Lecture 16: Quadratic Reciprocity + Cyclotomic Fields

p an odd rat'l prime. "a is a quadric residue."

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & a \text{ is a square mod } p \\ -1 & a \text{ not a square mod } p \end{cases} \quad [\text{Here } a \not\equiv 0 \bmod p]$$

$\left(\frac{a}{p}\right)$ is the hom $\mathbb{F}_p^\times \longrightarrow \mathbb{F}_p^\times / (\mathbb{F}_p^\times)^2 \cong \mathbb{Z}/2\mathbb{Z} \cong \{1,-1\}$

($(\mathbb{F}_p^\times)^2$ ← subgp of squares)

Quadratic Reciprocity: Suppose $p \neq q$ are odd rat'l primes. Then

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\frac{p}{q}\right) & \text{if either } p \text{ or } q \text{ is } \equiv 1 \bmod 4 \\ -\left(\frac{p}{q}\right) & \text{if } p \equiv q \equiv 3 \bmod 4. \end{cases}$$

Equivalently, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$.

Supplement: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{if } p \equiv 1 \bmod 4 \\ -1 & \text{if } p \equiv 3 \bmod 4 \end{cases}$ [On HW.]

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \bmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \bmod 8 \end{cases}$$

Cor: $\left(\frac{a}{p}\right)$ depends only on $p \bmod 4a$.

Pf: If a is odd, we have $a = q_1 q_2 \cdots q_n$ and so

$$\left(\frac{a}{p}\right) = \prod \left(\frac{q_i}{p}\right) = \pm \prod \left(\frac{p}{q_i}\right)$$

($\left(\frac{p}{q_i}\right)$ ← depends only on $p \bmod q_i$; $\pm$ ← depends only on $p \bmod 4$)

depends only on $p \bmod 4a$.

If $a = 2^e b$ with $e > 0$ and b odd, then

$\left(\frac{a}{p}\right) = \left(\frac{2}{p}\right)^e \left(\frac{b}{p}\right)$ ← dep on p mod b.

↑ dep on p mod 8, and $8 \mid 4a$

and so $\left(\frac{a}{p}\right)$ is det by p mod $4a$. ▨

Ex: $\left(\frac{123}{787}\right) = \left(\frac{3}{787}\right)\left(\frac{41}{787}\right) = -\left(\frac{787}{3}\right)\left(\frac{787}{41}\right) = -\left(\frac{1}{3}\right)\left(\frac{8}{41}\right) = -\left(\frac{2}{41}\right) = -1.$

↑ $3 \bmod 4$

Last time: a is square mod $p \iff p$ splits in $\mathcal{O}_{\mathbb{Q}(\sqrt{a})}$

[This suggests understanding Quad Recip by using quad fields. Possible, but better to bring cyclotomic fields into the picture.]

Notation: q an odd prime, set $q^* = \left(\frac{-1}{q}\right) q = (-1)^{\frac{q-1}{2}} q$

Q.R. is equivalent to $\left(\frac{p}{q}\right) = \left(\frac{q^*}{p}\right)$ since (using supplement 1.)

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

Fact: $\mathbb{Q}(\sqrt{q^*}) \subseteq \mathbb{Q}(\zeta_q)$ [On HW for this week.]

Lemma: $p \neq q$ odd rat'l primes. Then

p is totally split in $\mathbb{Q}(\sqrt{q^*}) = K$

$\iff$ p splits into an even number of prime ideals in $\mathbb{Q}(\zeta_q) = L$

Proof: Note that p is unramified in both K and L.

Suppose $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ with $\mathfrak{p}_1 \neq \mathfrak{p}_2$. Now $\exists\, \sigma \in Gal(L/\mathbb{Q})$ with $\sigma(\mathfrak{p}_1) = \mathfrak{p}_2$, and σ takes the primes above $\mathfrak{p}_i$ to those above $\mathfrak{p}_2$, and so $p\mathcal{O}_L$ splits into an even # of primes.

Conversely suppose $p\mathcal{O}_L = \mathfrak{q}_1\mathfrak{q}_2 \cdots \mathfrak{q}_{2k}$.

$Gal(L/\mathbb{Q})$ acts trans. on the $\mathfrak{q}_i$,

$$1 \to \underbrace{D}_{\substack{\text{decomp gp} \\ \text{for every } \mathfrak{q}_i}} \longrightarrow Gal(L/\mathbb{Q}) \longrightarrow \mathbb{Z}/2k\mathbb{Z} \to 1$$
$$\cong \mathbb{Z}/(g-1)\mathbb{Z}$$

Now $Gal(L/K)$ has index $[K:\mathbb{Q}] = 2$ in $Gal(L/\mathbb{Q})$, and so contains D_j thus $K \subseteq L_D$ ← the decomp. field.

Any prime above p in $\mathcal{O}_{L_D}$ has inertial deg $= 1$, and so the same is true for $\mathcal{O}_K$.

Thus $p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2$ and p is totally split in K.

∎

Thm: Let $n = \prod_p p^{v_p}$ be the prime decomp of $n \in \mathbb{N}$. Let f_p = order of p in $\left(\mathbb{Z}/(np^{-v_p}\mathbb{Z})\right)^\times$. Then in $\mathbb{Q}(\zeta_n)$,

$(p) = (\mathfrak{p}_1 \cdots \mathfrak{p}_r)^{\varphi(p^{v_p})}$ where the $\mathfrak{p}_i$ are distinct primes of inert deg f_p.

Special case:

① $p \nmid n$: p is unramified.