# Quadratic reciprocity

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x = y^2 \bmod p, \text{ some } y \in \mathbb{F}_p \\ -1 & \text{if } x \neq y^2 \bmod p \text{ any } y \in \mathbb{F}_p \\ 0 & \text{if } x = 0 \end{cases}$$

= Legendre symbol

$$\varepsilon(n) = \begin{cases} 1 & \text{if } n = 1 \bmod 4 \\ -1 & \text{if } n = 3 \bmod 4 \end{cases}$$

only odd $n$ needed.

## Facts

1. $\left(\frac{x}{p}\right)\cdot\left(\frac{y}{p}\right) = \left(\frac{xy}{p}\right)$ multiplicative character
2. $\left(\frac{-1}{p}\right) = \varepsilon(p)$

$-1$ not a square mod 3, 7, 11

$-1 = 2^2 = 4 \not\equiv -1 \bmod 5$

$-1 = 5^2 = 25 = 26 - 1 \bmod 13$

## Quadratic reciprocity theorem (Gauss, Legendre)

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

if $p = 1 \bmod 4$ or $q = 1 \bmod 4$ then

$p$ square $\iff$ $q$ square mod $p$

mod $q$

(2)

If $p \equiv 3 \bmod 4$, $q \equiv 3 \bmod 4$

then

$p$ square mod $q \iff q$ not square mod $p$

See square table

Proof (first Serre proof, Course in Arithmetic)

$w$ = primitive root of $q$ in $\overline{\mathbb{F}_p}$

$$y = \sum_{x \bmod q} w^x \left(\frac{x}{q}\right)$$ ← Gauss sum

anything of the form $\sum_{x \bmod q} w^x f(x)$

$f(x)$ = interesting number theory thing

$f(x+q) = f(x)$

(Discrete Fourier Transform)

Calculations in $\overline{\mathbb{F}_p}$

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

(2) $y^2 = (-1)^{\varepsilon(q)} \cdot q$

quadratic reciprocity

Claim These calculations imply QR

case 1: $q \equiv 1 \bmod 4$, $\varepsilon(q) = 0$, $y^2 = q$.

Then $q = y^2$ (is a square) in $\overline{\mathbb{F}_p}$

(1) Square Table

| | | (8) 3 | (1) 5 | (3) 7 | (3) 11 | (1) 13 | (1) 17 | (3) 19 |
|---|---|---|---|---|---|---|---|---|
| (3) | 3 | X | -1 | 1 | -1 | 1 | -1 | 1 |
| (1) | 5 | -1 | X | -1 | 1 | -1 | -1 | 1 |
| (3) | 7 | -1 | -1 | X | | | | |
| (3) | 11 | -1 | 1 | | X | | | |
| (1) | 13 | 1 | -1 | | | X | | |
| (1) | 17 | -1 | -1 | | | | X | |
| (3) | 19 | -1 | 1 | | | | | X |

$\left(\frac{5}{3}\right) = \left(\frac{-1}{3}\right) = -1$ $\quad [\, i^2 = 1,\ 2^2 = 4 = 1 \,]$

$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1$

$\left(\frac{11}{3}\right) = \left(\frac{-1}{3}\right) = -1$

$\left(\frac{13}{3}\right) = \left(\frac{1}{3}\right) = 1$

$\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = -1$

$\left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = 1$

(2)

Square table

$\left(\frac{3}{5}\right) = ?$ $\quad 2^2 = 4, \quad 3^2 = 9 = 4$

$= -1$

$\left(\frac{3}{7}\right) = -1 \quad 2^2 = 4, \quad 3^2 = 9 = 2 \quad 4^2 = \text{same}$

$\left(\frac{3}{11}\right) = -1 \quad 4^2 = 16 = 5 \quad 5^2 = 25 = 4 \quad 6^2 = 5^{-2}$

$\left(\frac{3}{13}\right) = 1 \quad 4^2 = 16 = 3$

$\left(\frac{3}{17}\right) = 1$ $\quad 5^2 = 25 = 8 \quad 6^2 = 36 = 2$

$8^2 = 64 = 30 = 13$

$7^2 = 49 = 51 - 2 = -2$

~~3~~ $\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1 \quad i^2 = 1, \; 2^2 = 4$

$\left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$

$\left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = -1$

$\left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) = -1$

$\left(\frac{19}{5}\right) = \left(\frac{-1}{5}\right) = 1$

(3)

square table

$\left(\frac{5}{7}\right) = -1$ $\quad 3^2 = 9 = 2$ $\quad 4^2 = \text{same}$

$\left(\frac{5}{11}\right) = 1$ $\quad 4^2 = 16 = 5$

$\left(\frac{5}{13}\right) = -1$ $\quad 4^2 = 16 = 3 \quad 5^2 = 25 = -1$
$6^2 = 36 = -3$

$\left(\frac{5}{17}\right) = -1$ $\quad 5^2 = 25 = 8$
$6^2 = 36 = 2$
$7^2 = 49 = 2+13 = 15$
$8^2 = 64 = 30 = 13$

$\left(\frac{5}{19}\right) = 1$ $\quad 25 = 6, \; 36 = 17 = -2$
$49 = 30 = 11$
$64 = 45 = 26 = 7$
$81 = 62 = 43 = 24 = 5$

(3)

and is a square in $\mathbb{F}_p$ if $y \in \mathbb{F}_p$

Frobenius: $y \in \mathbb{F}_p \iff y^p = y \iff y^{p-1} = 1$

But (1) says $y^{p-1} = 1 \iff p$ = square mod $q$.

Thus, if $q = 1 \bmod 4$, $p$ = square mod $q$

$\iff q$ = square mod $p$.

<u>case 2</u>: $p = 1 \bmod 4$. This is the same as case 1 because the theorem is $p \leftrightarrow q$ symmetric.

<u>case 3</u>: $p = 3$ and $q = 3 \bmod 4$.

Then (2) is $y^2 = (-1)^{\frac{q-1}{2}}$ in $\mathbb{F}_p$

But $-1$ is not a square in $\mathbb{F}_p$

so $q$ is a square $\iff y \notin \mathbb{F}_p$

by (1), $y \notin \mathbb{F}_p$ if $p$ not a square mod $q$.

<u>Pf of (1)</u> Frobenius again

$$y^p = \sum_{x \bmod q} \left(w^{\boxed{x}} \left(\frac{x}{q}\right)\right)^p = \sum w^{xp} \left(\frac{x}{q}\right)$$

$p$ odd $\Rightarrow \left(\frac{x}{q}\right)^p = \left(\frac{x}{q}\right)$.

necessary hypothesis

(4)

write $xp = z$ or $x = p^{-1}z \bmod q$

could say: choose $u \bmod q$ so that $up = 1 \bmod q$ and call it $p^{-1}$.

The set $x = \{1, 2, \dots, q-1\}$

is the same as $z = \{1, 2, \dots, q-1\}$

($q$ is prime)

$$y^p = \sum_{z \bmod q} w^z \left(\frac{p^{-1}z}{q}\right)$$

$$= \left(\frac{p^{-1}}{q}\right) \cdot \underbrace{\sum w^z \left(\frac{z}{q}\right)}_{y}$$

mod a prime, $x$ = square $\Leftrightarrow x^{-1}$ square

$$y^p = \left(\frac{p}{q}\right) \cdot y \quad \text{QED} \ \textcircled{1}.$$

(5)

$$y^2 = \sum_x \sum_z w^{x+z} \underbrace{\left(\frac{x}{q}\right)\left(\frac{z}{q}\right)}_{\left(\frac{xz}{q}\right)}$$

write $x+z=u$, $z=u-x$

$$y^2 = \sum_x \sum_u w^u \left(\frac{x(u-x)}{q}\right)$$

$x=0$ is not in the sum

Calculate: $x(u-x) = x^2(x^{-1}u - 1)$

$$= -x^2(1 - x^{-1}u)$$

$$\left(\frac{x(u-x)}{q}\right) = \left(\frac{-x^2}{q}\right)\left(\frac{1-x^{-1}u}{q}\right)$$

$$= \left(\frac{-1}{q}\right)\left(\frac{1-x^{-1}u}{q}\right)$$

$x^2 = q$ square & $x \neq 0$

$$y^2 = \left(\frac{-1}{q}\right) \underbrace{\sum_u w^u \sum_x \left(\frac{1-x^{-1}u}{q}\right)}_{q.}$$

# Prime ideals in number fields

Number field: ring (not field) of algebraic integers in $K/\mathbb{Q}$
(finite degree algebraic extension)

e.g. $\mathbb{Z}[i] \subset \mathbb{Q}[i]$, $K = \mathbb{Q}[i\sqrt{5}]$

Cyclotomic number fields
($K/\mathbb{Q}$ with Abelian Galois group)

Need a good definition of $\mathcal{O}_K$.

Notion of prime and prime factorization

- (Naive) $\mathcal{O}_K$ = integer combinations of generators of $K/\mathbb{Q}$
  - prime = irreducible $x \in \mathcal{O}_K$
  - Doesn't work.
- (Better) $\mathcal{O}_K$ = $x$ that satisfies monic integer polynomial eqn

$\mathfrak{p}$ = prime ideal in $\mathcal{O}_K$
= maximal (D addition domain)

ideal multiplication $\mathfrak{p}_1 \cdot \mathfrak{p}_2$ = ideal

$p \in \mathbb{Z}$ rational prime generates a principal ideal

$I_p = p\mathcal{O}_K \subseteq \mathcal{O}_K$

likely not prime

~~$\mathcal{O}_K$~~ $I_p \subseteq I$ ideal, $I \cap \mathbb{Z} = (p)$

$\Rightarrow I$ "lies over" $p$

$\mathfrak{p} \subseteq I_p$ prime ideal

Thm: Find $\mathfrak{p}$ by looking for a maximal ideal. $\mathfrak{p}$ is maximal.

Why is there a maximal ideal over $I_p$? Not every sequence has a maximum $(1, 2, 3, \dots)$

Noetherian: any increasing family of ideals has a maximum.

Thm $\mathcal{O}_K$ is Noetherian.

Unique factorization thm: $I \subseteq \mathcal{O}_K$

(Dedekind domain)

has unique $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ prime ideals (can have repeats) so that

$I = \mathfrak{p}_1 \cdots \mathfrak{p}_n$

Fractional ideal $M \subseteq K$ f.g. $\mathcal{O}_K$-module

Product of fractional ideals (easy)

Inverse of fractionals

$M \cdot N = \mathcal{O}_K$ = id in fract. ideals

$\mathcal{O}_K \cdot M = M$ (def of module)

eg $\mathfrak{p}^{-1} = \{x \in K \text{ with } xy \in \mathcal{O}_K \text{ all } y \in \mathfrak{p}\}$

Group of fractional ideals = $J_K$

fractional principal ideals = $P_K$

$J_K / P_K = CL_K$ = ideal class group

$|CL|$ = class number of $K/\mathbb{Q}$.

$< \infty$

$G = Gal(K/\mathbb{Q})$ acts on primes $\mathfrak{P}$ over $(p)$.

Transitive

## Noetherian Rings

Ascending chain condition, ACC

If $I_1 \subseteq I_2 \subseteq \cdots \subseteq I_n \subseteq \cdots$

then there is an $n$ with $I_k = I_n$ for $k \geq n$.

An ascending chain has a maximum.

Finite generation, FG

Any ideal $I \subseteq R$ has $g_1, \ldots, g_n$ so that $I = (g_1, \ldots, g_n)$

$g_1, \ldots, g_n$: generators

$(g_1, \ldots, g_n)$: Noetherian

Proposition: ACC $\Leftrightarrow$ FG

Proof that ACC $\Rightarrow$ FG:

Take $I \subseteq R$ ideal (non-zero) and any non-zero $g_1 \in I$

Either $(g_1) = I$ (then you are done)
or there is $g_2 \in I$, $g_2 \notin (g_1) = I_1$
Then $I_2 = (I_1, g_2)$ is strictly
larger than $I_1$. Continue like
this. Either $I_n = (g_1, \dots, g_n) = I$
or there is $g_{n+1} \in I$, $g_{n+1} \notin I_n$
and $I_{n+1} = (g_1, \dots, g_{n+1})$ is
properly larger than $I_n$.
This must terminate (ACC)
so $I = (g_1, \dots, g_n)$ some $n$.

Proof that FG $\Rightarrow$ ACC:

Let $I_{k_0} \subseteq I_{k_0+1} \subseteq \dots$
an ascending chain and
take the "limit" (union)

$$I = \bigcup_{k=1}^{\infty} I_k$$

Then $I$ is an ideal
($xy \in I$ if $x \in R$, $y \in I_k$)

If $I = (g_1, \dots, g_m)$ finite then for each $j$ there $\exists k_j$ with $g_j \in I_{k_j}$. Take $n = \max(k_1, \dots, k_m)$. Then $g_j \in I_n$ for each $j$. Therefore any $x \in I$ has $x = \sum_{j=1}^{m} f_j g_j \in I_n$, so $\bigcup I_n = I_n$.

**Proposition** $R$ Noetherian, $I \subseteq R$ ideal $\Rightarrow$ (1) $\overline{R} = R/I$ Noetherian

~~(2) $R' \subseteq R$ subring $\Rightarrow R'$ Noetherian~~

Pf: If $J \subseteq \overline{R}$, define $\tilde{J} \subseteq R$ by $x \in \tilde{J}$ if $\overline{x} \in J$. Then $\tilde{J}$ is an ideal, generated by $g_1, \dots, g_m$ (hypothesis: $R$ Noetherian) so $J$ gen by $\overline{g_1}, \dots, \overline{g_m}$.

**Proposition** $M$ finitely generated module over $R$, $M' \subseteq M$ submodule $\Rightarrow$ $M'$ finitely generated.

**Remark:** $\mathcal{O}_K \subseteq \mathbb{Q}^n$ (free module on $n$ generators $\mathbb{R}$, $n = \deg(K/\mathbb{Q})$)

The proposition implies that $\mathcal{O}_K$ has the ACC (Noetherian), which implies that there are maximal ideals $\mathfrak{p} \subseteq \mathcal{O}_K$ that lie over $(p)$.

Pf (soon)

**Hilbert basis theorem:** If $R$ is Noetherian then $R[x]$ is too.

**Remark:** Not Hilbert's point of view. Hilbert basis theorem was proved when Noether was a baby.

**Consequence:** Polynomial rings Noetherian $R[x_1, x_2] = (R[x_1])[x_2]$.

(8)

$f \in R[[x_1, x_2]]$ has

$$f = a_0 + a_{10}x_1 + a_{01}x_2 + a_{20}x_1^2 + a_{11}x_1x_2 + \cdots$$

$$= a_0 + a_{10}x_1 + a_{20}x_1^2 + \cdots \quad \text{elements of } R[x_1]$$

$$+ (a_{01} + a_{11}x_1 + \cdots)x_2$$

$$+ (\quad)x_2^2$$

$$+ \cdots$$

powers of $x_2$

Let $E \subseteq \mathbb{C}^n$ be any set

and define $I_E = \{ f \in \mathbb{C}[x_1, \ldots, x_n] \mid f = 0 \text{ on } E \}$

Then $I_E$ is an ideal.

Hilbert: There are polynomials

$g_1, \ldots, g_m(x_1, \ldots, x_n)$ so that

$(x_1, \ldots, x_m) \in E \iff g_j(x) = 0$ all $j = 1, \ldots, m$.

(made Hilbert famous).