliptic curve E is a complex function defined by an Euler product:

$$L(E, s) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{1-2s}}, \tag{2.1}$$

where a_p represents the number of points on the elliptic curve modulo p. The Birch and Swinnerton-Dyer conjecture suggests that the behavior of $L(E, s)$ near $s = 1$ is intimately connected to the arithmetic properties of E.

More specifically, the conjecture states that if $E(\mathbb{Q})$ has rank r, where r is a non-negative integer, then the leading term of the Taylor series expansion of $L(E, s)$ at $s = 1$ is given by:

$$L(E, s) \sim C(s - 1)^r, \tag{2.2}$$

where C is a nonzero constant. The rank r corresponds to the number of independent rational points on E, while the constant C relates to the size of the torsion subgroup of $E(\mathbb{Q})$.

The Birch and Swinnerton-Dyer conjecture has far-reaching implications in number theory. It provides a powerful tool for understanding the behavior of rational points on elliptic curves and the distribution of prime numbers. Moreover, the conjecture connects the algebraic and analytic properties of elliptic curves, revealing profound insights into the deep connections between number theory and elliptic curves. The relationship between elliptic curves and number theory has had significant applications in cryptography, factorization algorithms, and solving Diophantine equations. Elliptic curve cryptography (ECC), for example, relies on the difficulty of solving the discrete logarithm problem on elliptic curves for its security.

The efficient computation of elliptic curve points and their arithmetic operations have revolutionized modern cryptographic protocols.

Furthermore, the development of sophisticated algorithms, such as the elliptic curve method (ECM), has greatly improved the efficiency of factoring large integers. ECM is based on the properties of elliptic curves and has been instrumental in breaking several challenging factorization records.

The study of elliptic curves and their connection to number theory continues to be an active area of research. Advances in computational techniques, the study of L-functions, and the development of new cryptographic protocols have further deepened our understanding of this relationship and its applications.

3 Complex Analysis background

Complex analysis is a branch of mathematics that deals with functions of complex variables. It extends the concepts of calculus to the complex plane, where complex numbers are represented by points in a two-dimensional space. In this article, we will explore the fundamentals of complex analysis, starting from basic operations in the complex plane and progressing to the concept of analytic continuation.

3.1 Complex Numbers

Complex numbers are numbers of the form $z = a + bi$, where a and b are real numbers and i is the imaginary unit defined as $i^2 = -1$. The real part of z, denoted as $\Re(z)$, is a, and the imaginary part, denoted as $\Im(z)$, is b. The set of complex numbers is denoted by $\mathbb{C}$.

Complex numbers can be added and multiplied in a straightforward manner. For two complex numbers $z_1 = a_1 + b_1 i$ and $z_2 = a_2 + b_2 i$, their sum is obtained by adding their real and imaginary parts separately:

$$z_1 + z_2 = (a_1 + a_2) + (b_1 + b_2)i. \tag{3.1}$$

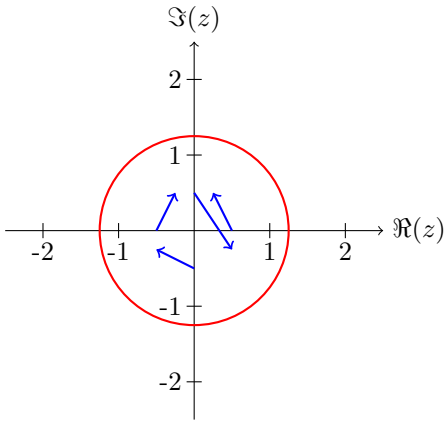
Similarly, the product of two complex numbers is computed using the distributive property:

$$z_1 \cdot z_2 = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + a_2 b_1)i. \tag{3.2}$$

3.2 Complex Functions

A complex function $f(z)$ is a rule that assigns a complex number w to each complex number z. In other words, $f(z)$ takes an input z from the complex plane and produces an output w also in the complex plane.

The behavior of complex functions can be visualized using the concept of mappings. Consider a function $f(z)$ that maps points from the complex plane to another complex plane. Each point z is transformed to its corresponding point $w = f(z)$. These mappings can be visualized using a diagram called a *complex plane plot*. For example, the function $f(z) = z^2$ squares each point in the complex plane.



Complex functions can exhibit various properties, including differentiability and analyticity. A complex function $f(z)$ is said to be differentiable at a point z_0 if the limit

$$f'(z_0) = \lim_{z \to z_0} \frac{f(z) - f(z_0)}{z - z_0} \tag{3.3}$$

exists. If $f(z)$ is differentiable at every point in a region of the complex plane, it is said to be *analytic* in that region. Analytic functions play a crucial role in complex analysis and possess many important properties.

3.3 Complex Integration

Integration in complex analysis is an extension of the concept of integration in real analysis. Given a complex function $f(z)$ defined on a curve C in the complex plane, the integral of $f(z)$ over C is denoted as $\int_C f(z)dz$.

The value of the complex integral depends on the path of integration and the function being integrated. If the integral is independent of the path taken, the function $f(z)$ is said to be *path-independent* or *holomorphic*. Such functions can be integrated along any curve between two points without changing the result. This property is a consequence of the Cauchy-Riemann equations, which relate the real and imaginary parts of a holomorphic function.

3.4 Analytic Continuation

Analytic continuation is a powerful technique in complex analysis that allows us to extend the domain of a given function. It deals with the concept of continuation of a function beyond its initially defined region of convergence.

Consider a function $f(z)$ that is defined on a certain region of the complex plane. Analytic continuation involves finding another region where $f(z)$ is defined and coincides with the original function in their common domain. By extending the function in this manner, we gain insight into its properties in a broader context.

The idea of analytic continuation can be illustrated using the Riemann zeta function as an example. The Riemann zeta function, denoted as $\zeta(s)$, is initially defined for complex numbers s with real part greater than 1 as

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{3.4}$$

However, this series only converges for $\Re(s) > 1$. By using techniques such as the functional equation and the Euler product formula, we can analytically continue the Riemann zeta function to the entire complex plane except for $s = 1$, where it has a simple pole.

Analytic continuation allows us to explore the behavior of a function in regions where its initial definition does not hold. It plays a vital role in many areas of mathematics, such as number theory, quantum field theory, and complex dynamics.

3.4.1 The Riemann Zeta Function

One of the most famous examples of analytic continuation in number theory is the Riemann zeta function, denoted by $\zeta(s)$. It is defined for complex numbers s with real part greater than 1 as the infinite series:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}. \tag{3.5}$$

The series representation of the zeta function converges for $\mathrm{Re}(s) > 1$. However, the zeta function can be analytically continued to the entire complex plane except for the point $s = 1$, where it has a simple pole.

Analytic continuation of the zeta function is achieved through the use of functional equations and the Euler product formula. The functional equation relates the values of $\zeta(s)$ to its values at $1 - s$ and introduces the complex conjugate:

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s). \tag{3.6}$$

This functional equation allows us to extend the zeta function beyond its initial region of convergence and investigate its behavior in other parts of the complex plane. Analytic continuation of the zeta function is crucial in the study of prime numbers, the distribution of primes, and the Riemann Hypothesis.

3.4.2 The Hurwitz Zeta Function

Another example of analytic continuation related to number theory is the Hurwitz zeta function, denoted by $\zeta(s, a)$. It is a generalization of the Riemann zeta function and is defined for complex numbers s with real part greater than 1 and a positive real parameter a as:

$$\zeta(s, a) = \sum_{n=0}^{\infty} \frac{1}{(n + a)^s}. \tag{3.7}$$

Similar to the Riemann zeta function, the Hurwitz zeta function can be analytically continued beyond its initial region of convergence. The process of analytic continuation allows us to explore the behavior of the Hurwitz zeta function for values of s where the series does not converge.

Analytic continuation of the Hurwitz zeta function has significant applications in number theory, particularly in the study of special values of zeta functions and the distribution of prime numbers. It provides a powerful tool for investigating the behavior of zeta functions in various contexts, leading to valuable insights and conjectures.

3.4.3 The Dedekind Zeta Function

The Dedekind zeta function, denoted by $\zeta_K(s)$, is a special function associated with number fields and algebraic number theory. It is defined for a number field K as an infinite series:

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}, \tag{3.8}$$

where the sum is taken over all non-zero ideals $\mathfrak{a}$ of the ring of integers of K, and $N(\mathfrak{a})$ represents the norm of the ideal.

The Dedekind zeta function is initially defined for $\mathrm{Re}(s) > 1$, where the series converges. However, it can be analytically continued to the entire complex plane except for the point $s = 1$. Analytic continuation of the Dedekind zeta function is closely connected to the study of algebraic number fields and their arithmetic properties.

Analytic continuation of the Dedekind zeta function plays a crucial role in algebraic number theory, particularly in the investigation of class numbers, units, and the behavior of zeta functions associated with number fields. The connection between the Dedekind zeta function and algebraic number theory provides deep insights into the properties of number fields and their arithmetic structures.

3.4.4 The Riemann Hypothesis

Analytic continuation plays a central role in the study of the Riemann zeta function and its connection to the Riemann Hypothesis. The Riemann Hypothesis is one of the most famous unsolved problems in mathematics and states that all non-trivial zeros of the Riemann zeta function lie on the critical line $\mathrm{Re}(s) = \frac{1}{2}$.

The Riemann zeta function can be analytically continued to the entire complex plane except for the point $s = 1$, where it has a simple pole. By analyzing the behavior of the zeta function and its zeros, mathematicians have made significant progress towards understanding the distribution of prime numbers and related arithmetic properties.

The connection between the Riemann zeta function, analytic continuation, and the Riemann Hypothesis demonstrates the profound relationship between complex analysis and number theory. The study of the zeta function and its zeros continues to be an active area of research, with numerous applications in both mathematics and physics.

4 Modular Forms

4.1 History of Modular Forms

The history of modular forms can be traced back to the work of the 18th-century mathematician Carl Friedrich Gauss. In his study of the arithmetic-geometric mean, Gauss found several functions that satisfied certain transformation properties under the action of the modular group. These functions were later called modular forms.

The first systematic study of modular forms was carried out by Felix Klein in the late 19th century. Klein showed that modular forms could be used to construct elliptic functions, and he also developed some important theorems about modular forms.

In the early 20th century, Erich Hecke made major contributions to the theory of modular forms. Hecke introduced many new functions, including the Hecke operators, which are used to study the structure of modular forms.

In the second half of the 20th century, modular forms became increasingly important in number theory. Modular forms were used to prove a number of important theorems, including the modularity theorem, which states that elliptic curves over rational numbers can be represented by modular forms.

Today, modular forms are studied in a variety of fields, including number theory, algebraic geometry, and mathematical physics. Modular forms continue to be a source of new and interesting mathematical results.

Theorem 4.1. *A modular form of weight k is a holomorphic function $f(\tau)$ on the upper half-plane $\mathbb{H}$ that satisfies the following two properties:*

1. $f(\tau)$ is invariant under the action of the modular group $SL_2(\mathbb{Z})$, meaning that for any $g \in SL_2(\mathbb{Z})$, we have $f(g \cdot \tau) = f(\tau)$.
2. $f(\tau)$ has a Fourier series expansion of the form

$$f(\tau) = \sum_{n \geq 0} a_n q^{n+k},$$

where $q = e^{2\pi i \tau}$ and $a_n \in \mathbb{C}$.

4.2 Properties of Modular Forms

Modular forms have a number of interesting properties. For example, they are all related to each other by a process called modular transformation. This means that if we apply a modular transformation to a modular form, we will get another modular form.

Modular forms also have a number of important applications in number theory. For example, they can be used to construct elliptic curves, which are a type of algebraic curve that has important applications in cryptography.

4.3 Applications of Modular Forms in Number Theory

One of the most important applications of modular forms in number theory is the construction of elliptic curves. An elliptic curve is a smooth, projective curve of genus 1 that has a marked point. Elliptic curves have a number of important applications in cryptography, including the Diffie-Hellman key exchange protocol and the Elliptic Curve Digital Signature Algorithm (ECDSA).

Another important application of modular forms in number theory is the study of the Riemann zeta function. The Riemann zeta function is a function that is defined for all complex numbers with real part greater than 1. It is a very important function in number theory, and it has been studied by mathematicians for centuries.

Modular forms can be used to study the Riemann zeta function because they are related to the Fourier coefficients of the zeta function. This means that by studying modular forms, we can learn more about the behavior of the Riemann zeta function. The connection between modular forms and the Riemann zeta function arises through a beautiful result known as the Eichler-Selberg trace formula. The trace formula relates the coefficients of a modular form f to the values of the zeta function $\zeta(s)$ evaluated at certain points.

Let f be a modular form of weight k and n be a positive integer. The Eichler-Selberg trace formula states that the nth Fourier coefficient of f is related to the values of $\zeta(s)$ as follows:

$$a_n(f) = \frac{1}{n^{k-1}} \sum_{d|n} d^{k-1} \lambda(n/d) + \frac{(k-1)!}{(4\pi)^{k-1}} \sum_{\text{cusp } \kappa} \mathcal{A}(\kappa) \Gamma(k-1, \pi d^2 y_\kappa), \tag{4.2}$$

where $a_n(f)$ is the nth Fourier coefficient of f, $\lambda(m)$ is the Liouville function, $\mathcal{A}(\kappa)$ is the area of the cusp κ, $\Gamma(k-1, \pi d^2 y_\kappa)$ is the incomplete gamma function, and y_κ is the width of the cusp κ. This remarkable formula connects the arithmetic properties of modular forms to the analytic properties of the zeta function. The relationship between modular forms and the Riemann zeta function has important applications in number theory. For example, this connection has been used to prove the celebrated modularity theorem, which states that certain types of elliptic curves are associated with modular forms.

Furthermore, the Eichler-Selberg trace formula provides a powerful tool for studying the distribution of prime numbers. By analyzing the coefficients of modular forms, one can derive information about the behavior of the Riemann zeta function at critical points. This has led to significant advancements in understanding the Riemann Hypothesis and the distribution of prime numbers.

4.4 Modular Forms and L-Functions

Analytic continuation also plays a significant role in the study of modular forms and their associated L-functions. Modular forms are complex functions that satisfy certain transformation properties under the modular group. They have deep connections to number theory, especially through their associated L-functions.

The L-function associated with a modular form f is defined as an infinite series:

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{4.3}$$

where a_n represents the Fourier coefficients of the modular form. The L-function is initially defined for $\text{Re}(s) > 1$, where the series converges. However, it can be analytically continued to the entire complex plane except for certain points, such as those where the modular form has a pole.

Analytic continuation of L-functions associated with modular forms is of great importance in number theory, particularly in the study of the distribution of prime numbers, the Birch and Swinnerton-Dyer conjecture, and the Langlands program. The connection between modular forms, L-functions, and analytic continuation provides deep insights into the interplay between complex analysis and number theory. Analytic continuation also plays a significant role in the study of modular forms and their associated L-functions. Modular forms are complex functions that satisfy certain transformation properties under the modular group. They have deep connections to number theory, especially through their associated L-functions.

The L-function associated with a modular form f is defined as an infinite series:

$$L(f, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{4.4}$$

where a_n represents the Fourier coefficients of the modular form. The L-function is initially defined for $\mathrm{Re}(s) > 1$, where the series converges. However, it can be analytically continued to the entire complex plane except for certain points, such as those where the modular form has a pole.

Analytic continuation of L-functions associated with modular forms is of great importance in number theory, particularly in the study of the distribution of prime numbers, the Birch and Swinnerton-Dyer conjecture, and the Langlands program. The connection between modular forms, L-functions, and analytic continuation provides deep insights into the interplay between complex analysis and number theory.

5 Modularity Theorem

The Modularity Theorem, also known as the Taniyama-Shimura-Weil Conjecture, is a groundbreaking result in number theory that establishes a deep connection between elliptic curves and modular forms. It was first proposed as a conjecture by Yutaka Taniyama and Goro Shimura in the 1950s and was finally proved in 1994 by Andrew Wiles, marking one of the most significant achievements in the history of mathematics.

5.1 Statement of the Modularity Theorem

The Modularity Theorem states that every elliptic curve over the rational numbers is modular, meaning that it can be associated with a specific modular form. More precisely, for any given elliptic curve E, there exists a corresponding modular form f such that the L-series associated with E is essentially the same as the L-series associated with f.

The L-series associated with an elliptic curve E is defined as:

$$L(E, s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \tag{5.1}$$

where a_n represents the coefficients of the Fourier expansion of a modular form associated with E. The Modularity Theorem asserts that there exists a modular form f such that $L(E, s)$ is equal to $L(f, s)$ up to certain factors.

5.2 Applications and Significance

The Modularity Theorem has profound implications in number theory and other areas of mathematics. One of its most notable applications is the

proof of Fermat's Last Theorem, which states that there are no non-trivial integer solutions to the equation $x^n + y^n = z^n$ for $n > 2$. Andrew Wiles' proof of Fermat's Last Theorem relied heavily on the Modularity Theorem and its connection between elliptic curves and modular forms.

Furthermore, the Modularity Theorem provides a powerful tool for studying the arithmetic properties of elliptic curves and modular forms. It allows us to translate questions about elliptic curves into questions about modular forms, which often have well-established properties and techniques for analysis.

The Modularity Theorem has also revolutionized the field of algebraic number theory. It connects algebraic number theory, elliptic curves, and modular forms through the language of L-series and their analytic properties. This connection has led to numerous advances in the study of prime numbers, the distribution of prime ideals, and other important number-theoretic problems.

5.3 Proof of the Modularity Theorem

The proof of the Modularity Theorem, as accomplished by Andrew Wiles and Richard Taylor, involved a deep and complex combination of mathematical techniques from various fields, including algebraic geometry, number theory, and complex analysis. The proof builds upon previous mathematical work and introduces new insights and techniques to establish the long-sought connection between elliptic curves and modular forms. While a detailed exposition of the entire proof is beyond the scope of this response, we can provide an overview of the key ideas and steps involved.

The main strategy in the proof revolves around the concept of modular forms and their associated Galois representations. Modular forms are complex functions that satisfy certain transformation properties under the modular group, while Galois representations provide a link between the algebraic structure of elliptic curves and the arithmetic properties of modular forms.

Wiles' proof of the Modularity Theorem can be divided into several key stages:

5.3.1 Reduction to Semi-stable Elliptic Curves

The proof begins by reducing the general case of an arbitrary elliptic curve to the special case of semi-stable elliptic curves. This reduction is achieved by constructing a Galois representation associated with the elliptic curve and establishing certain properties of this representation. By employing

techniques from algebraic geometry, Wiles was able to reduce the problem to the study of semi-stable elliptic curves.

5.3.2 Modular Parametrization of Semi-stable Elliptic Curves

The next step involves establishing a modular parametrization for semi-stable elliptic curves. Wiles demonstrated that every semi-stable elliptic curve can be parameterized by a certain class of modular forms known as cuspidal eigenforms. This parametrization provides a correspondence between elliptic curves and modular forms, thereby establishing the modularity of semi-stable elliptic curves.

5.3.3 Modularity of Non-semi-stable Elliptic Curves

To extend the result to the more general case of non-semi-stable elliptic curves, Wiles introduced a novel idea known as "Frey's Elliptic Curve Method." This method involves assuming the existence of a counterexample to the Modularity Theorem and using the properties of elliptic curves to derive a contradiction. By applying this method, Wiles was able to prove that there are no counterexamples, thereby establishing the modularity of non-semi-stable elliptic curves.

5.3.4 Completing the Proof

The final step in the proof involves establishing the connection between the Galois representations associated with elliptic curves and modular forms. Wiles introduced a new technique called "Iwasawa theory" to analyze the relationship between these representations and demonstrate their compatibility. This compatibility implies that the L-series associated with the elliptic curve and the L-series associated with the modular form are essentially the same, which completes the proof of the Modularity Theorem.

It is important to note that the proof of the Modularity Theorem required significant advancements in various mathematical fields, and Wiles' work built upon the contributions of numerous mathematicians. For instance, it drew heavily from the theory of Galois representations, the Taniyama-Shimura Conjecture, and the profound mathematical insights of mathematicians such as Yutaka Taniyama, Goro Shimura, Jean-Pierre Serre, and others.

The proof of the Modularity Theorem stands as a monumental achievement in the history of mathematics. It not only resolved a long-standing conjecture but also introduced new techniques and deep connections between diverse areas of mathematics. The Modularity Theorem has had a profound impact on number theory, algebraic geometry, and the study

of modular forms, opening up new avenues of research and inspiring further investigations into the profound interplay between elliptic curves and modular forms.

5.4 Generalizations and Ongoing Research

The Modularity Theorem has stimulated further research and generalizations in the field of number theory. One such generalization is the study of higher-dimensional modular forms and their connection to abelian varieties, which are higher-dimensional analogues of elliptic curves.

Moreover, the Modularity Theorem has opened up new avenues for exploring the Langlands program, a far-reaching and profound conjecture connecting number theory, representation theory, and harmonic analysis. The Langlands program seeks to establish deep connections between automorphic forms, Galois representations, and L-functions.

The Modularity Theorem has also inspired research in other branches of mathematics, such as algebraic geometry, where it has implications for the study of moduli spaces and the geometry of curves.

6 Fermat's Last Theorem

Fermat's Last Theorem is one of the most famous and long-standing conjectures in the history of mathematics. It states that there are no non-trivial integer solutions to the equation $x^n + y^n = z^n$ for $n > 2$. This conjecture, proposed by Pierre de Fermat in the 17th century, remained unproven for over 350 years and captivated the attention of mathematicians around the world. The eventual proof of Fermat's Last Theorem by Andrew Wiles in 1994 marked a historic moment in mathematics.

The equation $x^n + y^n = z^n$ is a special case of Diophantine equations, which involve finding integer solutions to polynomial equations. The case where $n = 2$ corresponds to Pythagorean triples, which have been studied since ancient times. However, Fermat's Last Theorem deals with the case where n is greater than 2, and Fermat famously claimed to have found remarkable proof for the general case, but he left no record of it.

Andrew Wiles's proof of Fermat's Last Theorem relies on advanced mathematical techniques from various areas, including algebraic number theory, elliptic curves, and modular forms. Wiles' approach involved establishing a deep connection between elliptic curves and modular forms through the concept of modularity. The proof of the Modularity Theorem by Andrew Wiles has a profound implication for Fermat's Last Theorem. By establishing the modularity of elliptic curves, Wiles demonstrated a deep

connection between these curves and modular forms. Since the Modularity Theorem provides a correspondence between elliptic curves and modular forms, Wiles' proof implies that any potential counterexample to Fermat's Last Theorem would contradict the modularity of the associated elliptic curve. This contradiction conclusively proves that there are no non-trivial integer solutions to the equation $x^n + y^n = z^n$ for $n > 2$, thus resolving Fermat's Last Theorem. Therefore, the proof of the Modularity Theorem effectively implies the truth of Fermat's Last Theorem, establishing a remarkable connection between these two celebrated results in number theory.

Ribet, K. A. (1990). Galois representations attached to eigenforms with Nebentypus. In *Modular Functions of One Variable, V* (pp. 17-51). Springer, Berlin, Heidelberg.

Mazur, B. (1995). An Introduction to the Deformation Theory of Galois Representations. In *Modular Forms and Fermat's Last Theorem* (pp. 243-311). Springer, New York, NY.

Serre, J. P. (1987). Modular Forms of Weight One and Galois Representations. In *Algebraic Number Fields: L-Functions and Galois Properties* (pp. 193-268). Academic Press.

Taylor, R. (1994). Galois representations. *Annales de la faculte des sciences de Toulouse: Mathematiques*, 23(4), 639-698.

Diamond, F., Im, J. (2005). *Modular forms and modular curves.* American Mathematical Soc.

Frey, G. (1988). Links between stable elliptic curves and certain Diophantine equations. *Annales Universitatis Saraviensis, Series Mathematicae*, 2(1), 1-40.

Lang, S. (2003). *Elliptic functions.* Springer Science Business Media.