Higher reciprocity law

William Sean H (10120026)

Advisor : Aleams Barra, S.Si., M.Si., Ph.D
Examiner : Prof. Dr. Muchtadi Intan Detiena, S.Si, M.Si

21 December 2023

Outline of talk

Table of Contents

Fermat

Fermat : $p \neq 2$,
$$p = x^2 + y^2 \iff p = 4n + 1$$

Fermat

Fermat : $p \neq 2$,

$$p = x^2 + y^2 \iff p = 4n + 1$$

Similarly, $p \neq 2$,

$$p = x^2 + 2y^2 \iff p = 8n + 1 \text{ or } p = 8n + 3$$

Reduction modulo p

For $a \in \mathbb{Z}$, classify a with its remainder on p

Reduction modulo p

For $a \in \mathbb{Z}$, classify a with its remainder on p

Define $\bar{a} + \bar{b} = \overline{(a+b)}$ and $\bar{a}\bar{b} = \overline{(ab)}$

Quadratic residues

If

$$p = ax^2 + bxy + cy^2$$

then

$$\bar{a}x^2 + \bar{b}xy + \bar{c}y^2$$

has a non-trivial solution modulo p

Quadratic residues

If

$$p = ax^2 + bxy + cy^2$$

then

$$\bar{a}x^2 + \bar{b}xy + \bar{c}y^2$$

has a non-trivial solution modulo p

$p = x^2 + y^2 \to x^2 + \bar{1}$ has a solution modulo $p \to x^2 + \bar{1} \equiv (x + \bar{t})(x + \bar{s})$ mod p

Gaussian integers

$$p = x^2 + y^2 = (x + iy)(x - iy)$$

For $x, y \in \mathbb{Z}$

Gaussian integers

$$p = x^2 + y^2 = (x + iy)(x - iy)$$

For $x, y \in \mathbb{Z}$

p is not a prime in $\mathbb{Z}(i)$

Table of Contents

Algebraic extension

$\mathbb{Q}(i)$ is an extension over $\mathbb{Q}$ with degree 2

Algebraic extension

$\mathbb{Q}(i)$ is an extension over $\mathbb{Q}$ with degree 2

Pick $f(x) \in \mathbb{Q}[x]$ and some roots $\alpha_1, ..., \alpha_n$

Algebraic extension

$\mathbb{Q}(i)$ is an extension over $\mathbb{Q}$ with degree 2

Pick $f(x) \in \mathbb{Q}[x]$ and some roots $\alpha_1, ..., \alpha_n$

We call $\mathbb{Q}(\alpha_1, ..., \alpha_n)$ as the field $\mathbb{Q}$ 'adjoined' by the numbers $\alpha_1, ..., \alpha_n$

Number Fields and Galois group

A finite degree extension K of $\mathbb{Q}$ is called a number field

Number Fields and Galois group

A finite degree extension K of $\mathbb{Q}$ is called a number field

The automorphisms of K, denoted by $\mathrm{Gal}(K/\mathbb{Q})$, form a finite group under composition

Number Fields and Galois group

A finite degree extension K of $\mathbb{Q}$ is called a number field

The automorphisms of K, denoted by $\mathrm{Gal}(K/\mathbb{Q})$, form a finite group under composition

K is normal if $|\,\mathrm{Gal}(K/\mathbb{Q})\,| = [K:\mathbb{Q}]$

Algebraic integers

Denote $\mathfrak{O}_K$ as the algebraic integers in K

Algebraic integers

Denote $\mathfrak{O}_K$ as the algebraic integers in K

The set $\mathfrak{O}_K$ form a ring

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

For ideals A and B, $A + B = \{a + b | a \in A, b \in B\}$

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

For ideals A and B, $A + B = \{a + b | a \in A, b \in B\}$

Every ideal in $\mathfrak{O}_k$ is finitely generated.

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

For ideals A and B, $A + B = \{a + b | a \in A, b \in B\}$

Every ideal in $\mathfrak{O}_k$ is finitely generated.

For the product, define $a\mathfrak{O}_K b\mathfrak{O}_K = ab\mathfrak{O}_K$ and continue it distributively

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

For ideals A and B, $A + B = \{a + b | a \in A, b \in B\}$

Every ideal in $\mathfrak{O}_k$ is finitely generated.

For the product, define $a\mathfrak{O}_K b\mathfrak{O}_K = ab\mathfrak{O}_K$ and continue it distributively

For example, $(a\mathbb{Z} + b\mathbb{Z})(c\mathbb{Z} + d\mathbb{Z}) = ac\mathbb{Z} + bc\mathbb{Z} + ad\mathbb{Z} + bd\mathbb{Z}$

Ideal numbers

For $\alpha \in \mathfrak{O}_K$, the principal ideal generated by a is the set of multiples of a in $\mathfrak{O}_K$

For ideals A and B, $A + B = \{a + b | a \in A, b \in B\}$

Every ideal in $\mathfrak{O}_k$ is finitely generated.

For the product, define $a\mathfrak{O}_K b\mathfrak{O}_K = ab\mathfrak{O}_K$ and continue it distributively

For example, $(a\mathbb{Z} + b\mathbb{Z})(c\mathbb{Z} + d\mathbb{Z}) = ac\mathbb{Z} + bc\mathbb{Z} + ad\mathbb{Z} + bd\mathbb{Z}$

For 2 ideals A and B in $\mathfrak{O}_K$, $|\mathfrak{O}_K/AB| = |\mathfrak{O}_K/A||\mathfrak{O}_K/B|$

Prime ideals

$p \in \mathbb{N}$ is prime if and only if $p\mathbb{Z}$ is maximal

Prime ideals

$p \in \mathbb{N}$ is prime if and only if $p\mathbb{Z}$ is maximal

So in an algebraic number field K, we can think of the primes as the maximal ideals in the ring $\mathfrak{O}_K$

Unique factorization

Adding 2 ideals and multiplying 2 ideals gives another ideal, and $a_1\mathbb{Z}...a_m\mathbb{Z} = (a_1...a_m)\mathbb{Z}$

Unique factorization

Adding 2 ideals and multiplying 2 ideals gives another ideal, and $a_1\mathbb{Z}...a_m\mathbb{Z} = (a_1...a_m)\mathbb{Z}$

We can generalize integer factorization into ideal factorization

Unique factorization

Adding 2 ideals and multiplying 2 ideals gives another ideal, and $a_1\mathbb{Z}...a_m\mathbb{Z} = (a_1...a_m)\mathbb{Z}$

We can generalize integer factorization into ideal factorization

Every ideal in a number field has unique factorization from prime ideals

Quadratic reciprocity law

$$p = x^2 + y^2 \text{ or } p = x^2 + 2y^2 \iff x^2 + 1 \text{ or } x^2 + 2\text{has a solution modulo} p$$

Quadratic reciprocity law

$$p = x^2 + y^2 \text{ or } p = x^2 + 2y^2 \iff x^2 + 1 \text{ or } x^2 + 2 \text{has a solution modulo} p$$

For prime $p \neq 2$

$$x^2 + \bar{1} \equiv (x + \bar{t})(x + \bar{s}) \mod p \iff p \equiv 1 \mod 4$$

Quadratic reciprocity law

Gauss's theorem says that the solvability of

$$x^2 + bx + c$$

modulo p only depends on p modulo $D = b^2 - 4c$

Nonquadratic example

$$x^3 - 3x + 1$$

Nonquadratic example

$$x^3 - 3x + 1$$

For $p \neq 3$, $x^3 - 3x + 1$ has a solution modulo $p \iff \bar{p} \equiv \bar{1}, -\bar{1} \mod 9$

Nonquadratic example

$$x^3 - 3x + 1$$

For $p \neq 3$, $x^3 - 3x + 1$ has a solution modulo $p \iff \bar{p} \equiv \bar{1}, -\bar{1} \mod 9$

For any f, can we determine its factorization modulo p?

Splitting of primes

For a prime $p \in \mathbb{Z}$, consider $p\mathfrak{O}_K$

Splitting of primes

For a prime $p \in \mathbb{Z}$, consider $p\mathfrak{O}_K$

What is its prime ideal factorization?

Splitting of polynomial

Let $f(x) \in \mathbb{Z}[x]$ be irreducible with a root α. Consider the extension $K = \mathbb{Q}(\alpha)$

Splitting of polynomial

Let $f(x) \in \mathbb{Z}[x]$ be irreducible with a root α. Consider the extension $K = \mathbb{Q}(\alpha)$

Then for all but a finite set of primes $p \in \mathbb{Z}$, the factorization of $f(x)$ modulo p is equivalent to the ideal factorization of $p\mathfrak{O}_K$

Action of the Galois group

Let K be a normal number field
For a prime $p \in \mathbb{Z}$, Suppose $\mathfrak{P}$ is a prime ideal factor of $p\mathfrak{O}_K$

Action of the Galois group

Let K be a normal number field
For a prime $p \in \mathbb{Z}$, Suppose $\mathfrak{P}$ is a prime ideal factor of $p\mathfrak{O}_K$

Then, the action of $\mathrm{Gal}(K/\mathbb{Q})$ on $\mathfrak{P}$ determines the factorization of $p\mathfrak{O}_K$

Table of Contents

Computational example

$-3+9x^2-6x^4+x^6$ is the minimal polynomial of $2\sin(\frac{2\pi}{9})$

Computational example

$-3+9x^2-6x^4+x^6$ is the minimal polynomial of $2\sin(\frac{2\pi}{9})$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{36}})$ with discriminant $2^6 3^9$

Computational example

$-3 + 9x^2 - 6x^4 + x^6$ is the minimal polynomial of $2\sin(\frac{2\pi}{9})$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{36}})$ with discriminant $2^6 3^9$

Let $\omega = e^{\frac{2\pi i}{36}}$
$2\sin(\frac{2\pi}{9}) = -i(e^{\frac{2\pi i}{9}} - e^{\frac{2\pi i}{9}}) = -\omega^9(\omega^4 - \omega^{-4})$

Computational example

$-3+9x^2-6x^4+x^6$ is the minimal polynomial of $2\sin(\frac{2\pi}{9})$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{36}})$ with discriminant $2^6 3^9$

Let $\omega = e^{\frac{2\pi i}{36}}$
$2\sin(\frac{2\pi}{9}) = -i(e^{\frac{2\pi i}{9}} - e^{\frac{2\pi i}{9}}) = -\omega^9(\omega^4 - \omega^{-4})$

Let $g(x) = -x^9(x^4 - x^{-4})$ and H be the set $\bar{k} \in (\mathbb{Z}/36\mathbb{Z})^\times$ such that $g(\omega^k) = g(\omega)$

Computational example

$-3 + 9x^2 - 6x^4 + x^6$ is the minimal polynomial of $2\sin(\frac{2\pi}{9})$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{36}})$ with discriminant $2^6 3^9$

Let $\omega = e^{\frac{2\pi i}{36}}$
$2\sin(\frac{2\pi}{9}) = -i(e^{\frac{2\pi i}{9}} - e^{\frac{2\pi i}{9}}) = -\omega^9(\omega^4 - \omega^{-4})$

Let $g(x) = -x^9(x^4 - x^{-4})$ and H be the set $\bar{k} \in (\mathbb{Z}/36\mathbb{Z})^\times$ such that $g(\omega^k) = g(\omega)$

$\mathrm{H} = \{\bar{1}, -\bar{1}\}$

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times/H$

Example

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times / H$

Example

$f(x) \equiv x^6 + 35x^4 + 9x^2 + 38 \mod (41)$

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times / H$

Example

$f(x) \equiv x^6 + 35x^4 + 9x^2 + 38 \mod (41)$
$f(x) \equiv (x+4)(x+16)(x+17)(x+20)(x+21)(x+33) \mod (37)$

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times/H$

Example

$f(x) \equiv x^6 + 35x^4 + 9x^2 + 38 \mod (41)$
$f(x) \equiv (x+4)(x+16)(x+17)(x+20)(x+21)(x+33) \mod (37)$
$f(x) \equiv x^6 + x^4 + 2x^2 + 4 \mod (7)$

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times/H$

Example

$$f(x) \equiv x^6 + 35x^4 + 9x^2 + 38 \mod (41)$$
$$f(x) \equiv (x+4)(x+16)(x+17)(x+20)(x+21)(x+33) \mod (37)$$
$$f(x) \equiv x^6 + x^4 + 2x^2 + 4 \mod (7)$$
$$f(x) \equiv (x^3 + 10x + 9)(x^3 + 10x + 4) \mod (13)$$

Computational example

For $p \nmid 2^6 3^9$, the factorization of $f(x) = -3 + 9x^2 - 6x^4 + x^6$ modulo p only depends on the order of pH in $(\mathbb{Z}/36\mathbb{Z})^\times/H$

Example

$f(x) \equiv x^6 + 35x^4 + 9x^2 + 38 \mod (41)$
$f(x) \equiv (x+4)(x+16)(x+17)(x+20)(x+21)(x+33) \mod (37)$
$f(x) \equiv x^6 + x^4 + 2x^2 + 4 \mod (7)$
$f(x) \equiv (x^3 + 10x + 9)(x^3 + 10x + 4) \mod (13)$
$f(x) \equiv (x^2 + 72)(x^2 + 38)(x^2 + 11) \mod (127)$

Computational examples

$-123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$ is the minimal polynomial of $\alpha = 6\cos(\frac{6\pi}{25}) + 6\cos(\frac{17\pi}{25}) + 42$

Computational examples

$-123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$ is the minimal polynomial of $\alpha = 6\cos(\frac{6\pi}{25}) + 6\cos(\frac{17\pi}{25}) + 42$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{25}})$ with discriminant $3^{20}5^{8}7^{2}$

Computational examples

$-123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$ is the minimal polynomial of $\alpha = 6\cos(\frac{6\pi}{25}) + 6\cos(\frac{17\pi}{25}) + 42$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{25}})$ with discriminant $3^{20}5^87^2$

Let $\omega = e^{\frac{2\pi i}{25}}$
$\alpha = 3(e^{\frac{6\pi i}{25}} + e^{\frac{-6\pi i}{25}} + e^{\frac{17\pi i}{25}} + e^{\frac{-17\pi i}{25}}) + 42 = 3(\omega^6 + \omega^{-6} + \omega^{17} + \omega^{-17}) + 42$

Computational examples

$-123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$ is the minimal polynomial of $\alpha = 6\cos(\frac{6\pi}{25}) + 6\cos(\frac{17\pi}{25}) + 42$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{25}})$ with discriminant $3^{20}5^8 7^2$

Let $\omega = e^{\frac{2\pi i}{25}}$
$\alpha = 3(e^{\frac{6\pi i}{25}} + e^{\frac{-6\pi i}{25}} + e^{\frac{17\pi i}{25}} + e^{\frac{-17\pi i}{25}}) + 42 = 3(\omega^6 + \omega^{-6} + \omega^{17} + \omega^{-17}) + 42$

Let $g(x) = 3(x^6 + x^{-6} + x^{17} + x^{-17}) + 42$ and define H as before

Computational examples

$-123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$ is the minimal polynomial of $\alpha = 6\cos(\frac{6\pi}{25}) + 6\cos(\frac{17\pi}{25}) + 42$

It is contained in $\mathbb{Q}(e^{\frac{2\pi i}{25}})$ with discriminant $3^{20}5^{8}7^{2}$

Let $\omega = e^{\frac{2\pi i}{25}}$
$\alpha = 3(e^{\frac{6\pi i}{25}} + e^{\frac{-6\pi i}{25}} + e^{\frac{17\pi i}{25}} + e^{\frac{-17\pi i}{25}}) + 42 = 3(\omega^{6} + \omega^{-6} + \omega^{17} + \omega^{-17}) + 42$

Let $g(x) = 3(x^{6} + x^{-6} + x^{17} + x^{-17}) + 42$ and define H as before

$\mathrm{H} = \{\bar{1}, -\bar{1}, \bar{7}, -\bar{7}\}$

Computational examples

So for $p \nmid 3^{20}5^{8}7^{2}$, the factorization of
$f(x) = -123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$
only depends on the order of pH in the quotient group $(\mathbb{Z}/25\mathbb{Z})^\times/H$

Example

Computational examples

So for $p \nmid 3^{20}5^{8}7^{2}$, the factorization of
$f(x) = -123818949 + 15071670x - 729405x^2 + 17550x^3 - 210x^4 + x^5$
only depends on the order of pH in the quotient group $(\mathbb{Z}/25\mathbb{Z})^\times/H$

Example

$f(x) \equiv 10 + 9x + 5x^2 + 5x^3 + 10x^4 + x^5 \mod (11)$
$f(x) \equiv (10 + x)(14 + x)(15 + x)(22 + x)(30 + x) \mod (43)$
$f(x) \equiv (6 + x)(68 + x)(82 + x)(109 + x)(121 + x) \mod (149)$
$f(x) \equiv 6 + 3x + 12x^2 + 11x^4 + x^5 \mod (13)$

Unramified primes, the Frobenius element, and the discriminant

A prime p is unramified if the factorization of $p\mathfrak{O}_K$ has no repeated prime factor

Unramified primes, the Frobenius element, and the discriminant

A prime p is unramified if the factorization of $p\mathfrak{O}_K$ has no repeated prime factor

For K normal, p unramified, and $\mathfrak{P} \mid p\mathfrak{O}_K$, associate $\mathfrak{P}$ with the Frobenius element $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$

Unramified primes, the Frobenius element, and the discriminant

A prime p is unramified if the factorization of $p\mathfrak{O}_K$ has no repeated prime factor

For K normal, p unramified, and $\mathfrak{P} \mid p\mathfrak{O}_K$, associate $\mathfrak{P}$ with the Frobenius element $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$

For $f(x) = (x - a_1)...(x - a_n)$, let $C = \{(a_i, a_j) | n \geq i > j \geq 1\}$

$$\mathrm{disc}(f) = \prod_{(a_i, a_j) \in C} (a_i - a_j)^2$$

Unramified primes, the Frobenius element, and the discriminant

A prime p is unramified if the factorization of $p\mathfrak{O}_K$ has no repeated prime factor

For K normal, p unramified, and $\mathfrak{P} \mid p\mathfrak{O}_K$, associate $\mathfrak{P}$ with the Frobenius element $\sigma_{\mathfrak{P}} \in \mathrm{Gal}(K/\mathbb{Q})$

For $f(x) = (x - a_1)...(x - a_n)$, let $C = \{(a_i, a_j) | n \geq i > j \geq 1\}$

$$\mathrm{disc}(f) = \prod_{(a_i, a_j) \in C} (a_i - a_j)^2$$

If $f(x) \in \mathbb{Z}[x]$ irreducible, then $\mathrm{disc}(f) \in \mathbb{Z} - \{0\}$
Primes $p \nmid \mathrm{disc}(f)$ is unramified in $\mathfrak{O}_{\mathbb{Q}(\alpha)}$

From group action to factorization

Suppose p is unramified, $\mathfrak{P} \mid p\mathfrak{O}_K$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the frobenius element of $\mathfrak{P}$

From group action to factorization

Suppose p is unramified, $\mathfrak{P} \mid p\mathfrak{O}_K$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the frobenius element of $\mathfrak{P}$

Then, $\mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{P}) = \langle \sigma \rangle$, $\;p\mathfrak{O}_K = \sigma_1(\mathfrak{P})...\sigma_m(\mathfrak{P})$ with $\sigma_1, ..., \sigma_m$ the representatives of the left cosets of $\langle \sigma \rangle$, and $|\mathfrak{O}_K/\sigma_i(\mathfrak{P})| = p^{\mathrm{ord}(\sigma)}$

From group action to factorization

Suppose p is unramified, $\mathfrak{P} \mid p\mathfrak{O}_K$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the frobenius element of $\mathfrak{P}$

Then, $\mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{P}) = \langle\sigma\rangle$, $p\mathfrak{O}_K = \sigma_1(\mathfrak{P})...\sigma_m(\mathfrak{P})$ with $\sigma_1, ..., \sigma_m$ the representatives of the left cosets of $\langle\sigma\rangle$, and $|\mathfrak{O}_K/\sigma_i(\mathfrak{P})| = p^{\mathrm{ord}(\sigma)}$

Suppose $K = \mathbb{Q}(\alpha)$ with α an algebraic integer and minimal polynomial $f(x)$, $p \nmid \mathrm{disc}(f)$

From group action to factorization

Suppose p is unramified, $\mathfrak{P} \mid p\mathfrak{O}_K$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the frobenius element of $\mathfrak{P}$

Then, $\mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{P}) = \langle \sigma \rangle$, $p\mathfrak{O}_K = \sigma_1(\mathfrak{P}) ... \sigma_m(\mathfrak{P})$ with $\sigma_1, ..., \sigma_m$ the representatives of the left cosets of $\langle \sigma \rangle$, and $|\mathfrak{O}_K/\sigma_i(\mathfrak{P})| = p^{\mathrm{ord}(\sigma)}$

Suppose $K = \mathbb{Q}(\alpha)$ with α an algebraic integer and minimal polynomial $f(x)$, $p \nmid \mathrm{disc}(f)$

If $f(x) \equiv f_1(x) ... f_m(x) \mod p$ with each $f_i(x)$ irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$

From group action to factorization

Suppose p is unramified, $\mathfrak{P} \mid p\mathfrak{O}_K$, and $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ is the frobenius element of $\mathfrak{P}$

Then, $\mathrm{Stab}_{\mathrm{Gal}(K/\mathbb{Q})}(\mathfrak{P}) = \langle\sigma\rangle$, $p\mathfrak{O}_K = \sigma_1(\mathfrak{P})...\sigma_m(\mathfrak{P})$ with $\sigma_1, ..., \sigma_m$ the representatives of the left cosets of $\langle\sigma\rangle$, and $|\mathfrak{O}_K/\sigma_i(\mathfrak{P})| = p^{\mathrm{ord}(\sigma)}$

Suppose $K = \mathbb{Q}(\alpha)$ with α an algebraic integer and minimal polynomial $f(x)$, $p \nmid \mathrm{disc}(f)$

If $f(x) \equiv f_1(x)...f_m(x) \mod p$ with each $f_i(x)$ irreducible in $(\mathbb{Z}/p\mathbb{Z})[x]$

Then $p\mathfrak{O}_K = \langle p, f_1(\alpha)\rangle...\langle p, f_m(\alpha)\rangle$, $f_i(x) \not\equiv f_j(x) \mod p$ for $i \neq j$, and $\mathfrak{O}_K/\sigma_i(\mathfrak{P}) \cong (\mathbb{Z}/p\mathbb{Z}[x])/\langle\overline{f_i(x)}\rangle$

Frobenius element of a cyclotomic extension

For every $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$, label $\sigma_{\bar{k}} \in \mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q})$ as the automorphism $\sigma_{\bar{k}}(e^{\frac{2\pi i}{n}}) = e^{\frac{2k\pi i}{n}}$

Frobenius element of a cyclotomic extension

For every $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$, label $\sigma_{\bar{k}} \in \mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q})$ as the automorphism $\sigma_{\bar{k}}(e^{\frac{2\pi i}{n}}) = e^{\frac{2k\pi i}{n}}$

If $K = \mathbb{Q}(e^{\frac{2\pi i}{n}})$ for $n \in \mathbb{N}$, then the Frobenius element of p for $p \nmid n$ is the automorphism $\sigma_{\bar{p}}$

Frobenius element of a cyclotomic extension

For every $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^{\times}$, label $\sigma_{\bar{k}} \in \mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/\mathbb{Q})$ as the automorphism $\sigma_{\bar{k}}(e^{\frac{2\pi i}{n}}) = e^{\frac{2k\pi i}{n}}$

If $K = \mathbb{Q}(e^{\frac{2\pi i}{n}})$ for $n \in \mathbb{N}$, then the Frobenius element of p for $p \nmid n$ is the automorphism $\sigma_{\bar{p}}$

The Frobenius element of p in $K' \subseteq K$ is then the Automorphism of K' obtained from $\sigma_{\bar{p}}$

The Cyclotomic Reciprocity Law

Theorem

Let $f(x)$ be a monic integer irreducible polynomial with α as a root. Suppose $\alpha \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

The Cyclotomic Reciprocity Law

Theorem

Let $f(x)$ be a monic integer irreducible polynomial with α as a root.
Suppose $\alpha \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Denote H as the subgroup defined by $\{\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^{\times} | \sigma_{\bar{k}}(\alpha) = \alpha\}$

The Cyclotomic Reciprocity Law

Theorem

Let $f(x)$ *be a monic integer irreducible polynomial with* α *as a root.*
Suppose $\alpha \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Denote H *as the subgroup defined by* $\{\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^{\times} | \sigma_{\bar{k}}(\alpha) = \alpha\}$
Suppose for a prime $p \nmid \operatorname{disc}(f)$, $f(x) \equiv f_1(x)...f_r(x) \mod p$ *where each* $f_i(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ *is irreducible*

The Cyclotomic Reciprocity Law

Theorem

Let $f(x)$ be a monic integer irreducible polynomial with α as a root. Suppose $\alpha \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Denote H as the subgroup defined by $\{\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times | \sigma_{\bar{k}}(\alpha) = \alpha\}$ Suppose for a prime $p \nmid \mathrm{disc}(f)$, $f(x) \equiv f_1(x)...f_r(x) \mod p$ where each $f_i(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is irreducible

Then, $f(x)$ has no repeated irreducible factors in $(\mathbb{Z}/p\mathbb{Z})[x]$, and for every i, $\deg(f_i(x)) = \mathrm{ord}(\bar{p}H)$ with $\bar{p}H \in (\mathbb{Z}/n\mathbb{Z})^\times/H$

The Cyclotomic Reciprocity Law

Theorem

Let $f(x)$ be a monic integer irreducible polynomial with α as a root. Suppose $\alpha \in \mathbb{Q}(e^{\frac{2\pi i}{n}})$

Denote H as the subgroup defined by $\{\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^{\times} | \sigma_{\bar{k}}(\alpha) = \alpha\}$ Suppose for a prime $p \nmid \mathrm{disc}(f)$, $f(x) \equiv f_1(x)...f_r(x) \mod p$ where each $f_i(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is irreducible

Then, $f(x)$ has no repeated irreducible factors in $(\mathbb{Z}/p\mathbb{Z})[x]$, and for every i, $\deg(f_i(x)) = \mathrm{ord}(\bar{p}H)$ with $\bar{p}H \in (\mathbb{Z}/n\mathbb{Z})^{\times}/H$

$f(x)$ has a solution mod p for $p \nmid disc(f)$ if and only if $\bar{p} \in H$, and if $\bar{p} \in H$
The number of solutions to $f(x)$ mod p is $\deg(f(x))$

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n
$\mathrm{disc}(x^2 - n) = 4n$

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n
$\operatorname{disc}(x^2 - n) = 4n$

Let $\left(\frac{a}{p}\right)$ be the Legendre symbol

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n
$\operatorname{disc}(x^2 - n) = 4n$

Let $\left(\frac{a}{p}\right)$ be the Legendre symbol

Then $p \equiv q \mod 4n \rightarrow \left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n
$\mathrm{disc}(x^2 - n) = 4n$

Let $\left(\frac{a}{p}\right)$ be the Legendre symbol

Then $p \equiv q \mod 4n \to \left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$

If $n > 0$, then the complex conjugation fixes $\sqrt{n}$

From quadratic reciprocity to cyclotomic reciprocity

$\sqrt{n} \in \mathbb{Q}(e^{\frac{2\pi i}{4n}})$ for nonzero integers n
$\mathrm{disc}(x^2 - n) = 4n$

Let $\left(\frac{a}{p}\right)$ be the Legendre symbol

Then $p \equiv q \mod 4n \to \left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$

If $n > 0$, then the complex conjugation fixes $\sqrt{n}$

From here, $p \equiv -q \mod 4n \to \left(\frac{n}{p}\right) = \left(\frac{n}{q}\right)$

The abelian reciprocity law

If K is the splitting field of $f(x)$ and $\mathrm{Gal}(K/\mathbb{Q})$ abelian

The abelian reciprocity law

If K is the splitting field of $f(x)$ and $\mathrm{Gal}(K/\mathbb{Q})$ abelian

The Kronecker-Weber theorem says $K \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$ for some $n \in \mathbb{N}$

Table of Contents

The Zeta functions

For $s > 1$, let $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}$

The Zeta functions

For $s > 1$, let $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + ... = \sum_{n=1}^{\infty} \frac{1}{n^s}$

We have $n = |\mathbb{Z}/n\mathbb{Z}|$ and all ideals of $\mathbb{Z}$ is just the set $\{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, ...\}$

The Zeta functions

For $s > 1$, let $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + ... = \sum_{n=1}^{\infty} \frac{1}{n^s}$

We have $n = |\mathbb{Z}/n\mathbb{Z}|$ and all ideals of $\mathbb{Z}$ is just the set $\{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, ...\}$

For a number field K, let S be the set of ideals in $\mathfrak{O}_K$. For an ideal I, let $N(I) = |\mathfrak{O}_K/I|$. The Dedekind Zeta function of K is defined as

$$\zeta_K(s) = \sum_{I \in S} \frac{1}{N(I)^s}$$

The Zeta functions

For $s > 1$, let $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}$

We have $n = |\mathbb{Z}/n\mathbb{Z}|$ and all ideals of $\mathbb{Z}$ is just the set $\{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \ldots\}$

For a number field K, let S be the set of ideals in $\mathfrak{O}_K$. For an ideal I, let $N(I) = |\mathfrak{O}_K/I|$. The Dedekind Zeta function of K is defined as

$$\zeta_K(s) = \sum_{I \in S} \frac{1}{N(I)^s}$$

The series converges for $s > 1$

The Zeta functions

For $s > 1$, let $\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}$

We have $n = |\mathbb{Z}/n\mathbb{Z}|$ and all ideals of $\mathbb{Z}$ is just the set $\{\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, \ldots\}$

For a number field K, let S be the set of ideals in $\mathfrak{O}_K$. For an ideal I, let $N(I) = |\mathfrak{O}_K/I|$. The Dedekind Zeta function of K is defined as

$$\zeta_K(s) = \sum_{I \in S} \frac{1}{N(I)^s}$$

The series converges for $s > 1$

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

Singularities and density problems

$$\zeta_K(1) = \infty$$

Singularities and density problems

$$\zeta_K(1) = \infty$$

Let $P \subseteq \mathbb{N}$ the set of primes such that $f(x)$ has a solution modulo p

Singularities and density problems

$$\zeta_K(1) = \infty$$

Let $P \subseteq \mathbb{N}$ the set of primes such that $f(x)$ has a solution modulo p

$$\sum_{p \in P} \frac{1}{p} = \infty$$

A similar problem

$$\beta(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} + \dots$$

A similar problem

$$\beta(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} + \dots$$

$$\beta(s) = \prod_{\substack{p \ \ prime \\ p \ = \ 4n+1}} \left(\frac{1}{1 - \frac{1}{p^s}} \right) \prod_{\substack{p \ \ prime \\ p \ = \ 4n+3}} \left(\frac{1}{1 + \frac{1}{p^s}} \right)$$

A similar problem

$$\beta(s) = \frac{1}{1^s} - \frac{1}{3^s} + \frac{1}{5^s} + \ldots$$

$$\beta(s) = \prod_{\substack{p \ prime \\ p \ = \ 4n+1}} \left(\frac{1}{1 - \frac{1}{p^s}}\right) \prod_{\substack{p \ prime \\ p \ = \ 4n+3}} \left(\frac{1}{1 + \frac{1}{p^s}}\right)$$

$$\sum_{\substack{p \ prime \\ p \ = \ 4n+1}} \frac{1}{p} = \sum_{\substack{p \ prime \\ p \ = \ 4n+3}} \frac{1}{p} = \infty$$

Dirichlet's theorem in arithmetic progression

Let $\gcd(a, b) = 1$ for $a, b \in \mathbb{N}$

Dirichlet's theorem in arithmetic progression

Let $\gcd(a, b) = 1$ for $a, b \in \mathbb{N}$

Let S denote the set of primes p such that $p \equiv b \mod a$

Dirichlet's theorem in arithmetic progression

Let $\gcd(a, b) = 1$ for $a, b \in \mathbb{N}$

Let S denote the set of primes p such that $p \equiv b \mod a$

$$\sum_{p \in S} \frac{1}{p} = \infty$$

Dirichlet L-series

Let $\hat{\chi}$ be an irreducible character of $(\mathbb{Z}/n\mathbb{Z})^\times$ over $\mathbb{C}$

Dirichlet L-series

Let $\hat{\chi}$ be an irreducible character of $(\mathbb{Z}/n\mathbb{Z})^\times$ over $\mathbb{C}$

Then we can define the Dirichlet characters χ as follows :

Dirichlet L-series

Let $\hat{\chi}$ be an irreducible character of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ over $\mathbb{C}$

Then we can define the Dirichlet characters χ as follows :

If $\gcd(m, n) = 1$, $\chi(m) = \hat{\chi}(\bar{m})$ with $\bar{m}$ being the reduction of m modulo n and $\chi(m) = 0$ whenever $\gcd(m, n) \neq 1$

Dirichlet L-series

Let $\hat{\chi}$ be an irreducible character of $(\mathbb{Z}/n\mathbb{Z})^\times$ over $\mathbb{C}$

Then we can define the Dirichlet characters χ as follows :

If $\gcd(m, n) = 1$, $\chi(m) = \hat{\chi}(\bar{m})$ with $\bar{m}$ being the reduction of m modulo n and $\chi(m) = 0$ whenever $\gcd(m, n) \neq 1$
Then define the series

$$L(s, \chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}$$

Dirichlet L-series

Let $\hat{\chi}$ be an irreducible character of $(\mathbb{Z}/n\mathbb{Z})^{\times}$ over $\mathbb{C}$

Then we can define the Dirichlet characters χ as follows :

If $\gcd(m, n) = 1$, $\chi(m) = \hat{\chi}(\bar{m})$ with $\bar{m}$ being the reduction of m modulo n and $\chi(m) = 0$ whenever $\gcd(m, n) \neq 1$
Then define the series

$$L(s, \chi) = \sum_{k=1}^{\infty} \frac{\chi(k)}{k^s}$$

The series has an Euler product

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

The non-vanishing problem

$$log(L(s,\chi)) = \left(\sum_{g\in(\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$$

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g \in (\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s \to 1^+} r_\chi(s)$ converges

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g \in (\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s \to 1^+} r_\chi(s)$ converges

The orthogonality relations implies $\forall g \in (\mathbb{Z}/n\mathbb{Z})^\times$,

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g\in(\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s\to 1^+} r_\chi(s)$ converges

The orthogonality relations implies $\forall g \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{p,\ \bar{p}=g} \left(\frac{1}{p^s}\right) = \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^\times|}\left(\sum_{\chi} \chi(g^{-1}) log(L(s,\chi))\right) + t_g(s)$$

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g\in(\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s\to 1^+} r_\chi(s)$ converges

The orthogonality relations implies $\forall g \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{p,\ \bar{p}=g} \left(\frac{1}{p^s}\right) = \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^\times|}\left(\sum_{\chi} \chi(g^{-1}) log(L(s,\chi))\right) + t_g(s)$$

Where $\lim_{s\to 1^+} t_g(s)$ converges

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g\in(\mathbb{Z}/n\mathbb{Z})^\times} \sum_{p,\ \bar{p}=g} \left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s\to 1^+} r_\chi(s)$ converges

The orthogonality relations implies $\forall g \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{p,\ \bar{p}=g} \left(\frac{1}{p^s}\right) = \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^\times|}\left(\sum_\chi \chi(g^{-1}) log(L(s,\chi))\right) + t_g(s)$$

Where $\lim_{s\to 1^+} t_g(s)$ converges

It's easily shown that for non trivial characters χ
$\lim_{s\to 1^+} L(s,\chi)$ converges

The non-vanishing problem

$log(L(s,\chi)) = \left(\sum_{g\in(\mathbb{Z}/n\mathbb{Z})^\times}\sum_{p,\ \bar{p}=g}\left(\frac{\chi(g)}{p^s}\right)\right) + r_\chi(s)$
Where $\lim_{s\to 1^+} r_\chi(s)$ converges

The orthogonality relations implies $\forall g \in (\mathbb{Z}/n\mathbb{Z})^\times$,

$$\sum_{p,\ \bar{p}=g}\left(\frac{1}{p^s}\right) = \frac{1}{|(\mathbb{Z}/n\mathbb{Z})^\times|}\left(\sum_\chi \chi(g^{-1})log(L(s,\chi))\right) + t_g(s)$$

Where $\lim_{s\to 1^+} t_g(s)$ converges

It's easily shown that for non trivial characters χ
$\lim_{s\to 1^+} L(s,\chi)$ converges

For the trivial character χ_1
$\lim_{s\to 1^+}(s-1)L(s,\chi_1) = \frac{|(\mathbb{Z}/n\mathbb{Z})^\times|}{n}$

Decompositon of the Zeta function

The cyclotomic reciprocity law implies that for $K \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$, $H \leq (\mathbb{Z}/n\mathbb{Z})^{\times}$ associated with $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/K)$, and Dirichlet characters χ over $(\mathbb{Z}/n\mathbb{Z})^{\times}$

Decompositon of the Zeta function

The cyclotomic reciprocity law implies that for $K \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$, $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ associated with $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/K)$, and Dirichlet characters χ over $(\mathbb{Z}/n\mathbb{Z})^\times$

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \text{ prime} \\ \mathfrak{p} | n}} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \right) \prod_{\substack{\chi \\ H \subseteq \ker(\chi)}} L(s, \chi)$$

Decompositon of the Zeta function

The cyclotomic reciprocity law implies that for $K \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$, $H \leq (\mathbb{Z}/n\mathbb{Z})^\times$ associated with $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/K)$, and Dirichlet characters χ over $(\mathbb{Z}/n\mathbb{Z})^\times$

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \ prime \\ \mathfrak{p}|n}} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \right) \prod_{\substack{\chi \\ H \subseteq \ker(\chi)}} L(s, \chi)$$

$(s-1)\zeta_K(s)$ near 1 is equivalent to the behaviour of $(s-1)\left(\prod_{\chi,\ H\subseteq \ker(\chi)} L(s,\chi)\right)$

Decompositon of the Zeta function

The cyclotomic reciprocity law implies that for $K \subseteq \mathbb{Q}(e^{\frac{2\pi i}{n}})$, $H \leq (\mathbb{Z}/n\mathbb{Z})^{\times}$ associated with $\mathrm{Gal}(\mathbb{Q}(e^{\frac{2\pi i}{n}})/K)$, and Dirichlet characters χ over $(\mathbb{Z}/n\mathbb{Z})^{\times}$

$$\zeta_K(s) = \prod_{\substack{\mathfrak{p} \ prime \\ \mathfrak{p}|n}} \left(\frac{1}{1 - \frac{1}{N(\mathfrak{p})^s}} \right) \prod_{\substack{\chi \\ H \subseteq \ker(\chi)}} L(s, \chi)$$

$(s-1)\zeta_K(s)$ near 1 is equivalent to the behaviour of $(s-1)\left(\prod_{\chi,\ H\subseteq \ker(\chi)} L(s,\chi)\right)$

The simple pole of the Dedekind Zeta function at s=1 implies Dirichlet's theorem