A Survey of the Taniyama-Shimura Conjecture

Kady Schneiter
Utah State University

Follow this and additional works at: https://digitalcommons.usu.edu/gradreports

Part of the Mathematics Commons

Recommended Citation
https://digitalcommons.usu.edu/gradreports/1281

This Report is brought to you for free and open access by the Graduate Studies at DigitalCommons@USU. It has been accepted for inclusion in All Graduate Plan B and other Reports by an authorized administrator of DigitalCommons@USU. For more information, please contact digitalcommons@usu.edu.
A Survey of the Taniyama-Shimura Conjecture

by

Kady Schneiter

A report submitted in partial fulfillment
of the requirements for the degree
of
Master of Science
in
Mathematics

UTAH STATE UNIVERSITY
Logan, Utah
2000
A Survey of the Taniyama Shimura conjecture

Kady Schneiter

April 17, 2000
Contents

I The History

I.1 Introduction ................................................. 5
I.2 Historical Background .......................................... 7
  I.2.1 Pierre de Fermat ........................................ 7
  I.2.2 Evariste Galois ......................................... 10
  I.2.3 Henri Poincare ......................................... 12
  I.2.4 Yutaka Taniyama and Goro Shimura .................... 14
  I.2.5 Andre Weil ............................................ 17
  I.2.6 Recent History ......................................... 18
  I.2.7 Andrew Wiles .......................................... 20
  I.2.8 The Full Proof ......................................... 22
II The Mathematics

II.1 Elliptic Curves ............................................. 24
  II.1.1 Structure ............................................. 24
  II.1.2 Weierstrass Form ..................................... 26
  II.1.3 Valuation ............................................. 28
  II.1.4 Minimal Weierstrass Form ............................ 30
  II.1.5 Reduction ............................................ 32
  II.1.6 Conductor ............................................ 35
  II.1.7 Rational Roots ...................................... 36
II.2 Modular Forms ............................................ 37
II.3 The Conjecture ............................................ 39
  II.3.1 Statement of the Conjecture .......................... 39
  II.3.2 Modularity of an elliptic curve with conductor 11 39
List of Figures

II.1 Group operation of an elliptic curve ............................. 27

II.2 Non-singular elliptic curve: $E : y^2 = x^3 - 4x, \Delta = 4096$ .................. 29

II.3 Elliptic curve with cusp only: $E : y^2 = x^3, \Delta = 0, c_4 = 0$ .............. 30
List of Tables

II.1 Classification of elliptic curves ........................................... 33
II.2 Rational points for a curve with conductor $N = 14$ ......................... 37
II.3 Rational points for a curve with conductor $N = 166$ ........................ 37
II.4 Prime power term coefficients of Fourier series for modular forms of level $N$ ........................ 39
II.5 Rational points of an elliptic curve with conductor $N = 11$ ................. 42
Chapter I

The History

I.1 Introduction

Perhaps the most famous problem in all of mathematics is the theorem that states that the equation $a^n + b^n = c^n$ has no non-trivial solutions for integers $a$, $b$, and $c$, and $n \geq 2$. This theorem was proposed by a seventeenth century French mathematician named Pierre de Fermat. Though the theorem is easy to understand, the proof has been elusive. Over the past 350 years many mathematicians have attempted to prove Fermat's theorem. They have used a variety of methods and many have been successful in proving the theorem in specific cases. However, until 1994, nobody had produced an accurate proof for the theorem in the general case. Because the theorem resisted proof for so long, it became known as Fermat's last theorem.

Interestingly, though the theorem has generated very much excitement over the years, it is of little inherent importance. Indeed, Fermat's last theorem has few, if any, important implications even within the field of number theory. John Coates of Cambridge University
has said, “not all mathematical problems are useless. Fermat’s one really is useless, I think, in a certain sense. It’s got no practical value whatsoever [10, p.6].” For most of its history, the chief allure of the theorem was simply its resistance to proof. However, in the mid-1980’s, through the work of Gerhard Frey, Jean-Pierre Serre and Kenneth Ribet, Fermat’s last theorem was linked to one of the most important conjectures in modern number theory, the Taniyama-Shimura conjecture. The work of these mathematicians showed that Fermat’s Last theorem and a specific case of the Taniyama-Shimura conjecture (for semi-stable elliptic curves) are mutually implicative. That is, if one is true, then so is the other. This meant if the Taniyama-Shimura conjecture were proved, the 350-year-old Fermat problem would follow.

Simply put, the Taniyama-Shimura conjecture states that all elliptic curves are modular. Elliptic curves are cubic equations in two variables of the form $y^2 = x^3 + ax^2 + bx + c$ where $a$, $b$, and $c$ are rational numbers. Modular forms, which will be defined more precisely later on, are “functions on the complex plane that are inordinately symmetric [10, p.8].” The two concepts appear at first to be unrelated, but the Taniyama-Shimura conjecture asserts that, in fact, they are very closely connected.

The Taniyama-Shimura conjecture has been used as a foundation to build some of the most innovative ideas in modern mathematics. Andrew Wiles, a professor at Princeton University had a lifelong ambition to prove Fermat’s last theorem. Once the link between the theorem and the conjecture was established, he began to see how this goal might be accomplished. Though he was motivated by his interest in Fermat’s last theorem, Wiles also made great progress toward a complete proof of the Taniyama-Shimura conjecture.

It is the purpose of this paper to give an explanation of the historical setting in which
the Taniyama-Shimura conjecture arose, the background of some of the mathematicians who contributed to its proof, and some of the mathematics involved in the conjecture.

I.2 Historical Background

One of the many intriguing qualities of the Taniyama-Shimura conjecture is the number of mathematicians whose work was involved in its proof. Among the mathematicians who influenced, directly or indirectly, the completion of the proof of the Taniyama-Shimura conjecture were Pierre de Fermat, Henri Poincare, and Evariste Galois. Additionally, many prominent twentieth century mathematicians, including Barry Mazur of Harvard University, Kenneth Ribet of the University of California at Berkeley, and Andrew Wiles of Princeton University, have contributed to the work. As a means of orienting ourselves with our topic, we will begin with a historical account of the conjecture and of some of the mathematicians whose work was important to it.

I.2.1 Pierre de Fermat

The history of the Taniyama-Shimura conjecture is inseparably connected with the work of many mathematicians. The most well-known of these is perhaps the seventeenth-century mathematician Pierre de Fermat.

The well-known biographer of mathematicians Eric Temple Bell has called Pierre de Fermat "the greatest mathematician of the seventeenth century [3, p.56].” He is also one of the most widely known mathematicians of all time. He accomplished such great feats as developing differential calculus years before the birth of either Newton or Leibniz. He
independently invented analytic geometry. With Pascal, he created modern mathematical probability, and he is the founder of number theory. With so many accomplishments to his credit, it is no wonder that his fame is so far-reaching.

Pierre de Fermat was born in Beaumont de Lomagne, France, in August of 1601. His early academic endeavors were conducted at home in his native town. Later, he continued his studies in Toulouse. Despite the many varied and important contributions that Fermat made to the study of mathematics, very little is known about his education and upbringing. However, because he made discoveries far beyond the knowledge of most mathematicians in his time, his educational background could have had little influence on his successes. "The fields in which he did his greatest work, not having been opened up while he was a student, could scarcely have been suggested by his studies [3, p.58]."

Fermat married in 1631 and in that same year became a commissioner of requests at Toulouse. Later he was promoted to a king's councillorship in the local parliament of Toulouse. His life was peaceful and full of hard work. Mathematics was for Fermat, a hobby, a means of resting from his political work. Though he studied mathematics only for amusement or relaxation, Fermat was amazingly prolific in his mathematical works and produced results that continue to be important to the mathematical community today.

Fermat's connection with the Taniyama-Shimura conjecture is indirect though extremely important. In about the year 1637 he produced what has become known as Fermat's last theorem (last because it was the last to have a known proof, not because it was his final work). He asserted that the equation \( a^n + b^n = c^n \) has no non-trivial solutions for integers \( a, b, \) and \( c, \) and \( n \geq 3. \) Fermat recorded his observation in the margin of his copy of Diophantus's Arithmetica and added that he had a proof of the assertion, which was too
lengthy to fit into the margin. His proof has never been found and there is some question among mathematicians as to whether he actually had a valid proof. Certainly, if he did, it was not the same as the proof provided by Andrew Wiles in 1994. Wiles' proof, as we shall see, involved some of the most advanced math of the twentieth century, in particular, the Taniyama-Shimura conjecture. This is mathematics that was certainly beyond Fermat's reach in the 1600s.

Speaking of the field of number theory, Barry Mazur has said, "The field produces, without effort, innumerable problems which have a sweet, innocent air about them, tempting flowers; and yet...the quests for the solutions of these problems have been known to lead to the creation (from nothing) of theories which spread their light on all of mathematics [9, p.593]." Fermat's last theorem is just such a problem. It has inspired many of the world's greatest mathematicians to try their hands at it. The list of these mathematicians includes: Leonhard Euler, Sophie Germain, Peter Dirichlet, Henri Lebesgue, Ernst Eduard Kummer, and Andrew Wiles.

Over the years, experienced and novice mathematicians have produced a huge number of incorrect proofs of the theorem. Many have tried to use high school mathematics, some have used more advanced methods, some people have even claimed to have found their proofs via revelations or psychic powers. In addition to those who have tried to find the proof themselves, many people have offered rewards for a correct proof. At various times cash prizes have been available to any person who produces a rigorous proof of the theorem.
1.2.2 Evariste Galois

The connection between elliptic curves and modular functions was studied in large part through the work of the nineteenth century mathematician Evariste Galois. In his work on the proof of the Taniyama-Shimura conjecture, Andrew Wiles wanted to show that there are the same number of elliptic curves and modular elliptic curves. He found that he could count them more easily by converting them into algebraic structures known as Galois representations.

Evariste Galois was a nineteenth century mathematician who contributed greatly to the field of algebra. Though he died when he was only twenty, his enterprising work was far ahead of his time and continues to have unexplored implications in the twentieth century.

Evariste Galois was born in Bourg-la-Reine, France (just outside Paris) on October 25, 1811. His father Nicolas-Gabriel Galois was intellectual, anti-royalty and a lover of liberty. He became mayor of the town where he lived, but after being disgraced through the intrigues of a corrupt priest, became disillusioned with his life and committed suicide.

Adelaide-Marie Demante, Galois' mother, was his only teacher until he was 12 years old. She had received a religious and classical education from her father and passed these on to Evariste. She died in 1872 at the age of 84.

After leaving his mother's tutelage, Galois' education was stormy and difficult. At age twelve, he entered the Lycee of Louis-le-Grand in Paris. The environment at the school was restrictive and very controlled. The tyranny under which he lived made him more liberal in his views. At first, Galois won prizes in his studies of the classics, but eventually, his success was replaced by boredom. His teachers advised that Galois be demoted.
His aptitude for mathematics was apparent from an early age. As a young teen he read Legendre from cover to cover and mastered it. Most young men in his school took on average two years to understand the work. He also read Lagrange and Abel when he was 14 or 15 years old, but was contemptuous of the schoolbook algebra. Purportedly because of lack of intellectual stimulation, his schoolwork was mediocre.

He had an interesting and useful ability to think about mathematical questions in his head before committing them to paper. However, he was not careful with what he considered to be the more trivial details. People around him found him strange and claimed that he had “affected” originality.

Galois dreamed of entering l’Ecole Polytechnique, the most prestigious school in France. He believed that there he would find people who understood him and who could help him to advance his work. However, when he took the entrance exams for the school, his habit of working things out in his head put him at a disadvantage. The test was conducted at the chalkboard. And there he was unable to supply the details that his examiners required of him. He took the exam the allowable two times and after realizing that he would fail for the second time, threw the eraser in the examiner’s face. One of the most brilliant minds of his time, Galois was denied entrance to l’Ecole Polytechnique. Later, Terquem, the editor of “Nouvelles annales de Mathematiques” (a journal connected with the school) said, speaking in reference to Galois’ case, “a candidate of superior intelligence is lost with an examiner of inferior intelligence [3, p.367].”

Unable to continue in school, Galois tried to become a private tutor, giving lessons in algebra, but no one wanted him.
Bitterness at his failure to gain access to the school and at the death of his father turned Galois to the republican cause. He was arrested several times for his involvement in the movement. Once he was charged with a threat on the life of the King, and later he was taken without charge because he was considered dangerous. While on parole from Prison, Galois met a girl and fell in love with her. It appears that the girl became involved with Galois through a royalist plot to get rid of a man they considered to be a dangerous revolutionary. Galois was challenged to a duel over the girl’s honor and was thus caught in the plan for his destruction.

The night before the duel was to occur, Galois hurriedly wrote down his theories. He then sent them together with some of his other manuscripts to his friend Auguste Chevalier.

Participating in the duel, Galois was shot in the abdomen. He died the next day, May 31, 1832. He was twenty years old.

The work that Galois sent to his friend was edited and published by Joseph Lousiville in 1846. It contained far-reaching results in the theory of solutions to equations. He introduced a tool to use to determine whether a given equation can be solved by radicals. These results, called Galois theory, proved to play a fundamental role in the proof of the Taniyama-Shimura conjecture.

I.2.3 Henri Poincare

Early work into the area of the modular functions was conducted by the renowned mathematician Henri Poincare. Poincare was another mathematician of extraordinary ability and influence. He has been labeled by Bell, “the last universalist [3, p.526],” meaning that he
was the last mathematician to master and make contributions in all areas of mathematics. Poincare was born in Nancy, Lorraine, France, April 29, 1854. Like Galois, he was principally tutored by his mother in his early childhood. His brilliance was apparent at a young age. However, his interest was not initially directed toward mathematics. In elementary school he was intrigued by natural history. He began to show his aptitude for mathematics around age 15.

Poincare, like Galois, possessed the ability to do complicated mathematical reasoning in his head, without putting anything down on paper. And like Galois, Poincare’s genius was often overlooked in his early years. Many people described him as absent-minded and he scored abysmally on the Binet intelligence test. He received his first degree, bachelor of letters and science, at the age of seventeen though he nearly failed in math.

By the time Poincare took his examinations for L’Ecole Polytechnique, the school had learned from its experiences with Galois. Had it not been for his great renown as a mathematician, Poincare too would have been denied entrance to the university. The head examiner commented, “Any student other than Poincare would have been plucked [3, p.535].”

Poincare did important work in the study of automorphic functions of which modular forms are a subset. However, his research was not limited to this area of inquiry, nor even to mathematics. In fact, his scope of study was very broad. He made progress in the fields of analysis, number theory, algebra, and mathematical astronomy.

Poincare’s genius was widely recognized during his lifetime. He became a renowned authority on many areas of public concern in addition to mathematics.

On July 17, 1912, at the age of 58, Poincare suffered an embolism and died. However, his
many contributions to the field of mathematics insure that he will maintain an important position in the history of science.

### 1.2.4 Yutaka Taniyama and Goro Shimura

The two men for whom the Taniyama-Shimura conjecture is named were contemporaries and colleagues at the University of Tokyo in the 1950s. This was a time when Japanese university students relied heavily on each other for support and motivation, feeling that the older professors had very little desire or ability to be of help [11, p.]. In this environment, Yutaka Taniyama and Goro Shimura formed a friendship and began to collaborate in the areas of mathematics that would produce this conjecture. Since Taniyama died young and relatively unknown, it is principally from Shimura’s reminiscences of their friendship in “Yutaka Taniyama and his time: Very Personal Recollections” that the following information was collected.

Yutaka Taniyama was born to Sahei and Kaku Taniyama on November 12, 1927. His father was a country doctor in Kisai, Japan, where Taniyama was born and raised. Little information is available about his early years in Kisai, but it is known that he contracted tuberculosis in high school and was consequently delayed two years in graduating. As a result of his years of sickness, Taniyama was somewhat older than his peers when he entered the University of Tokyo to study mathematics. Shimura also attended the University of Tokyo and was one year ahead of Taniyama, though Shimura was the younger of the two men.

Although Shimura has asserted that the professors at the University of Tokyo were seldom inspiring and had little concern for the work of the students there, Taniyama once wrote that his interest in number theory was influenced by Masao Sugawara, a professor from whom he
took an algebra course.

The first non-elementary paper that Taniyama wrote was entitled “On n-division of abelian function fields” and served as a sort of senior thesis, though none was required. The paper was a proof of the Mordell-Weil theorem and was based on the ideas of Hasse and Weil. Shimura believed that at that time Taniyama knew more about the topic than any other person in Japan [11, p.189].

After his graduation in 1953, Taniyama stayed on at the University of Tokyo as a special research assistant. Shimura, who also remained as an assistant, later said, “Whatever positions we held, our real status in 1954-1955 was, in all practical senses, that of graduate students with no advisor, but with a certain teaching load [11, p.188].” Eventually Taniyama reached the status of associate professor, the position he held at the time of his death in 1958.

Personally Taniyama was unexceptional. He enjoyed classical music and going to the movies. He had few extracurricular hobbies, but enjoyed writing about academic matters.

As a mathematician he kept odd hours, working late into the night. Shimura said that one of his enviable characteristics was the ability to make useful mistakes, “Though he was by no means a sloppy type, he was gifted with the special capability of making many mistakes, mostly in the right direction [11, p.190].”

Although Shimura and Taniyama studied math at the same university, they were not closely associated until after their graduation when they were brought together by similar research interests. In 1957, they published a joint work in Japanese entitled, “Modern Number Theory.” They had hoped to translate the paper into English, but Taniyama did
not live long enough to accomplish this goal.

Though at the time of his death he had only reached the position of associate professor, Taniyama left behind him a significant contribution to mathematics. The International Symposium on Algebraic Number Theory which was held in Tokyo and Nikko in September of 1955, was principally organized by Taniyama and Shimura. At the symposium, participants received copies of thirty-six problems, four of which had been posed by Taniyama. From two of these problems which concerned automorphic functions, originated what has been known as the Taniyama-Shimura conjecture.

It was years after the Tokyo-Nikko conference that the importance of Taniyama’s work began to be apparent. Unfortunately, he did not live long enough to expand upon his ideas or provide proof of his intuitions. On November 17, 1958, Taniyama was found dead in his apartment. He had committed suicide. He left behind a lengthy note disposing of his possessions, explaining what point he had reached in his lectures at the university, and apologizing for any inconvenience or unhappiness caused by his death. In regards to reasons for his suicide, he said, “I am in a frame of mind that I lose confidence in my future [11, p.193].”

At the time of his death, he was planning to marry Misako Suzuki. A few weeks later in early December, 1958, she too committed suicide.

Shimura had left Japan some time before Taniyama’s death. He eventually became a professor at Princeton University.

In the 1960s, Shimura, who had continued his research in number theory, again looked at the problems proposed by Taniyama at the Tokyo-Nikko conference. Shimura corrected
the errors he found in the problems, specified the rational numbers as the domain of the elliptic curves and formulated “a different, bolder, and more precise conjecture [8, p. ].” His conjecture was that elliptic curves over the rational numbers are modular. Modular forms are more specific than the automorphic functions that appeared in Taniyama’s problems. This work by Shimura resulted in the familiar form of the Taniyama-Shimura conjecture.

1.2.5 Andre Weil

It was Taniyama who originally put forth the basic presumptions of the conjecture and Shimura who formulated it into its present condition. However, in addition to the titles the “Taniyama-Shimura conjecture,” or the “Shimura-Taniyama conjecture,” the work has sometimes been referred to as the “Taniyama-Weil conjecture,” or the “Taniyama-Shimura-Weil” conjecture. Although these titles may imply otherwise, Andre Weil had very little to do with the formulation of the conjecture. In fact, he made statements which show that he did not agree with the theories of Taniyama as put forth in the conjecture. For instance, when Shimura asked Weil’s opinion of the plausibility of the modularity of elliptic curves, Weil commented, “I don’t see any reason against it, since one and the other of these sets are denumerable, but I don’t see any reason for this hypothesis [8, p.1301].”

In explanation of why his name is associated with the conjecture in question, Weil said,

As to attaching names to concepts, theorems or conjectures, I have often said: (a) that, when a proper name gets attached to (say) a concept, this should never be taken as a sign that the author in question had anything to do with the concept; more often that not, the opposite is true... (b) proper names tend ...to
get replaced by more appropriate ones [8, p.1307].

1.2.6 Recent History

The more recent history of the mathematics involved in the Taniyama-Shimura conjecture begins, of course, with its inception by Taniyama in the 1950s. In the 1960s, after Taniyama’s death, Shimura produced a more precise formulation of the conjecture. Very little progress was made until the mid-1980s when Gerhard Frey and Kenneth Ribet established a link between the Taniyama-Shimura conjecture and Fermat’s last theorem.

Frey conjectured and Ribet proved that the Taniyama-Shimura conjecture (in the case of semi-stable elliptic curves) implies Fermat’s last theorem and vice versa. The result is that it is impossible to discuss either conjecture or theorem without mentioning the implications of their relationship. And though Fermat’s last theorem has few known implications in itself, the Taniyama-Shimura conjecture defines a very important relationship in modern number theory. Speaking of the conjecture, Andrew Wiles said, “We built more and more conjectures stretched further and further into the future, but they would all be completely ridiculous if Taniyama-Shimura was not true [10, p.9].”

To draw his conclusions about Fermat’s last theorem, Frey’s approach was to suppose that the theorem were not true. Then there would exist a solution to Fermat’s equation for some power greater than 2. That is, there would exist integers $a$, $b$, and $c$ such that $a^p + b^p = c^p$ for some prime $p \geq 3$. These integers would lead to a specific elliptic curve, $y^2 = x(x - a^p)(x + b^p)$, which would not be modular. Therefore, it presented a counterexample to one case of the Taniyama-Shimura conjecture. The conclusion was that if the Taniyama-Shimura conjecture could be proved, the proof would imply Fermat’s last theorem
and the truth of Fermat’s last theorem implies the Taniyama-Shimura conjecture in this specific case. Thus if Frey’s intuitions could be proved, the link between the two ideas would be established.

Since Frey’s particular curve is semi-stable (the reduced curve for the Weirstrass equation has a cusp or a node, that is, bad reduction), the proof of Fermat’s last theorem depended on the proof of the Taniyama-Shimura conjecture only in the case in which the elliptic curve is semi-stable.

Serre formulated Frey’s conjectures somewhat more precisely in what has become known as the Epsilon conjecture. This remained a conjecture only a very short time, in 1986 it was proved by Kenneth Ribet. At this point, mathematicians believed that the further progress in proving the Taniyama-Shimura conjecture would be slow. Many did not believe that a proof of the Taniyama-Shimura conjecture would be possible in this century. John Coates, Wiles’ advisor at Cambridge University said of the conjecture, “I did not think that the Shimura-Taniyama conjecture was accessible to proof at present. I thought I probably wouldn’t see a proof in my lifetime [10, p.12].” Ken Ribet expressed a similar viewpoint,

I was one of the vast majority of people who believed that the Shimura-Taniyama conjecture was just completely inaccessible, and I didn’t bother to prove it - even think about trying to prove it. Andrew Wiles is probably one of the few people on earth who had the audacity to dream that you could actually go and prove this conjecture [10, p.13].

At the time that Andrew Wiles began his mathematical studies, Fermat’s last theorem and elliptic curves appeared to be completely unrelated. However, once the connection was
established, Andrew Wiles, who was studying elliptic curves, was able to pursue his lifelong dream of proving Fermat’s last theorem. In the process, he made enormous progress in the development of a proof of the Taniyama-Shimura conjecture.

1.2.7 Andrew Wiles

All of the work of these mathematicians finally began to come together through the research of Princeton mathematician Andrew Wiles. Though Wiles proved the Taniyama-Shimura conjecture for elliptic curves which are semi-stable, his principle interest in the conjecture was through its connection with Fermat’s last theorem.

Andrew Wiles became interested in Fermat’s last theorem when he was a young boy in England. At the public library, he came across a book on mathematics and read about the theorem. It seemed so simple and yet the proof had been so elusive to so many people. As a child Wiles tried to prove Fermat’s theorem with the mathematics accessible to him. Through the years, as he continued his studies in mathematics, he maintained his interest in the theorem and his desire to find a proof of it.

Wiles went on to study mathematics and to graduate from Cambridge University. Under his advisor John Coates, he studied number theory, particularly elliptic curves. Wiles began his study of elliptic curves before the work of Frey, Serre, and Ribet had linked them to Fermat’s last theorem. He did not know that his studies were in the very field that would enable him to accomplish his childhood ambition of proving the renowned theorem.

In 1986, Wiles heard the news that Ribet had proved the Epsilon conjecture, inextricably connecting Fermat’s last theorem with the Taniyama-Shimura conjecture. Describing his
reaction to the news of Ribet’s proof, Wiles said, “I was just electrified. I knew that moment the course of my life was changing, because this meant that to prove Fermat’s last theorem, I just had to prove Taniyama-Shimura conjecture. From that moment, that was what I was working on [10, p.12].”

Since Wiles’ main desire was to prove Fermat’s last theorem, he had only to look at the Taniyama-Shimura conjecture for the specific case when an elliptic curve is semi-stable. Wiles discontinued his other research and began to devote himself to the proof of the Taniyama-Shimura conjecture. He worked in almost complete secrecy and isolation for seven years.

In 1993 at a conference held at the Newton Institute, Wiles presented a lecture entitled “Elliptic Curves and Modular Forms.” In the lecture he discussed the methods he had used in his proof and ended by stating that he had proved Fermat’s last theorem.

Later, an error was found in the proof, but with the help of his former student Richard Taylor, Wiles revised the proof and produced a correct and completed version in 1994. The proof caught the public’s attention. The News that Fermat’s 350 year old theorem was proved made newspaper headlines across the country. Wiles was thrust into celebrity.

As stated above, though Fermat’s last theorem and the Taniyama-Shimura conjecture are so intimately linked, Wiles’ work provided the proof only in the case in which elliptic curves are semi-stable. However, the conjecture still remained to be proved in the general case.
1.2.8 The Full Proof

Once Wiles' proof was published, mathematicians began to have a better idea of how to approach the general case. In 1997 Fred Diamond, Brian Conrad, and Richard Taylor established the Taniyama-Shimura conjecture in all cases when the conductor is not divisible by 27.

In June of 1999 a conference of the Park City Mathematics Institute was held in Park City, Utah. Brian Conrad was one of the organizers of the event. During the course of the conference, Conrad gave two lectures during which he discussed a full proof of the Taniyama-Shimura conjecture. The proof had been completed some weeks earlier by Conrad, Diamond, Taylor and Christophe Breuille. Thus the Taniyama-Shimura conjecture is now a theorem.

The establishment of the Taniyama-Shimura conjecture has many important results. As previously mentioned, the conjecture implies Fermat's last theorem. Additionally, many important theories have been built upon the conjecture and its proof now gives them a secure foundation. One of these theories is the Langlands program, "a far-reaching web of conjectures due to Robert Langlands that relates congruences over finite fields to infinite-dimensional representation theory [6, p.863]."

The complete proof of the Taniyama-Shimura conjecture represents a landmark in the history of mathematics. It is the means of putting to rest the 350-year-old Fermat puzzle, the culmination of the work of scores of mathematicians, and a foundation for new and innovative developments in the field of mathematics.

In chapter two of this paper we will look at some of the mathematics associated with elliptic curves and modular forms, look at examples which illustrate the close correspondence
between them, and present a precise statement of the Taniyama-Shimura conjecture.
Chapter II
The Mathematics

II.1 Elliptic Curves

II.1.1 Structure

An elliptic curve over a field \( k \) consists of the set of solutions of a cubic equation, together with a point at infinity, \( \infty \). That is, \( E(k) = \{ y^2 = f(x) \mid f(x) = x^3 + ax^2 + bx + c \} \cup \{ \infty \} \). For the purposes of this paper, we will consider elliptic curves defined over \( \mathbb{Q} \), in other words, elliptic curves whose coefficients are rational numbers. Under this definition, the solutions of the elliptic curve form an abelian group. The operation of this group is defined geometrically by drawing a line through any two points on the elliptic curve, then reflecting across the x-axis the third point where the line intersects the curve. In the following summary, the binary operation is designated by \( + \):

- Let \( r \) and \( s \) be points on the curve \( E \) with distinct x-coordinates, then the line passing through \( r \) and \( s \) intersects \( E \) in three points. The first two are, of course, \( r \) and \( s \), we
will designate the third point by \((x, y)\). Then \(r + s = (x, -y)\). (See figure II.1, pg. 27).

- Let \(r\) be a point such that the \(y\)-coordinate is not zero, then \(r + r = (x, -y)\) where \((x, y)\) is a second point on \(E\) intersected by the line tangent to \(E\) at \(r\).

- For \(r \neq 0\), if \(r = (x, y)\), then \(-r = (x, -y)\).

- \(\infty\) is the identity element of the group, i.e. \(r + \infty = \infty + r = r\).

- For any element \(r\) on \(E\), \(s\) is the inverse of \(r\) (i.e. \(r + s = \infty\)) if \(r\) and \(s\) have the same \(x\)-coordinate but distinct \(y\)-coordinates.

- Let \(r\) be a point with the \(y\)-coordinate equal to zero, then \(r + r = \infty\).

Moreover, the group operation is closed over the field of rational numbers. Consider the following proof of the case \(r = (x_1, y_1)\), and \(s = (x_2, y_2)\).

**Proof:** Let \(l\) be a line intersecting the curve \(E : y^2 = x^3 + ax^2 + bx + c\), where \(l\) intersects \(E\) at the rational points \((x_1, y_1)\) and \((x_2, y_2)\). Then we can express \(l\) as

\[
l : y = \frac{y_2 - y_1}{x_2 - x_1} x + y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1.
\]

Let \(\frac{y_2 - y_1}{x_2 - x_1} = d\) and \(y_1 - \frac{y_2 - y_1}{x_2 - x_1} x_1 = f\). \(d\) and \(f\) are rational numbers. This gives the equation

\[
(dx + f)^2 = x^3 + ax^2 + bx + cd.
\]

Thus

\[
0 = x^3 + (a - d^2)x^2 + (b - 2df)x + d - f^2.
\]
Let \( a - d^2 = A, \ b - 2df = B, \ d - f^2 = C \). We now have

\[
0 = x^3 + Ax^2 + Bx + C,
\]

with \( A, B, \) and \( C \) rational. Since we began with the assumption that \( x_1 \) and \( x_2 \) are solutions to this equation, it can be factored into the form

\[
0 = (x - x_1)(x - x_2)(hx + g).
\]

\( x \cdot x \cdot h = x^3 \) implies that \( h = 1 \). Also \( -x_1 \cdot -x_2 \cdot g = C \) thus \( g = \frac{C}{x_1 \cdot x_2} \). This quotient is rational, therefore \( g = x_3 \) is rational. By substituting \( x_3 \) back into the equation for \( l \), it is apparent that \( y_3 \) is also rational.

\section*{II.1.2 Weierstrass Form}

Every elliptic curve is associated with a Weierstrass equation which gives the curve in the form

\[
E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6
\]

where \( a_1, a_2, a_3, a_4, a_6 \) are in the algebraic numbers (the algebraic closure of the rational numbers). Performing a change of variables will produce an equation of the form

\[
E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6.
\]

From this form, one can define certain quantities important to the discussion of elliptic curves. The change of variables is performed according to the following formulas:

\[
b_2 = a_1^2 + 4a_2,
\]
From these values, we define

\[ b_4 = 2a_4 + a_1a_3, \]
\[ b_6 = a_3^2 + 4a_6. \]

From these values, we define

\[ b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2, \]
\[ \Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \]
\[ c_4 = b_2^2 - 24b_4. \]
The quantity $\Delta$, called the discriminant of the elliptic curve, must always be non-zero in order for the curve to be non-singular and satisfy the definition of an elliptic curve.

The values $\Delta$ and $c_4$ facilitate classification of an elliptic curve in Weierstrass form.

- The curve is non-singular if and only if $\Delta \neq 0$.
- The curve has a node if and only if $\Delta = 0$ and $c_4 \neq 0$.
- The curve has a cusp if and only if $\Delta = 0$ and $c_4 = 0$. (See Figure 1.3).

II.1.3 Valuation

Before proceeding further in the explanation of elliptic curves, it is necessary to define a map called the valuation. This map will enable the elliptic curve to be transformed to its most useful form and will give us important information about the rational points of the curve defined over $\mathbb{F}_p$.

A valuation is a map $v$ of $\mathbb{Q}^*$ onto $\mathbb{Z}$, $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, the multiplicative group of $\mathbb{Q}$, such that

\begin{align*}
(1) \quad & v(xy) = v(x) + v(y), \\
(2) \quad & v(x + y) \geq \min(v(x), v(y)).
\end{align*}

Let $R = \{x \in \mathbb{Q} \mid v(x) \geq 0\} \cup \{0\}$ be the valuation ring of $v$. 

28
Figure II.2: Non-singular elliptic curve: \( E : y^2 = x^3 - 4x, \ \Delta = 4096 \)

The valuation map necessary for this discussion is evaluated as follows: for any non-zero, rational \( x \) and fixed prime \( p \), \( x \) can be uniquely written in the form \( x = p^a y \), where \( a \) is an integer and the numerator and denominator of \( y \) are both relatively prime to \( p \), then the valuation of \( x \) at \( p \) is defined by \( v_p(x) = a \).

**Example**

Let \( x = 756 = 7^1 3^3 2^2 \).

Then \( v_7(756) = 1, \ v_3(756) = 3, \ v_2(756) = 2, \)

and \( v_p(756) = 0 \) for any \( p \neq 2, 3, \) or 7.
II.1.4 Minimal Weierstrass Form

The valuation enables us to convert the elliptic curve to its most useful form, the minimal Weierstrass form. There is a minimal Weierstrass equation associated with every elliptic curve and this form is unique up to a change of variables. A Weierstrass equation is minimal for the elliptic curve \( E \) at \( v \) if \( v(\Delta) < 12 \) and \( a_1, a_2, a_3, a_4, a_6 \) are in \( R \) [12, p.172].

**Example**: The curve defined by the equation

\[
E : y^2 = x^3 - x^2 + 4x - 4
\]
is minimal. The non-zero coefficients of this equation are

\[ a_2 = -1, \ a_4 = 4, \ \text{and} \ a_6 = -4. \]

Furthermore

\[ \Delta = -6400. \]

Since

\[ a_2 = -1 = p^0(-1), \]

it is apparent that

\[ v_p(-1) = 0 \] for any prime \( p \).

Additionally,

\[ a_4 = 4 = 2^2, \] thus \( v_2(4) = 2 \).

For any \( p \neq 2, \ 4 = p^0(4), \]

thus \( v_p(4) = 0 \) for any odd prime.

Finally,

\[ -4 = 2^2(-1) \] signifying that \( v_2(-4) = 2 \)

and \( v_p(-4) = 0 \) for any prime greater than 2.

Therefore,

\[ v_p(-1) \geq 0, \ v_p(4) \geq 0, \]

and \( v_p(-4) \geq 0 \) for any prime \( p \),

and it is apparent that the coefficients of \( E \) are in \( R \). Moreover,

\[ \Delta = -6400 = -2^85^2, \]

31
implies that

\[ v_2(\Delta) = 8 \text{ and } v_5(\Delta) = 2, \]
\[ v_p(\Delta) = 0 \text{ for any } p \neq 2 \text{ or } 5. \]

Therefore, \( v_p(\Delta) < 12 \) for any prime \( p \). In conclusion,

\[ y^2 = x^3 - x^2 + 4x - 4 \]

is a minimal Weierstrass equation for \( E \).

**II.1.5 Reduction**

In addition to its usefulness in defining the conditions under which an equation is in minimal Weierstrass form, the valuation also gives us important information about how the elliptic curve behaves under reduction at certain primes. The curve is said to have good or bad reduction, stable, semi-stable or, unstable reduction according to the following conditions:

- An elliptic curve has good reduction at a prime \( p \) if and only if \( v_p(\Delta) = 0 \), this is also called stable reduction.

- There are two cases in which an elliptic curve may have bad reduction, these are called multiplicative reduction and additive reduction.
  
  - An elliptic curve has multiplicative or semi-stable reduction at a prime \( p \) if and only if \( v_p(\Delta) > 0 \) and \( v_p(c_4) = 0 \). An elliptic curve reduced modulo \( p \) has a node if and only if it has multiplicative reduction at \( p \).
An elliptic curve has additive or unstable reduction at a prime $p$ if and only if $v_p(\Delta) > 0$ and $v_p(c_4) > 0$. An elliptic curve reduced modulo $p$ has a cusp if and only if it has additive reduction at $p$.

- For a given elliptic curve $E$, there are only finitely many primes where $E$ has bad reduction, either multiplicative or additive.

<table>
<thead>
<tr>
<th>Characteristic 0</th>
<th>Characteristic $p$ (reduction modulo $p$)</th>
</tr>
</thead>
<tbody>
<tr>
<td>non-singular</td>
<td>$\Delta \neq 0$</td>
</tr>
<tr>
<td></td>
<td>$\Delta = 0$</td>
</tr>
<tr>
<td>node</td>
<td>$\Delta = 0$, $c_4 \neq 0$</td>
</tr>
<tr>
<td>cusp</td>
<td>$\Delta = 0$, $c_4 = 0$</td>
</tr>
</tbody>
</table>

**Example** (multiplicative reduction): Let $E$ be the curve given by the equation

$$E : y^2 + xy + y = x^3 - x^2 + 2x - 3.$$  

Then

$$a_1 = 1, \ a_2 = -1, \ a_3 = 1, \ a_4 = 2, \ and \ a_6 = -3.$$  

From these values we compute that

$$b_2 = -3, \ b_4 = 5, \ b_6 = -11, \ b_8 = 2,$$

$$\Delta = -2800, \ and \ c_4 = -111.$$
Since
\[ \Delta = -2800 = -7^1 5^2 2^2, \]
then
\[ v_7(\Delta) = 1, \ v_5(\Delta) = 2, \text{ and } v_2(\Delta) = 2. \]

Additionally,
\[ v_p(\Delta) = 0 \text{ for all primes not equal to 3, 5 or 7.} \]

Furthermore,
\[ c_4 = -111 = -3^1 3^1, \]
thus
\[ v_{37}(c_4) = 1, \ v_3(c_4) = 1, \text{ and } v_p(c_4) = 0 \text{ for all primes not equal to 37 or 3.} \]

In particular,
\[ v_p(c_4) = 0 \text{ when } p \text{ is 2, 5 or 7.} \]

Therefore, \( E \) has multiplicative reduction at 2, 5, and 7 and good reduction at all other primes.

**Example** (additive reduction): Let \( E \) be the curve defined by
\[ E : y^2 = x^3 + 2x^2 + 4x. \]

Then
\[ a_2 = 2 \text{ and } a_4 = 4, \]
Moreover
\[ b_2 = 8, \ b_4 = 8, \ b_8 = -16, \]

34
\[ \Delta = -3072 = -2^{10}, \text{ and } c_4 = -128 = -2^7. \]

Thus

\[ v_2(\Delta) = 10, \text{ and } v_3(\Delta) = 1. \]

\[ v_p(\Delta) = 0 \text{ for } p \neq 2, \text{ or } 3. \]

Also,

\[ v_2(c_4) = 7, \text{ and } v_p(c_4) = 0 \text{ for } p \neq 2. \]

Thus \( E \) has additive reduction at 2, multiplicative reduction at 3, and good reduction at all other primes.

II.1.6 Conductor

Knowing the type of reduction that an elliptic curve has at a given prime makes possible the formulation of a quantity called the conductor associated with each elliptic curve. The conductor provides information about the complexity of the corresponding curve. The conductor \( N \) of an elliptic curve is computed according to the formula

\[ N = \prod_p p^{f_p} \]

where

\[ f_p = \begin{cases} 
0 & \text{if } E \text{ has good reduction at } p \\
1 & \text{if } E \text{ has multiplicative reduction at } p 
\end{cases} \]

\[ f_p \geq 2 \text{ if } E \text{ has additive reduction at } p. \]

In particular \( f_p = 2 \) if \( p \neq 2 \) or 3. For a description of how \( f_p \) can be found in the additive case, see [12, p.361].

35
**Example**: In the first example under reduction, we found that the curve

\[ E : y^2 + xy + y = x^3 - x^2 + 2x - 3 \]

has multiplicative reduction at each of the primes, 2, 5, and 7, which divide the conductor of \( E \). Therefore

\[ f_2 = f_5 = f_7 = 1 \]

and

\[ f_p = 0 \] for all other primes.

Thus the conductor of \( E \) is given by

\[ N = 2^1 5^1 7^1 = 70. \]

The primes which divide the conductor are exactly those primes at which the curve has bad reduction.

**II.1.7 Rational Roots**

Let \( S_p \) be the number of solutions of the reduced equation of \( E \) modulo \( p \). Also let \( a_p(E) = p - S_p \). Then some basic arithmetic information about the curve \( E \) can be ascertained from the sequence \( \{a_p(E)\}_p \) which is indexed by the primes of good reduction.

**Example**: Table 2.2 gives the first several elements of \( \{a_p(E)\}_p \) for the curve

\[ E : y^2 + xy + y = x^3 - x, \]

which has conductor \( N = 14 \).
Table II.2: Rational points for a curve with conductor $N = 14$

<table>
<thead>
<tr>
<th>p</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_p$</td>
<td>-5</td>
<td>5</td>
<td>-11</td>
<td>17</td>
<td>11</td>
<td>17</td>
<td>23</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td>35</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$a_p$</td>
<td>-2</td>
<td>0</td>
<td>-4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>-6</td>
<td>-4</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Example 7: Table 2.3 gives the first several elements of $\{a_p(E)\}_p$ for the curve $E : y^2 + xy = x^3 + x^2 - 6x + 4$.

Table II.3: Rational points for a curve with conductor $N = 166$

<table>
<thead>
<tr>
<th>p</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_p$</td>
<td>-4</td>
<td>7</td>
<td>6</td>
<td>16</td>
<td>15</td>
<td>20</td>
<td>21</td>
<td>19</td>
<td>32</td>
<td>30</td>
<td>36</td>
<td>35</td>
<td></td>
</tr>
<tr>
<td>$a_p$</td>
<td>-1</td>
<td>-2</td>
<td>1</td>
<td>-5</td>
<td>-2</td>
<td>-3</td>
<td>-2</td>
<td>4</td>
<td>-3</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

II.2 Modular Forms

A modular form of weight $k$ is an analytic function defined on the complex upper half plane $\{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$ which satisfies a transformation rule of the form $f(\frac{az+b}{cz+d}) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in $\Gamma$ where $\Gamma$ is a subgroup of $SL_2(\mathbb{Z})$ [5, p.1398]. Any nontrivial modular function for $SL_2(\mathbb{Z})$ has even weight.

For the purposes of this paper, the modular forms of interest are those of weight two where the $\Gamma$ is the subgroup of $SL_2(\mathbb{Z})$ in which the lower left entries of the matrices are
congruent to 0 modulo \( N \). \( N \) is called the level of the modular form and will correspond to the conductor of an elliptic curve. These modular forms can be expressed by a Fourier series

\[
f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i z}.
\]

**Example** : For a modular form of weight 2, level 11, the generating function \( f(z) \) of the Fourier series can be calculated explicitly according to the following formula where \( f(z) \) is a constant multiple of \( g(z) \).

\[
g(z) = (\psi(z)\psi(11z))^2
\]

\[
\psi(z) = e^{\pi iz/12} \prod_{n} (1 - q^n), \quad q = e^{2\pi iz}
\]

thus

\[
g(z) = q(\prod_{n} (1 - q^n)^2(1 - q^{11n})^2).
\]

\[
g(x) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12}
\]

\[
+ 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} - q^{23}
\]

\[
- 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 2q^{30} + 7q^{31} + 8q^{32} - q^{33} + 4q^{34}
\]

\[
- 2q^{35} - 4q^{36} + 3q^{37} - 4q^{39} - 8q^{41} + \ldots
\]

Though closed forms for generating functions of the Fourier series associated with modular forms are not always easily computed, the following table gives some of the coefficients of prime power terms for modular forms of the given levels.
Table II.4: Coefficients of prime power terms of Fourier series for modular functions of level N [4, p.265].

<table>
<thead>
<tr>
<th>Level (N)</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>-4</td>
<td>-2</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>7</td>
<td>3</td>
<td>-8</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>-</td>
<td>-2</td>
<td>0</td>
<td>-4</td>
<td>6</td>
<td>2</td>
<td>0</td>
<td>-6</td>
<td>-4</td>
<td>2</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>70</td>
<td>-</td>
<td>0</td>
<td>-4</td>
<td>-6</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>6</td>
<td>8</td>
<td>-10</td>
<td>2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>166</td>
<td>-</td>
<td>-1</td>
<td>-2</td>
<td>1</td>
<td>-5</td>
<td>-2</td>
<td>-3</td>
<td>-2</td>
<td>4</td>
<td>-3</td>
<td>1</td>
<td>1</td>
<td>6</td>
</tr>
</tbody>
</table>

II.3 The Conjecture

II.3.1 Statement of the Conjecture

The Taniyama Shimura conjecture identifies a very close relationship between elliptic curves and modular forms. For an elliptic curve $E$ defined over the rational numbers, the conjecture states that there is an integer $N$ and a weight two modular form of level $N$ (normalized so that $a_1(f) = 1$), such that

$$a_p(E) = a_p(f)$$

for all primes $p$ where $E$ has good reduction [5, p. 1398]. Thus, the terms of the sequence $\{a_p(E)\}_p$ correspond to the coefficients of prime power terms of the modular form. The level $N$ of the modular form corresponds to the conductor of the elliptic curve.

II.3.2 Modularity of an elliptic curve with conductor 11

Consider the elliptic curve given in minimal Weierstrass form

$$E : y^2 + y = x^3 - x^2 - 10x - 20.$$
For this curve,

\[ a_1 = 0, \quad a_2 = -1, \quad a_3 = 1, \quad a_4 = -10, \quad \text{and} \quad a_6 = -20. \]

Performing a change of variables yields that

\[ b_2 = -4, \quad b_4 = -20, \quad \text{and} \quad b_6 = -79. \]

Furthermore,

\[ b_8 = -21, \quad \Delta = -161051, \quad \text{and} \quad c_4 = 496. \]

When

\[ x = a_1, \quad a_2, \quad \text{or} \quad a_3 \]

it is apparent that

\[ v_p(x) = 0 \text{ at any prime } p. \]

\[ v_2(a_4) = 1, \quad v_5(a_4) = 1, \quad \text{and} \quad v_p(a_4) = 0 \text{ for all other primes}. \]

Also,

\[ v_2(a_6) = 2, \quad v_5(a_6) = 1, \quad \text{and} \quad v_p(a_6) = 0 \text{ for all other primes}. \]

Therefore

\[ a_i \in R \text{ for } i = 1, 2, 3, 4, 6. \]

The discriminant

\[ \Delta = -161051 = -11^5. \]

Thus

\[ v_{11}(\Delta) = 5, \quad \text{and} \quad v_p(\Delta) = 0 \text{ for any other prime } p. \]

\[ v_p(\Delta) < 12 \text{ for any prime } p. \]

Hence, E is in minimal Weierstrass form.
Reduction

Since

\[ v_p(\Delta) \geq 0 \]

for any prime \( p \), to determine the type of reduction of \( E \), it is necessary only to find the valuation \( v_p(c_4) \) where \( p \) is any prime dividing \( \Delta \).

\[ c_4 = 496 = 2^4 \cdot 31. \]

11 is the only prime divisor of the discriminant \( \Delta \) and

\[ v_{11}(c_4) = 0, \]

thus \( E \) has multiplicative reduction at 11 and good reduction at all other primes.

Conductor

Since \( E \) has multiplicative reduction at 11, \( f_{11} = 1 \). \( E \) has good reduction at all other primes giving that \( f_p = 0 \) for any \( p \neq 11 \). Thus the formula for the conductor of an elliptic curve

\[ N = \prod p^{f_p} \]

shows that \( N = 11 \).

Rational points

Below is a table giving \( S_p \), the number of solutions of the reduced equation of \( E \) modulo \( p \) for each prime \( p \leq 41 \). Also shown are the corresponding elements of the sequence \( \{a_p(E)\}_{p} \).
Table II.5: Rational points of an elliptic curve with conductor $N = 11$

<table>
<thead>
<tr>
<th>$p$</th>
<th>2</th>
<th>3</th>
<th>5</th>
<th>7</th>
<th>11</th>
<th>13</th>
<th>17</th>
<th>19</th>
<th>23</th>
<th>29</th>
<th>31</th>
<th>37</th>
<th>41</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_p$</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>9</td>
<td>-</td>
<td>9</td>
<td>19</td>
<td>19</td>
<td>24</td>
<td>29</td>
<td>24</td>
<td>34</td>
<td>49</td>
</tr>
<tr>
<td>$a_p$</td>
<td>-2</td>
<td>-1</td>
<td>1</td>
<td>-2</td>
<td>-</td>
<td>4</td>
<td>-2</td>
<td>0</td>
<td>-1</td>
<td>0</td>
<td>7</td>
<td>3</td>
<td>-8</td>
</tr>
</tbody>
</table>

**Modular form**

Finally, since the curve $E$ under examination has conductor $N = 11$, the corresponding modular form is of level 11. In Example 8, we calculated the generating function $J(z)$ for the Fourier series associated with a weight two modular form of level 11. Some of the terms generated by that function are again listed below.


$g(x) = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12}$

$+ 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + 4q^{18} + 2q^{20} + 2q^{21} - 2q^{22} - q^{23}$

$- 4q^{25} - 8q^{26} + 5q^{27} - 4q^{28} + 2q^{30} + 7q^{31} + 8q^{32} - q^{33} + 4q^{34}$

$- 2q^{35} - 4q^{36} + 3q^{37} - 4q^{39} - 8q^{41} + \ldots$

In the preceding function, the terms with prime exponents have been highlighted. Comparing the coefficients of these terms with the chart giving $\{a_p(E)\}_p$ above, it is apparent that the terms for the sequence correspond exactly with the coefficients of the modular function.
Bibliography


