

MATH407: Advanced Number Theory

Notes by Yuval Amit

Instructor: Niranjan Ramachandran

Fall 2025

Contents

Finite Fields	3
1 Preliminaries	3
2 Equations Over a Finite Field	6
2.1 The Chevalley-Waring Theorem	7
3 Quadratic Reciprocity	9
3.1 Preliminaries	9
3.2 The Legendre Symbol	10
3.3 Quadratic Reciprocity	12
 p-Adic Fields	 15
4 The Ring $\mathbb{Z}_p$ and the Field $\mathbb{Q}_p$	15
5 The p-Adic Absolute Value	18
6 The Exponential Function	21
7 Roots of Polynomials	21
8 Hensel's Lemma	24
9 Structure of $\mathbb{Q}_p^\times$	26
 The Hilbert Symbol	 30
10 Quadratic Extensions/Squares	30
11 Intro and Properties of the Hilbert Symbol	30
12 Systems of Hilbert Symbols	34

Dirichlet's Theorem	37
13 Characters on Finite Abelian Groups	37
14 Quick Tour of Complex Analysis	39
15 Dirichlet's Theorem	43
16 Results	46

Finite Fields

1. Preliminaries

Let K be a field. Then, $(K^\times, \cdot)$ is an abelian group. We have a homomorphism $\mathbb{Z} \rightarrow K$ by $1 \mapsto 1$, and its image $\text{Img}(\mathbb{Z}) \subset K$ is a domain. So, either

$$\mathbb{Z} \hookrightarrow K \quad (\text{char } K = 0), \quad \text{or} \quad \mathbb{Z} \twoheadrightarrow \mathbb{Z}/p\mathbb{Z} \hookrightarrow K \quad (\text{char } K = p).$$

In the first case, $\mathbb{Z} \hookrightarrow K$ is equivalent to $\mathbb{Q} \hookrightarrow K$.

Observation

If K has characteristic p , then there exists a ring homomorphism $\phi : K \rightarrow K$ given by $\phi(x) = x^p$, since

$$\phi(x + y) = (x + y)^p = x^p + y^p + 0.$$

Since K is a field, ϕ must be injective, since the kernel must be trivial.

Definition

1.1

Let K have characteristic p . Then, K is **perfect** if $\phi : K \rightarrow K$ is an automorphism.

Example 1.2. 1. An algebraically closed field $K = \overline{K}$ of characteristic p .
2. $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Definition

1.3

The map ϕ is called the **Frobenius map**.

Theorem

1.4

Let R be a finite domain. Then, R must be a field.

Proof. For $x \neq 0$, the map $\phi_x : R \rightarrow R$ given by $y \mapsto xy$ is a bijection, so $\phi_x(y) = 1$ has a solution. □

Theorem

1.5

Let K be a finite field.

- (1) $\text{char } K = p > 0$, and $|K| = p^f$.
- (2) Let $q = p^f$, $f \geq 1$, and let Ω be an algebraically closed field of characteristic p . Then, there exists a unique subfield of Ω of order q , denoted

$$\mathbb{F}_q = \{\text{roots of } x^q - x \text{ in } \Omega\}.$$

- (3) Any finite field of order q is isomorphic to $\mathbb{F}_q$.

Proof.

- (1) K has characteristic p because $\mathbb{Q} \not\hookrightarrow K$, hence $\mathbb{Z}/p\mathbb{Z} \hookrightarrow K$. So, K is a vector space over $\mathbb{Z}/p\mathbb{Z}$, and $\dim(K)$ over $\mathbb{F}_p$ is finite. The degree of the extension is the same as the dimension of the vector space, so $|K| = p^f$, where f is the degree.
- (2) Let Ω be an algebraically closed field of characteristic p , and let $\phi : \Omega \rightarrow \Omega$ be given by $\phi(x) = x^q$. Then, ϕ is injective, and surjective by algebraic closure, hence is an automorphism. For any automorphism $T : E \rightarrow E$ of a field, the set

$$F = \{x \in E \mid T(x) = x\} \subset E$$

is a subfield. Let $\mathbb{F}_q$ be the set of elements fixed by ϕ . All of its elements are roots of $x^q - x$, which has at most q roots. Note that

$$\frac{d}{dx}(x^q - x) = qx^{q-1} - 1 = -1 \neq 0,$$

hence $x^q - x$ has no repeated roots. That is, $|\mathbb{F}_q| = q$.

□

Lemma

1.6

$$\mathbb{F}_{p^e} \subset \mathbb{F}_{p^f} \iff e \mid f.$$

Proof. This follows by degree considerations. □

Proof of (3). Given K with $|K| = q$, there exists an algebraically closed field Ω containing K . For example, we could take $\Omega = \overline{K}$. Then, Ω has characteristic p . Let

$$\mathbb{F}_q = \{a \in \Omega : a^q = a\} \subset \Omega.$$

We want to show that $K = \mathbb{F}_q$. We have $a^q - a = a(a^{q-1} - 1)$. Let $a \in K \setminus \{0\}$. Then, $a \in K^\times$ and $|K^\times| = q - 1$, hence $a^{q-1} = 1$, so $a \in \mathbb{F}_q$. Also, $0 \in \mathbb{F}_q$, so $K \subseteq \mathbb{F}_q$. However, $|K| = |\mathbb{F}_q|$, hence $K = \mathbb{F}_q$. □

Example 1.7. 1. $\mathbb{F}_{32} \cong \mathbb{F}_3[x]/(x^2 + 1)$.

2. More generally, $\mathbb{F}_p[x]/(x^2 + 1) = \mathbb{F}_{p^2} \iff p \equiv 3 \pmod{4}$.

3. $\mathbb{F}_{33} \cong \mathbb{F}_3[x]/(x^3 + 2x + 1)$.

Recall

$(\mathbb{Z}, +)$ has no non-zero elements of finite order.

Definition

1.8

For G abelian, let $G_t = \{g \in G : |g| < \infty\}$, called the **torsion** of G .

Example 1.9. $\mathbb{Q}/\mathbb{Z}$ is a torsion group.

Definition**1.10**

Let A be an abelian group. A is **divisible** if for every map $A \rightarrow A$ given by $a \mapsto na$ with $n \in \mathbb{Z} \setminus \{0\}$ (where $na = a + \cdots + a$), the map is surjective. Note that these maps are always homomorphisms.

Example 1.11. 1. $(\mathbb{Z}, +)$ is not divisible.

2. $(\mathbb{Q}, +)$ is divisible.

3. $\mathbb{Q}/\mathbb{Z}$ is divisible.

Definition**1.12**

A is **uniquely divisible** if all of those maps are automorphisms.

Example 1.13. Consider the torsion of $(K^\times, \times)$ for the following fields K :

K	Torsion of $K^\times$
$\mathbb{Q}$	$\{\pm 1\}$
$\mathbb{R}$	$\{\pm 1\}$
$\mathbb{C}$	$\{\text{roots of unity}\} \cong \mathbb{Q}/\mathbb{Z}$
$\overline{\mathbb{Q}}$	$\mathbb{Q}/\mathbb{Z}$

Theorem**1.14**

$(\mathbb{F}_q)^\times$ is cyclic. For $q = p$, this is equivalent to there being a primitive root modulo p .

Proof.

Fact

Let $C_n = \langle \sigma \rangle$ be the cyclic group of order n , so $|\sigma| = n$. Then, $|\sigma^k| = \frac{n}{(k,n)}$. So,

$$\#\{x \in C_n : |x| = n\} = \varphi(n).$$

That is, C_n has exactly $\varphi(n)$ generators.

Lemma**1.15**

Let $n \in \mathbb{N}$. Then, $n = \sum_{d|n} \varphi(d)$.

Proof. Let $\Phi_d = \{\text{elements of order } d \text{ in } C_n\}$. Then,

$$C_n = \bigsqcup_{d|n} \Phi_d \implies \#C_n = \sum_{d|n} \#\Phi_d = \sum_{d|n} \varphi(d).$$

□

Recognition of Finite Cyclic Groups**1.16**

Let H be finite and abelian, with $\#H = n$. Suppose that for all $d \mid n$, we have $\#\{a \in H : a^d = 1\} \leq d$. Then, $H \cong C_n$.

Proof. Let $d \mid n$, and let $H_d = \{a \in H : a^d = 1\}$. If there exists $x \in H$ of order d , then $\langle x \rangle$ has

size d , and all elements $y \in \langle x \rangle$ satisfy $y^d = 1$. So, any $z \in H$ with $z^d = 1$ must be in $\langle x \rangle$. That is, $H_d \leq \langle x \rangle$. Hence, all elements of order d are generators of $\langle x \rangle \leq H$, so there are exactly $\varphi(d)$ elements of order d in H . So, if $d \mid n$, the number of elements of order d in H is either 0 or $\varphi(d)$. Since $\#H = \sum_{d \mid n} \varphi(d)$, by counting we need an element of every order. In particular, H has an element of order n . $\square$

Now, let $H = (\mathbb{F}_q)^\times$, $n = q - 1$, and $H_d = \{a \in \mathbb{F}_q^\times : a^d = 1\}$. That is, $H_d = \{\text{roots of } x^d - 1 = 0\}$, and $x^d - 1$ has at most d roots. So, $\#H_d \leq d$, hence H is cyclic. $\square$

Note

With the same argument, for any field K , any finite subgroup $H \leq K^\times$ is cyclic.

Example 1.17. In $\mathbb{F}_5[x]$, we have $x^2 + 1 = (x + 2)(x - 2)$, so $\mathbb{F}_5[x]/(x^2 + 1) = \mathbb{F}_5[x]/(x + 2)(x - 2)$. Note that we have

$$\begin{array}{ccc} \mathbb{F}_5[x] & \xrightarrow{\quad} & \mathbb{F}_5[x]/(x + 2) \\ \downarrow & \nearrow \exists & \\ \mathbb{F}_5[x]/(x^2 + 1) & & \end{array}$$

where the dashed map exists because $x^2 + 1 \mapsto 0$. So, we get maps

$$\mathbb{F}_5[x]/(x^2 + 1) \rightarrow \mathbb{F}_5[x]/(x + 2) \cong \mathbb{F}_5, \quad \mathbb{F}_5[x]/(x^2 + 1) \rightarrow \mathbb{F}_5[x]/(x - 2) \cong \mathbb{F}_5,$$

which combine to give $\mathbb{F}_5[x]/(x^2 + 1) \rightarrow \mathbb{F}_5 \times \mathbb{F}_5$.

2. Equations Over a Finite Field

We look at equations over finite fields, and search for solutions.

Definition

2.1

Let $g(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$. The **solution set** of g is

$$V(g) = \{(a_1, \dots, a_n) \in \mathbb{Z}^n \mid g(a_1, \dots, a_n) = 0\}.$$

Example 2.2. Let $f(x) = x^2 + 1$. If $f(a) = 0$, then $f(a) \equiv 0 \pmod{p}$ for all p . That is, f has a root in $\mathbb{F}_p$. Let

$$V_p(f) = \{\bar{a} \in \mathbb{F}_p : f(\bar{a}) = 0\}.$$

If we can show $V_p(f)$ is empty for some prime p , then $V(f)$ is empty. Indeed, $V_3(f) = \emptyset$, hence $V(f) = \emptyset$.

Example 2.3. Let $V(h) = \{(a, b, c) \mid a^5 + b^5 + c^5 = 0\}$. Does $V_p(h)$ non-empty imply $V(h)$ non-empty? **No.**

Questions

- (1) Is every element of $\mathbb{F}_q$ a sum of 2 squares? That is, does $x^2 + y^2 - a$ have a root for all $a \in \mathbb{F}_q$?
- (2) Let $g(x, y, z) = 3x^2 + 5y^2 + 7z^2$, and let $a_p = |V_p(g)|$ be the number of solutions of g in $\mathbb{F}_p$. What can we say about a_p ? Is $\lim_{p \rightarrow \infty} a_p = \infty$, or is it bounded?

2.1. The Chevalley-Warning Theorem**Chevalley-Warning Theorem**

2.4

Let $K = \mathbb{F}_q$ be a finite field, $R = K[x_1, \dots, x_n]$, and $f_1, \dots, f_r \in R$. Let $d = \deg f_1 + \dots + \deg f_r$, and

$$V = \{(a_1, \dots, a_n) \in K^n : f_j(a_1, \dots, a_n) = 0 \text{ for all } 1 \leq j \leq r\}.$$

If $d < n$, then $\#V \equiv 0 \pmod{p}$.

Corollary

2.5

Suppose in addition that $f_1, \dots, f_r$ have no constant term. Then, V is non-empty because of the zero solution, hence $\#V \geq p$.

Corollary

2.6

Let $f(x, y, z) = ax^2 + by^2 + cz^2 + dxy + exz + gyz$ be a quadratic form. Observe that $f(\lambda x, \lambda y, \lambda z) = \lambda^2 f(x, y, z)$. Since $f(0, 0, 0) = 0$, f has a non-trivial solution in $\mathbb{F}_q$ as well.

We can use this to answer question (1). Fix $a \in \mathbb{F}_q$, and consider $g(x, y, z) = x^2 + y^2 - az^2$. The theorem also answers question (2).

We can prove Chevalley-Warning with power sums.

Example 2.7. Let $K = \mathbb{F}_{11} = \{0, \dots, 10\}$. For $m \geq 0$, let $f(x) = x^m$, and let $S_m = \sum_{a \in \mathbb{F}_{11}} a^m$. Note that

$$S_0 = 0 \text{ (taking } 0^0 = 1), \quad S_1 = 0, \quad S_{10} = 0 + 1 + \dots + 1 = -1.$$

What are S_2 and S_3 ?

Observe

For a group G and $g_0 \in G$, the map $g \mapsto g_0 g$ is a bijection.

Lemma

2.8

Let $K = \mathbb{F}_q$ have characteristic p , with $q = p^f$. Let $S_m = \sum_{a \in K} a^m$, and more generally, if $f(x) = x^m$, let $S(f) = \sum_{a \in K} f(a)$. Then,

- (1) $S_0 = 0$.
- (2) If $m \geq 1$ and $q - 1 \mid m$, then $S_m = -1$.

(3) If $m \geq 1$ and $q - 1 \nmid m$, then $S_m = 0$.

Proof.

(1) $m = 0$ is clear.

(2) Suppose $q - 1 \mid m$. Then, for $a \in \mathbb{F}_q$, $a = 0 \implies a^m = 0$. Also, $a \neq 0 \implies a^m = 1$, since $\#\mathbb{F}_q^\times = q - 1$. So, $S_m = 0 + 1 + 1 + \cdots + 1 = -1$.

(3) Suppose $q - 1 \nmid m$. Then, there exists $y \neq 0$ in K such that $y^m \neq 1$, because $K^\times$ is cyclic. Now, consider the map $K^\times \rightarrow K^\times$ given by $a \mapsto ay$, which is a bijection. Then,

$$S_m = \sum_{a \in K^\times} a^m = \sum_{a \in K^\times} (ay)^m = y^m \sum_{a \in K^\times} a^m = y^m S_m.$$

Thus, $(1 - y^m)S_m = 0$, and $1 - y^m \neq 0$, hence $S_m = 0$. □

Lemma

2.9

Let $g(x_1, \dots, x_n) \in R$ be a monomial, i.e. $g = x_1^{e_1} \cdots x_n^{e_n}$, and suppose $\sum e_i < (q - 1)n$. As g is a function $K^n \rightarrow K$, we can consider

$$S(g) = \sum_{(a_1, \dots, a_n) \in K^n} g(a_1, \dots, a_n).$$

Then, $S(g) = 0 \in K$.

Proof. By assumption, there exists i with $e_i < q - 1$. Without loss of generality, suppose $i = 1$. Then,

$$S(g) = \sum a_1^{e_1} \cdots a_n^{e_n} = \sum_{a_2, \dots, a_n} a_2^{e_2} \cdots a_n^{e_n} \left(\sum_{a_1 \in K} a_1^{e_1} \right),$$

but that last factor is 0 by Lemma 2.8, because $e_1 = 0$ or $q - 1 \nmid e_1$. □

Example 2.10. Let $W \subset \mathbb{R}$. The *characteristic function* of W is

$$\chi_W(x) = \begin{cases} 1 & x \in W \\ 0 & x \notin W \end{cases}$$

Definition

2.11

Let

$$P(x_1, \dots, x_n) = \prod_{i=1}^r (1 - f_i^{q-1}),$$

where $f_1, \dots, f_r$ are the polynomials in Theorem 2.4. Note that $\deg f_i^{q-1} = (q - 1) \deg f_i$, so $\deg P = (q - 1)d < (q - 1)n$.

Observe that

$$(a_1, \dots, a_n) \in V \implies P(a_1, \dots, a_n) = 1, \quad (a_1, \dots, a_n) \notin V \implies P(a_1, \dots, a_n) = 0.$$

Hence, P is a **characteristic function** of V .

Lemma**2.12**

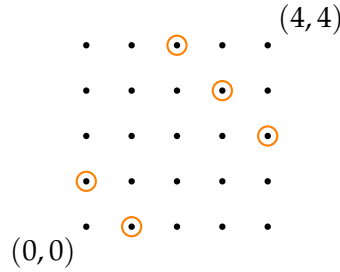
$S(P) \equiv \#V \pmod{p}$. (Not $=$, because we are working mod p .)

Proof of Theorem 2.4. To finish the proof, we want to show that $S(P) \equiv 0$. Write

$$P(x_1, \dots, x_n) = \sum c_{e_1, \dots, e_n} x_1^{e_1} \cdots x_n^{e_n}.$$

If g is one such monomial, then $\deg g < (q-1)n$, hence $S(g) = 0$ by Lemma 2.9. Therefore, $S(P) = \sum S(g) = 0$. $\square$

Example 2.13. Let $K = \mathbb{F}_5$, $f = x + y - 1$, and $V = V(f)$. The points of V are circled below.

**Warning's Theorem****2.14**

Let $K = \mathbb{F}_q = \mathbb{F}_{p^f}$, $f_1, \dots, f_r \in K[x_1, \dots, x_n]$, $d = \sum \deg f_i$, and $V = V(f_1) \cap \cdots \cap V(f_r)$. If $V \neq \emptyset$, then $\#V \geq q^{n-d}$.

3. Quadratic Reciprocity

3.1. Preliminaries

We want to understand the perfect squares in $\mathbb{F}_q^\times$.

Theorem**3.1**

Let $q = p^f$.

- (1) If $p = 2$, all elements of $\mathbb{F}_q$ are squares.
- (2) If $p > 2$, then the squares form a subgroup of $\mathbb{F}_q^\times$ of index 2.

Proof of (1). Let K have characteristic 2. Then, the map $K \rightarrow K$ given by $x \mapsto x^2$ is a homomorphism of fields. So, it must be injective, and if K is finite, then the map is surjective. $\square$

Proof of (2). Let $\psi : \mathbb{F}_q^\times \rightarrow \{\pm 1\}$ be given by $\psi(a) = a^{\frac{q-1}{2}}$. Then, ψ is a homomorphism of groups. Let $c = \psi(a) = a^{\frac{q-1}{2}}$. Then, $c^2 = 1$, hence c is a root of $x^2 - 1 = 0$. So, $a^{\frac{q-1}{2}}$ can only be ± 1 .

Now, we claim $\ker \psi = \{a \in \mathbb{F}_q^\times \mid \psi(a) = 1\}$ is the set of squares in $\mathbb{F}_q^\times$. Suppose $a \in (\mathbb{F}_q^\times)^2$, i.e. $a = b^2$ for some $b \in \mathbb{F}_q^\times$. Then, $\psi(a) = 1$. Hence, $(\mathbb{F}_q^\times)^2 \subseteq \ker \psi$. Conversely, if $a \in \ker \psi$, we need to show $a \in (\mathbb{F}_q^\times)^2$.

Is ψ onto? Yes: $\mathbb{F}_q^\times$ is cyclic, so it has a generator g , hence $g^{\frac{q-1}{2}} = -1$. Hence, $\mathbb{F}_q^\times / \ker \psi \cong \{\pm 1\}$,

so $|\ker \psi| = \frac{q-1}{2}$. This means $\langle g^2 \rangle = \ker \psi$ (a cyclic group has only one subgroup of a given order), so everything in $\ker \psi$ is a square. $\square$

Definition

3.2

Let A, B, C be abelian groups, and consider homomorphisms

$$0 \rightarrow A \xrightarrow{f} B \xrightarrow{g} C \rightarrow 0$$

with $g(f(a)) = 0$ for all $a \in A$. This is a **sequence**. We say it's **exact on the left** if f is injective, and **exact on the right** if g is surjective. We say it's **exact in the middle** if $\text{Im} f = \ker g$. We say it's an **exact sequence** if all 3 hold.

Proposition

3.3

If we have an exact sequence as above, then $B / \ker g \cong C$, so $B / \text{Im} f \cong C$. Since $A \cong \text{Im} f$, we have $B / A \cong C$.

Example 3.4. The following sequences are exact:

1. $0 \rightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \xrightarrow{\text{mod } 2} \mathbb{Z}/2\mathbb{Z} \rightarrow 0$
2. $0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0$
3. $1 \rightarrow \{\pm 1, \pm i\} \xrightarrow{\times} \mathbb{C}^\times \xrightarrow{a^4} \mathbb{C}^\times \rightarrow 1$. (We use 1 instead of 0 as a convention, since 1 is the identity.)
4. $1 \rightarrow (\mathbb{F}_q^\times)^2 \rightarrow \mathbb{F}_q^\times \xrightarrow{\psi} \{\pm 1\} \rightarrow 1$, where ψ is the map from before.

Example 3.5. Let G be abelian, and consider the map $\phi_n : G \rightarrow G$ given by $\phi_n(a) = a^n$. Then, $\ker \phi_n = \{g \in G : g^n = e\}$. For example, we have the exact sequence

$$1 \rightarrow \{\pm 1\} \rightarrow \mathbb{F}_q^\times \xrightarrow{\phi_2} (\mathbb{F}_q^\times)^2 \rightarrow 1.$$

Principle

To check if $a \in \mathbb{F}_q^\times$ is a square, we need to check whether $\sqrt{a} = b \in \Omega$ satisfies $b^{q-1} = 1$.

3.2. The Legendre Symbol

We now only consider prime fields.

Definition

3.6

Let $a \in \mathbb{Z}$, and p be prime. The **Legendre symbol** is

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square in } \mathbb{F}_p \\ -1 & \text{otherwise} \end{cases}$$

for $p \nmid a$, and $\left(\frac{0}{p}\right) = 0$.

Note

$\left(\frac{a}{p}\right)$ depends only on the congruence class of a modulo p .

Proposition

3.7

If $b \in \Omega$ satisfies $b^2 = a \in \mathbb{F}_p^\times$, then

$$\psi(a) = a^{\frac{p-1}{2}} = b^{p-1},$$

which is 1 if and only if $b \in \mathbb{F}_p$. So, $\left(\frac{a}{p}\right) = b^{p-1} \in \mathbb{F}_p^\times$, i.e. $\psi(a) = \left(\frac{a}{p}\right)$. Since $\psi(ab) = \psi(a)\psi(b)$, we have

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

Proposition

3.8

We have

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a = 0 \\ 1 & a \text{ is a square} \\ -1 & a \text{ is not a square} \end{cases}$$

so $\sum_{a \in \mathbb{F}_p} \left(\frac{a}{p}\right) = 0$.

Now, it helps to compute the Legendre symbol in special cases. In particular, we want to compute $\left(\frac{-1}{p}\right)$ and $\left(\frac{2}{p}\right)$.

Definition

3.9

Let $n \in \mathbb{Z}$ be odd. We define two maps:

$$\varepsilon(n) \in \mathbb{Z}/2\mathbb{Z}, \quad \varepsilon(n) = \frac{n-1}{2} \bmod 2 = \begin{cases} 0 & n \equiv 1 \pmod{4} \\ 1 & n \equiv 3 \pmod{4} \end{cases}$$

$$\omega(n) \in \mathbb{Z}/2\mathbb{Z}, \quad \omega(n) = \frac{n^2-1}{8} \bmod 2 = \begin{cases} 0 & n \equiv \pm 1 \pmod{8} \\ 1 & n \equiv \pm 3 \pmod{8} \end{cases}$$

Theorem

3.10

Let p be an odd prime. Then,

- (1) $\left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$, so $\left(\frac{-1}{p}\right) = 1 \iff p \equiv 1 \pmod{4}$.
- (2) $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$, so $\left(\frac{2}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{8}$.

Proof.

- (1) If $-1 = c^2$ in $\mathbb{F}_p^\times$, then c has order 4. This requires $4 \mid p-1$, i.e. $p \equiv 1 \pmod{4}$, and further

$p \equiv 3 \pmod{4} \implies \left(\frac{-1}{p}\right) = -1$. Now, suppose $p \equiv 1 \pmod{4}$. Since $\mathbb{F}_p^\times$ is cyclic, let $\mathbb{F}_p^\times = \langle g \rangle$, so $g^{\frac{p-1}{4}} = g^k$ has order 4. So, $-1 = (g^k)^2$, hence $\left(\frac{-1}{p}\right) = 1$.

(2) Let $\alpha \in \Omega$ be a primitive 8^{th} root of unity. So, $\alpha^8 = 1$, and

(i) $\alpha^4 = -1$.

(ii) $\alpha^2 + \alpha^{-2} = 0$. Indeed, $(\alpha^2 + \alpha^{-2})^2 = \alpha^4 + \alpha^{-4} + 2\alpha^2\alpha^{-2} = -1 + (-1) + 2 = 0$.

(iii) Let $y = \alpha + \alpha^{-1}$. Then, $y^2 = 2$. Indeed, $y^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2\alpha\alpha^{-1} = 0 + 2 = 2$.

To compute $\left(\frac{2}{p}\right)$, we need $2^{\frac{p-1}{2}} = y^{p-1}$. Now,

$$y^p = (\alpha + \alpha^{-1})^p = \alpha^p + \alpha^{-p}.$$

If $p = 8k + 1$, then $y^p = \alpha^{8k+1} + \alpha^{-1-8k} = \alpha + \alpha^{-1} = y$, so $y^{p-1} = 1$, hence $y \in \mathbb{F}_p^\times$. Hence, $\left(\frac{2}{p}\right) = 1$. The case $p = 8k - 1$ is similar.

If $p = 8k + 5$, then

$$y^p = \alpha^{8k+5} + \alpha^{-5-8k} = \alpha^5 + \alpha^{-5} = \alpha\alpha^4 + \alpha^{-1}\alpha^{-4} = -(\alpha + \alpha^{-1}) = -y,$$

hence $y^p = -y$, so $y^{p-1} = -1$, showing $\psi(2) = -1$, and thus $\left(\frac{2}{p}\right) = -1$. The case $p = 8k - 5$ is similar. □

Example 3.11. Let $f(x) = ax^2 + bx + c \in \mathbb{F}_p[x]$, with $p \nmid a$. By the quadratic formula, f has roots $\iff \left(\frac{b^2-4ac}{p}\right) = 1$. In particular, $\mathbb{F}_p[x]/(f)$ is a field $\iff \left(\frac{b^2-4ac}{p}\right) = -1$.

3.3. Quadratic Reciprocity

Quadratic Reciprocity (Carl “G-money” Gauss)

3.12

Let p, ℓ be odd primes, $p \neq \ell$. Then,

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

Corollary

3.13

$\left(\frac{p}{\ell}\right) = \left(\frac{\ell}{p}\right)$, unless $p \equiv \ell \equiv 3 \pmod{4}$.

Example 3.14. Let $\ell = 4003$ and $p = 5$. Computing $\left(\frac{5}{4003}\right)$ directly is hard, but $\left(\frac{4003}{5}\right)$ is easy:

$$-1 = \left(\frac{4003}{5}\right) = \left(\frac{5}{4003}\right).$$

Proof of Theorem 3.12. Fix $\mathbb{F}_p$, with $\mathbb{F}_p \subset \Omega$ algebraically closed. Let ω be a primitive ℓ^{th} root of unity in Ω .

Lemma

3.15

$$1 + \omega + \omega^2 + \cdots + \omega^{\ell-1} = 0.$$

Also, recall that $\left(\frac{a}{p}\right) = b^{p-1}$ if $b^2 = a$.

Consider the (well-defined) function $\mathbb{F}_\ell \rightarrow \{\pm 1\}$ given by $a \mapsto \left(\frac{a}{\ell}\right)$. Note that ω^a depends only on $a \bmod \ell$, so we can also consider the function $\mathbb{F}_\ell \rightarrow \Omega$ given by $a \mapsto \omega^a$. Let

$$y = \sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right) \omega^a \in \Omega.$$

This y is called a **Gauss sum**.

Lemma**3.16**

$$y^2 = (-1)^{\varepsilon(\ell)} \ell.$$

Lemma**3.17**

$$y^{p-1} = \left(\frac{p}{\ell}\right).$$

We will show these lemmas imply quadratic reciprocity, and then prove them. As $y^2 = (-1)^{\varepsilon(\ell)} \ell$, we get from the note above (with $b = y$) and [Lemma 3.17](#) that

$$\left(\frac{(-1)^{\varepsilon(\ell)} \ell}{p}\right) = y^{p-1} = \left(\frac{p}{\ell}\right).$$

As the Legendre symbol is multiplicative,

$$\left(\frac{(-1)^{\varepsilon(\ell)} \ell}{p}\right) = \left(\frac{-1}{p}\right)^{\varepsilon(\ell)} \left(\frac{\ell}{p}\right) = \left((-1)^{\varepsilon(p)}\right)^{\varepsilon(\ell)} \left(\frac{\ell}{p}\right).$$

So, $\left(\frac{p}{\ell}\right) = (-1)^{\varepsilon(p)\varepsilon(\ell)} \left(\frac{\ell}{p}\right)$, hence

$$\left(\frac{p}{\ell}\right) \left(\frac{\ell}{p}\right) = (-1)^{\varepsilon(p)\varepsilon(\ell)},$$

as desired. □

Proof of [Lemma 3.15](#). As ω is a primitive ℓ^{th} root of 1, ω is a root of

$$\frac{x^\ell - 1}{x - 1} = 1 + x + \cdots + x^{\ell-1},$$

so $1 + \omega + \cdots + \omega^{\ell-1} = 0$. □

(Rama really wants us to understand this proof.)

Proof of [Lemma 3.17](#). Let $y = \sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right) \omega^a$. As Ω has characteristic p ,

$$y^p = \left(\sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right) \omega^a\right)^p = \sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right)^p \omega^{ap} = \sum_{a \in \mathbb{F}_\ell} \left(\frac{a}{\ell}\right) \omega^{ap}.$$

Let $c = ap \in \mathbb{F}_\ell$, so that $a = cp^{-1} \in \mathbb{F}_\ell$. So, we have

$$\sum_{c \in \mathbb{F}_\ell} \left(\frac{cp^{-1}}{\ell}\right) \omega^c = \sum_{c \in \mathbb{F}_\ell} \left(\frac{c}{\ell}\right) \left(\frac{p^{-1}}{\ell}\right) \omega^c = \left(\frac{p^{-1}}{\ell}\right) \sum_{c \in \mathbb{F}_\ell} \left(\frac{c}{\ell}\right) \omega^c.$$

Note that $\left(\frac{p}{\ell}\right) \left(\frac{p^{-1}}{\ell}\right) = 1$, so $\left(\frac{p}{\ell}\right) = \left(\frac{p^{-1}}{\ell}\right)$. Hence, this equals

$$\left(\frac{p}{\ell}\right) \sum_{c \in \mathbb{F}_\ell} \left(\frac{c}{\ell}\right) \omega^c = \left(\frac{p}{\ell}\right) y.$$

So, $y^p = \left(\frac{p}{\ell}\right) y$, hence $y^{p-1} = \left(\frac{p}{\ell}\right)$. □

Proof of Lemma 3.16. Note the following:

- The map $\mathbb{F}_\ell^\times \rightarrow \mathbb{F}_\ell^\times$ given by $t \mapsto t^{-1}$ is bijective.
- For $u \in \mathbb{F}_\ell^\times$, the maps $t \mapsto ut$ and $t \mapsto -ut$ are bijections.
- The map $\mathbb{F}_\ell \rightarrow \mathbb{F}_\ell$ given by $t \mapsto t + 1$ is a bijection, and $\mathbb{F}_\ell^\times$ is mapped to $\mathbb{F}_\ell \setminus \{1\}$.

Now, we want to show $y^2 = (-1)^{\varepsilon(\ell)} \ell$. By definition,

$$\begin{aligned} y^2 &= y \cdot y = \left(\sum_{x \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \omega^x \right) \left(\sum_{z \in \mathbb{F}_\ell} \left(\frac{z}{\ell}\right) \omega^z \right) \\ &= \sum_{x, z \in \mathbb{F}_\ell} \left(\frac{x}{\ell}\right) \left(\frac{z}{\ell}\right) \omega^{x+z} = \sum \left(\frac{xz}{\ell}\right) \omega^{x+z}. \end{aligned}$$

For $u \in \mathbb{F}_\ell$, we want the coefficient of ω^u , so $x + z = u$, i.e. $z = u - x$. We now have

$$y^2 = \sum_{u \in \mathbb{F}_\ell} B_u \omega^u, \quad \text{where } B_u = \sum_{t \in \mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right).$$

Now,

$$\begin{aligned} B_u &= \sum_{t \in \mathbb{F}_\ell} \left(\frac{t(u-t)}{\ell}\right) = \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{t(u-t)}{\ell}\right) = \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{-t^2(1-ut^{-1})}{\ell}\right) \\ &= \sum \left(\frac{-1}{\ell}\right) \left(\frac{t^2}{\ell}\right) \left(\frac{1-ut^{-1}}{\ell}\right) = \sum (-1)^{\varepsilon(\ell)} \left(\frac{1-ut^{-1}}{\ell}\right) = (-1)^{\varepsilon(\ell)} \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{1-ut^{-1}}{\ell}\right). \end{aligned}$$

So, let $B_u = (-1)^{\varepsilon(\ell)} C_u$, where $C_u = \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{1-ut^{-1}}{\ell}\right)$. For $u = 0$,

$$C_0 = \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{1}{\ell}\right) = \ell - 1.$$

Now, if $u \neq 0$, then $t \mapsto t^{-1} \mapsto -ut^{-1} \mapsto 1 - ut^{-1}$ is a bijection $\mathbb{F}_\ell^\times \rightarrow \mathbb{F}_\ell \setminus \{1\}$. So,

$$C_u = \sum_{t \in \mathbb{F}_\ell^\times} \left(\frac{1-ut^{-1}}{\ell}\right) = \sum_{s \in \mathbb{F}_\ell \setminus \{1\}} \left(\frac{s}{\ell}\right) = -1 + \sum_{s \in \mathbb{F}_\ell} \left(\frac{s}{\ell}\right) = -1.$$

Hence, using Lemma 3.15,

$$\begin{aligned} y^2 &= \sum_{u \in \mathbb{F}_\ell} B_u \omega^u = (-1)^{\varepsilon(\ell)} \sum C_u \omega^u = (-1)^{\varepsilon(\ell)} \left(\ell - 1 + \left(\sum_{u \in \mathbb{F}_\ell^\times} \omega^u \right) (-1) \right) \\ &= (-1)^{\varepsilon(\ell)} (\ell - 1 + 1) = (-1)^{\varepsilon(\ell)} \ell. \end{aligned}$$

□

p -Adic Fields

4. The Ring $\mathbb{Z}_p$ and the Field $\mathbb{Q}_p$

Definition

4.1

An **inverse system** of sets/groups/rings/(category) is

- (i) A sequence A_n of sets/groups/rings and
- (ii) A sequence of morphisms $f_n : A_n \rightarrow A_{n-1}$

$$\cdots \rightarrow A_3 \xrightarrow{f_3} A_2 \xrightarrow{f_2} A_1$$

Definition

4.2

The **inverse limit** of the system $(A_n, f_n)_{n \geq 1}$ is $A = \varprojlim A_n$ defined as $A = \{(\dots, a_2, a_1) \mid a_n \in A_n, f_n(a_n) = a_{n-1} \forall n \geq 2\}$. Note then that $A \subset \prod_{n \geq 1} A_n$

Example 4.3 (Main example). Let p be a prime number, $A_n = \mathbb{Z}/p^n\mathbb{Z}$, $\phi_n : A_n \rightarrow A_{n-1}$, defined by $\bar{a} \mapsto a \pmod{p^{n-1}}$. Note that ϕ_n are all surjective. We then define $\mathbb{Z}_p = \varprojlim A_n$, called the **p -adic integers**, a ring. In particular, if $\vec{a} = (\dots, a_2, a_1)$ and $\vec{b} = (\dots, b_2, b_1)$, then $\vec{a} + \vec{b} = (\dots, a_2 + b_2, a_1 + b_1)$ and $\vec{a} \cdot \vec{b} = (\dots, a_2 b_2, a_1 b_1)$, and one can verify these remain in the p -adic integers

Example 4.4. In $\mathbb{Z}_p$, we have multiplicative identity $\vec{1} = (\dots, 1, 1, 1)$ and the additive identity $\vec{0} = (\dots, 0, 0)$. For any $m \in \mathbb{Z}$, we can look at $\vec{m} = (\dots, m, m, m)$. Thus, we have a map $\mathbb{Z} \rightarrow \mathbb{Z}_p$ by $m \mapsto \vec{m}$, which is also a homomorphism. Suppose $m \in \mathbb{Z}$ satisfies $\vec{m} = \vec{0}$. Then, we must have $m = 0$, hence the kernel of the map is trivial. (We can sort of say $\mathbb{Z}_p$ is a characteristic 0 ring, which will be more important later)

Example 4.5 (What else is in $\mathbb{Z}_p$). $1/2 \notin \mathbb{Z}$, but we do have $1/2 \in \mathbb{Z}_7$. We also have $\sqrt{2} \in \mathbb{Z}_7, 2^{1/5} \in \mathbb{Z}_7$, but $2^{1/3} \notin \mathbb{Z}_7$

Definition

4.6

We have a homomorphism $\varepsilon_n : \mathbb{Z}_p \rightarrow A_n = \mathbb{Z}/p^n\mathbb{Z}$ by $\varepsilon_n(\vec{a}) = a_n$

Theorem

4.7

There exists an exact sequence $0 \rightarrow \mathbb{Z}_p \xrightarrow{\cdot p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} A_n \rightarrow 0$, so ε_n is surjective, and we'll also show multiplication by p^n is injective. This also says $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Proof. Consider the map $\mathbb{Z}_p \rightarrow \mathbb{Z}_p$ by $\vec{a} \mapsto p\vec{a}$. Observe that for $c \in \mathbb{Z}/p^n\mathbb{Z}$, we have that $pc = 0 \implies p^{n-1} \mid c$. Now, suppose $\vec{a} \in \mathbb{Z}_p$ satisfies $p\vec{a} = \vec{0}$, so $pa_1 = 0 \in A_1$, $pa_2 = 0 \in A_2$, etc. This means that for all n , $pa_n = 0 \in A_n = \mathbb{Z}/p^n\mathbb{Z}$, thus $a_n = p^{n-1}b_n$ for some $b_n \in A_n$. By

$\vec{a} \in \mathbb{Z}_p$, we know $\phi(a_n) = a_{n-1}, \phi(n+1) = a_n$, etc. Furthermore,

$$a_n = \phi(a_{n+1}) = \phi(p^n b_{n+1}) = p^n \phi(b_{n+1}) = 0 \in A_n.$$

Thus, $\vec{a} = 0$, so multiplication by p is injective, and it follows that multiplication by p^n is injective.

Now, for any $\vec{c} \in \mathbb{Z}/p^n\mathbb{Z}$, we have that $\varepsilon_n(\dots, c, c, c) = \vec{c}$, hence ε_n is surjective.

Finally, we'll show $\ker \varepsilon_n = p^n \mathbb{Z}_p$. $p^n \mathbb{Z}_p \subset \ker \varepsilon_n$ is clear. Let $\vec{a} \in \ker \varepsilon_n$. We want to show $\vec{a} = p^n \vec{b}$ for $\vec{b} \in \mathbb{Z}_p$. As $\vec{a} \in \ker \varepsilon_n$, we know $a_n = 0 \implies a_{n-1} = 0 = a_{n-2} + \dots = a_1$. Now, consider $A_{n+1} \xrightarrow{\phi_{n+1}} A_n$ by $a_{n+1} \mapsto a_n = 0$, hence $a_{n+1} \in \ker \phi_{n+1}$, so $a_{n+1} = p^n b_{n+1}$. A similar argument can be made for a_{n+2} with composing maps, and inductively we have $a_{n+j} = p^n b_{n+j}$. So, it's left to us to check $(\dots, b_{n+2}, b_{n+1}, b_n, \dots, b_1) \in \mathbb{Z}_p$. $\square$

Example 4.8 (Another inverse system). Let K be a field, $R = K[x]$, $B_n = K[x]/(x^n) = R/(x^n)$. What is $B = \varprojlim B_n$?

Question

What is $\mathbb{Z}_7^\times$?

For $\vec{a} = (a_n) \in \prod A_n$ to be a unit, we certainly need a_n is a unit in A_n .

Structure of Units

4.9

Let $a \in \mathbb{Z}_p, a \neq 0$. Then

1. $\vec{a}$ unit in $\mathbb{Z}_p \iff a_1 \in \mathbb{F}_p^\times = (\mathbb{Z}/p\mathbb{Z})^\times$
2. Let $U = \mathbb{Z}_p^\times$ in $\mathbb{Z}_p$. Then, any $a \in \mathbb{Z}_p$ non-zero can be written as $p^n \vec{b}$ for $n \geq 0$ and $\vec{b} \in U$ uniquely.

Proof. 1. ($\implies$) obvious.

Now, let $a \in \mathbb{Z}_p$ with $a_1 \in \mathbb{F}_p^\times$. We want to show $a_n \in A_n^\times$ for all $n \geq 1$. Let $a_1^{-1} = b_1$, and as $A_2 \rightarrow A_1$ is surjective, for a_2 mapping to a_1 , there exists some $b_2 \in A_2$ which is mapped to A_1 . Then $\phi_2(a_2 b_2) = 1 = \phi_2(1)$, so $a_2 b_2 - 1 \in \ker \phi_2$. Hence, $a_2 b_2 = 1 - pz$ for some $z \in A_2$. Now, $a_2 b_2(1 + pz) = (1 - pz)(1 + pz) = 1 - p^2 z = 1$. In general, for $a_n \mapsto a_1$, there exists some $b_n \mapsto b_1$, and once again $a_n b_n - 1 \in \ker(\mathbb{Z}/p^n\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z})$. Thus, $a_n b_n = 1 - pz$. Recall $(1 - t)(1 + t + \dots + t^{n-1}) = (1 - t^n)$. Hence, $a_n b_n(1 + pz + p^2 z^2 + \dots + p^n z^n) = 1 - p^n z^n = 1$. $\square$

Corollary

4.10

$m \in \mathbb{Z}_p^\times$ if $p \nmid m$.

Proof of (2) of Theorem 4.9. Suppose $\vec{a} \in \mathbb{Z}_p$ is nonzero. Then, $\varepsilon_m(\vec{a}) \neq 0$ for some m . Let n be the largest integer such that $\varepsilon_n(\vec{a}) = 0$, recalling that $\varepsilon_{n-k}(\vec{a}) = 0$ for all $k \geq 0$. In particular, $\vec{a} \in \ker \varepsilon_n \implies \vec{a} = p^n \vec{b}$ for some $\vec{b} \in \mathbb{Z}_p$ by Theorem 4.7. Now, **show** $b_1 \neq 0$. Thus, $\vec{b}$ is a unit in $\mathbb{Z}_p$, proving (2). $\square$

Definition

4.11

If $\vec{a} \in \mathbb{Z}_p$ is nonzero, then we know $\vec{a} = p^n \vec{b}$ for $\vec{b}$ a unit and $n \geq 0$. So, let the **p -adic valuation** of $\vec{a}$ by $v_p(\vec{a}) = n$. Note $v_p(\vec{a}) = 0 \iff a$ is a unit in $\mathbb{Z}_p$. We will also declare $v_p(0) = \infty$.

Remark 4.12. $v_p(\vec{a}\vec{b}) = v_p(\vec{a}) + v_p(\vec{b})$, and $v_p(a+b) \geq \min\{v_p(a), v_p(b)\}$. We call this **non-Archimedean equality**.

Corollary

4.13

$\mathbb{Z}_p$ is an integral domain.

Proof. If a, b are non-zero, then they have finite p -adic valuation, so the p -valuation of their product is also finite. $\square$

Definition ($\mathbb{Q}_p$)

4.14

Let $\mathbb{Q}_p$ be the field of fractions of $\mathbb{Z}_p$, i.e. the smallest field containing $\mathbb{Z}_p$.

Remark 4.15. For any $a \neq 0$, let $a = p^n b$, where b is a unit. Then, the inverse of a in $\mathbb{Q}_p$ is $p^{-n} b^{-1}$. It's worth noting that $b^{-1} \in \mathbb{Z}_p$, so the only thing we have to 'add' is p^{-n} . Thus, $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$.

Let's make $\mathbb{Z}_p$ more concrete. Recall $\mathbb{Z}_p = \varprojlim \mathbb{Z}/p^n \mathbb{Z}$.

Let $\vec{a} = (a_n)$, and for the usual map $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$, consider $a_{n+1} \mapsto a_n$, where $a_{n+1} \in \{0, \dots, p^{n+1} - 1\}$ and $a_n \in \{0, \dots, p^n - 1\}$. So, we can see that $a_{n+1} = a_n + p^n b_n$, with $0 \leq b_n \leq p - 1$. This is like $31 \bmod 100$ and $31, 131, \dots, 931 \bmod 1000$. Now, consider the sequence $b_0 = a_1, b_1 = \frac{a_2 - a_1}{p}, b_2 = \frac{a_3 - a_2}{p}, \dots, b_n = \frac{a_{n+1} - a_n}{p^n}, \dots$. By definition,

$$a_n = b_0 + b_1 p + \dots + b_{n-1} p^{n-1}$$

Definition (p -adic Expansion)

4.16

The sequence $(b_0, b_1, \dots)$ described above is called the **p -adic expansion of $\vec{a}$**

Theorem

4.17

There is a bijection between $\mathbb{Z}_p \longleftrightarrow$ sequences (b_n) , with $b_i \in \{0, \dots, p-1\}$

Proof. For $\vec{a} \in \mathbb{Z}_p$, we showed above how to obtain (b_n) by $b_n = \frac{a_{n+1} - a_n}{p^n}$. Conversely, let (b_n) be such a sequence. We can take the formula with which we constructed the b_n 's earlier to try $a_1 = b_0, a_2 = b_0 + p b_1, a_3 = b_0 + p b_1 + p^2 b_2$, and generally $a_n = b_0 + \dots + b_{n-1} p^{n-1}$. Indeed, for the map $\mathbb{Z}/p^{n+1}\mathbb{Z} \rightarrow \mathbb{Z}/p^n\mathbb{Z}$, observe

$$b_0 + \dots + b_{n-1} p^{n-1} + b_n p^n \mapsto b_0 + \dots + b_{n-1} p^{n-1},$$

so we indeed have a p -adic integer. Check that this relation is bijective. $\square$

Example 4.18. $1 + 1 \cdot 3 + 1 \cdot 3^2 + \dots$ is like the power series $\frac{1}{1-x}$, so this is the p -adic expansion of $\frac{1}{-2}$. If $\vec{a} = b_0 + b_1 p + b_2 p^2 + \dots \longleftrightarrow (b_0, b_1, \dots)$, then $p\vec{a} \longleftrightarrow (0, b_0, b_1, \dots)$

Let's revisit the sequence $0 \rightarrow \mathbb{Z}_p \xrightarrow{p^n} \mathbb{Z}_p \xrightarrow{\varepsilon_n} \mathbb{Z}/p^n\mathbb{Z} \rightarrow 0$. Let's show $\ker \varepsilon_n = p^n\mathbb{Z}_p$. $\vec{a} \in \ker \varepsilon_n \iff a_n = 0 \implies a_{n-1} = \dots = a_1 = 0$, so the p -adic expansion of $\vec{a}$ is $(0, \dots, 0, a_{n+1}, \dots)$, which we see is in $p^n\mathbb{Z}_p$, like in the example above. This is the analog of saying "an integer with three zeroes at the end must be divisible by 1000".

5. The p -Adic Absolute Value

Definition (The p -adic Absolute Value)

5.1

The **p -adic absolute value** of $\vec{a}$ is $|\vec{a}|_p = \frac{1}{p^{v_p(a)}}$. In particular, the higher the p -valuation of a number is, the 'smaller' it is. Note $|0|_p = \frac{1}{p^\infty} = 0$

Remark 5.2. Before, we said $1 + 1 \cdot 3 + 1 \cdot 3^2 + \dots$, is $\frac{1}{1-3}$ because it's a geometric series. We now see this is ok, because $|p|_p = \frac{1}{p} < 1$.

Example 5.3. Let $a \in \mathbb{Z}_5$, $a = \sum_{i=0}^{\infty} b_i p^i$. We can practice finding expansions

$$-1 = 5 - 1 - 5 = 4 + 5(-1) = 4 + 4 \cdot 5 - 25 = 4 + 4 \cdot 5 + 25(-1) = \dots$$

$$-1 = (\dots, 4, 4, 4)$$

Properties of the p -adic Absolute Value

5.4

$|a|_p \geq 0$, and $|a|_p = 0 \iff a$ is a unit. $|ab|_p = |a|_p |b|_p$, and $|a + b|_p \leq \max\{|a|_p, |b|_p\}$. This is the **ultrametric inequality**

Definition (Distance on $\mathbb{Z}_p$)

5.5

For $a, b \in \mathbb{Z}_p$, we define $d(a, b) = |a - b|_p$. Observe that $d(a, a) = 0$, $d(a, b) = d(b, a)$, and $d(a, b) + d(b, c) \geq d(a, c)$. In fact, $|a - c|_p \leq \max\{|a - b|_p, |b - c|_p\}$, which is an even stronger version of the triangle inequality, called a **non-Archimedean inequality**.

Note that p -adic valuation can be extended to $\mathbb{Q}_p$, and we have that $|a|_p \leq 1 \iff a \in \mathbb{Z}_p$.

Example 5.6. $|a|_p = 1/p \iff a \in p\mathbb{Z}_p \setminus p^2\mathbb{Z}_p$

$$|a|_p = 1/p^2 \iff a \in p^2\mathbb{Z}_p \setminus p^3\mathbb{Z}_p$$

In general, we can think of $\mathbb{Z}_p$ as the closed unit disk with radius less than 1, and it's a union of circles like that. We can also see

$$\mathbb{Q}_p \setminus \{0\} = \sqcup_{n \in \mathbb{Z}} p^n \mathbb{Z}_p^\times$$

Proposition

5.7

Any triangle in $\mathbb{Q}_p$ is isosceles.

Proof. With one vertex of the triangle at 0, let the edges be $x, y, y - x$, then $|x - y|_p \leq \max\{|x|_p, |y|_p\}$. Suppose $|x|_p < |y|_p$. Then, $|x - y|_p \leq |y|_p$. On the other hand, $|y|_p = |x - (x - y)|_p \leq \max\{|x|_p, |x - y|_p\}$. Since we assumed $|y|_p \not\leq |x|_p$, we must have $|y|_p \leq |x - y|_p$.

Thus, $|y|_p = |x - y|_p$, proving the triangle is isosceles. $\square$

Proposition

5.8

We may define $B_r(a)$ to be the disk of radius r centered at $a \in \mathbb{Z}_p$, $\{x \in \mathbb{Q}_p : |x - a|_p < r\}$. Then, if $b \in B_r(a)$, we have that $B_r(a) = B_r(b)$.

Proof. Exercise. $\square$

Let K be a field, and let $A_n = K[t]/(t^n)$. Then, there is a ring homomorphism $\phi_n : A_n \rightarrow A_{n-1}$ by $\phi(a_0 + a_1t + \cdots + a_nt^n) = \phi(a_0 + a_1t + \cdots + a_{n-1}t^{n-1})$. We then get an inverse limit $\varprojlim K[t]/(t^n)$, which is the power series ring $K[[t]]$.

Definition

5.9

Let K be a field. An **absolute value** on K is a map $|\cdot| : K \rightarrow \mathbb{R}$ such that

1. $|x| > 0$ unless $x = 0$. $|0| = 0$.
2. $|xy| = |x||y|$
3. $|x + y| \leq |x| + |y|$ (Triangle Inequality)

We say that an absolute value is **non-Archimedean** if $|x + y| \leq \max\{|x|, |y|\}$.

Example 5.10. We have the usual absolute value over $\mathbb{Q}$: $|a|_\infty = \sqrt{a^2}$. We have also shown that $|\cdot|_p : \mathbb{Q} \rightarrow \mathbb{R}$ is an absolute value for any prime p .

Example 5.11. Let $c \in K$ be a root of unity. As $c^n = 1$, we also have $|c|^n = 1$, so $|c| = \pm 1 \implies |c| = 1$.

Definition

5.12

For K any field, we have the **trivial absolute value** $|a| = 1, |0| = 0$.

Proposition

5.13

When K is a finite field, the trivial absolute value is the only absolute value.

Definition

5.14

Let $|\cdot|_1, |\cdot|_2$ be absolute values on K . We say they are **equivalent** if $|\cdot|_1 = |\cdot|_2^c$ for some $c \in \mathbb{R}_{>1}$

Example 5.15. Instead of $|a|_p = \frac{1}{p^{v_p(a)}}$, we can use $|a|_p = \frac{1}{e^{v_p(a)}}$, which is equivalent.

Proposition

5.16

$|\cdot|_1$ and $|\cdot|_2$ are equivalent if for any $a \in K$, $|a|_1 < 1 \iff |a|_2 < 1$. Furthermore, a sequence $\{a_n\}_{n \geq 1}$ is Cauchy with respect to $|\cdot|_1$ iff it's Cauchy with respect to $|\cdot|_2$.

Definition

5.17

A sequence $\{a_n\}_{n \geq 1}$ on K is **Cauchy** with respect to $|\cdot|$ if for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$ such that $n, m \geq N \implies |a_n - a_m| < \varepsilon$.

Furthermore, we say K is **complete** with respect to $|\cdot|$ if every Cauchy sequence has a limit in K .

For example, $\mathbb{R}$ is complete with respect to the usual absolute value, but $\mathbb{Q}$ is not complete with both the usual absolute value and $|\cdot|_p$.

Theorem

5.18

$\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Ostrowski's Theorem

5.19

Any non-trivial absolute value on $\mathbb{Q}$ is equivalent to $|\cdot|_\infty$ or $|\cdot|_p$ for some prime p . Furthermore, if $p \neq q$ are distinct primes, then $|\cdot|_p$ is not equivalent to $|\cdot|_q$.

Product Formula

5.20

Let $a \in \mathbb{Q}$ non-zero. Then,

$$\prod_{p \leq \infty} |a|_p = 1$$

This product is well defined because only finitely many $|a|_p \neq 1$.

Example 5.21. Let $a = 10$. Then, $|10|_2 = \frac{1}{2}$, $|10|_3 = 1$, $|10|_5 = \frac{1}{5}$, $|10|_7 = 1$, $|10|_n = 1$ for $n \geq 11$, and $|10|_\infty = 10$.

Proof. If a is some prime p , then $|p|_p = \frac{1}{p}$, $|p|_q = 1$, $|p|_\infty = p$, so the claim holds for primes.

Now, define $\phi : (\mathbb{Q}^\times, \times) \rightarrow (\mathbb{R}^\times, \times)$ by $\phi(a) = \prod_{p \leq \infty} |a|_p$. Then ϕ is a homomorphism, as $\phi(ab) = \phi(a)\phi(b)$. One can confirm that $\phi(-1) = 1$, and we showed $\phi(p) = 1$. Furthermore, $\phi(p) = 1 \implies \phi(p^n) = 1$ for any $n \in \mathbb{Z}$. Now, for any $a \in \mathbb{Q}^\times$, we have $a = \pm p_1^{e_1} \cdots p_n^{e_n}$, and the claim for $\phi(a)$ follows. $\square$

Remark 5.22. Suppose $\{a_n\}$ is a sequence in $\mathbb{R}$ such that for any $\varepsilon > 0$, there exists $N > 1$ with $|a_{n+1} - a_n| < \varepsilon$ for any $n > N$. This is a weaker condition than being Cauchy in $\mathbb{R}$. However, in $\mathbb{Q}_p$, this condition is equivalent to being Cauchy, as $|\cdot|_p$ is non-Archimedean.

Thus, for a sequence $\{a_n\}$ in $\mathbb{Q}_p$ to converge, all that is needed is that for any $\varepsilon > 0$, there exists $N \in \mathbb{N}$, $n \geq N \implies |a_{n+1} - a_n|_p < \varepsilon$. Consequently, any series $\sum_{n=1}^\infty x_n$ converges in $\mathbb{Q}_p$ so long as $\{x_n\}$ converges.

This is another reason why we can say $b_0 + b_1p + b_2p^2 + \cdots$ is well defined in $\mathbb{Q}_p$.

Example 5.23. The sequence $1, 1/2, 1/3, \dots$ converges in $\mathbb{R}$, but diverges in $\mathbb{Q}_p$.

Proposition

5.24

The sequence $\{u_n\}_{n \geq 1}$ converges in $\mathbb{Q}_p$ if and only if $\lim_{n \rightarrow \infty} |u_n - u_{n-1}|_p = 0$. Similarly, $\sum_{n=1}^{\infty} b_n$ converges if and only if $\lim_{n \rightarrow \infty} |b_n|_p = 0$.

6. The Exponential Function**Recall**

$$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

We are curious about the convergence of this series when $x \in \mathbb{Z}_p$.

Question

What is $|x^n/n!|_p$?

Let $n = b_0 + b_1p + b_2p^2 + \cdots + b_rp^r$, where $0 \leq b_i \leq p-1$. Then, $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \cdots + \lfloor n/p^r \rfloor$. Observe that

$$\lfloor n/p \rfloor = b_1 + b_2p + b_3p^2 + \cdots + b_rp^{r-1}$$

$$\lfloor n/p^2 \rfloor = b_2 + b_3p + b_4p^2 + \cdots + b_rp^{r-2}$$

$$\lfloor n/p^r \rfloor = b_r$$

Thus,

Proposition

6.1

$$v_p(n!) = b_0 \frac{p^0 - 1}{p - 1} + b_1 \frac{p^1 - 1}{p - 1} + b_2 \frac{p^2 - 1}{p - 1} + \cdots + b_r \frac{p^r - 1}{p - 1} = \frac{n - \sum b_i}{p - 1}$$

Now,

$$v_p(x^n/n!) = v_p(x^n) - v_p(n!) = n(v_p(x) - \frac{1}{p-1}) + \frac{\sum b_i}{p-1}$$

From this, we see $v_p(x^n/n!) \rightarrow \infty$ if $v_p(x) \geq \frac{1}{p-1}$.

Proposition

6.2

If $|x|_p < \frac{1}{p^{1/(p-1)}}$, then, $\exp(x)$ converges.

7. Roots of Polynomials

Let $f(x) = x^2 + 1$, and we want to find roots in $\mathbb{Z}_5$. Note that if f has a root like $f(a) = 0$ in $\mathbb{Z}_p$, then f has a root in $\mathbb{Z}/p^n\mathbb{Z}$ for every n .

$f(x)$ has a root in $A_1 = \mathbb{Z}/5\mathbb{Z}$, for example $x = 2$. Suppose a_n is a root of $f(x)$ in $A_n = \mathbb{Z}/5^n\mathbb{Z}$. That is, $a_n^2 + 1 \equiv 0 \pmod{5^n}$. We want to find a root a_{n+1} in A_{n+1} . Note that we need $a_{n+1} = a_n + p^n b_n$ for $0 \leq b_n \leq p - 1$. Observe

$$a_{n+1}^2 + 1 = (a_n + p^n b_n)^2 + 1 = a_n^2 + 2 \cdot 5^n a_n b_n + 5^{2n} b_n^2 + 1 \equiv a_n^2 + 2 \cdot 5^n a_n b_n + 1 \pmod{5^{n+1}}$$

So, $2 \cdot 5^n a_n b_n \equiv -(a_n^2 + 1) \pmod{5^{n+1}}$, but $a_n^2 + 1$ is 0 in A_n , so $a_n^2 + 1 = 5^n d_n$, thus

$$2 \cdot 5^n a_n b_n \equiv 5^n d_n \pmod{5^{n+1}} \iff 2a_n b_n \equiv d_n \pmod{5}.$$

Modulo 5, we assumed $a_n \equiv 2 \pmod{5}$, so $4b_n \equiv d_n \pmod{5}$. As 4 is a unit modulo 5, we can indeed properly solve for a b_n .

In this particular case there is a nice formula for the 5-adic root of $x^2 + 1$: Newton's binomial formula says $(1 - x)^{1/2} = \sum_{n=0}^{\infty} (-1)^n \binom{1/2}{n} x^n$. We are looking for $\sqrt{-1}$, and observe

$$\sqrt{-1} = \frac{1}{2} \sqrt{1 - 5} = \sum_{n=0}^{\infty} (-1)^n \binom{1/2}{n} 5^n,$$

which converges in $\mathbb{Z}_5$.

Question

What is the algebraic closure of $\mathbb{Q}_p$? To close $\mathbb{R}$, we only need to add i . What are the irreducible polynomials in $\mathbb{Q}_p$? How do we check if a polynomial has roots.

Observe

Let $f(x) \in \mathbb{Q}_p[x]$. We can multiply (or divide) f by an appropriate power of p so that f becomes a polynomial in $\mathbb{Z}_p[x]$, with not all coefficients divisible by p .

Remark 7.1. Let $f(x) \in \mathbb{Z}_p[x]$ with $f(a) = 0$. Then, $f(\bar{a}) \equiv 0 \pmod{p^n}$ for all n . This follows from $\varepsilon_n : \mathbb{Z}_p \rightarrow \mathbb{Z}/p^n\mathbb{Z}$ being a ring homomorphism.

Question

If f has a root in $\mathbb{Z}/p^n\mathbb{Z}$ for all n , does f have a root in $\mathbb{Z}_p$? More generally, let $f(x_1, \dots, x_n) \in \mathbb{Z}_p[x_1, \dots, x_n]$. Then, we ask if $V_n(f)$ nonempty implies $V(f)$ is nonempty.

Definition (General Inverse Limits)

7.2

Let $D_1, D_2, \dots$ be sets, with **transition maps** $D_{n+1} \rightarrow D_n$. Then, let D be the **inverse limit** of D_n , i.e. $(d_n) \in D$ if $d_{n+1} \mapsto d_n$ for all n .

Lemma

7.3

If D_n 's are all finite and nonempty, then D is nonempty.

Proof. The conclusion is clear if all transition maps are surjective. Our idea to prove it in general is to reduce to this case.

Fix $n \geq 1$. Let $D_{n,1} = \text{Img}(D_{n+1} \rightarrow D_n)$, $D_{n,2} = \text{Img}(D_{n+2} \rightarrow D_{n+1} \rightarrow D_n)$, and generally

$$D_{n,k} = \text{Img}(D_{n+k} \rightarrow D_n).$$

Observe that $D_n \supset D_{n,1} \supset D_{n,2} \supset \cdots$. By our assumption, $D_{n,k}$ are all finite and nonempty. So, there exists a $K \gg 0$ such that $D_{n,k} = D_{n,k+1}$ for all $k \geq K$. Call E_n the set which they stabilize to. In the homework, we will prove E_{n+1} surjects onto E_n . It follows that $\lim E_n \hookrightarrow \lim D_n$, and by surjectivity $\lim E_n$ is nonempty. $\square$

$$\begin{array}{ccc} E_{n+1} & \longrightarrow & E_n \\ \uparrow & & \uparrow \\ D_{n+1} & \longrightarrow & D_n \end{array}$$

$V_{n+1}(f) \rightarrow V_n(f)$ is a transition map, so if they're all nonempty, it follows from [Lemma 7.3](#) that $V(f)$ is nonempty.

Theorem

7.4

Let $f \in \mathbb{Z}_p[x_1, \dots, x_n]$, $V(f)$ be the solution set of f , and $V_n(f)$ be the solution set of f in $\mathbb{Z}/p^n\mathbb{Z}$. Then, $V(f) \neq \emptyset \iff V_n(f) \neq \emptyset$ for all $n \in \mathbb{Z}_+$.

Special Case of Hensel's Lemma

7.5

Let $f(x) \in \mathbb{Z}_p[x]$. Let $a_0 \in \mathbb{F}_p$ be a simple root of $f \bmod p$. That is, $f'(a_0) \not\equiv 0 \pmod{p}$. Then, there exists a unique root a of $f(x)$ with $a \equiv a_0 \pmod{p}$.

Proof. We will construct a Cauchy sequence $\{a_n\}$ in $\mathbb{Z}_p$, and show that $a = \lim_{n \rightarrow \infty} a_n$ satisfies $f(a) = 0$. Suppose $a_n \in \mathbb{Z}_p$ with the property $f(a_n) \equiv 0 \pmod{p^{n+1}}$ and $a_n \equiv a_0 \pmod{p}$. Now, let $a_{n+1} = a_n + hp^{n+1}$ for $h \in \mathbb{Z}_p$, and we want to have $f(a_{n+1}) \equiv 0 \pmod{p^{n+2}}$. Well, $f(a_n + hp^{n+1}) = f(a_n) + hp^{n+1}f'(a_n) + (0)$. Let $h = -f(a_n)/p^{n+1} \cdot f'(a_n)^{-1} = -c_n \cdot f'(a_n)^{-1}$, and we know $f'(a_n)$ is a unit in $\mathbb{Z}_p$ by assumption. Moreover, $a_{n+1} - a_n = h \cdot p^{n+1}$, so $|a_{n+1} - a_n|_p \leq \frac{1}{p^{n+1}}$, hence a_n is a Cauchy sequence, and the claim follows. $\square$

Example 7.6. Let $f(x) = x^p - x \in \mathbb{Z}_p[x]$. In $\mathbb{F}_p[x]$, we have $f(x) = x(x-1) \cdots (x-p+1)$, and these are all simple roots. It follows that $x^p - x$ has p distinct roots in $\mathbb{Z}_p$. Moreover, $x^p - x = x(x^{p-1} - 1)$, so $\mathbb{Q}_p$ contains the $p-1$ 'th roots of unity.

Example 7.7. Let $f : \mathbb{R} \rightarrow \mathbb{R}$ be real analytic (or $f : \mathbb{C} \rightarrow \mathbb{C}$ holomorphic). Suppose $f(5) = 0$. If we're looking for the multiplicity of 5 as a root of f , we can look at $f'(5), f''(5)$, etc. until $f^{(n)}(5) \neq 0$. If n is minimal, we can say $v_5(f) = n$. Moreover, $v_5(fg) = v_5(f) + v_5(g)$.

Example 7.8. Let K be any field. Then $v : K^\times \rightarrow \mathbb{Z}$ is called the **discrete valuation** on K satisfying

- $v(ab) = v(a) + v(b)$
- $v(a+b) \geq \min\{v(a), v(b)\}$

The set $A = \{a \in K \mid v(a) \geq 0\}$ is a subring of K called the **discrete valuation ring** (DVR). The set $m = \{a \in K \mid v(a) > 0\}$ is a maximal and a principal ideal.

Example 7.9. Let $K = \mathbb{Q}$, and we can write any element of $\mathbb{Q}$ as $\frac{a}{b} = \frac{r}{s} \cdot 5^n$, where $n \in \mathbb{Z}$ and $5 \nmid rs$. We can then define $v : \mathbb{Q}^\times \rightarrow \mathbb{Z}$ by $\frac{r}{s} \cdot 5^n \mapsto n$. Then, $A = \{\frac{a}{b} \in \mathbb{Q} \mid 5 \nmid b\}$, which we call $\mathbb{Z}_{(5)}$ (not to be confused with $\mathbb{Z}_5$).

Remark 7.10. We may complete a DVR as follows: there is an inverse limit by the maps $\cdots \rightarrow A/m^3 \rightarrow A/m^2 \rightarrow A/m$, and the inverse limit is what we call $\widehat{A}$.

Example 7.11. Suppose $\hookrightarrow A_3 \hookrightarrow A_2 \hookrightarrow A_1$. Then, $A = \lim_{\leftarrow} A_n = \cap A_n$

8. Hensel's Lemma

Recall our special case of Hensel's Lemma:

Recall

Let $f(x) \in \mathbb{Z}_p[x]$. Suppose $a_0 \in \mathbb{Z}_p$ is a simple root of $f(x) \pmod{p}$. Then, there exists a unique $a \in \mathbb{Z}_p$ with $f(a) = 0$ and $a \equiv a_0 \pmod{p}$.

In the homework, we showed $a \equiv b \pmod{p}$ implies $a^p \equiv b^p \pmod{p^2}$. Raising to the p' th power is therefore a contraction in $\mathbb{Z}_p$.

Lemma

8.1

Let $f(x) \in \mathbb{Z}_p[x]$. Fix $x, y \in \mathbb{Z}_p$. Then, there exists $z \in \mathbb{Z}_p$ such that $f(x + y) = f(x) + f'(x)y + y^2z$

One Variable Hensel's Lemma

8.2

Let $f(x) \in \mathbb{Z}_p[x], f'(x) \in \mathbb{Z}_p[x]$. Suppose $a_0 \in \mathbb{Z}_p$ is such that $f(a_0) \equiv 0 \pmod{p^n}$, and $v_p(f'(a_0)) = k \geq 0$, where $n > 2k$. Then, f has a root $a \in \mathbb{Z}_p$ such that $f(a) = 0 \in \mathbb{Z}_p$, $a \equiv a_0 \pmod{p^{n-k}}$.

Proof. We will prove by induction that for each integer $r \geq 0$, there exists $a_{r+1} \in \mathbb{Z}_p$ such that

- (i) $f(a_{r+1}) \equiv 0 \pmod{p^{n+r+1}}$
- (ii) $a_{r+1} \equiv a_r \pmod{p^{n-k+r}}$
- (iii) $v_p(f'(a_{r+1})) = k$

Inductively, we are assuming $f(a_r) \equiv 0 \pmod{p^{n+r}}$. We then want $a_{r+1} = a_r + p^{n-k+r}b$ satisfying the above conditions. By the identity in [Lemma 8.1](#),

$$f(a_{r+1}) = f(a_r + p^{n-k+r}b) = f(a_r) + f'(a_r)p^{n-k+r}b + p^{2n-2k+2r}b^2z, \quad z \in \mathbb{Z}_p$$

Now, let $f(a_r) = p^{n+r}c$, and we also have $v_p(f'(a_r)) = k$, so $f'(a_r) = p^k u$, $u \in \mathbb{Z}_p^\times$. Moreover, by the assumption that $n > 2k$, we know $n + n - 2k > n$, and if $r \geq 1$, we know $2r \geq r + 1$ as well. Thus,

$$f'(a_r) = p^{n+r}c + p^k u \cdot p^{n-k+r}b = p^{n+r}(c + ub),$$

so to get an extra p , we need $c + ub \equiv 0 \pmod{p}$. As u is a unit, we can indeed solve for an

appropriate b . □

Multivariable Hensel's Lemma

8.3

Let $F(t_1, \dots, t_m) \in \mathbb{Z}_p[t_1, \dots, t_m]$, and suppose $\vec{x} = (x_1, \dots, x_m) \in \mathbb{Z}_p^m$ is such that $F(x_1, \dots, x_m) \equiv 0 \pmod{p^n}$, and $v_p(\frac{\partial F}{\partial t_j}(\vec{x})) = k$ for some j in $1 \leq j \leq m$, and $0 \leq 2k < n$. Then, there exists $\vec{y} = (y_1, \dots, y_m) \in \mathbb{Z}_p^m$ with $F(y_1, \dots, y_m) = 0$, and $y \equiv x \pmod{p^{n-k}}$

Proof. If $m = 1$, we're done from Hensel's single variable lemma. We assume that j has the least p -adic valuation for the partial derivative with respect to t_j . Then, set

$$f(t) = F(x_1, x_2, \dots, x_{j-1}, t, x_{j+1}, \dots, x_m)$$

and $f'(t) = \frac{\partial F}{\partial t_j}$. We can thus apply single variable Hensel to f and x_j , and we obtain $y_j = a \in \mathbb{Z}_p$. Thus, $\vec{y} = (x_1, x_2, \dots, x_{j-1}, y_j, x_{j+1}, \dots, x_m)$ is our desired root. □

Example 8.4. Let $f(x) = x^2 - 8$. In $\mathbb{F}_7$, f has a simple root 1. Note that in $\mathbb{F}_7[x]$, the polynomial f is $x^2 - 1$, and moreover any polynomial of the form $x^2 - 7k - 1$ reduces to that polynomial. It follows that any number of the form $1 + 7k$ is a square root in $\mathbb{Z}_7$. More generally, $1 + a$ has a square root in $\mathbb{Z}_7$ if $v_p(a) > 0$.

Generally, if $b \in 1 + p\mathbb{Z}_p$, then b is a square in $\mathbb{Z}_p$.

Example 8.5. Let $n \in \mathbb{Z}$. When is n a square in $\mathbb{Z}_p$? That is, we want to find out whether $f(x) = x^2 - n$ has roots in $\mathbb{Z}_p$. In $\mathbb{F}_p[x]$, $f(x) = x^2 - \bar{n}$. If $\left(\frac{n}{p}\right) = 1$, then $n = a_0^2$ in $\mathbb{F}_p$. That is, $f(a_0) \equiv 0 \pmod{p}$, and $f'(x) = 2x$, so assuming p is odd any $n \not\equiv 0 \pmod{p}$, $f'(a_0) \not\equiv 0 \pmod{p}$.

Remark 8.6. $n \in \mathbb{Z}$ with $p \nmid n$ is a square in $\mathbb{Z}_p \iff \left(\frac{n}{p}\right) = 1$.

Example 8.7. Let $f(x) = x^p - x$ in $\mathbb{Z}_p[x]$. Does f have roots in $\mathbb{Z}_p$? $\mathbb{Q}_p$?

In $\mathbb{F}_p[x]$, $x^p - x$ has p simple roots (everything is a root). Thus, by Hensel's, all of these roots can be lifted to roots in $\mathbb{Z}_p$, i.e. $x^p - x$ has p roots in $\mathbb{Z}_p$. Aside from $x = 0$, all the other roots satisfy $x^{p-1} - 1 = 0$, so the rest of the roots are $p - 1$ roots of unity. (In fact, these are the only roots of unity in $\mathbb{Z}_p$)

From the homework, for $a \in \mathbb{Z}_p$, $\lim_{n \rightarrow \infty} a^{p^n}$ is a root of $x^p - x$.

Definition

8.8

We say an n -tuple $(a_1, \dots, a_n) \in \mathbb{Z}_p^n$ is **primitive** if one of the a_i 's is a unit.

Remark 8.9. For an n -tuple in $\mathbb{Q}_p^n$, we can clear the denominators by multiplying by a power of p to get a primitive tuple in $\mathbb{Z}_p^n$.

For Some Reason

8.10

$$\lim_{\leftarrow} \mathbb{Z}/n\mathbb{Z} = \prod_{p \text{ prime}} \mathbb{Z}_p =: \widehat{\mathbb{Z}}$$

Here's what's going on:

$$\begin{array}{ccc} \mathbb{Z}/6\mathbb{Z} & & \mathbb{Z}/4\mathbb{Z} \\ \downarrow & \searrow & \downarrow \\ \mathbb{Z}/3\mathbb{Z} & & \mathbb{Z}/2\mathbb{Z} \end{array}$$

The stuff you take an inverse limit of doesn't have to be a totally ordered set, it can be a partially ordered set.

9. Structure of $\mathbb{Q}_p^\times$

$$0 \longrightarrow \mathbb{R}_{>0} \longrightarrow \mathbb{R}^\times \begin{array}{c} \xrightarrow{\pi} \\ \xleftarrow{s} \end{array} \{\pm 1\} \longrightarrow 0$$

where $s(1) = 1, s(-1) = -1$. Since $\{\pm 1\}$ embeds in $\mathbb{R}^\times$, this exact sequence demonstrates $\mathbb{R}^\times \cong \mathbb{R}_{>0} \times \{\pm 1\}$. Moreover, $\mathbb{R}_{>0} \cong (\mathbb{R}, +)$, so $\mathbb{R}^\times \cong (\mathbb{R}, +) \times \{\pm 1\}$.

Now, recall that for any $a \in \mathbb{Q}_p^\times$, $a = up^n$, with $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^\times$. Hence,

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z},$$

so to understand $(\mathbb{Q}_p^\times, \times)$, we need to understand $(\mathbb{Z}_p^\times, \times)$.

Let $\varepsilon_1 : \mathbb{Z}_p^\times \rightarrow \mathbb{F}_p^\times$ be the projection on to the first coordinate. The kernel of ε_1 is $U_1 = \{1 + p\mathbb{Z}_p\} \leq \mathbb{Z}_p^\times$. Generally, we define $U_j = \{1 + p^j\mathbb{Z}_p\}$. Now, we have an exact sequence.

$$0 \longrightarrow U_1 \longrightarrow \mathbb{Z}_p^\times \xrightarrow{\varepsilon_1} \mathbb{F}_p^\times \longrightarrow 0$$

Next, we know

$$U_1 \geq U_2 \geq U_3 \geq \cdots$$

and one can show

$$\bigcap_{n=1}^{\infty} U_n = \{1\}$$

Thinking about how $x \in \mathbb{F}_p^\times \iff x^{p-1} = 1$, recall from a previous discussion that the limit of the Cauchy sequence $1, j, j^p, j^{p^2}, \dots$ also satisfies $\tilde{j}^{p-1} = 1$, where $j \in \{1, \dots, p-1\}$. Hence, we may define a homomorphism $s : \mathbb{F}_p^\times \rightarrow \mathbb{Z}_p^\times$ by $s(j) = \tilde{j}$.

$$0 \longrightarrow U_1 \longrightarrow \mathbb{Z}_p^\times \begin{array}{c} \xrightarrow{\varepsilon_1} \\ \xleftarrow{s} \end{array} \mathbb{F}_p^\times \longrightarrow 0$$

It follows by the sequence being exact that

$$\mathbb{Z}_p^\times \cong U_1 \times \mathbb{F}_p^\times$$

$$\mathbb{Q}_p^\times \cong U_1 \times \mathbb{F}_p^\times \times \mathbb{Z}$$

We therefore now want to understand U_1 .

Definition

9.1

Consider the exact sequence below. A homomorphism s (like in the previous sequences) is called a **section** if $f(s(c)) = c$ for all $c \in C$. If such a section exists, we have that $B \cong A \times C$.

$$0 \longrightarrow A \longrightarrow B \begin{array}{c} \xrightarrow{f} \\ \xleftarrow{s} \end{array} C \longrightarrow 0$$

Let's talk about why we care about the structure of $\mathbb{Q}_p^\times$

Recall

$\mathbb{Q}^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}[\text{primes}]$, where $\mathbb{Z}[\text{primes}]$ denotes the abelian free group of primes.

Let $K = \mathbb{Q}[x]/(f(x))$ be a quadratic extension, where $f(x) = ax^2 + bx + c$. Then, we see that $K = \mathbb{Q}(\sqrt{b^2 - 4ac})$. In general a quadratic extension looks like $K = \mathbb{Q}(\sqrt{d})$, and it can be shown that d can always be an integer. Moreover, we want d to be squarefree, and it follows that quadratic number fields are in bijection with $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$.

Definition (Direct Products and Direct Sums)

9.2

Let $G_1, G_2, \dots$ be an infinite list of groups. We can make a group G out of $G = \prod_{n=1}^\infty G_n$, where the operations are taken component-wise as expected. This is called the **direct product**

Moreover, there exists a subgroup $\oplus G_n \leq \prod G_n$ which is all sequence such that only finitely many are not the identity. This is called the **direct sum**.

Remark 9.3. $\mathbb{Q}^\times \cong \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}[\text{primes}] \cong \mathbb{Z}/2\mathbb{Z} \times \oplus \mathbb{Z}$

Corollary

9.4

$$\mathbb{Q}^\times / (\mathbb{Q}^\times)^2 = \{\pm 1\} \times \oplus (\mathbb{Z}/2\mathbb{Z})$$

This is why understanding the structure is so helpful.

Now, back to $\mathbb{Q}_p$.

Recall

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}_p \cong U_1 \times \mathbb{F}_p^\times \times \mathbb{Z}, \text{ where } U_1 = 1 + p\mathbb{Z}_p \leq \mathbb{Z}_p^\times.$$

Claim

We claim that for p odd, $(U_1, \times) \cong (\mathbb{Z}_p, +)$. This means the squares in U_1 are isomorphic to $2\mathbb{Z}_p$, but since 2 is a unit (for $p \geq 3$), $2\mathbb{Z}_p = \mathbb{Z}_p$. That is, everything in U_1 is a square.

The result is that for $p \geq 3$,

$$\begin{aligned} \mathbb{Q}_p^\times &\cong \mathbb{Z}_p^\times \times \mathbb{F}_p^\times \times \mathbb{Z} & (\mathbb{Q}_p^\times)^2 &\cong \mathbb{Z}_p^\times \times (\mathbb{F}_p^\times)^2 \times 2\mathbb{Z} \\ (\mathbb{Q}_p^\times) / (\mathbb{Q}_p^\times)^2 &\cong (\mathbb{F}_p^\times) / (\mathbb{F}_p^\times)^2 \times \mathbb{Z}/2\mathbb{Z} &\cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\cong V_4 \end{aligned}$$

Before, we saw that $\mathbb{Q}$ has infinitely many quadratic extensions, since $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ was infinite.

However, $\mathbb{Q}_p$ only has 3 non-trivial quadratic extensions.

Proof. We assume p is odd. Let U_n be the set $1 + p^n \mathbb{Z}_p$, and note $U_n \geq U_{n+1}$ for all $n \geq 1$. Consider the surjective homomorphism $\phi_n : U_n \rightarrow \mathbb{Z}/p\mathbb{Z}$ by

$$\phi_n(1 + p^n a) = a \pmod{p} = \varepsilon_1(a).$$

This is a homomorphism as

$$(1 + p^n a)(1 + p^n b) = 1 + p^n(a + b) + p^{2n}ab = 1 + p^n(a + b + p^n ab)$$

and modulo p , $a + b + p^n ab$ is just $a + b$. Moreover,

$$\ker \phi_n = \{1 + p^n a \mid a \equiv 0 \pmod{p}\} = \{1 + p^n a \mid a \in p\mathbb{Z}_p\} = U_{n+1}.$$

Therefore, $U_n/U_{n+1} \cong \mathbb{Z}/p\mathbb{Z}$. By the third isomorphism theorem $(U_1/U_3)/(U_2/U_3) \cong U_1/U_2$, and it follows that $|U_1/U_3| = p^2$. Generally,

$$|U_1/U_{n+1}| = p^n.$$

“Whenever you have a p -adic number and you don’t know what to do with it, raise it to the p -th power.” — Rama

Lemma

9.5

Let $u \in U_n \setminus U_{n+1}$. Then, $u^p \in U_{n+1} \setminus U_{n+2}$

Proof. Let $u = 1 + p^n a$, $a \in \mathbb{Z}_p$. Then,

$$u^p = (1 + p^n a)^p = 1 + p \cdot p^n a + \frac{p(p-1)}{2}(p^n a)^2 + \cdots \in 1 + p^{n+1} \mathbb{Z}_p$$

Furthermore, by the assumption that $u \notin U_{n+1}$, we know that a is a unit, and it follows from the above equality that $u^p \notin 1 + p^{n+2} \mathbb{Z}_p$, proving indeed that $u^p \in U_{n+1} \setminus U_{n+2}$. $\square$

Now back to the original proof. Consider $\alpha = 1 + p \in U_1 \setminus U_2$. Then, $\alpha^p \in U_2 \setminus U_3$, and generally $\alpha^{p^n} \in U_{n+1} \setminus U_{n+2}$. Now, define $\psi_n : \mathbb{Z}/p^n \mathbb{Z} \rightarrow U_1/U_{n+1}$ by

$$\psi_n(z) = \bar{\alpha}^z$$

Since $\psi_n(z+w) = \bar{\alpha}^{z+w} = \bar{\alpha}^z \bar{\alpha}^w = \psi_n(z) \psi_n(w)$, it’s clear that ψ_n is a homomorphism, and it’s not hard to check that it’s well defined. Moreover, note that $\alpha^{p^{n-1}} \in U_n \setminus U_{n+1}$, and therefore $\bar{\alpha}^{p^{n-1}} \neq 1$ in U_1/U_{n+1} . This tells us that $|\bar{\alpha}| = p^n = |U_1/U_{n+1}|$, hence $\bar{\alpha}$ is a generator of U_1/U_{n+1} , and therefore is a cyclic group of order p^n , i.e. isomorphism to $\mathbb{Z}/p^n \mathbb{Z}$. Let $h_j : U_1/U_{j+2} \rightarrow U_1/U_{j+1}$ be the canonical projection, and $f_j : \mathbb{Z}/p^{j+1} \mathbb{Z} \rightarrow \mathbb{Z}/p^j \mathbb{Z}$ be the canonical projection. Then observe the below diagram of inverse systems (below the proof): it’s an exercise to check that $h_n \circ \psi_{n+1}(a) = \psi_n \circ f_n(a)$, and therefore the inverse limits will be the same. That is, $\mathbb{Z}_p = \lim_{\leftarrow} \mathbb{Z}/p^n \mathbb{Z} \cong \lim_{\leftarrow} U_1/U_{n+1}$. It’s another exercise to check that $\lim_{\leftarrow} U_1/U_{n+1} \cong U_1$, finishing the proof. $\square$

$$\begin{array}{ccccccc}
 \cdots & \longrightarrow & U_1/U_4 & \xrightarrow{h_2} & U_1/U_3 & \xrightarrow{h_1} & U_1/U_2 \\
 & & \uparrow \psi_3 & & \uparrow \psi_2 & & \uparrow \psi_1 \\
 & & | & & | & & | \\
 \cdots & \longrightarrow & \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{f_2} & \mathbb{Z}/p^2\mathbb{Z} & \xrightarrow{f_1} & \mathbb{Z}/p\mathbb{Z}
 \end{array}$$

The Hilbert Symbol

10. Quadratic Extensions/Squares

Theorem

10.1

Let p be odd. Then, $a = p^n u \in \mathbb{Q}_p^\times$ is a square if and only if n is even and $\left(\frac{u}{p}\right) = 1$

Proof. $\mathbb{Z}_p = 2\mathbb{Z}_p, (\mathbb{F}_p^\times)^2$ is identified with the Legendre Symbol, and $2\mathbb{Z}$ is even integers. $\square$

Corollary

10.2

$\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, with the isomorphism $1 \mapsto (0,0)$, $p \mapsto (0,1)$, $u \mapsto (1,0)$, where u is a non-square unit mod p , and $pu \mapsto (1,1)$.

Let K be a field, $\text{char } K \neq 2$. Let L be a quadratic extension of K . That is, $\dim_K(L) = 2 = [L : K]$. Let $1, \alpha \in L$ be a basis for L over K . This works with any $\alpha \in L \setminus K$. Now, we have $\alpha^2 \in L$, and we must have $\alpha^2 \in \text{Span}\{1, \alpha\}$, so $\alpha^2 = c + b\alpha$, $c, b \in K$. So, $\alpha^2 - b\alpha - c = 0$. If $\alpha \notin K$, then this polynomial is irreducible.

Let $f_\alpha(x) = x^2 - bx - c$, which is irreducible in K . Its roots are $\frac{-b \pm \sqrt{b^2 - 4c}}{2}$, so we know $\sqrt{b^2 - 4c} \in L \setminus K$. This shows $L = K(\alpha) = K(\sqrt{b^2 - 4c})$, hence any quadratic extension can be given by attaching a square root.

In particular, the only quadratic extensions of $\mathbb{Q}_p$ (for p odd) are $\mathbb{Q}_p(\sqrt{p})$, $\mathbb{Q}_p(\sqrt{u})$, $\mathbb{Q}_p(\sqrt{pu})$.

11. Intro and Properties of the Hilbert Symbol

Definition

11.1

Let $K = \mathbb{Q}_p$ or $\mathbb{R}$. Let $a, b \in K^\times$. The Hilbert Symbol (a, b) relative to K is 1 if $z^2 - ax^2 - by^2$ has a non-trivial zero, and -1 otherwise.

Example 11.2. Consider $z^2 - x^2 - y^2$, which always has a solution $(1, 1, 0)$ in any field. Therefore, $(1, 1) = 1$ relative to any field. For similar reasons, $(1, 3) = 1$ and $(-1, 1) = 1$. On the other hand, over $\mathbb{R}$, $z^2 + x^2 + y^2$ has no non-trivial solutions, so $(-1, -1) = -1$ in $\mathbb{R}$.

$z^2 - 7x^2 - 3y^2$ has a solution $(\sqrt{10}, 1, 1)$, so $(7, 3) = 1$. Notice also how $z^2 - 7 \cdot 4x^2 - 3 \cdot 25y^2$ has a solution $(\sqrt{10}, \frac{1}{2}, \frac{1}{5})$, hence $(7 \cdot 4, 3 \cdot 25) = 1$.

Proposition**11.3**

Over any field K ,

1. $(a, b) = (b, a)$
2. $(c^2a, d^2b) = (a, b)$

Proof. If $z^2 - ax_0^2 - by_0^2 = 0$, then $z^2 - c^2a(x_0/c)^2 - d^2b(y_0/d)^2 = 0$ □

Corollary**11.4**

The previous proposition demonstrates that scaling by a square doesn't matter. So, all we really care about is $a, b \in K^\times / (K^\times)^2$. That is, $(,)$ is a function $K^\times / (K^\times)^2 \times K^\times / (K^\times)^2 \rightarrow \{\pm 1\}$

In particular, $\mathbb{R}^\times / (\mathbb{R}^\times)^2 \cong C_2$, so all we need to check is

$$(1, 1) = 1, (1, -1) = 1, (-1, 1) = 1, (-1, -1) = -1$$

Thus, for $K = \mathbb{R}$,

$$(a, b) = \begin{cases} +1 & a \text{ or } b \text{ positive} \\ -1 & a, b < 0 \end{cases}$$

Example 11.5. Let $K = \mathbb{Q}_5$, and we know $\mathbb{Q}_5^\times / (\mathbb{Q}_5^\times)^2 = \{1, 5, 2, 10\}$.

Proposition**11.6**

Let $a, b \in K^\times$, and let $K_b = K(\sqrt{b})$, which is $\neq K \iff b$ is not a square. Consider the norm homomorphism $N : K_b^\times \rightarrow K^\times$, and denote $NK_b^\times \leq K^\times$ the image of the norm. Then,

$$(a, b) = 1 \iff a \in NK_b^\times$$

In particular, if $K_b = K$, then $NK_b^\times = K^\times$, hence $(a, b) = 1$ for all $a \in K^\times$.

Proof. Suppose b is not a square in K , and let $\beta^2 = b, \beta \in K_b$. So, any element in $w \in K_b$ can be written as $w = z + \beta y$ for $z, y \in K$. Then, $N(w) = (z + \beta y)(z - \beta y) = z^2 - by^2$.

($\Leftarrow$) Suppose $a \in NK_b^\times$. Then, $a = z^2 - b^2 = N(w)$ for some w . That is, $z^2 - a(1)^2 - by^2 = 0$, giving a non-trivial solution to the desired equation, hence $(a, b) = 1$.

($\Rightarrow$) Suppose $(a, b) = 1$. That is, $z^2 - ax^2 - by^2$ has a non-trivial solution (x_0, y_0, z_0) . In particular, $ax_0^2 = z_0^2 + by_0^2 = N(z_0 + \beta y_0)$. If $x_0 \neq 1$, write $a = \frac{z_0^2 - by_0^2}{x_0^2} = N(\frac{z_0 + \beta y_0}{x_0})$ as desired. If $x_0 = 0$, we derive a contradiction as b will be a square. Thus, $a \in NK_b^\times$. □

Properties of the Hilbert Symbol**11.7**

- (i) $(a, b) = (b, a)$ and $(a, c^2) = 1$.
- (ii) $(a, -a) = 1$ and $(a, 1 - a) = 1$ (assuming $a \neq 1$)
- (iii) If $(a, b) = 1$, then $(aa', b) = (a', b)$.
- (iv) $(a, b) = (a, -ab) = (a, (1 - a)b)$.

(v) $(aa', b) = (a, b)(a', b)$. That is, the Hilbert symbol is **bimultiplicative**.

Proof.

(i) Clear

(ii) $z^2 - ax^2 - (-a)y^2 = 0$ has solution $(0, 1, 1)$. $z^2 - ax^2 - (1-a)y^2$ has solution $(1, 1, 1)$.

(iii) If $(a, b) = 1$, then $a \in NK_b^\times$. So, $(aa', b) = 1 \iff aa' \in NK_b^\times \iff a' \in NK_b^\times \iff (a', b) = 1$.

(iv) $(-ab, a) = (b, a)$ by (ii) and (iii). The other one is an exercise.

(v) Proved soon. □

Theorem

11.8

(i) Let $K = \mathbb{R}$. Then,

$$(a, b) = \begin{cases} +1 & a \text{ or } b \text{ positive} \\ -1 & a, b < 0 \end{cases}$$

(ii) Let $K = \mathbb{Q}_p$ for p odd. Let $a = p^m u, b = p^n v, u$ and v units. Let $\varepsilon(p) = \frac{p-1}{2}$. Then,

$$(a, b) = (-1)^{mne(p)} \left(\frac{u}{p}\right)^n \left(\frac{v}{p}\right)^m$$

(Note the exponent swap).

To prove this theorem, we first need the following lemma:

Lemma

11.9

Let $v \in \mathbb{Z}_p$ be a unit. If $z^2 - px^2 - vy^2 = 0$ has a non-trivial solution in $\mathbb{Q}_p$, then it has a solution (x_0, y_0, z_0) , where y_0, z_0 are units in $\mathbb{Z}_p$, and $x_0 \in \mathbb{Z}_p$.

Proof. Let $(x_0, y_0, z_0) \in \mathbb{Z}_p^3$ be a primitive solution (obtained by multiplying denominators, and one of them is a unit). Suppose y_0 or z_0 is not a unit. Then, one of $y_0, z_0 \in p\mathbb{Z}_p$. But, $z_0^2 - vy_0^2 = 0 \pmod{p}$ considering our original equations. So, if $y_0 \in p\mathbb{Z}_p$, then so is z_0 , and vice-versa. So, z_0, y_0 are both in $p\mathbb{Z}_p$, so $z_0^2, y_0^2 \in p^2\mathbb{Z}_p$. Again, considering the original equation, $-px_0^2 \equiv 0 \pmod{p^2}$, so $x_0 \in p\mathbb{Z}_p$ as well. Hence, the solution is not primitive, a contradiction. Therefore, y_0 and z_0 must both be units, as desired. □

We can now prove (ii) from the theorem ((i) was proved earlier).

Proof of (ii). Note that the formula in (ii) only depends on the parity of m, n . So, we only four cases to check:

1. $m = 0, n = 0$: We need to check $(u, v) = 1$. Consider the equation $z^2 - ux^2 - vy^2 = 0$. By Chevalley-Warning (Theorem 2.4), this has a non-trivial solution $(x_1, y_1, z_1) \pmod{p}$. Now $f_x = -2ux, f_y = -2vy, f_z = 2z$. One of these must be non-zero when we plug in our non-trivial solution, so by Hensel we get a non-trivial solution in $\mathbb{Z}_p$. Thus, $(u, v) = 1$.

2. $m = 1, n = 0$: We need to check $(pu, v) = \left(\frac{v}{p}\right)$. If v is a square, then immediately $(pu, v) = 1 = \left(\frac{v}{p}\right)$. Now, suppose v is not a square mod p . Recall by property (iii) in the proposition that $(pu, v) = (p, v)$. Now, if $z^2 - px^2 - vy^2 = 0$ had a non-trivial solution in $\mathbb{Q}_p$, then by the lemma there exists $x_0, y_0, z_0 \in \mathbb{Z}_p$ with y_0, z_0 units which are a solution. Modulo p , $v = (z_0/y_0)^2$, a contradiction. Finally, if v is a square mod p , by Hensel's it must also be a square in $\mathbb{Z}_p$, so we've checked all the cases.
3. $m = 0, n = 1$: This is equivalent to (2) by symmetry.
4. $m = 1, n = 1$: We need to check $(pu, pv) = (-1)^{\epsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$. Recall that we proved $(a, b) = (a, -ab)$. Thus, $(pu, pv) = (pu, -p^2uv) = (pu, -uv)$. Thus, by case (2), $(pu, -uv) = \left(\frac{-uv}{p}\right) = \left(\frac{-1}{p}\right) \left(\frac{u}{p}\right) \left(\frac{v}{p}\right) = (-1)^{\epsilon(p)} \left(\frac{u}{p}\right) \left(\frac{v}{p}\right)$.

The last thing we need to prove, to actually know that these are all the cases, is that the Hilbert symbol is non-degenerate. That is, for a fixed $b \in K^\times$, if $(a, b) = 1$ for all $a \in K^\times$, then b is a square.

Taking the contrapositive, suppose b is not a square. Considering $\mathbb{Q}_p^\times / (\mathbb{Q}_p^\times)^2$, we just need to consider $b = p, u, up$ where $\left(\frac{u}{p}\right) = -1$ is a unit. Indeed, if $b = p$, take $a = u$, if $b = u$, take $a = p$, and if $b = up$, take $a = u$, and we're done. $\square$

Corollary**11.10**

This proves property (v) from before.

Corollary**11.11**

For $u, v \in \mathbb{Q}_p^\times$, we have $(u, v) = 1$. Also $(p, p) = (-1)^{\epsilon(p)}$

Now we have to consider $p = 2$:

First question: What are the squares in $\mathbb{Q}_2^\times$? Recall $\mathbb{Q}_2^\times \cong \mathbb{Z}_2^\times \times \mathbb{Z}$. Observe $U_1 = 1 + 2\mathbb{Z}_2 = \mathbb{Z}_2^\times$. So,

$$\mathbb{Z}_2^\times \cong \{\pm 1\} \times U_2.$$

Moreover,

$$(U_2, \times) \cong (4\mathbb{Z}_2, +)$$

Thus,

$$\mathbb{Q}_2^\times \cong \{\pm 1\} \times 4\mathbb{Z}_2 \times \mathbb{Z}.$$

Thus,

$$(\mathbb{Q}_2^\times)^2 \cong 8\mathbb{Z}_2 \times 2\mathbb{Z}$$

and

$$\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2 \cong \{\pm 1\} \times \{\pm 1\} \times \mathbb{Z}/2\mathbb{Z}$$

which has order 8. Moreover, for any arbitrary $a \in \mathbb{Q}_2^\times$, we may write $a = 2^m u$ for $u \in \mathbb{Z}_p$ a unit. Then a is a square if and only if m is even and $u = \cdots 001$. Thus, a is a square if and only if $a \equiv 1 \pmod{8}$. The representatives of $\mathbb{Q}_2^\times / (\mathbb{Q}_2^\times)^2$ are $\{\pm 1, \pm 2, \pm 5, \pm 10\}$.

Recall the function $\omega(n) = \frac{n^2-1}{8}$, and $\left(\frac{2}{p}\right) = (-1)^{\omega(p)}$ (Theorem 3.10).

Theorem**11.12**

Let $K = \mathbb{Q}_2$. Let $a = 2^m u, b = 2^n v$ for $u, v \in \mathbb{Z}_2^\times$. Then,

$$(a, b) = (-1)^{\varepsilon(u)\varepsilon(v) + m\omega(v) + n\omega(u)}$$

Proof. Skip. □

We now want to consider quadratic reciprocity in general number fields.

Hilbert's Product Formula**11.13**

Let $a, b \in \mathbb{Q}^\times$. We'll use the notation $(a, b)_p$ to denote the Hilbert symbol of a and b in $\mathbb{Q}_p$ when p is finite, or $\mathbb{R}$ when $p = \infty$. Then,

$$\prod_{p \leq \infty} (a, b)_p = 1$$

Proof. Given $a, b \in \mathbb{Q}^\times$. For p sufficiently large, both a and b are units. So, $(a, b)_p = 1$ in that case. Let V be the set of all primes and infinity. Let $F(a, b) = \prod_{v \in V} (a, b)_v$. Recall that $(a, b)_v (a', b)_v = (aa', b)_v$. Therefore, $F(aa', b) = F(a, b)F(a', b)$. Since we can reduce integers to a product of primes, it therefore suffices to prove the claim for $a, b = -1$ or a prime.

Case: $F(-1, -1) = (-1, -1)_\infty (-1, -1)_2 (-1, -1)_3 \cdots$. For any odd prime, -1 is a unit, so we're only left with $(-1, -1)_\infty (-1, -1)_2$. In $\mathbb{R}$, $z^2 + x^2 + y^2$ doesn't have a non-trivial root, so $(-1, -1)_\infty = -1$. The same holds for $(-1, -1)_2$ based on the previous formula. Thus, $F(-1, -1) = 1$.

Case: $F(-1, 2) = (-1, 2)_\infty (-1, 2)_2 (-1, 2)_3 \cdots$. In this case, everything is 1, so $F(-1, 2) = 1$.

Case: $F(-1, p) = (-1, p)_\infty (-1, p)_2 (-1, p)_p \prod_{l \neq p} (-1, p)_l$ for p an odd prime. Since $p > 0$, we know $(-1, p)_\infty = 1$. Next, $(-1, p)_p = \left(\frac{-1}{p}\right) = (-1)^{\varepsilon(p)}$. Furthermore, we can check $(-1, p)_2 = (-1)^{\varepsilon(p)}$ as well. Thus, $F(-1, p) = 1$.

Case: $F(p, l) = (p, l)_\infty (p, l)_2 (p, l)_p (p, l)_l \prod_{j \neq p, l} (p, l)_j$ for p and l distinct odd primes. We know all the $(p, l)_j$ are all 1. p and l are positive, so $(p, l)_\infty = 1$. Also, $(p, l)_2 = (-1)^{\varepsilon(p)\varepsilon(l)}$. Next, $(p, l)_p = \left(\frac{l}{p}\right)$ and $(p, l)_l = \left(\frac{p}{l}\right)$. So, $F(p, l) = (-1)^{\varepsilon(p)\varepsilon(l)} \left(\frac{p}{l}\right) \left(\frac{l}{p}\right) = 1$ by QR.

Case: $F(2, p) = \cdots = \left(\frac{2}{p}\right) (-1)^{\omega(p)} = 1$. □

Note that this theorem is more or less equivalent to quadratic reciprocity (Theorem 3.12). Also, it can be formalized and proved for general number fields.

12. Systems of Hilbert Symbols

Example 12.1. Let $v \in V = \{\text{primes}, \infty\}$. We consider the problem $(3, *)_v = 1$ or -1 . That is, given any v , can we find x such that $(3, x)_v = 1$, and y such that $(3, y)_v = -1$? What about for a system, like $(3, x)_\infty = 1, (3, x)_3 = -1, (3, x)_5 = -1, (3, x)_7 = -1, (3, x)_p = 1, p > 7$? In this system, we have

an odd amount of negatives, so by Hilbert's theorem this isn't possible. We answer this problem with the following theorem.

Theorem**12.2**

Pick $a_1, \dots, a_d \in \mathbb{Q}^\times$, $i \in I = \{1, 2, \dots, d\}$. Pick $\{\varepsilon_{i,v}\}_{i \in I, v \in V}$ with each $\varepsilon_{i,v} = \pm 1$. Then, there exists $x \in \mathbb{Q}^\times$ such that $(x, a_i)_v = \varepsilon_{i,v}$ for all $i \in I, v \in V$ if and only if

1. There is a finite amount of $\varepsilon_{i,v} = -1$
2. For each $i \in I$, $\prod_{v \in V} \varepsilon_{i,v} = 1$
3. For each $v \in V$, there exists $x_v \in \mathbb{Q}_v^\times$ such that $(x_v, a_i)_v = \varepsilon_{i,v}$ (That is, there are local solutions in each case)

Proof. ($\implies$) This is clear by Hilbert's product formula

($\impliedby$) We need three lemmas:

Lemma**12.3**

Let $a_1, \dots, a_n \geq 0$ and $m_1, \dots, m_n \geq 1$ be integers with $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then, there exists $a \in \mathbb{Z}$ such that $a \equiv a_i \pmod{m_i}$ for all i .

Lemma**12.4**

Let $S \subset V$ be finite. Then, $\mathbb{Q} \subset \prod_{v \in S} \mathbb{Q}_v$ is dense. That is, for fixed $a_v \in \mathbb{Q}_v, v \in S$ and $\varepsilon_v > 0, v \in S$, there exists $x \in \mathbb{Q}$ such that $|x - a_v| < \varepsilon_v$ for all $v \in S$.

Dirichlet's Theorem on Arithmetic Progressions**12.5**

Let $a > 0, m > 1$ with $\gcd(a, m) = 1$. Then, there exists infinitely many primes p such that $p \equiv a \pmod{m}$. In other words, the arithmetic progression $a, a + m, a + 2m, \dots$ contains infinitely many primes.

This lemma will be the main focus of the rest of the semester. We won't fully prove [Theorem 12.2](#), but look at an example of how the condition is sufficient. $\square$

Let $a_1 = 5$ ($d = 1$), and we want $(x, 5)_3 = -1, (x, 5)_7 = -1$, and all others $+1$. We first want local solutions $(x_3, 5)_3 = -1, (x_7, 5)_7 = -1$. Note

$$(3, 5)_3 = \left(\frac{5}{3}\right) = -1, \quad (7, 5)_7 = \left(\frac{5}{7}\right) = -1.$$

Observe how our local solutions don't work globally, so there's still more work to do. Let

$$S := \{2, 5, \infty\}, T := \{3, 7\}.$$

S was chosen to have $2, \infty$, and all primes dividing a_1 . T was chosen to have all v 's where we want negative Hilbert Symbols. Fix $m = 40, a = 21$. Since $\gcd(a, m) = 1$, there exists a prime $p \equiv a \pmod{m}$ with $p \notin S \cup T$, in particular it's $p = 61$. We claim $x = a \cdot p = 3 \cdot 7 \cdot 61$ is a

working global solution. Well

$$(3 \cdot 7 \cdot 61, 5)_3 = \left(\frac{5}{3}\right) = -1, (3 \cdot 7 \cdot 61, 5)_7 = \left(\frac{5}{7}\right) = -1$$

One can also verify that $(3 \cdot 7 \cdot 61, v) = 1$ for all other v . To summarize we selected $T = \{v \in V \mid \text{at least one } \varepsilon_{i,v} = -1\}$, $S = \{2, \infty, \text{all prime factors of } a_i \text{ for all } i\}$. If $S \cap T = \emptyset$, we take $a = \prod_{l \in T \setminus \{\infty\}} l$ and $m = 8 \prod_{p \in S \setminus \{2, \infty\}} p$. We're skipping $S \cap T \neq \emptyset$.

Dirichlet's Theorem

Our goal for the rest of the semester is the following theorem:

Dirichlet's Theorem

Let $a, m \geq 1$ with $\gcd(a, m) = 1$. Then, there are infinitely many primes p such that $p \equiv a \pmod{m}$.

To prove this, we must use complex analysis to study $(\mathbb{Z}/m\mathbb{Z})^\times$. We will define a function $L : \mathbb{C} \rightarrow \mathbb{C}$, which we write as $L(s, \chi)$, where χ is a character. Characters are our first target.

13. Characters on Finite Abelian Groups

Definition

13.1

Let G be a finite abelian group. A **character** of G is a homomorphism from G to $(\mathbb{C}^\times, \times)$. We denote $\widehat{G} := \text{Hom}(G, \mathbb{C}^\times)$, called the **dual group**.

Example 13.2. In $\widehat{G}$, we have $\varepsilon : G \rightarrow \mathbb{C}^\times, g \mapsto 1$. This is the **trivial character**. Note that for $\phi, \psi \in \widehat{G}$, we have the group law $(\phi \star \psi)(g) = \phi(g)\psi(g)$. Moreover, $\phi^{-1}(g) = (\phi(g))^{-1}$, and $\phi \star \phi^{-1} = \varepsilon$.

Example 13.3. Let $G = \langle \sigma \rangle$ be cyclic. Let $\chi \in \widehat{G}$ be a character, and let $\chi(\sigma) = w$. Observe how it must be the case that $w^{\text{ord}(\sigma)} = 1$, hence $w \in \mu_n$. Moreover, for any $w \in \mu_n$, there is a unique $\chi \in \widehat{G}$ such that $\chi(g) = w$. In other words, $\widehat{G} \cong \mu_n$, with the isomorphism $\chi \mapsto \chi(\sigma)$.

Example 13.4. Let $G = \langle \sigma \rangle$, and $\text{ord}(\sigma) = 4$. Write $\chi_1, \chi_{-1}, \chi_i, \chi_{-i}$ to be the four expected elements of $\widehat{G}$. We get the following table:

	χ_1	χ_{-1}	χ_i	χ_{-i}
e	1	1	1	1
σ	1	-1	i	$-i$
σ^2	1	1	-1	-1
σ^3	1	-1	$-i$	i

Consider the map $\mathbb{C}^\times \rightarrow \mathbb{C}^\times, z \mapsto z^n$. Since $\mathbb{C}$ is algebraically closed, this map is surjective, and the kernel is the n 'th roots of unity, which we denote $(\mu_n, \times)$. Note that μ_n is cyclic of order n . In general, if G is a group for which $G \rightarrow G, g \mapsto g^n$ is surjective, we call G **divisible**.

Proposition

13.5

Suppose $H \leq G$, where G is finite abelian. Then there exists a surjective homomorphism $\widehat{G} \rightarrow \widehat{H}$. In particular, any character $\chi \in H$ can be extended to a character $\tilde{\chi} \in \widehat{G}$.

Proof. Given any $\chi \in \widehat{G}$, we may map $\chi \mapsto \chi|_H$, which is χ restricted to H . We now need to show

that for any $\chi \in \widehat{H}$, there exists $\tilde{\chi} \in \widehat{G}$ such that $\tilde{\chi}|_H = \chi$. We will prove this by induction on the index $|G : H|$. If $|G : H| = 1$, the claim is trivial as $G = H$.

If $|G : H| \neq 1$, pick $x \in G, x \notin H$, and set $H' := \langle H, x \rangle$. Note $H \subsetneq H'$. Let n be the smallest integer such that $x^n \in H$, and set $\chi(x^n) = t \in \mathbb{C}^\times$. Now, because $\mathbb{C}^\times$ is divisible, there exists $w \in \mathbb{C}^\times$ such that $w^n = t$. So, define $\chi' : H' \rightarrow \mathbb{C}^\times$ by

$$\chi'(h') = \chi'(hx^a) = \chi(h)w^a.$$

One can check that this is a well-defined homomorphism, hence χ' is a character on H' . Furthermore $\chi'|_H = \chi$. Moreover, $|G : H'| < |G : H|$, so by induction χ' extends to a character $\tilde{\chi} \in \widehat{G}$ such that $\tilde{\chi}|_{H'} = \chi'$, hence $\tilde{\chi}|_H = \chi$. $\square$

Proposition

13.6

Given G_1, G_2 finite abelian, we have $\widehat{G_1 \times G_2} \cong \widehat{G_1} \times \widehat{G_2}$.

Now, we have a surjection $\widehat{G} \rightarrow \widehat{H} \rightarrow 0$, and the kernel of the map is

$$\ker(\widehat{G} \rightarrow \widehat{H}) = \{\chi \in \widehat{G} \mid \chi(h) = 1 \forall h \in H\}$$

Let χ be in the kernel. Now, for any $x \in G$, it's in some coset xH , and for any $h \in H$, $\chi(xh) = \chi(x)\chi(h) = \chi(x)$. Therefore, χ is constant on cosets of H . We may therefore see that the kernel is $\widehat{G/H}$.

Proposition

13.7

Given $H \leq G$ finite abelian, we have the following pair of exact sequences:

$$0 \rightarrow H \rightarrow G \rightarrow G/H \rightarrow 0$$

$$0 \rightarrow \widehat{G/H} \rightarrow \widehat{G} \rightarrow \widehat{H} \rightarrow 0$$

Proposition

13.8

For G finite abelian, $G \cong \widehat{\widehat{G}}$ non-canonically, and $G \cong \widehat{\widehat{\widehat{G}}}$ canonically.

Proof. Previous homeworks. $\square$

Let's think about Euler's proof on the infinitude of primes.

Proof. Consider $\sum_{n=1}^{\infty} \frac{1}{n}$, which we know diverges. By FTA, for $n > 1$, we know $n = p_1^{e_1} \cdots p_r^{e_r}$ for p_i distinct primes, $e_i > 0$. Then, we observe

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{\text{primes}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) = \prod_{\text{primes}} \frac{1}{1 - \frac{1}{p}}.$$

Hence, if we had finitely many primes, the RHS would be finite, contradicting the LHS diverging. $\square$

The process of converting the harmonic sum to a product over primes is super important. This also hints at how we'll prove Dirichlet's theorem. We want to prove

$$\prod_{p \equiv a \pmod m} \frac{1}{1 - \frac{1}{p}} = \sum_{n=1}^{\infty} (?)$$

and show the RHS diverges.

Orthogonality Relations

13.9

Let G be finite abelian with $|G| = n$. Then,

1. For a fixed $\chi \in \widehat{G}$, $\sum_{g \in G} \chi(g) = \begin{cases} n & \chi = 1 \\ 0 & \chi \neq 1 \end{cases}$.
2. For a fixed $g \in G$, $\sum_{\chi \in \widehat{G}} \chi(g) = \begin{cases} n & g = 1 \\ 0 & g \neq 1 \end{cases}$

Example 13.10. Let $G = (\mathbb{Z}/m\mathbb{Z})^\times$ (Serre calls this $G(m)$), and $m = 4$. Then, $\widehat{G(4)}$ has a unique non-trivial element χ , which maps $\chi(1) = 1$ and $\chi(3) = -1$. This allows us to make a function on $\mathbb{Z}$: $0 \mapsto 0, 1 \mapsto 1, 2 \mapsto 0, 3 \mapsto -1$ periodic. In particular, we see this is $\chi(a)$ when $(a, m) = 1$, and 0 otherwise. More on this later.

14. Quick Tour of Complex Analysis

Definition

14.1

If $z = re^{i\theta}$, for $\pi < \theta \leq \pi$, we say $\text{Arg}(z) = \theta$, and we set

$$\arg(z) = \{\text{Arg}(z) + 2\pi k \mid k \in \mathbb{Z}\}$$

Definition

14.2

$f : \mathbb{C} \rightarrow \mathbb{C}$ is **differentiable** at $z_0 \in \mathbb{C}$ if $\lim_{z \rightarrow z_0} \frac{f(z) - f(z_0)}{z - z_0}$ exists.

Example 14.3. Polynomials in z are differentiable. $\bar{z}$ is not differentiable.

Definition

14.4

For an open set $U \subset \mathbb{C}$, $f : \mathbb{C} \rightarrow \mathbb{C}$ is **analytic** or **holomorphic** on U if

1. f is differentiable at all points of U
2. f' is continuous on U .

Remark 14.5. Goursat showed condition 2 is unnecessary, as it's implied by 1.

Cauchy-Riemann Equations

14.6

Let $f(z) = u(x, y) + iv(x, y)$. Then, f is analytic $\iff \frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}$ and $\frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$

Corollary

14.7

If the 2nd order partial derivatives of u, v are continuous, then $\Delta u = \Delta v = 0$, where $\Delta = \frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}$

Corollary

14.8

If $f : \mathbb{C} \rightarrow \mathbb{C}$ is real-valued and analytic, then f is constant.

Green's Theorem

14.9

Let $D \subset \mathbb{R}^2$ be a domain (open, simply connected), and let C be a curve in D . Then,

$$\oint_{C=\partial R} Pdx + Qdy = \int \int_R (Q_x - P_y) dx dy$$

Cauchy's Theorem

14.10

If f is analytic on U , then for any domain $D \subset U$, and $C = \partial D$,

$$\oint_C f(z) dz = 0$$

Corollary (Cauchy's Integral Formula)

14.11

Let f be analytic on U , and let $C \subset U$ be a closed curve encircling z_0 . Then,

$$f(z_0) = \frac{1}{2\pi i} \oint_C \frac{f(w)}{w - z_0} dw$$

Moreover,

$$f^{(m)}(z_0) = \frac{m!}{2\pi i} \oint_C \frac{f(z)}{(w - z_0)^{m+1}} dw$$

Corollary

14.12

Suppose f is analytic on a domain D , and suppose that $|f(z)| \leq M$ for all $z \in \partial D$. Then, for $z_0 \in D$ and a disk of radius ρ centered at z_0 contained in D ,

$$|f^{(m)}(z_0)| \leq \frac{m!}{\rho^m} M$$

Corollary

14.13

Suppose $f : \mathbb{C} \rightarrow \mathbb{C}$ is analytic on all of $\mathbb{C}$ (i.e. it's **entire**). Moreover, suppose f is bounded, i.e. there exists M such that $|f(z)| \leq M$ for all $z \in \mathbb{C}$. Then, f is constant.

Proposition

14.14

Suppose f is analytic on a domain D , let $z_0 \in D$, and let $z_0 \in E = D_\rho(z_0) \subset D$. Then, f on E is

given by a power series

$$f(z) = \sum_{n=0}^{\infty} a_n(z - z_0)^n, \quad a_n = \frac{f^{(n)}(z_0)}{n!}$$

for all $|z - z_0| < \rho$.

Definition

14.15

f has a **pole** at a of order k if $(z - a)^k f(z)$ is analytic in U containing a , and $(z - a)^{k-1} f(z)$ is not analytic. If f has only finitely many poles in $\mathbb{C}$, we say f is **meromorphic**.

Proposition

14.16

Let h be harmonic. Then, integrating around a circle of radius r around a , we have $h(a) = \int h(a + re^{i\theta}) \frac{d\theta}{2\pi}$

Proof of Cauchy's Integral Formula. Assume C is a circle of radius ε centered at z_0 . For some $w \in C$, we can parametrize $w = z_0 + \varepsilon e^{i\theta}$, $0 \leq \theta \leq 2\pi$. Moreover, $dw = i\varepsilon e^{i\theta} d\theta$, and $w - z_0 = \varepsilon e^{i\theta}$. So,

$$\frac{1}{2\pi i} \oint \frac{f(w)}{w - z_0} dw = \frac{1}{2\pi i} \int_0^{2\pi} \frac{f(z_0 + \varepsilon e^{i\theta}) i\varepsilon e^{i\theta}}{\varepsilon e^{i\theta}} d\theta = \frac{1}{2\pi i} \int_0^{2\pi} f(z_0 + \varepsilon e^{i\theta}) d\theta = f(z_0)$$

since $f = u + iv$ with u, v harmonic. □

Lemma

14.17

Let $\{f_n\}_{n=1}^{\infty}$ be a sequence of $f_n : U \rightarrow \mathbb{C}$ holomorphic for U open. Suppose $f_n \rightarrow f$ converges uniformly on any compact subset $K \subset U$. Then, there exists some $n \gg 0$ such that for all $x \in K$, $|f_n(x) - f(x)| < \varepsilon$ for any ε . Therefore, f is holomorphic.

Abel's Summation By Parts

14.18

Let $\{a_n\}_{n=1}^{\infty}, \{b_n\}_{n=1}^{\infty}$ be sequences of real numbers. Then,

$$\sum_{n=1}^N a_n b_n = b_{N+1} A_N - \sum_{n=1}^N (b_{n+1} - b_n) A_n, \quad A_n = \sum_{i=1}^n a_i$$

The name comes from the fact that if you view sums as integrals, this becomes integration by parts.

Lemma

14.19

Let $0 < \alpha < \beta$ be real, and $z = x + iy$ with $x > 0$. Then,

$$|e^{-\alpha z} - e^{-\beta z}| \leq \left| \frac{z}{x} \right| (e^{-\alpha x} - e^{-\beta x})$$

Definition

14.20

We define the **Riemann Zeta Function**

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s},$$

where $s \in \mathbb{C}$, and $n^s = e^{s \ln(n)}$. More generally, for some sequence $\{a_n\} \subset \mathbb{C}$, we define a **Dirichlet series**

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

Proposition

14.21

Suppose $a_n = h(n)$ with $h(mn) = h(m)h(n)$. Then,

$$\sum_{n=1}^{\infty} \frac{h(n)}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{h(p)^s}}$$

Theorem

14.22

Let $U \subset V$ be two open sets in $\mathbb{C}$. Suppose $f, g : V \rightarrow \mathbb{C}$ are analytic. If $f|_U = g|_U$, then $f = g$. This leads to a notion of analytic continuous.

Theorem

14.23

Plainly, $\zeta(s)$ is defined for all $s \in \mathbb{C}$ with $\operatorname{Re}(s) > 1$. But, $\zeta(s)$ has a **meromorphic continuation** to all of $\mathbb{C}$, with a simple pole at $s = 1$. Moreover,

$$\psi(s) = \zeta(s) - \frac{1}{s-1}$$

extends to an analytic function on all of $\mathbb{C}$.

Definition

14.24

The **Abcissa of Convergence** of a Dirichlet series $f(s)$ is the (minimal) value $\rho \in \mathbb{R} \cup \{\infty, -\infty\}$ such that $f(s)$ converges for all $\operatorname{Re}(s) > \rho$. The Abcissa of convergence for $\zeta(s)$ is $\rho = 1$. Recall that if we know $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ converges at some $s \in \mathbb{C}$, then we know it converges at all $\operatorname{Re}(z) > \operatorname{Re}(s)$.

The **Abcissa of Absolute Convergence** is the (minimal) $\rho^+ \in \mathbb{R} \cup \{\infty, -\infty\}$ such that $\sum_{n=1}^{\infty} \frac{|a_n|}{n^s}$ converges for all $\operatorname{Re}(s) > \rho^+$

Proposition

14.25

Let $f(s) = \sum \frac{a_n}{n^s}$ be a Dirichlet series, and suppose $a_n \in \mathbb{R}_{\geq 0}$ for all n . Suppose $f(s)$ converges for $\operatorname{Re}(s) > \rho \in \mathbb{R}$, and that f can be extended analytically to a meromorphic function in an open set around ρ . Then, f converges for all $\operatorname{Re}(s) > \rho - \varepsilon$ for some $\varepsilon > 0$.

Observation (Gauss - Early 1800s)

Let $\pi(n)$ be the number of primes $\leq n$. Then,

$$\pi(n) \sim \frac{n}{\log(n)}.$$

That is, if you picked a number in the range $1, \dots, n$ at random, the probability that it's prime

is $\frac{1}{\log(n)}$

Proposition

14.26

$$\zeta(s) = \zeta(1-s)$$

Therefore, ζ has a line of symmetry at $x = \frac{1}{2}$

Riemann Hypothesis

All the non-trivial zeros of $\zeta(s)$ lie on $\text{Re}(s) = 1/2$

Hadamard-Poussin Theorem

14.27

$\zeta(1+it) \neq 0$ for all $t \in \mathbb{R}$, and this implies Gauss's prime number theorem.

15. Dirichlet's Theorem

Fact

Let

$$f(s) = \sum \frac{a_n}{n^s}, g(s) = \sum \frac{b_n}{n^s}.$$

Then, if we have some ρ such that $f(s) = g(s)$ for all $\text{Re}(s) > \rho$, then $a_n = b_n$ for all n .

We know that a Dirichlet series converges to the right of the Abscissa, and diverges to the left, but we don't know what it does on the line $\text{Re}(s) = \rho$.

Theorem

15.1

If all $a_n \in \mathbb{R}$ with $a_n \geq 0$ for all n , and ρ is the Abscissa of convergence of

$$f(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

then f has a pole at $s = \rho$.

Theorem

15.2

If $|a_n| \leq M$, then the respective Dirichlet series has Abscissa $\rho \leq 1$. If $\left| \sum_{n=1}^N a_n \right|$ is bounded, then $f(s)$ converges for $\text{Re}(s) > 0$.

Remark 15.3. Let $G(m) = (\mathbb{Z}/m\mathbb{Z})^\times$, and let $\chi : G(m) \rightarrow \mathbb{C}^\times$ be a character. We may consider the sequence $a_n = \chi(n)$, when defined, and 0 otherwise. We can then consider the Dirichlet series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \nmid m} \frac{1}{1 - p^{-s} \chi(p)}.$$

This converges for $\text{Re}(s) > 0$ provided χ is not the trivial character.

Remark 15.4. Let P be the set of primes. Let $\zeta(s) = \prod_{p \in P} (1 - \frac{1}{p^s})^{-1}$. Then, observe

$$\log \zeta(s) = - \sum_{p \in P} \log \left(1 - \frac{1}{p^s} \right).$$

Moreover, we know

$$-\log(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \cdots.$$

Therefore,

$$\log \zeta(s) = \sum_{p \in P} \frac{1}{p^s} + \sum_{p \in P} (\text{finite as } s \rightarrow 1)$$

hence

$$\sum_{p \in P} \frac{1}{p^s} \sim \log \left(\frac{1}{s-1} \right).$$

Similarly,

$$L(s, \chi) \sim \sum_{p \in P} \frac{\chi(p)}{p^s} =: f_\chi(s)$$

Lemma

15.5

In $G(m)$, for $p \nmid m$, let $f(p)$ be the order of p . Define $g(p)$ so that $g(p)f(p) = \varphi(m)$. Then,

$$\prod_{\chi \in \widehat{G}(m)} (1 - \chi(p)T) = (1 - T^{f(p)})^{g(p)}$$

Example 15.6. Let $m = 101$, $p = 37$, then $f = 25$, so $g = 4$. Then,

$$\chi(37) \in W = \langle e^{2\pi i/25} \rangle \leq \mathbb{C}^\times,$$

and $e^{2\pi i/25}$ occurs exactly 4 times.

Definition

15.7

Let

$$\zeta_m(s) := \prod_{\chi \in \widehat{G}(m)} L(s, \chi) = \prod_{p \nmid m} \frac{1}{(1 - \frac{1}{p^{f(p)s}})^{g(p)}}.$$

In particular, if we write $\zeta_m(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, then $a_n \geq 0$ for all n . Therefore, we only need to understand $\zeta_m(s)$ on the real line.

Proposition

15.8

$$\zeta_m(s) = L(s, 1) \prod_{\chi \neq 1} L(s, \chi),$$

where 1 denotes the trivial character. The first factor has a simple pole at $s = 1$, and the rest converges for $\text{Re}(s) > 0$. So, ζ_m certainly converges for $\text{Re}(s) > 1$.

Theorem

15.9

1. $\zeta_m(s)$ has a simple pole at $s = 1$
2. $L(1, \chi) \neq 0$ for all $\chi \neq 1$.

(2) $\implies$ (1)

Proof. Suppose (2) were not the case, so there exists some $\chi \neq 1$ such that $L(1, \chi) = 0$. Since $L(s, 1)$ has a *simple* pole at $s = 1$, it follows that $\zeta_m(s)$ is now holomorphic for $\operatorname{Re}(s) > 0$. We claim this cannot be the case.

Observe

$$\zeta_m(s) = \prod_{p \nmid m} \left(1 - \frac{1}{p^{f(p)s}}\right)^{-g(p)} > \prod_{p \nmid m} \left(1 - \frac{1}{p^{\phi(m)s}}\right)^{-1} = \zeta(\phi(m)s),$$

which has a pole at $\frac{1}{\phi(m)} > 0$, a contradiction. $\square$

Definition

15.10

We define the Dirichlet density $A \subset P$ to be

$$k = \lim_{s \rightarrow 1} \frac{\left(\sum_{p \in A} \frac{1}{p^s}\right)}{\log\left(\frac{1}{s-1}\right)}$$

when the limit exists. If A is finite, then $k = 0$, and if $k \neq 0$, then A is infinite.

Definition

15.11

Let

$$P_a := \{p \in P \mid p \equiv a \pmod{m}\}$$

for $(a, m) = 1$. Our goal is to show P_a is infinite. Moreover, define

$$g_a(s) = \sum_{p \in P_a} \frac{1}{p^s}$$

Lemma

15.12

$$g_a(s) = \frac{1}{\phi(m)} \sum_{\chi \in \widehat{G}(m)} \chi(a)^{-1} f_\chi(s)$$

Proof.

$$\frac{1}{\phi(m)} \sum_{\chi \in \widehat{G}(m)} = \frac{1}{\phi(m)} \sum_{\chi} \sum_{p \nmid m} \frac{\chi(p) \chi(a^{-1})}{p^s} = \frac{1}{\phi(m)} \sum_{p \nmid m} \sum_{\chi} \frac{\chi(pa^{-1})}{p^s} = \sum_{p \in P_a} \frac{1}{p^s}$$

$\square$

It follows that $\lim_{s \rightarrow 1} \frac{g_a(s)}{\log \frac{1}{s-1}} = \frac{1}{\phi(m)} \neq 0$, hence P_a is infinite!

16. Results

Question

Can we find an explicit list polynomials $f_1, f_2, \dots$ such that $\overline{\mathbb{Q}} = \mathbb{Q}(\text{roots of } f_1, f_2, \dots)$?

Answer

No.

Question

Can we understand $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$?

Can we show that every finite group is a quotient of $G_{\mathbb{Q}}$?

Answer

No.

Values of ζ

16.1

$$\zeta(2) = 1 + \frac{1}{4} + \frac{1}{9} + \dots = \frac{\pi^2}{6}$$

$$\zeta(12) = \frac{691\pi^{12}}{638512875}$$

$$1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots = \pi/4$$

$$1 - \frac{1}{3} - \frac{1}{5} + \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \dots = \frac{1}{\sqrt{2}} \log(1 + \sqrt{2})$$

$$\zeta(0) = "1 + 1 + 1 + \dots" = -1/2$$

$$\zeta(-1) = "1 + 2 + 3 + \dots" = -1/12$$

$$\zeta(-2) = "1 + 4 + 9 + \dots" = 0$$

Euler's Theorem

16.2

$$\zeta(2k) = \pi^{2k} \cdot q$$

for some $q \in \mathbb{Q}$.

Let

$$h_1(t) = \frac{1+t}{2(1-t)}, h_2(t) = t \frac{d}{dt} h_1(t), \dots, h_{r+1}(t) = t \frac{d}{dt} h_r(t)$$

$$h_1(t) = \frac{1+t}{2(1-t)}, h_2(t) = \frac{t}{(1-t)^2}, h_3(t) = \frac{t+t^2}{(1+t)^3}, \dots, h_r(t) \in \mathbb{Q}[t, \frac{1}{1-t}]$$

Proposition**16.3**

Let $x \in \mathbb{C} \setminus \mathbb{Z}$, and $t = e^{2\pi i x}$, $t \neq 1$. Then,

$$h_1(t) = \frac{-1}{2} \cdot \frac{1}{2\pi i} \left(\sum_{n \in \mathbb{Z}} \left(\frac{1}{x+n} + \frac{1}{x-n} \right) \right) \quad (1)$$

$$h_r(t) = (r-1)! \left(-\frac{1}{2\pi i} \right)^r \sum_{n \in \mathbb{Z}} \frac{1}{(x+n)^r}, \quad r \geq 2 \quad (2)$$

Proof. (Sketch) $\frac{\sin(\pi x)}{\pi x} = \prod_{n=1}^{\infty} (1 - \frac{x^2}{n^2}) = \dots$ □

Corollary**16.4**

For $m > 1$ and $\chi : G(m) \rightarrow \mathbb{C}^\times$, let $r \geq 1$ be such that $\chi(-1) = (-1)^r$. Let $\zeta_m = e^{2\pi i/m}$ be a primitive m' th root. Then,

$$L(r, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^r} = \frac{1}{(r-1)!} \left(\frac{-2\pi i}{m} \right)^r \frac{1}{2} \sum_{a \in G(m)} \chi(a) h_r(\zeta_m^a)$$

Definition**16.5**

Let $\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} \frac{B_n}{n!} x^n$. B_n is called the n 'th **Bernoulli number**. We know $B_n \in \mathbb{Q}$ for all n , and $B_n = 0$ for all odd $n \geq 3$. Euler found

$$\zeta(1-2k) = -\frac{B_{2k}}{2k}$$

for $k \geq 1$.

Kummer's Theorem**16.6**

Let $m, m' < 0$, with $m \equiv m' \not\equiv 1 \pmod{p-1}$. Then, $\zeta(m) \equiv \zeta(m') \pmod{p}$.

Definition**16.7**

Let

$$\mathbb{I} = \{(x_\infty, x_2, x_3, \dots) \mid x_p \in \mathbb{Z}_p^\times, p \gg 0\} \subset \mathbb{R}^\times \times \left(\prod_p \mathbb{Q}_p^\times \right)$$

called the **idele group of $\mathbb{Q}$** . Call $C_{\mathbb{Q}} = \mathbb{I}/\mathbb{Q}^\times$ the **idele class group**. Define

$$\mathbb{N}x = ||x|| = \prod_{p \leq \infty} |x_p|_p$$

Then, $\mathbb{N} : \mathbb{I} \rightarrow \mathbb{C}^\times$ is a character.

Tate's Theorem**16.8**

All L -functions live in $\text{Hom}(C_{\mathbb{Q}}, \mathbb{C}^\times)$

"To study number theory, you have to study all of mathematics: analysis, algebra, geometry, etc. All of math was invented to solve problems in number theory. They don't know that though." —
Niranjan Ramachandran