Classes: Mo/Fr 10:30 - 11:45 am

Section: Th 1:30 - 2:45 pm

Fabian's OH: Mo, Fr noon - 1 pm
or appointment

Kenz's OH: Tu 1:30 - 2:45 pm

Grading: 70% HW
30% final paper

0. Motivation

0.1. Generalizing quadratic reciprocity

Let $p \neq 2$ be a prime number.

<u>Def</u> An integer a is a <u>quadratic residue mod p</u> if $a \equiv x^2 \bmod p$ for some $x \in \mathbb{Z}$.

<u>Lemma 0.1</u>

$$a^{\frac{p-1}{2}} \equiv \underbrace{\begin{cases} 0, & a \equiv 0 \bmod p \\ +1, & a \not\equiv 0 \text{ quadr. res. mod } p \\ -1, & a (\not\equiv 0) \text{ not quadr. res. mod } p \end{cases} \bmod p}_{\text{Legendre symbol } \left(\frac{a}{p}\right)}$$

<u>Pf</u> Let $a \not\equiv 0 \bmod p$.

$$\Rightarrow \left(a^{\frac{p-1}{2}}\right)^2 \equiv a^{p-1} \underset{\substack{\uparrow \\ \text{little Fermat}}}{\equiv} 1 \bmod p$$

$$\Rightarrow a^{\frac{p-1}{2}} \equiv \pm 1.$$

If $a \equiv x^2$, then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv +1$.

The polynomial $a^{\frac{p-1}{2}} - 1$ has at most $\frac{p-1}{2}$ roots in $\mathbb{F}_p^\times$.

But $\mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times$ has kernel $\{\pm 1\}$, so its
$x \longmapsto x^2$

image has size $\frac{\# \mathbb{F}_p^\times}{2} = \frac{p-1}{2}$.

$\Rightarrow$ There are $\frac{p-1}{2}$ quadr. res. mod p.

nonzero

$\Rightarrow a^{\frac{p-1}{2}} \not\equiv 1$ if a is not a quadr. res.

$\Downarrow$

$a^{\frac{p-1}{2}} \equiv -1$ $\square$

Obviously, $\left(\frac{a}{p}\right)$ is periodic in a for fixed p:

depends only on a mod p.

Surprisingly, $\left(\frac{a}{p}\right)$ is "periodic in p" for fixed a;

depends only on p mod $4a$.

Ex $\left(\frac{1}{p}\right) = +1$ for any p

$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ only depends on p mod 4.

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ only depends on p mod 8.

One way to show "periodic in p":

Quadratic reciprocity law

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$ for all odd primes $p \neq q$.

Sadly, whether 5 is a cubic residue mod p

($\exists x \in \mathbb{Z} : x^3 \equiv 5 \mod p$) is not "periodic in p":

doesn't depend only on $p \mod n$ for any fixed $n \geq 1$.

Interestingly, the number of roots mod p of $x^3 - 3x + 1$ depends only on $p \mod 9$.

Questions: Why? Which polynomials behave "periodically in p"? What's the period? Can we generalize quadr. reciprocity? Can we generalize to number fields other than $\mathbb{Q}$? ...

0.2. Local-global principle

For example, fix a polynomial

$$f(X_1, \dots, X_n) \in \mathbb{Z}[X_1, \dots, X_n].$$

Let $V(R) = \{(x_1, \dots, x_n) \in R^n \mid f(x_1, \dots, x_n) = 0\}$ for any ring R.

$V(\mathbb{Z}) \neq \emptyset$? ($\Leftrightarrow$ $f(x_1, \dots, x_n) = 0$ has integer sol.)

$\Downarrow$

Ex $X_1^2 + X_2^2 + 1 = 0$ ⇝ (no real sol.)

Ex $X_1^2 + 3X_2^2 - 2 = 0$ $\Rightarrow x_1^2 \equiv 2 \bmod 3$ ⇝ (no sol. mod 3)

$V(\mathbb{R}) \neq \emptyset$ and $V(\mathbb{Z}/n\mathbb{Z}) \neq \emptyset$ $\forall n \geq 1$ ($\Leftrightarrow f = 0$ has sol. mod n)

$\Updownarrow$ Chinese remainder theorem

$V(\mathbb{Z}/p^k\mathbb{Z}) \neq \emptyset$ $\forall k \geq 0$ $\forall$ prime p.

Collect "compatible" residues mod powers of a fixed prime p:

Def The <u>ring of p-adic integers $\mathbb{Z}_p$</u> consists of sequences $(a_0, a_1, \dots) = (a_k)_{k \geq 0} \in \prod_{k \geq 0} \mathbb{Z}/p^k\mathbb{Z}$ of residue classes $a_k \in \mathbb{Z}/p^k\mathbb{Z}$ such that

$$a_k \equiv a_l \bmod p^k \text{ for } k < l.$$

Addition and multiplication are defined element-wise.

$$(a_n)_{n\geq 0} \pm (b_n)_{n\geq 0} = (a_n \pm b_n)_{n \geq 0}.$$

Rmk The natural map
$$\mathbb{Z} \longrightarrow \mathbb{Z}_p$$
$$x \longmapsto (x \bmod p^k)_{k\geq 0}$$
is injective, so we'll say $\mathbb{Z} \subseteq \mathbb{Z}_p$.

Pf If $x \equiv y \bmod p^k$ but $x \neq y$, then $|x-y| \geq p^k$. □

can't be true for all k.

Cor If $V(\mathbb{Z}) \neq \emptyset$, then $\underbrace{V(\mathbb{R}) \neq \emptyset \text{ and } V(\mathbb{Z}_p) \neq \emptyset \ \forall p}_{V(\mathbb{R} \times \prod_p \mathbb{Z}_p) \neq \emptyset}$.

"global" (undecidable)

"local" (easier)

If the converse holds, we say that V satisfies the local-global principle (also called Hasse principle).

Ex $V = \{x \mid x^n = a\}$ satisfies the local-global principle (over $\mathbb{Z}$) for any fixed $n \geq 1$ and $a \in \mathbb{Z}$.

Ex $V = \{x \mid (x^2+1)(x^2+\overset{17}{\cancel{3}})(x^2-\overset{17}{\cancel{3}}) = 0\}$ doesn't!

Ex (Minkowski)

For any homogeneous degree 2 polynomial $f(x_1, \dots, x_n) \in \mathbb{Z}[x_1, \dots, x_n]$,

$V = \{(x_1, \dots, x_n) \mid f(x_1, \dots, x_n) = 0, (x_1, \dots, x_n) \neq (0, \dots, 0)\}$

satisfies the local-global principle.

Ex (Selmer)

$V = \{(x,y,z) \mid 3x^3 + 4y^3 + 5z^3 = 0, \ (x,y,z) \neq (0,0,0)\}$

doesn't!

Goal: Study the ring $\mathbb{Z}_p$ and its field of fractions $\mathbb{Q}_p$. (For example, how to tell whether $V(\mathbb{Z}_p) \neq \emptyset$?) Identify some more problems that satisfy a local-global principle.

$\mathbb{R} =$ "$\mathbb{Z}_\infty$"

Def The ring of profinite integers $\hat{\mathbb{Z}}$ consists of sequences $(a_1, a_2, \ldots) = (a_n)_{n \geq 1} \in \prod_{n \geq 1} \mathbb{Z}/n\mathbb{Z}$ of residue classes $a_n \in \mathbb{Z}/n\mathbb{Z}$ such that $a_n \equiv a_m \bmod n$ for all $n \mid m$.

Thm (Chinese remainder theorem)

The natural map

$$\hat{\mathbb{Z}} \longrightarrow \prod_p \mathbb{Z}_p$$

$$(a_n)_{n \geq 1} \longmapsto \left((a_{p^k})_{k \geq 0} \right)_p$$

(forgetting residues mod non-prime-powers) is an isomorphism.

We write $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p$.

1. Local fields

1.0. Reminder on Dedekind domains

<u>Def</u> A <u>Dedekind domain</u> is an integral domain R (which is not a field) in which any nonzero ideal I factors uniquely as a product of prime ideals.

<u>Ex</u> Any principal ideal domain, e.g. $\mathbb{Z}$ or $K[T]$ for any field K.

<u>Notation</u> If $\mathcal{O}_K$ is a ring, denote its field of fractions by K. If $L|K$ is a field ext., we denote the integral closure of $\mathcal{O}_K$ in L by $\mathcal{O}_L$.

<u>Rmk</u> If $\mathcal{O}_K$ is a Dedekind dom. and $L|K$ is a finite ext., then $\mathcal{O}_L$ is also a Dedekind dom.

<u>Ex</u> The ring of integers $\mathcal{O}_K$ of a number field K is a Dedekind domain.