Prime Ideal Theorem on Number Fields

Hikmet Burak Özcan

İzmir Institute of Technology, Dokuz Eylül University

06 December 2019

Overview

The function $\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$ is known as the **prime counting function**. For example, $\pi(10) = 4$, $\pi(100) = 25$, $\pi(1000) = 168$.

- **Euclid** offered a proof of the infinitude of primes for the first time in his work *"Elements"* c. 300 BC. So, we have that

$$\lim_{x \to \infty} \pi(x) = \infty.$$

- In 1896, **Jacques Hadamard** and **Charles Jean de la Vallée Poussin** proved independently **Prime Number Theorem**

Prime Number Theorem (1896)

There is an asymptotic formula for the prime counting function $\pi(x)$:

$$\pi(x) \sim \frac{x}{logx}.$$

Our main purpose is to generalise of the *Prime Number Theorem* to number fields. This talk will consist of two main parts.

- I. Algebraic Part
  - Number Fields
  - The ring of integers of a number field
- II. Analytic Part
  - Dedekind zeta function and its analytic properties
  - Prime Ideal Theorem

Definition

A complex number α is said to be **algebraic** if it is a root of a non-zero polynomial $f(x) \in \mathbb{Z}[x]$. If α is not algebraic, then it is called **transcendental**.

Examples

1. $\pm\sqrt{2}$ are algebraic, as they are roots of $X^2 - 2$.
2. e and π are transcendental.

Lemma

If α is algebraic, then there is a unique monic polynomial $f(X) \in \mathbb{Q}[X]$ of smallest degree with α as a root.

Definition

Let α be an algebraic number. The **minimal polynomial** of α over $\mathbb{Q}$ is the monic polynomial over $\mathbb{Q}$ of smallest degree with α as a root.

- The minimal polynomial $m(X)$ of the algebraic number α is irreducible.
- If α is a root of some polynomial $f(X) \in \mathbb{Q}[X]$, then $m(X)|f(X)$.

Definition

A field K is a **number field** if it is a finite degree extension of $\mathbb{Q}$. The **degree** of K is the dimension of K as a vector space over $\mathbb{Q}$.

Examples

1. $\mathbb{Q}$ itself is a number field.
2. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ is a number field of degree 2.
3. $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} | a, b, c, d \in \mathbb{Q}\}$ is a number field of degree 4.

- We want to do number theory in number fields, enlarged versions of the rational numbers. That is, we are going to study prime numbers, divisibility, and so on, in these larger fields.
- When we "do number theory", we usually refer to properties of the integers $\mathbb{Z}$, rather than $\mathbb{Q}$. So, in order to work in a number field K, we need to define a subset $\mathbb{Z}_K$ of "integers in K".
- It would be nice if this subset satisfies the same algebraic properties of $\mathbb{Z}$ namely, $\mathbb{Z}_K$ should be a ring, so that we can add, subtract and multiply within $\mathbb{Z}_K$.
- We would like the integers in $\mathbb{Q}$ to turn out to be $\mathbb{Z}$!

Definition

Let α be an algebraic number. We say that α is an **algebraic integer** if the minimal polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.

Examples

1. i is an algebraic integer, as its minimal polynomial is $X^2 + 1$.
2. $\omega = (-1 + \sqrt{3})/2$ is not an algebraic integer, as its minimal polynomial is $X^2 + X - \frac{1}{2}$, which involves a rational coefficient.

When it comes to checking whether or not a given algebraic number α is an algebraic integer, it is sometimes convenient to check a weaker condition.

Lemma

Suppose that α satisfies a monic polynomial with coefficients in $\mathbb{Z}$. Then α is an algebraic integer.

Proposition

Let $\alpha \in \mathbb{C}$. The following are equivalent:

1. *α is an algebraic integer.*
2. *$\mathbb{Z}[\alpha]$ is a finitely generated module over $\mathbb{Z}$.*

Corollary

The set of all algebraic integers forms a ring.

Definition

Let K be a number field. Then the integers in K are

$$\mathbb{Z}_K = \{\alpha \in K | \alpha \textit{ is an algebraic integer}\}.$$

We say that $\mathbb{Z}_K$ is the **ring of integers** of K.

The ring of integers of $\mathbb{Q}$ is $\mathbb{Z}$, as one hopes.

Proposition

Every algebraic number has an integer multiple which is an algebraic integer, i.e. $\mathbb{Q}\mathbb{Z}_K = K$.

Suppose that K is a number field and $[K : \mathbb{Q}] = n$. Then, there exists an element $\gamma \in K$ such that $K = \mathbb{Q}(\gamma)$. Let f be the minimal polynomial of γ of degree n over $\mathbb{Q}$. We can factor $f(X)$ completely over $\mathbb{C}$ as

$$f(X) = \prod_{i=1}^{n}(X - \gamma_i),$$

where $\gamma_1, \ldots, \gamma_n \in \mathbb{C}$ are the roots of f. Of course, one of these is γ itself.

Definition

If $f(X) \in \mathbb{Q}[X]$ is the minimal polynomial of $\gamma \in K$, then the roots $\gamma_1, \ldots, \gamma_n$ are the **conjugates** of γ.

Given any element of K, we can write it as a polynomial expression in γ with coefficients in $\mathbb{Q}$, because $K = \mathbb{Q}(\gamma)$. For each $k = 1, \ldots, n$, the map

$$\sigma_k : \mathbb{Q}(\gamma) \longrightarrow \mathbb{Q}(\gamma_k) \subset \mathbb{C}.$$

$$\sum_{i=0}^{n-1} a_i \gamma^i \mapsto \sum_{i=0}^{n-1} a_i \gamma_k^i$$

is an **embedding**, i.e. injective field homomorphism.

Proposition

If K is a number field of degree n, then the maps $\sigma_1, \ldots, \sigma_n$ are all of the n distinct embeddings $K \longrightarrow \mathbb{C}$.

Example

Let $K = \mathbb{Q}(i)$. The conjugates of i are i and $-i$, so we have two embeddings from K into $\mathbb{C}$, given by

$$\sigma_1(a + bi) = a + bi,$$

$$\sigma_2(a + bi) = a - bi.$$

This gives us two ways to think of $\mathbb{Q}(i)$ as a subfield of $\mathbb{C}$.

Let K be a number field, with $[K : \mathbb{Q}] = n$ and $\alpha \in K$. Then, the multiplication by α gives a $\mathbb{Q}$-linear map

$$\begin{aligned} \mu_\alpha : K &\longrightarrow K \\ x &\mapsto \alpha x. \end{aligned}$$

This map is represented by an $n \times n$ matrix.

Definition

We define the **trace** of α, denoted by $Tr_{K/\mathbb{Q}}(\alpha)$, to be the trace of this matrix, and the **norm** of α, denoted by $N_{K/\mathbb{Q}}(\alpha)$, to be its determinant.

- If $\alpha \in K$, then $N_{K/\mathbb{Q}}(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Q}$.
- $N_{K/\mathbb{Q}}(\alpha) = \prod_{k=1}^{n} \sigma_k(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha) = \sum_{k=1}^{n} \sigma_k(\alpha)$
- If $\alpha \in \mathbb{Z}_K$, then $N_{K/\mathbb{Q}}(\alpha)$ and $Tr_{K/\mathbb{Q}}(\alpha)$ are both in $\mathbb{Z}$.

Suppose that $\omega_1, \ldots, \omega_n$ be arbitrary elements in the number field K of degree n. Consider the matrix:

$$M = \begin{pmatrix} \sigma_1(\omega_1) & \sigma_1(\omega_2) & \cdots & \sigma_1(\omega_n) \\ \sigma_2(\omega_1) & \sigma_2(\omega_2) & \cdots & \sigma_2(\omega_n) \\ \vdots & \vdots & \ddots & \vdots \\ \sigma_n(\omega_1) & \sigma_n(\omega_2) & \cdots & \sigma_n(\omega_n) \end{pmatrix}.$$

Definition

The **discriminant** of $\{\omega_1, \ldots, \omega_n\}$, denoted by $\Delta\{\omega_1, \ldots, \omega_n\}$, is defined as $(\det(M))^2$.

Lemma

If $T = (T_{ij})$ is a matrix with $T_{ij} = Tr_{K/\mathbb{Q}}(\omega_i\omega_j)$, then $\Delta\{\omega_1, \ldots, \omega_n\} = \det(T)$.

Corollary

If $\{\omega_1, \ldots, \omega_n\} \subset \mathbb{Z}_K$, then $\Delta\{\omega_1, \ldots, \omega_n\} \in \mathbb{Z}$.

Proposition

Suppose that the elements of two sets $\{\omega_1, \ldots, \omega_n\}$ and $\{\omega'_1, \ldots, \omega'_n\}$ are related by $\omega'_i = c_{1i}\omega_1 + \cdots + c_{ni}\omega_n$ for rational numbers $c_{ij} \in \mathbb{Q}$. If $C = (c_{ij})$, then

$$\Delta\{\omega'_1, \ldots, \omega'_n\} = (\det(C))^2 \Delta\{\omega_1, \ldots, \omega_n\}.$$

Proposition

The set $\{\omega_1, \ldots, \omega_n\}$ is a basis of K over $\mathbb{Q}$ if and only if $\Delta\{\omega_1, \ldots, \omega_n\} \neq 0$.

Theorem

Let K be a number field. Then, the ring of integers $\mathbb{Z}_K$ a free abelian group of rank $n = [K : \mathbb{Q}]$.

Z_K is a Dedekind Domain

Proposition

$\mathbb{Z}_K$ *is* **integrally closed**.

Proposition

Let K be a number field. Then, every non-zero prime ideal $\mathfrak{p}$ in $\mathbb{Z}_K$ is maximal.

Proposition

If K is a number field, then $\mathbb{Z}_K$ is **Noetherian**.

Definition

An integral domain R is said to be a **Dedekind domain** if one of the following equivalent statements is satisfied:

1. R is an integrally closed, Noetherian domain with Krull dimension one (i.e., every nonzero prime ideal is maximal).
2. Every nonzero proper ideal factors into primes.

Theorem

Let K be a number field with the ring of integers $\mathbb{Z}_K$. Then, $\mathbb{Z}_K$ is a Dedekind domain.

This is what we want to prove throughout this talk.

Definition

The **norm** $N_{K/\mathbb{Q}}(\mathfrak{a})$ of a non-zero ideal $\mathfrak{a}$ in $\mathbb{Z}_K$ is the cardinality $|\mathbb{Z}_K/\mathfrak{a}|$.

- $N_{K/\mathbb{Q}}(\mathfrak{a})$ is finite for every non-zero ideal $\mathfrak{a}$ of $\mathbb{Z}_K$.
- $N_{K/\mathbb{Q}}(\mathfrak{ab}) = N_{K/\mathbb{Q}}(\mathfrak{a})N_{K/\mathbb{Q}}(\mathfrak{b})$ for every non-zero ideal $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathbb{Z}_K$.

Dedekind zeta function

Definition

The **Dedekind zeta function** of a number field K is defined for s with $Re(s) > 1$ by the Dirichlet series

$$\zeta_K(s) = \sum_{\mathfrak{a}} \left(\frac{1}{N_{K/\mathbb{Q}}(\mathfrak{a})} \right)^s,$$

where the sum is over all non-zero ideals $\mathfrak{a}$ of $\mathbb{Z}_K$.

- Euler product exists:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}},$$

where the product is over all prime ideals $\mathfrak{p}$ of $\mathbb{Z}_K$.

Proposition

For any $s = \sigma + it \in \mathbb{C}$ with $\sigma > 1$, $\zeta_K(s)$ converges absolutely.

Proof:

$$|\zeta_K(s)| = \left| \prod_{\mathfrak{p}} \frac{1}{1 - N_{K/\mathbb{Q}}(\mathfrak{p})^{-s}} \right| \leq \prod_{p} (1 - \frac{1}{p^{\sigma}})^{-n} = \zeta(\sigma)^n,$$

since there are at most $n = [K : \mathbb{Q}]$ many primes $\mathfrak{p}$ lying above each rational prime p and $N_{K/\mathbb{Q}}(\mathfrak{p}) \geq p$.

It is natural to ask for generalisations of Riemann's result for $\zeta(s)$ to $\zeta_K(s)$.

- *Dirichlet* showed that $\zeta_K(s)$ has a singularity at $s = 1$ and computed the limit

$$\lim_{s \to 1}(s-1)\zeta_K(s).$$

- $\zeta_K(s)$ has a simple pole at $s = 1$, and Dirichlet's formula gives the residue.

Prime Ideal Theorem

Theorem (Landau, 1903)

Let $\pi_K(x) = |\{\mathfrak{p} \subset \mathbb{Z}_K | N_{K/\mathbb{Q}}(\mathfrak{p}) \leq x\}|$. *Then, there is an asymptotic formula for* $\pi_K(x)$*:*

$$\pi_K(x) \sim x/\log(x).$$

- If $K = \mathbb{Q}$, then $\pi_K(x) = \pi(x)$ and hence the "*Prime Ideal Theorem*" is the extended "*Prime Number Theorem*".

PIT for $\mathbb{Z}_{\mathbb{Q}(i)} = \mathbb{Z}(i)$

If $p = 4k + 3$ be a prime number with $p \leq \sqrt{x}$,then

- $\mathfrak{p} = (p) \subset \mathbb{Z}[i]$ is a prime ideal.
- $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}) = p^2$.

If $p = 4k + 1$ be a prime number with $p \leq x$, then

- $p = a^2 + b^2$ for some integer a, b,
- $p = (a + bi)(a - bi) \in \mathbb{Z}[i]$,
- $\mathfrak{p}_1 = (a + bi)$ and $\mathfrak{p}_2 = (a - bi)$ are prime ideals,
- $N_{\mathbb{Q}(i)/\mathbb{Q}}(\mathfrak{p}_{1,2}) = p$.

Therefore,

$$\pi_{\mathbb{Q}(i)}(x) \sim \frac{\pi(\sqrt{x})}{2} + \frac{2\pi(x)}{2} \sim \frac{x}{log(x)}.$$

Further Topics

Extended Riemann Hypothesis

The nontrivial zeros of the Dedekind zeta function of any number field K lie on the critical line: $Re(s) = 1/2$.

- If $K = \mathbb{Q}$, then the "*Extended Riemann Hypothesis*" is, indeed the "*Riemann Hypothesis*".

References

 F. Oggier, Lecture Notes on Introduction to Algebraic Number Theory.

 F. Jarvis, Algebraic Number Theory, Springer, 2014.

 Hugh L. Montgomery, Robert C. Vaughan, Multiplicative Number Theory: I. Classical Theory, Cambridge University Press, 2006.