Computational explorations of reciprocity laws in number theory

Chul-hee Lee

Korea Institute for Advanced Study

August 8-9, 2023

References

1. F. R. Villegas. Chapter 2 of "Experimental Number Theory." Oxford Graduate Texts in Mathematics, 2007.
2. B. F. Wyman. "What is a Reciprocity Law?", The American Mathematical Monthly, Vol. 79, No. 6 (Jun. - Jul., 1972), pp. 571-586.
3. P. Stevenhagen, H. W. Lenstra. "Chebotarëv and his density theorem." The Mathematical Intelligencer 18, 26–37 (1996).
4. Jürgen Neukirch. "Algebraic Number Theory." (Grundlehren der mathematischen Wissenschaften), Springer, 1999.

Visit the GitHub repository at the following URL:

`https://github.com/chlee-0/exp_math`.

Click the Binder icon launch binder to launch the interactive PARI/GP environment.

Quadratic Reciprocity Law

Let p and q be distinct odd prime numbers. The Legendre symbol $\left(\frac{p}{q}\right)$ is defined as:

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{if } p \text{ is a quadratic residue modulo } q, \\ -1 & \text{if } p \text{ is a quadratic non-residue modulo } q. \end{cases}$$

The quadratic reciprocity law states that:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

Factorization of $x^2 - q$ modulo a prime p

- If $\left(\frac{q}{p}\right) = 1$, then there exists an integer α such that $\alpha^2 \equiv q \mod p$. In this case, $x^2 - q$ factors as $(x - \alpha)(x + \alpha)$ modulo p.
- If $\left(\frac{q}{p}\right) = -1$, then there does not exist an integer α such that $\alpha^2 \equiv q \mod p$. In this case, $x^2 - q$ is irreducible modulo p.
- The Quadratic Reciprocity Law implies that the factorization of $x^2 - q$ modulo a prime p depends on the congruence class of p modulo $4q$:
  - If $p \equiv 1 \pmod 4$, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.
  - If $p \equiv 3 \pmod 4$, then $\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right)$.

Reciprocity Laws

What is a reciprocity law? A rough and tentative answer is :

> A reciprocity law is a rule to describe the factorization of a monic polynomial with integral coefficients as a function of the prime numbers.

Factorization type of f modulo p

- Let $f \in \mathbb{Z}[x]$ be a monic polynomial of degree n with $\Delta(f) \neq 0$, i.e., all the n roots of f are distinct.
- Consider a prime number p and the reduction of f modulo p.
- Suppose that f factors into irreducible polynomials modulo p with degrees $n_1, n_2, \ldots, n_k$ in descending order, i.e., $n_1 \geq n_2 \geq \cdots \geq n_k$.
- We call $\tau_p := [n_1, n_2, \ldots, n_k]$ as the *factorization type* of f modulo p.
- Then τ_p is a partition of n.

Factorization type of f modulo p

Consider the polynomial $f = x^4 + 3x^2 + 7x + 4$.

- Factorizing f modulo 2, we find $f \equiv x \cdot (x^3 + x + 1)$. Both x and $x^3 + x + 1$ are irreducible over $\mathbb{F}_2$. Therefore, $\tau_2 = [3, 1]$.
- However, modulo 11, f decomposes as $f \equiv (x^2 + 5x - 1) \cdot (x^2 - 5x - 4)$. Both factors are irreducible over $\mathbb{F}_{11}$. Therefore, $\tau_{11} = [2, 2]$.
- This proves that f is irreducible over $\mathbb{Z}$.

We can use τ_p to check the irreducibility of f.

Cubic Case

Let us consider $f = x^3 + x^2 - 2x - 1$. Look at the table for the factorization types of f modulo prime numbers.
We can observe that

$$\tau_p = \begin{cases} [1,1,1] & \text{if } p \equiv \pm 1 \bmod 7, \\ [3] & \text{otherwise.} \end{cases}$$

Cubic Case

- What about $g = x^3 + x + 1$?
- Our observation can be illustrated as follows:

$$\tau_p = \begin{cases} [2,1] & \text{if } p \equiv 3, 6, 11, 12, 13, 15, 17, 21, 22, 23, \\ & \quad 24, 26, 27, 29, 30 \mod 31, \\ [3] \text{ or } [1,1,1] & \text{if } p \equiv 1, 2, 4, 5, 7, 8, 9, 10, 14, \\ & \quad 16, 18, 19, 20, 25, 28 \mod 31 \end{cases}$$

- We observe that $\tau_p = [2, 1]$ if the Legendre symbol $\left(\frac{p}{31}\right) = -1$. However, distinguishing between the factorization types [3] and [1, 1, 1] presents a challenge when using congruences on p alone.
- Given a value of N, we can search for two prime numbers p and q such that $p \equiv q \mod N$ but the factorization types τ_p and τ_q are different.

Cyclotomic polynomial

The n-th cyclotomic polynomial, denoted by $\Phi_n(x)$, is the polynomial whose roots are precisely the primitive n-th roots of unity.

Properties:

- $\Phi_n(x)$ has degree $\phi(n)$, where ϕ is Euler's totient function.
- The coefficients of $\Phi_n(x)$ are integers.
- $\Phi_n(x)$ is irreducible over $\mathbb{Q}$.
- The Galois group of the splitting field $\mathbb{Q}(\zeta_n)$ of $\Phi_n(x)$ over $\mathbb{Q}$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$, the group of units modulo n.

Factorization of cyclotomic polynomial

Let's examine the factorization type of the cyclotomic polynomial Φ_m modulo p.
For example, consider $\Phi_{12} = x^4 - x^2 + 1$.
The factorization type of Φ_{12} modulo p depends solely on the residue class of p modulo 12:

$$\tau_p = \begin{cases} [1,1,1,1] & \text{if } p \equiv 1 \mod 12, \\ [2,2] & \text{if } p \equiv 5,7,11 \mod 12, \end{cases}$$

Factorization of cyclotomic polynomial

Consider the cyclotomic polynomial $\Phi_{10} = x^4 - x^3 + x^2 - x + 1$.
The factorization type of this polynomial, given $m = 10$, depends solely on the residue class of p modulo 10:

$$\tau_p = \begin{cases} [1,1,1,1] & \text{if } p \equiv 1 \mod 10, \\ [4] & \text{if } p \equiv 3,7 \mod 10, \\ [2,2] & \text{if } p \equiv 9 \mod 10. \end{cases}$$

Quartic polynomials

Consider a different quartic polynomial. Let $f = x^4 - x - 1$.
The factorization type can be described as follows:

$$\tau_p = \begin{cases} [4] \text{ or } [2,1,1] & \text{if } \left(\frac{p}{283}\right) = -1 \\ [3,1] \text{ or } [2,2] \text{ or } [1,1,1,1] & \text{if } \left(\frac{p}{283}\right) = 1 \end{cases}$$

However, it is challenging to distinguish between the different factorization types using congruences on p alone.

Weak form of a reciprocity law for abelian polynomials

Let $f \in \mathbb{Z}[x]$ with $\Delta(f) \neq 0$. This ensures that f factors into distinct irreducible factors as

$$f = f_1 \cdot \ldots \cdot f_r$$

and each $K_i = \mathbb{Q}[x]/(f_i)$ is a number field.

Theorem

There exists a natural number m such that τ_p is only dependent on p mod m if and only if each extension $K_i/\mathbb{Q}$ is abelian, that is, it is Galois and its Galois group is abelian.

Abelian vs. Non-abelian

- Let $f \in \mathbb{Z}[x]$ be monic irreduible.
- Let $K = \mathbb{Q}[x]/(f)$, and let $L/\mathbb{Q}$ be its Galois closure, i.e., the field obtained by adjoining all roots of f.
- Set $G := \mathrm{Gal}(L/\mathbb{Q})$.
- In the case of cubic extensions, there are two possibilities:
  - $K = L$ and G is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.
  - $K \subsetneq L$ and G isomorphic to the non-abelian group S_3.
- We saw two cubic examples $f = x^3 + x^2 - 2x - 1$ and $g = x^3 + x + 1$.
- Here, $\mathbb{Q}[x]/(f)$ is abelian, and $\mathbb{Q}[x]/(g)$ is not.

Frobenius Density Theorem

- Let $f \in \mathbb{Z}[x]$ be monic with $\Delta(f) \neq 0$.
- Let $L/\mathbb{Q}$ be the field obtained by adjoining all roots of f, and G be the Galois group.
- We have an action of G on the roots of the polynomial f, which, after labeling them in some way, gives an embedding $\iota : G \hookrightarrow S_n$, where $n = \deg(f)$.
- Recall that any $\sigma \in S_n$ has an essentially unique decomposition into disjoint cycles $\sigma = \eta_1 \cdot \ldots \cdot \eta_k$. Reorder these cycles so that $n_1 \geq n_2 \geq \ldots \geq n_k$, where n_j is the length of η_j. The conjugacy class of σ in S_n is uniquely determined by this partition.
- The lengths of these cycles give the *cycle pattern* $[n_1, n_2, \ldots, n_k]$ of σ, which is a partition of n.

Frobenius Density Theorem

The Frobenius Density Theorem states that the density of primes p for which a polynomial f has a given factorization type $[n_1, n_2, ..., n_k]$ exists, and it is equal to $\frac{1}{|G|}$ times the number of $\sigma \in G$ with cycle pattern $[n_1, n_2, ..., n_k]$.

Example

Consider $f = x^4 - x^3 + x^2 - x + 1$.
The factorization type of f depends solely on the residue class of p modulo 10:

$$\tau_p = \begin{cases} [1,1,1,1] & \text{if } p \equiv 1 \mod 10, \\ [4] & \text{if } p \equiv 3,7 \mod 10, \\ [2,2] & \text{if } p \equiv 9 \mod 10. \end{cases}$$

The Galois group is isomorphic to the cyclic group of order 4:

$$C_4 = \{(), (1234), (13)(24), (1432)\}$$

whose elements have cycle patterns $[1,1,1,1]$, $[4]$, $[2,2]$, and $[4]$, respectively.

Example

Consider $f = x^4 - x^2 + 1$.
The factorization type of f depends solely on the residue class of p modulo 12:

$$\tau_p = \begin{cases} [1,1,1,1] & \text{if } p \equiv 1 \mod 12, \\ [2,2] & \text{if } p \equiv 5, 7, 11 \mod 12, \end{cases}$$

The Galois group is isomorphic to the Klein 4 group:

$$V_4 = \{(), (12)(34), (13)(24), (14)(23)\}$$

whose elements have cycle patterns $[1,1,1,1]$, $[2,2]$, $[2,2]$, and $[2,2]$, respectively.

Cubic Case

The table presents the density of primes p for which f modulo p exhibits a specific factorization type.

f	[3]	[2, 1]	[1, 1, 1]
$x^3 + x^2 - 2x - 1$	$2/3$	0	$1/3$
$x^3 + x + 1$	$1/3$	$1/2$	$1/6$

Quartic case

The table presents the results of similar experiments conducted on several quartic polynomials, showing the apparent density of primes p for which f modulo p exhibits a specific factorization type.

f	[4]	[3, 1]	[2, 2]	[2, 1, 1]	[1, 1, 1, 1]
$x^4 - x - 1$	$1/4$	$1/3$	$1/8$	$1/4$	$1/24$
$x^4 - x^2 + 1$	0	0	$3/4$	0	$1/4$
$x^4 - x^3 + x^2 - x + 1$	$1/2$	0	$1/4$	0	$1/4$
$x^4 - x^2 - 1$	$1/4$	0	$3/8$	$1/4$	$1/8$
$x^4 + 3x^2 + 7x + 4$	0	$2/3$	$1/4$	0	$1/12$

Quartic case

The last column indicates that the Galois groups of the five polynomials in the table have orders 24, 4, 4, 8, and 12, respectively.

- The Galois group of order 24 corresponds to the symmetric group S_4.
- The Galois groups of order 4 correspond to the Klein four-group V_4 and the cyclic group C_4.
- The Galois group of order 8 corresponds to the dihedral group D_4.
- The Galois group of order 12 corresponds to the alternating group A_4.

This provides a complete list of transitive subgroups of S_4. Consequently, every irreducible polynomial f of degree 4 behaves similarly to one of the polynomials in the table.

We can use τ_p to identify the Galois group of a polynomial statistically.

Application of Frobenius density theorem

We say that the factorization type of $x^{12} - 1$ modulo p depends solely on the residue class of p modulo 12:

$$\tau_p = \begin{cases} [1,1,1,1,1,1,1,1,1,1,1,1] & \text{if } p \equiv 1 \mod 12, \\ [2,2,2,2,1,1,1,1] & \text{if } p \equiv 5 \mod 12, \\ [2,2,2,1,1,1,1,1,1] & \text{if } p \equiv 7 \mod 12, \\ [2,2,2,2,2,1] & \text{if } p \equiv 11 \mod 12. \end{cases}$$

According to Frobenius density theorem, each factorization type has non-zero density. This implies the special case $m = 12$ of Dirichlet's theorem, namely, there are infinitely many primes in each congruence class modulo 12.

Application of Frobenius density Theorem

The factorization type of $x^{10} - 1$ depends solely on the residue class of p modulo 10:

$$\tau_p = \begin{cases} [1,1,1,1,1,1,1,1,1,1] & \text{if } p \equiv 1 \mod 10, \\ [4,4,1,1] & \text{if } p \equiv 3,7 \mod 10, \\ [2,2,2,2,1,1] & \text{if } p \equiv 9 \mod 10. \end{cases}$$

Frobenius density theorem implies that there are infinitely many primes p whose $\tau_p = [4,4,1,1]$. But, we are not able to distinguish between the residue classes $3 \mod 10$ and $7 \mod 10$. So we cannot prove the special case $m = 10$ of Dirichlet's theorem from Frobenius density theorem.

Chebotarev Density Theorem

- Let $f \in \mathbb{Z}[x]$ be monic with $\Delta(f) \neq 0$.
- Let $L/\mathbb{Q}$ be the field obtained by adjoining all roots of f, and G be the Galois group.
- For a prime p, there is a way to attach a conjugacy class of G, denoted by Frob_p, known as the Frobenius element.
- The Frobenius element Frob_p gives finer information than the factorization type τ_p.
- The Chebotarev Density Theorem states that for a conjugacy class C of G, the set of primes p whose Frobenius elements Frob_p equal C has a density given by $\frac{|C|}{|G|}$.

Application of Chebotarev theorem

The factorization type of $x^{10} - 1$:

$$\tau_p = \begin{cases} [1,1,1,1,1,1,1,1,1,1] & \text{if } p \equiv 1 \mod 10, \\ [4,4,1,1] & \text{if } p \equiv 3,7 \mod 10, \\ [2,2,2,2,1,1] & \text{if } p \equiv 9 \mod 10. \end{cases}$$

An element of the Galois group is determined by the image of $\alpha := e^{2\pi i/10}$ and

$$\mathrm{Frob}_p = \begin{cases} (\alpha \mapsto \alpha) & \text{if } p \equiv 1 \mod 10, \\ (\alpha \mapsto \alpha^3) & \text{if } p \equiv 3 \mod 10, \\ (\alpha \mapsto \alpha^7) & \text{if } p \equiv 7 \mod 10, \\ (\alpha \mapsto \alpha^9) & \text{if } p \equiv 9 \mod 10. \end{cases}$$

We can prove the special case $m = 10$ of Dirichlet's theorem from the Chebotarev density theorem.

Computing Frob_p

If $f = f_1 \cdot \ldots \cdot f_r$ with $f_j \in \mathbb{F}_p[x]$ being irreducible polynomials of degree n_j for $j = 1, \ldots, r$, then

$$\mathbb{F}_p[x]/(f) \cong \mathbb{F}_{p^{n_1}} \times \ldots \times \mathbb{F}_{p^{n_r}},$$

where $\mathbb{F}_{p^{n_j}} \cong \mathbb{F}_p[x]/(f_j)$.
Each of the finite field extensions $\mathbb{F}_{p^{n_j}}/\mathbb{F}_p$ has an automorphism $x \mapsto x^p$. This automorphism is called the *Frobenius automorphism*. It arises from a unique $\sigma_j \in G$ of order n_j.

Computing Frob_p : steps

1. Assume that f is irreducible.
2. Find all the conjugate roots $g_k(x)$ of f as a polynomial in x, i.e.,
$$f(g_k(x)) \equiv 0 \mod f.$$
3. Let $f = f_1 \cdot \ldots \cdot f_r$ with $f_j \in \mathbb{F}_p[x]$ irreducible of degree n_j for $j = 1, \ldots, r$.
4. For each $p \notin S_f$ and $j = 1, 2, \ldots, r$, there exists a unique $g_k(x)$ such that
$$x^p \equiv g_k(x) \mod f_j, \text{ in } \mathbb{F}_p[x].$$
This element g_k represents $\sigma_j \in G$.
5. Then Frob_p can be written as a list $[\sigma_1, \ldots, \sigma_r]$. Here σ_j are conjugate elements in G.

We can use factorization of a polynomial modulo p to compute Frob_p.

Computing Frob_p: example

Let $f = x^4 - x^3 + x^2 - x + 1$.

p	τ_p	Frob_p
7	[4]	[3]
11	[1, 1, 1, 1]	[1, 1, 1, 1]
13	[4]	[2]
17	[4]	[3]
19	[2, 2]	[4, 4]
23	[4]	[2]
29	[2, 2]	[4, 4]
31	[1, 1, 1, 1]	[1, 1, 1, 1]
37	[4]	[3]
41	[1, 1, 1, 1]	[1, 1, 1, 1]
43	[4]	[2]

This shows that there are 4 conjugacy classes in the Galois group parametrized by:

$$[1], [2], [3], [4]$$

Computing Frob_p

Let $f = x^8 + 2x^7 + 2x^6 - 2x^5 - 2x^4 - 2x^3 + 2x^2 + 2x + 1$.

p	τ_p	Frob_p
7	[4, 4]	[2, 7]
11	[2, 2, 2, 2]	[3, 3, 4, 4]
13	[2, 2, 2, 2]	[5, 5, 8, 8]
17	[2, 2, 2, 2]	[5, 5, 8, 8]
19	[2, 2, 2, 2]	[3, 3, 4, 4]
23	[4, 4]	[2, 7]
29	[1, 1, 1, 1, 1, 1, 1, 1]	[1, 1, 1, 1, 1, 1, 1, 1]
31	[2, 2, 2, 2]	[3, 3, 4, 4]
37	[2, 2, 2, 2]	[5, 5, 8, 8]
41	[2, 2, 2, 2]	[6, 6, 6, 6]
43	[4, 4]	[2, 7]

This shows that there are 5 conjugacy classes in the Galois group parametrized by:

$$[1], [2, 7], [3, 4], [5, 8], [6]$$

A form of the Artin reciprocity law

Let $f \in \mathbb{Z}[x]$ be monic and irreducible.

Theorem

Assume that $K = \mathbb{Q}[x]/(f)$ is abelian. There exists a natural number m such that Frob_p is only dependent on $p \mod m$.

For more details, refer to Section VI.7 of Neukirch's book on algebraic number theory.

Dedekind zeta function

- The Dedekind zeta function $\zeta_K(s)$ associated with a number field K is defined as:
$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{N(\mathfrak{a})^s}$$
- The sum runs over all non-zero ideals $\mathfrak{a}$ in the ring of integers $\mathcal{O}_K$ of K.
- The norm $N(\mathfrak{a})$ of an ideal $\mathfrak{a}$ is defined as the cardinality of the quotient ring $\mathcal{O}_K/\mathfrak{a}$.

Euler Product

- The Euler product is a way to express zeta functions as an infinite product over all prime numbers.
- For the Riemann zeta function, the Euler product is given by:

$$\zeta(s) = \zeta_{\mathbb{Q}}(s) = \prod_{p} \left(1 - p^{-s}\right)^{-1}$$

  where the product is over all prime numbers p.
- Similarly, the Dedekind zeta function $\zeta_K(s)$ can also be expressed as an Euler product:

$$\zeta_K(s) = \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

  where the product runs over all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$.
- This is derived from the unique factorization of ideals in the ring of integers $\mathcal{O}_K$.

Norm computation

- For a prime ideal $\mathfrak{p}$, the quotient ring $\mathcal{O}_K/\mathfrak{p}$ is a finite field.
- Therefore, the norm $N(\mathfrak{p})$ is of the form p^f for some prime p and integer f.
- To determine the factors in the Euler product, we need a way to find $N(\mathfrak{p})$.

Norm and inertia degree of a prime ideal

Let $K/\mathbb{Q}$ be a finite extension, and let $\mathcal{O}_K$ be the ring of integers of K.

$$\begin{array}{ccc} \mathbb{Z} & \hookrightarrow & \mathcal{O}_K \\ \downarrow & & \downarrow \\ \mathbb{Q} & \hookrightarrow & K \end{array}$$

Let p be a prime in $\mathbb{Z}$. The unique factorization of ideals in $\mathcal{O}_K$ leads to

$$p\mathcal{O}_K = \prod_{j=1}^{g} \mathfrak{p}_j^{e_j}.$$

Here, the ideal $p\mathcal{O}_K$ is decomposed into a product of distinct prime ideals $\mathfrak{p}_j$, with multiplicities e_j.
The field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ naturally embeds into $F_j = \mathcal{O}_K/\mathfrak{p}_j$ for every j. The degree $f_j = [\mathcal{O}_K/\mathfrak{p}_j : \mathbb{F}_p]$ is called the *inertia degree* of $\mathfrak{p}_j$ over p.

Computing prime factorization

To factorize $p\mathcal{O}_K$ for a prime $p \in \mathbb{Z}$ into primes of $\mathcal{O}_K$, we follow these steps:

1. Select an integer θ in $\mathcal{O}_K$ that generates K over $\mathbb{Q}$, i.e., $K = \mathbb{Q}(\theta)$.
2. Find the minimal polynomial $h(x) \in \mathbb{Z}[x]$ of θ.
3. Factorize $h(x)$ into distinct irreducible polynomials $\bar{h}_1(x), \bar{h}_2(x), \dots, \bar{h}_n(x)$ in $\mathbb{F}_p[x]$, with $h_i(x) \in \mathbb{Z}[x]$ being monic.
4. The factorization of $p\mathcal{O}_K$ in $\mathcal{O}_K$ is given by $p\mathcal{O}_K = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$, where $\mathfrak{p}_j = p\mathcal{O}_K + h_j(\theta)O_K$.

In particular, the inertia degree of $\mathfrak{p}_j$ is the degree of h_j.

We can use factorization of a polynomial modulo p to find prime ideal decompositions.

Frobenius element

Let $K/\mathbb{Q}$ be a Galois extension, and $\mathfrak{p}$ be a prime ideal in K above p. Let $D_{\mathfrak{p}}$ be the subgroup of $\mathrm{Gal}(K/\mathbb{Q})$ preserving $\mathfrak{p}$
If p is unramified in K, then $D_{\mathfrak{p}}$ is canonically isomorphic to the Galois group of the extension of residue fields $\mathcal{O}_K/\mathfrak{p}$ over $\mathbb{Z}/p\mathbb{Z}$.
The Frobenius element associated with $\mathfrak{p}$, denoted as $\mathrm{Frob}_{\mathfrak{p}}$ or $\left(\frac{K/\mathbb{Q}}{\mathfrak{p}}\right)$, is the unique element in $D_{\mathfrak{p}}$ that acts as the Frobenius automorphism on the residue field extension, i.e.,

$$\mathrm{Frob}_{\mathfrak{p}}(x) \equiv x^p \mod \mathfrak{p}.$$

Example: The Gaussian Integers

- Consider the field extension $\mathbb{Q}(i)/\mathbb{Q}$.
- The ring of integers $\mathcal{O}_K$ in $\mathbb{Q}(i)$ is simply $\mathbb{Z}[i]$, the Gaussian integers.
- We will examine the behavior of prime ideals in this extension by factoring $x^2 + 1$ modulo p.

Example: The Gaussian Integers (Continued)

- Let's consider $p = 13$.
- The polynomial $x^2 + 1$ factorizes modulo 13 as $(x+5)(x-5)$.
- Hence, two prime ideals over (13) are $(13, i+5)$ and $(13, i-5)$, respectively.
- As $\mathbb{Z}[i]$ is a principal ideal domain, we can find single generators for these prime ideals:

$$(13, i+5) = (2+3i) \quad \text{and} \quad (13, i-5) = (2-3i).$$

- The residue fields $\mathbb{Z}[i]/(2+3i)$ and $\mathbb{Z}[i]/(2-3i)$ are both isomorphic to the finite field with 13 elements.
- In general, for primes $p \equiv 1 \mod 4$ in $\mathbb{Z}$, they split into two distinct prime ideals in $\mathbb{Z}[i]$, and each of these prime ideals has an inertia degree of 1.

Example: The Gaussian Integers (Continued)

- Let's take $p = 7$ as an example.
- The polynomial $x^2 + 1$ is irreducible modulo 7.
- The prime (7) remains prime in $\mathbb{Z}[i]$.
- The residue field $\mathbb{Z}[i]/(7)$ is a finite field with 7^2 elements, isomorphic to $\mathbb{F}_7[x]/(x^2 + 1)$.
- In general, for primes $p \equiv 3 \mod 4$ in $\mathbb{Z}$, they remain prime in $\mathbb{Z}[i]$, and the prime ideal has an inertia degree of 2.

Example: The Gaussian Integers (Continued)

- For the prime $p = 2$ in $\mathbb{Z}$, it ramifies in $\mathbb{Z}[i]$.
- The ideal (2) in $\mathbb{Z}[i]$ can be factored as $(1+i)^2$.
- The residue field extension $\mathbb{Z}[i]/(1+i)$ is a finite field with 4 elements:
- Thus, the norm $N((1+i)) = 2^2 = 4$.

Dedekind zeta function of quadratic fields

- For a quadratic field $K = \mathbb{Q}(\sqrt{d})$, the ideal $(p) \subseteq \mathcal{O}_K$ factors into three types:
  1. (**Split**) $(p) = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = p$.
  2. (**Inert**) $(p) = \mathfrak{p}$ with $N(\mathfrak{p}) = p^2$.
  3. (**Ramify**) $(p) = \mathfrak{p}^2$ with $N(\mathfrak{p}) = p$.
- The Dedekind zeta function becomes:

$$\zeta_K(s) = \prod_{p:\text{split}} \left(1 - p^{-s}\right)^{-2} \cdot \prod_{p:\text{inert}} \left(1 - p^{-2s}\right)^{-1} \cdot \prod_{p:\text{ramify}} \left(1 - p^{-s}\right)^{-1}$$

- This can be written as

$$\zeta_K(s) = \zeta(s) \prod_{p:\text{split}} \left(1 - p^{-s}\right)^{-1} \prod_{p:\text{inert}} \left(1 + p^{-s}\right)^{-1}.$$

- The quadratic reciprocity law implies that we can differentiate between the split and inert cases using a congruence condition.

Dedekind zeta function of cyclotomic fields

The factorization type of $\Phi_{10}(x) = x^4 - x^3 + x^2 - x + 1$:

$$\tau_p = \begin{cases} [1,1,1,1] & \text{if } p \equiv 1 \mod 10, \\ [4] & \text{if } p \equiv 3,7 \mod 10, \\ [2,2] & \text{if } p \equiv 9 \mod 10. \end{cases}$$

Hence, the Dedekind zeta function $\zeta_K(s)$ of $K = \mathbb{Q}(\zeta_{10})$ (up to factors for the ramified primes) is

$$\zeta_K(s) = \prod_{p:p\equiv 1} \left(1 - p^{-s}\right)^{-4} \prod_{p:p\equiv 3,7} \left(1 - p^{-4s}\right)^{-1} \prod_{p:p\equiv 9} \left(1 - p^{-2s}\right)^{-2}$$

Dirichlet L-functions

- A Dirichlet character is a completely multiplicative arithmetic function $\chi : \mathbb{Z} \to \mathbb{C}$ that is periodic with some period $k > 0$, and satisfies $\chi(n) = 0$ if $\gcd(n, k) > 1$.
- Given a Dirichlet character χ, the associated Dirichlet L-function $L(s, \chi)$ is defined by

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, \quad \Re(s) > 1$$

- Euler product :

$$L(s,\chi) = \prod_{p} \left(1 - \chi(p)p^{-s}\right)^{-1}$$

where the product is over all prime numbers p.

Dirichlet characters modulo 10

Here, the table provides the values of Dirichlet characters $\chi_i(n)$ for different congruence classes of n modulo 10.

	$n \equiv 1$	$n \equiv 3$	$n \equiv 7$	$n \equiv 9$
$\chi_0(n)$	1	1	1	1
$\chi_1(n)$	1	$-i$	i	-1
$\chi_2(n)$	1	-1	-1	1
$\chi_3(n)$	1	i	$-i$	-1

For a given prime number p, we have

$$\prod_{i=0}^{3}(1-\chi_i(p)p^{-s})^{-1} = \begin{cases} (1-p^{-s})^{-4}, & \text{if } p \equiv 1, \\ \left(1-p^{-4s}\right)^{-1}, & \text{if } p \equiv 3, 7, \\ \left(1-p^{-2s}\right)^{-2}, & \text{if } p \equiv 9. \end{cases}$$

Using this, we can factor the Dedekind zeta function of $K = \mathbb{Q}(\zeta_{10})$ in terms of Dirichlet L-functions.

Factorization of Dedekind Zeta Function for cyclotomic Fields

- More generally, the Dedekind zeta function of the cyclotomic field $K = \mathbb{Q}(\zeta_n)$ can be expressed as a product of Dirichlet L-functions:

$$\zeta_K(s) = \zeta_{\mathbb{Q}}(s) \prod_{\chi \neq \chi_0} L(s, \chi),$$

  where the product is taken over all non-trivial Dirichlet characters modulo n.
- This follows from the fact that the factorization type of the cyclotomic polynomial modulo p is determined by the congruence condition of p modulo n, which is itself a consequence of the abelian nature of the field extension $K/\mathbb{Q}$.

In other words, the factorization of $\zeta_K(s)$ into a product of Dirichlet L-functions is a consequence of the reciprocity law.

For a Galois extension L/K with the Galois group $G(L|K)$, there is a factorization

$$\zeta_L(s) = \zeta_K(s) \prod_{\chi:\chi\neq 1} \mathcal{L}(L|K,\chi,s)^{\chi(1)},$$

where χ varies over the non-trivial irreducible characters of $G(L|K)$, and $\mathcal{L}(L|K,\chi,s)$ is the Artin L-function.
Artin studied the question of whether $\zeta_L(s)/\zeta_K(s)$ is entire.

- When L/K is abelian, $\mathcal{L}(L|K,\chi,s)$ can be identified with the Hecke L-series $\mathcal{L}(\widetilde{\chi},s)$ for the the Grössencharacter $\widetilde{\chi}$. The existence of $\widetilde{\chi}$ is a consequence of class field theory, where the Artin reciprocity is the central result.
- In general, $\mathcal{L}(L|K,\chi,s)$ is still unknown to be entire. This is the Artin conjecture. One of the aims of the Langlands program is to establish this.

Thank You!