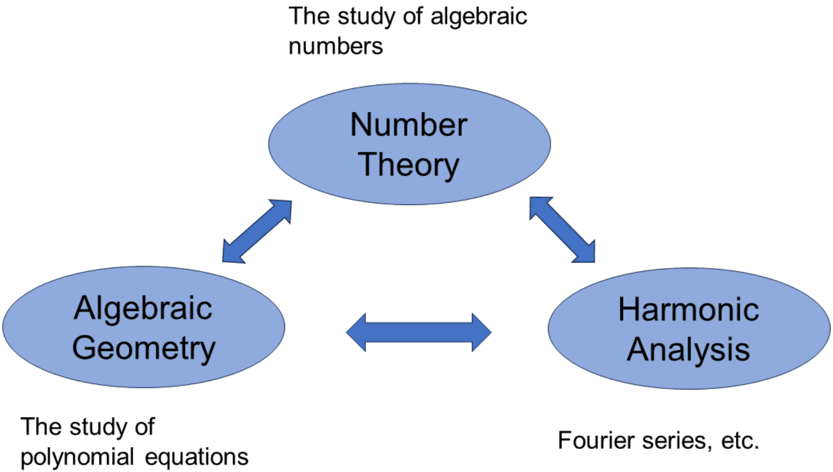
Introduction to Number Theory

Jean-Stefan Koskivirta

October 13, 2023


The study of algebraic numbers
Number Theory
Algebraic Geometry
Harmonic Analysis
The study of polynomial equations
Fourier series, etc.

Diophantine equations

A Diophantine equation is a polynomial equation with integer coefficients. For example:

$$x^n + y^n = z^n, \quad n \geq 1$$
$$y^2 = x^3 + x$$
$$x^2 = 2$$

are Diophantine equations. We can also take a system of such equations ("this is called an algebraic variety").

Integer solutions

Sometimes Diophantine equations have integer solutions, and sometimes they do not. For example, the equation

$$z^2 = x^2 + y^2$$

has many integer solutions:

$$(3, 4, 5), (5, 12, 13), (8, 15, 17), \ldots$$

Theorem (Fermat's Last Theorem)

For $n > 2$, the only integer solutions to the equation

$$z^n = x^n + y^n$$

are the trivial ones, i.e $x = 0$ or $y = 0$.

Solutions modulo p

Let X be a system of Diophantine equations. Fix a prime number p. We can look for solutions inside the field

$$\mathbb{Z}/p\mathbb{Z} = \{\overline{1}, \overline{2}, \ldots, \overline{p-1}\}.$$

For example, consider the equation:

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

and take $p = 7$. The solutions in $\mathbb{Z}/7\mathbb{Z}$ are:

$$\begin{aligned}
(x, y) &= (\overline{0}, \overline{0}) \\
(x, y) &= (\overline{1}, \overline{3}) \\
(x, y) &= (\overline{1}, \overline{4}) \\
(x, y) &= (\overline{3}, \overline{3}) \\
(x, y) &= (\overline{3}, \overline{4}) \\
(x, y) &= (\overline{5}, \overline{2}) \\
(x, y) &= (\overline{5}, \overline{5}).
\end{aligned}$$

Finite fields

Let p be a prime number. For each $n \geq 1$, there is a unique finite field (a commutative ring where every nonzero element is invertible) with p^n elements, denoted by $\mathbb{F}_{p^n}$. For example, take $p = 2$, $n = 2$. The field $\mathbb{F}_4$ has four elements

$$\mathbb{F}_4 = \{0, 1, \alpha, \beta\}$$

where addition and multiplication are defined as follows:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\times$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Local Zeta function

Consider an algebraic variety X (a system of Diophantine equations). Write N_{p^n} for the number of solutions of X in the field $\mathbb{F}_{p^n}$.

Definition

Define the Zeta function of X at p as follows:

$$\zeta_{X,p}(s) = \exp\left(\sum_{n\geq 1} \frac{N_{p^n}}{n} p^{-sn}\right), \qquad s \in \mathbb{C}.$$

Weil conjectures

Let X be a projective algebraic variety, non-singular at p, of dimension n.

Theorem (Grothendieck 1965, Deligne 1974)

(1) *$\zeta_{X,p}(s)$ is a rational function in the variable $t = p^{-s}$.*

(2) *More precisely, there are integral polynomials $P_i(t)$ such that*

$$\zeta_{X,p}(s) = \frac{P_1(t) \dots P_{2n-1}(t)}{P_0(t) \dots P_{2n}(t)}$$

(3) *Any complex root of $P_i(t)$ has absolute value $p^{i/2}$ (Riemann hypothesis).*

(4) *There is a functional equation: $\zeta_{X,p}(n-s) = \pm p^{nE/2-Es}\zeta_{X,p}(s)$ for some integer E.*

Hasse–Weil Zeta function

For each prime number p, For each prime number p, we have a Zeta function $\zeta_{X,p}(s)$ at p.

Definition

The function

$$\zeta_X(s) := \prod_p \zeta_{X,p}(s).$$

is called the Hasse–Weil Zeta function of X.

Example

Take a single point $X = \{\bullet\}$. Then $N_{p^n} = 1$ for all prime p and all $n \geq 1$. Hence:

$$\zeta_p(s) = \exp\left(\sum_{n\geq 1} \frac{p^{-ns}}{n}\right) = \exp(-\log(1-p^{-s})) = \frac{1}{1-p^{-s}}$$
$$\zeta(s) = \prod_p \frac{1}{1-p^{-s}} = \sum_{n\geq 1} \frac{1}{n^s}$$

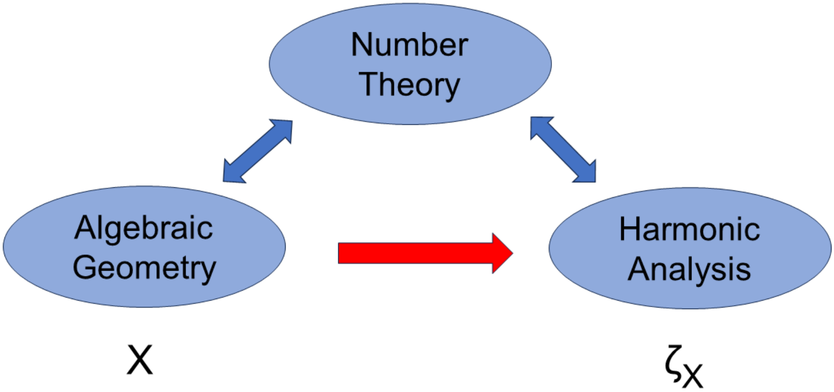
is the usual Riemann Zeta function.

Hasse–Weil Conjecture

Conjecture (Hasse–Weil)

(1) $\zeta_X(s)$ *extends to a meromorphic function on* $\mathbb{C}$.
(2) ζ_X *satisfies a functional equation.*

The usual Riemann Zeta function ζ satisfies these two properties.


Number Theory
Algebraic Geometry
Harmonic Analysis
X
ζ_X

Number fields

A number field is a finite field extension of $\mathbb{Q}$. For example, the following sets are number fields:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$
$$\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}.$$

Let K be a number field. The ring of algebraic integers of K is

$$\mathcal{O}_K := \{x \in K \mid \exists P \in \mathbb{Z}[X] \text{ monic, } P(x) = 0\}.$$

For example:

$$\mathcal{O}_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$$
$$\mathcal{O}_{\mathbb{Q}(i)} = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Dedekind Zeta function

Let K be a number field.

Definition

The Dedekind Zeta function of K is

$$\zeta_K(s) := \sum_{\mathfrak{a}} \frac{1}{|\mathcal{O}_K/\mathfrak{a}|^s}, \qquad s \in \mathbb{C}$$

where $\mathfrak{a}$ ranges over all nonzero ideals of $\mathcal{O}_K$.

For example if $K = \mathbb{Q}$ then $\zeta_{\mathbb{Q}}(s) = \sum_{n\in\mathbb{N}} \frac{1}{n^s}$ is the usual Riemann Zeta function.

Artin's Conjecture

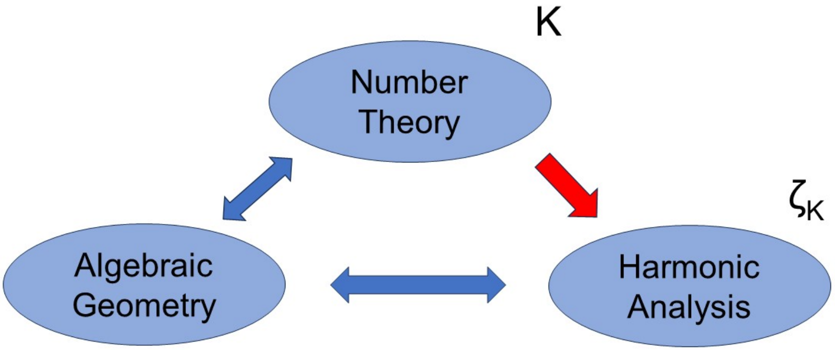
One can show that $\zeta_K(s)$ can be written as a product

$$\zeta_K(s) = \zeta(s) L_K(s)$$

for a certain function $L_K(s)$.

Conjecture (E. Artin)

$L_K(s)$ is holomorphic on $\mathbb{C}$.


K
Number Theory
ζ_K
Algebraic Geometry
Harmonic Analysis

Galois representations

Let L/K be a finite Galois extension of number fields.

Definition

A Galois representation is a group homomorphism

$$\rho\colon \operatorname{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$$

where $n \geq 1$ is an integer. One can also replace $\mathbb{C}$ by other fields.

For each (unramified) prime ideal $\mathfrak{p} \subset \mathcal{O}_K$, there is a Frobenius element $\mathrm{Frob}_{\mathfrak{p}} \in \operatorname{Gal}(L/K)$ characterized by

$$\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^q \pmod{\mathfrak{p}}, \quad q = |\mathcal{O}_K/\mathfrak{p}|.$$

Artin L-function

Let $\rho\colon \mathrm{Gal}(L/K) \to \mathrm{GL}_n(\mathbb{C})$ be a Galois representation.

Definition

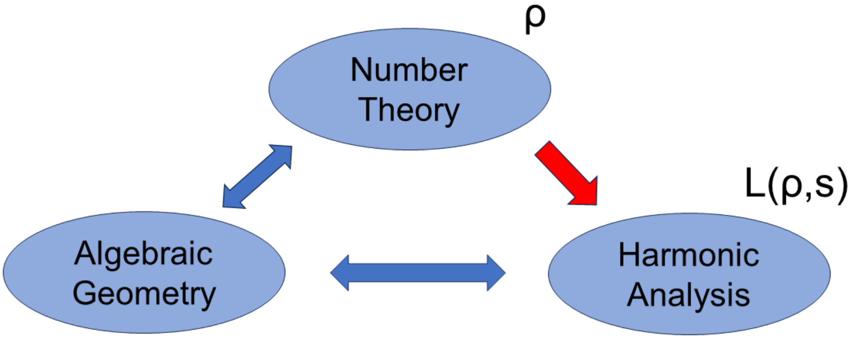
The Artin L-function of ρ is

$$L(\rho, s) := \prod_{\mathfrak{p}} \frac{1}{\det(E_n - t\rho(\mathrm{Frob}_{\mathfrak{p}}))}, \qquad t = |\mathcal{O}_K/\mathfrak{p}|^s,$$

where $\mathfrak{p}$ ranges over all prime ideals of $\mathcal{O}_K$.

Conjecture (E. Artin)

$L(\rho, s)$ is meromorphic on $\mathbb{C}$.

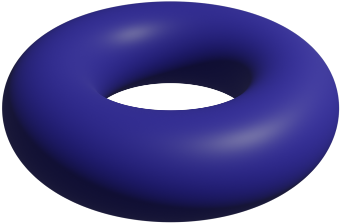

ρ
Number Theory
L(ρ,s)
Algebraic Geometry
Harmonic Analysis

Example: Elliptic curves

For example, consider the equation

$$y^2 = x^3 + ax + b, \quad a, b \in \mathbb{Z}.$$

This type of object is called an "elliptic curve". The solutions $(x, y) \in \mathbb{C}^2$ to this equation look like a torus.



The Zeta function of an elliptic curve has the form

$$\zeta_{X,p}(s) = \frac{pt^2 - a_p t + 1}{(1-t)(1-pt)}, \quad t = p^{-s},\ a_p = p + 1 - N_p.$$

Taking a product over all primes, we get

$$\zeta_X(s) = \frac{\zeta(s)\zeta(s-1)}{L(X,s)}$$

where

$$L(X,s) = \prod_p (p^{-2s+1} - a_p p^{-s} + 1)$$

Theorem (A. Wiles, completed by Breuil–Conrad–Diamond–Taylor)

$L(X,s)$ is the L-function of a modular form.

This theorem was previously known as the "Shimura–Taniyama Conjecture". It was main step in the proof of Fermat's Last Theorem.

Modular form

Set $\mathcal{H} = \{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$.

Definition

A modular form of weight $k \geq 0$ is a function $f\colon \mathcal{H} \to \mathbb{C}$ satisfying:

1. f is holomorphic,
2. $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$.
3. Growth condition: $f(iz)$ is bounded as $\text{Im}(z) \to +\infty$.

Conditions 2 and 3 imply that $f(z+1) = f(z)$ and that we can write f as a Fourier series:

$$f(z) = \sum_{n \geq 0} a_n e^{2i\pi nz}.$$

When $a_0 = 0$, it is called a cusp form.

L-function of a modular form

To a cusp form f, we can attach the L-function:

$$L(f,s) := \sum_{n\geq 1} \frac{a_n}{n^s}.$$

Theorem (A. Wiles, completed by Breuil–Conrad–Diamond–Taylor)

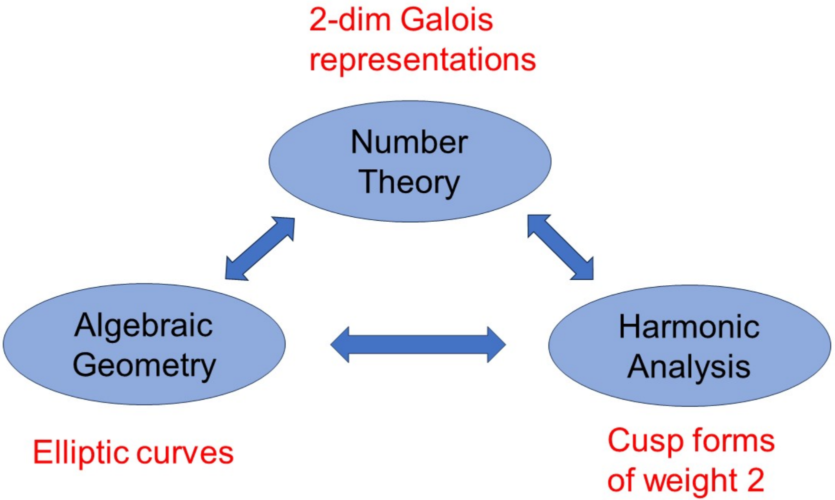
Let X be an elliptic curve over $\mathbb{Q}$. Then there exists a cusp form of weight 2 satisfying

$$L(X,s) = L(f,s).$$

To an elliptic curve X over $\mathbb{Q}$, one can also attach naturally a 2-dimensional Galois representation

$$\rho\colon \operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Q}_\ell)$$

which satisfies $L(\rho,s) = L(X,s)$.


2-dim Galois
representations
Number
Theory
Algebraic
Geometry
Harmonic
Analysis
Elliptic curves
Cusp forms
of weight 2

Langlands Correspondence

Conjecture (Langlands)

There is a correspondence between Galois representations $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_n(\mathbb{Q}_\ell)$ *and automorphic forms* f*, such that*

$$L(\rho, s) = L(f, s).$$

An automorphic form is a generalization of a modular form. Furthermore, if X is an algebraic variety of dimension n over $\mathbb{Q}$, one can attach to X a Galois representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ by taking the etale cohomology:

$$H^i_{et}(X \otimes_{\mathbb{Q}} \overline{\mathbb{Q}}, \mathbb{Q}_\ell).$$

where $i \geq 0$ (the most interesting one is usually for $i = n$). The above

Conjecture would imply the meromorphicity of the zeta function $\zeta_X(s)$ and the L-function $L(\rho, s)$ (Hasse–Weil Conjecture, Artin Conjecture).