Math 531 Tom Tucker
NOTES FROM CLASS 10/27

Recall from last time...

We can use cyclotomic fields to prove the quadratic reciprocity theorem. Recall the definition the quadratic residue symbol for a prime p. It is defined for an integer a coprime to p as

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

When $p = 2$, $\left(\frac{a}{2}\right) = 1$ for any odd a. When p is odd and $(a, p) = 1$, we have

(1) $\left(\frac{a}{p}\right) = a^{(p-1)/2}$;
(2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;
(3) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$;
(4) $\left(\frac{a}{p}\right) = (-1)^{\frac{p-1}{\mathrm{ord}(a)}}$, where $\mathrm{ord}_p(a)$ denotes the order of $a \pmod{p}$.

Properties 2, 3, and 4 follow immediately from 1. Property 1 follows from the fact that $(\mathbb{Z}/p\mathbb{Z})^*$ has a primitive root θ and a is square mod p if and only if $a = \theta^r$ for some even r. Now, $(\theta^r)^{(p-1)/2} = 1$ if r is even and -1 is r is odd, so we are done.

Continuing with quadratic reciprocity...

From now on, p and q are distinct primes. Let's also assume that q is odd. Quadratic reciprocity relates $\left(\frac{p}{q}\right)$ with $\left(\frac{q}{p}\right)$. It says that for p and q odd we have

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

What has this got to do with cyclotomic fields? The first fact is that $\left(\frac{p}{q}\right) = 1$ if and only if $x^2 - p$ factors mod q. When $p \equiv 1 \pmod{4}$, and $B = \mathbb{Z}[\sqrt{q}]$, this is the same thing as saying that

$$pB = \mathcal{Q}_1\mathcal{Q}_2$$

(one prime for each factor). Why is this helpful? Because $\mathbb{Q}(\xi_q)$ contains a unique quadratic field.

Lemma 24.1. *The field $\mathbb{Q}(\xi_q)$ contains exactly one quadratic field. It is $\mathbb{Q}(\sqrt{(-1)^{(q-1)/2}q})$.*

Proof. The field $\mathbb{Q}(\xi_q)$ is Galois since all the conjugates of ξ_q are powers of ξ_q and hence Φ_q splits completely in $\mathbb{Q}(\xi_q)$. It is clear that the Galois group is $(\mathbb{Z}/a\mathbb{Z})^*$ which is cyclic of even order, so there is exactly one

subgroup of index 2, and one subfield of degree 2. Since $\mathbb{Q}(\xi_q)$ only ramifies at p, this quadratic field cannot ramify at 2, so it must have discriminant divisible only by q. There are only two possibilities $\mathbb{Q}(\sqrt{q})$ and $\mathbb{Q}(\sqrt{-q})$. By checking the ramification at 2, we see that if $q \equiv 1 \pmod 4$ it is $\mathbb{Q}(\sqrt{q})$, if $q \equiv 3 \pmod 4$, then $-q \equiv 1 \pmod 4$, so it must be $\mathbb{Q}(\sqrt{-q})$. □

Let us denote $(-1)^{(q-1)/2}$ as $\epsilon(q)$.

Proposition 24.2. *Suppose that p is odd. There are an even number of distinct primes $\mathcal{Q}$ of $\mathbb{Z}[\xi_q]$ lying over p if and only if $p\mathbb{Z}[\sqrt{\epsilon(q)q}q]$ factors as two distinct primes.*

Proof. Let $\mathcal{M}$ be a prime in $\mathbb{Z}[\xi_q]$ such that $\mathcal{M} \cap \mathbb{Z} = p\mathbb{Z}$. Let G denote the Galois group $\mathrm{Gal}(\mathbb{Q}(\xi_q)/\mathbb{Q})$, let E denote $\mathbb{Q}(\sqrt{\epsilon(q)q})$, let G_E denote the part of G that acts identically on E, and let D be the part of G that sends $\mathcal{M}$ to itself. Recall that G acts transitively on the set of primes of $\mathbb{Z}[\xi_q]$ lying over p. Thus, the number of primes lying over p is equal to $[G : D]$. The index $[G : D]$ is even if and only if $D \subseteq G_E$, since G_E is the unique subgroup of index 2 in G.

Now, let's let $\mathcal{Q}$ be a prime of $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ for which $\mathcal{Q} \cap \mathbb{Z} = p\mathbb{Z}$. The group G_E acts transitively on the set of primes of $\mathbb{Z}[\xi_q]$ lying over $\mathcal{Q}$. If this set is the same as the set of all primes in $\mathbb{Z}[\xi_q]$ lying over $\mathcal{P}$, then $\mathcal{Q}$ must be the only prime in $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ lying over p. Otherwise, there must be two primes in $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ lying over p.

We claim that G_E acts transitively on the set of all $\mathcal{M}$ lying over p if and only if D is not contained in G_E. Note that if D is not contained in G_E, then the $[G_E : D \cap G_E] = [G : D]$, which means that the number of primes in the G-orbit of $\mathcal{M}$ is the same as the number of primes in G_E-orbit of $\mathcal{M}$, which means that G_E acts transitively on the $\mathcal{M}$ lying over p. If $D \subseteq G_E$, then $[G : D] = 2[G_E : D]$ and G_E does not act transitively on this set. □

Corollary 24.3. *Suppose that p is odd. Then $\left(\frac{\epsilon(q)q}{p}\right) = 1$ if and only if p splits into an even number of primes in $\mathbb{Z}[\xi_q]$.*

Proof. $\left(\frac{\epsilon(q)q}{p}\right) = 1$ if and only if $x^2 - \epsilon(q)q$ factors over p, which happens if and only if $p\mathbb{Z}[\sqrt{\epsilon(q)q}]$ factors as two distinct primes, since $\mathbb{Z}[\sqrt{\epsilon(q)q}]$ localized at an odd prime of $\mathbb{Z}$ is integrally closed. □

Let T_p denote the number of primes lying over p in $\mathbb{Z}[\xi_q]$. From what we've just seen, $(-1)^{T_P} = \epsilon(q)$.

The next two proposition and corollary work for any p (including 2).

Proposition 24.4. *The degree of the field extension* $\mathbf{F}_p[\xi_q]$ *is equal to* $\mathrm{ord}_q(p)$ *(the order of* p *in* $\mathbf{F}_q$*).*

Proof. We know that any finite field is cyclic and that the order of $\mathbf{F}_{p^f}$ is $p^f - 1$. Thus, $\xi_q \in \mathbf{F}_{p^f}$ if and only if $p^f \equiv 1 \pmod{q}$. Therefore, the degree of degree of the field extension $\mathbf{F}_p[\xi_q]$ is equal to the smallest f such that $p^f \equiv 1 \pmod{q}$, which is equal to the order of p in $\mathbf{F}_q$. □

Corollary 24.5. *Suppose that there are* T_p *primes in* $\mathbb{Z}[\xi_q]$ *lying above* p*. Then* $\mathrm{ord}_q(p)$ *is equal to* $(q-1)/T_p$*.*

Proof. Since p doesn't ramify, it must factor as

$$p\mathbb{Z}[\xi_q] = \mathcal{Q}_1 \cdots \mathcal{Q}_{T_p}.$$

Therefore, the relative degree $[\mathbb{Z}[\xi_q]/\mathcal{Q}_i : \mathbb{Z}/p\mathbb{Z}] = (q-1)/m$ for every i. Since

$$\mathbb{Z}[\xi_q]/\mathcal{Q}_i \cong \mathbf{F}_p[\xi_q],$$

it follows from the preceding proposition that the order of $p \pmod{q}$ is equal to $(q-1)/(T_P)$. □

Theorem 24.6. *(Quadratic reciprocity for odd primes) Let* p *and* q *be odd primes,* $p \neq q$*. Then*

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

Proof. Let $\mathrm{ord}_q(p)$ denote the order of $p \pmod{q}$. We see that

$$\begin{aligned}\left(\frac{\epsilon(q)q}{p}\right) &= (-1)^{T_p} \quad \text{(Corollary 24.3)} \\ &= (-1)^{\frac{q-1}{\mathrm{ord}_q(p)}} \quad \text{(Corollary 24.5)} \\ &= \left(\frac{p}{q}\right) \quad \text{(Property (iv))}.\end{aligned}$$

Thus,

$$\left(\frac{p}{q}\right) = \left(\frac{\epsilon(q)q}{p}\right) = \left(\frac{-1^{(q-1)/2}}{p}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{q}{p}\right).$$

Multiplying $\left(\frac{p}{q}\right)$ by $\left(\frac{q}{p}\right)$ then finishes the proof. □

Next time: quadratic reciprocity for $p = 2$.