Modular Forms & Elliptic Curves

Arkit Ray

Euler Circle

July 13

Introduction

- Elliptic Curves
- Modular forma
- Fermants Last Theorem

Elliptic Curves

- Elliptic curves are mathematical objects that can be used in cryptography.
- They are useful for cryptography because the addition of points on an elliptic curve can be defined in a way that is very difficult to reverse.
- This makes elliptic curves well-suited for use in digital signature schemes and key exchange protocols.
- In addition to their cryptographic applications, elliptic curves are also used in number theory, physics, and computer graphics.

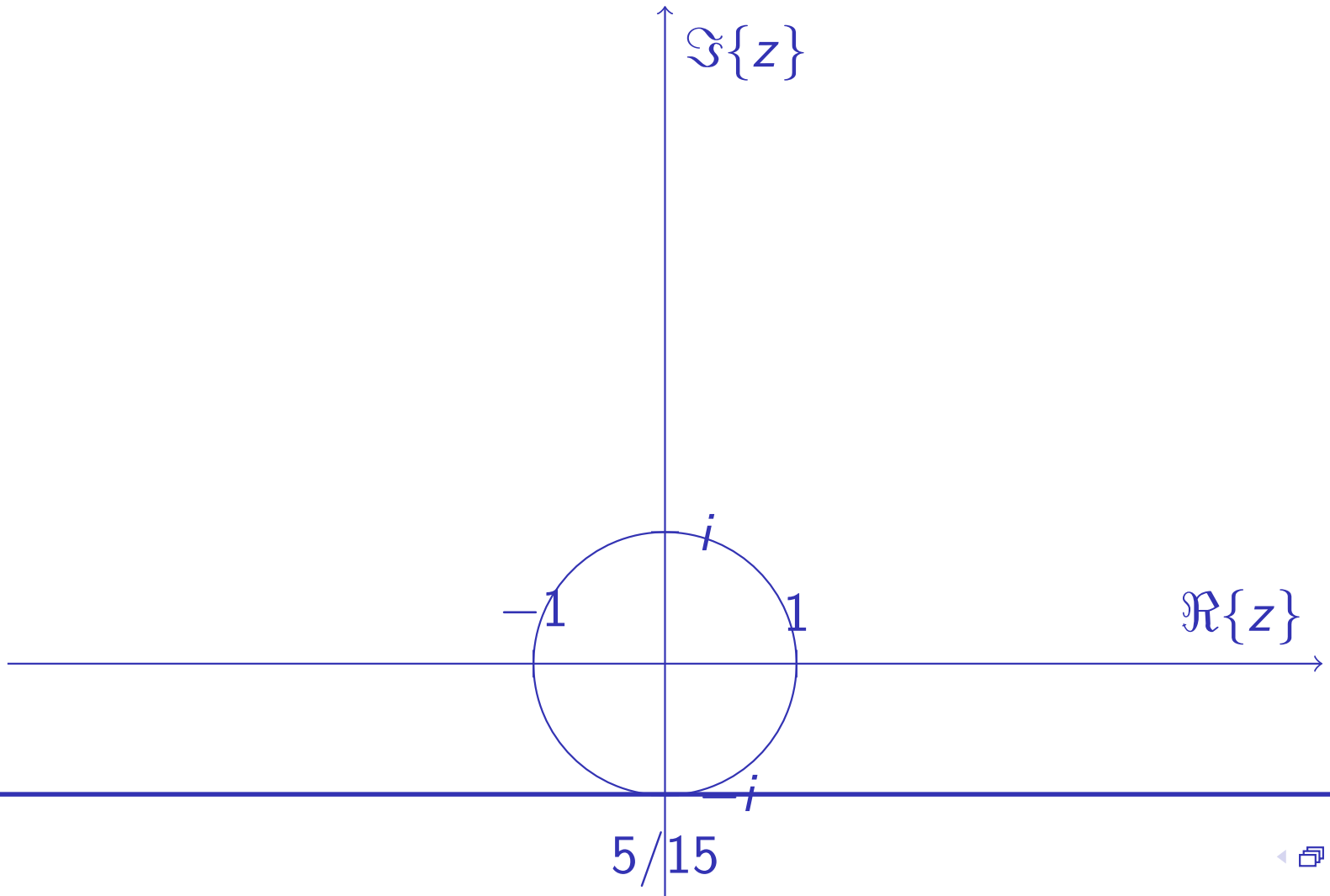
An elliptic curve is defined as

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

History of Elliptic Curves

- The first known mention of elliptic curves was in the work of Pierre de Fermat in the 17th century.
- In the 18th century, Leonhard Euler studied elliptic curves in the context of solving Diophantine equations.
- In the 19th century, Niels Henrik Abel and Carl Jacobi developed the theory of elliptic functions, which are closely related to elliptic curves.
- In the early 20th century, David Hilbert proved that the Mordell conjecture, which states that the set of rational points on an elliptic curve is finite, is true.
- In the late 20th century, elliptic curves became increasingly important in cryptography, thanks to the work of Andrew Wiles and others.
- Today, elliptic curves are used in a wide variety of applications, including cryptography, number theory, and algebraic geometry.

The complex plane is a two-dimensional plane that is used to visualize complex numbers. The real numbers are plotted on the horizontal axis, and the imaginary numbers are plotted on the vertical axis.



A complex number z can be represented as a point in the complex plane by its real and imaginary parts, $\Re\{z\}$ and $\Im\{z\}$. For example, the complex number $z = 1 + 2i$ is plotted as the point $(1, 2)$ in the complex plane.
The complex plane can be used to visualize many different concepts in complex analysis. For example, the addition of two complex numbers can be visualized as the addition of two points in the complex plane. Similarly, the multiplication of two complex numbers can be visualized as the rotation and scaling of a point in the complex plane.

A complex function is a function that takes a complex number z as an input and returns a complex number as an output.
We can visualize a complex function by plotting its graph in the complex plane.
The real part of the function is represented by the x-axis, and the imaginary part of the function is represented by the y-axis.

SL2 Matrix

An SL2 matrix is a 2x2 matrix with integer entries and determinant 1. It can be represented by the set of all transformations of the form

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az + b}{cz + d}$$

for $a, b, c, d \in \mathbb{Z}$ and $ad - bc = 1$.

A modular form is a complex function $f(z)$ that satisfies the following two conditions:
1. $f(z)$ is holomorphic (i.e., it has no singularities) on the complex upper half-plane $\mathbb{H}$. 2. $f(z)$ is invariant under the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$.

Examples of Modular Forms

A modular form of weight k is a complex function $f(z)$ that satisfies the following two conditions:
1. $f(z)$ is holomorphic (i.e., it has no singularities) on the complex upper half-plane $\mathbb{H}$. 2. $f(z)$ is invariant under the action of the modular group $\mathrm{SL}_2(\mathbb{Z})$, meaning that

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

for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$.
The weight of a modular form is important because it determines the behavior of the function at infinity. For example, a modular form of weight 0 will have a constant limit as $z \to \infty$, while a modular form of weight 1 will have a logarithmic limit.

Proof that $f(z) = \frac{1}{z}$ is a modular form of weight 0:

$$\begin{aligned} f\left(\frac{az+b}{cz+d}\right) &= \frac{1}{\frac{az+b}{cz+d}} \\ &= \frac{cz+d}{az+b} \\ &= \frac{1}{z} \end{aligned}$$

for all $a, b, c, d \in \mathbb{Z}$ with $ad - bc = 1$.

One way in which modular forms and elliptic curves are connected is through the modular parameterization of elliptic curves. This parameterization states that every elliptic curve can be represented as the quotient of the upper half-plane by a subgroup of the modular group. This means that modular forms can be used to study elliptic curves, and vice versa.
Another way in which modular forms and elliptic curves are connected is through the modularity theorem. This theorem states that the L-functions of certain elliptic curves are equal to the modular forms of certain weights. This theorem has a wide range of applications in number theory, and it has been used to prove many important results.

Modularity Theorem

The modularity theorem states that the L-function of an elliptic curve is equal to a modular form of a certain weight. The weight of a modular form is a number that determines its behavior at infinity. The modularity theorem was proved by Andrew Wiles in 1995. Some appliations are:

- Proof of Fermat's Last Theorem
- Study of elliptic curves
- Construction of new modular forms
- Applications to Physics- String Theory
- Study of the Birch and Swinnerton-Dyer conjecture
- Construction of new algebraic varieties

Fermats Last Therorem

- Pierre de Fermat (1637): In the margin of his copy of Diophantus's *Arithmetica*, Fermat wrote a note claiming that no three positive integers a, b, and c can satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2. This became known as Fermat's Last Theorem.
- Carl Friedrich Gauss (early 19th century): Gauss studied elliptic curves and their relationship to modular forms. He showed that the L-functions of elliptic curves are modular forms.
- Yutaka Taniyama and Shimura (1950s): Taniyama and Shimura conjectured that every elliptic curve over the rational numbers is modular. This conjecture is now known as the Taniyama–Shimura conjecture.
- Andrew Wiles (1995): Wiles proved the Taniyama–Shimura conjecture. This was a major breakthrough in number theory, and it led to the proof of Fermat's Last Theorem.

Wiles's proof was based on the work of many other mathematicians, including Gauss, Taniyama, Shimura, and Ken Ribet. It was a long and difficult proof, and it took Wiles several years to complete. The proof of Fermat's Last Theorem was a major achievement in mathematics. It showed the power of modular forms and elliptic curves, and it opened up new areas of research in number theory.