# Lecture 17: Primes in cyclotomic fields

Reminder: Exam on Monday
Special Schedule this week: Wed: Scott Ahlgren,
Fri: No class.

Office hours this week:
Me: Mon 10-11 Sun: TBA
Jonah: Tue 3-4, Fri 3-4 Cobol B1.

---

Thm: $n = \prod p^{v_p}$ the prime factorization of $n \in \mathbb{N}$.
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
$f_p$ = order of $p$ in $\mathbb{Z}/(np^{-v_p}\mathbb{Z})$.

[Recall motivation re: quadratic reciprocity.]

Proof: Let $L = \mathbb{Q}(\zeta_n)$. As $\mathcal{O}_L = \mathbb{Z}[\zeta]$ the factorization of $p\mathcal{O}_L$ is det by that of $\Phi_n(x)$ mod $p$.

cyclotomic poly.

Case $p \nmid n$, i.e. $v_p = 0$. Let $\mathfrak{p} \subseteq \mathcal{O}_L$ be a prime above $p$.

First, observe $\begin{pmatrix} n\text{th roots} \\ \text{of } 1 \text{ in } \mathcal{O}_L \end{pmatrix} \longrightarrow \mathcal{O}_L/\mathfrak{p}$ is injective,

since $X^n - 1$ has distinct roots in $\mathcal{O}_L/\mathfrak{p}$
(note that $X^n - 1$ and $nX^{n-1}$ have no common roots since $p \nmid n$.)

In particular, $\mathcal{O}_L/\mathfrak{p}$ is the extension of $\mathbb{F}_p$ gotten by adjoining all of the $n^{th}$ roots of unity.

Now $\mathcal{O}_L/\mathfrak{p} = \mathbb{F}_{p^f}$ and $n$ divides $|\mathbb{F}_{p^f}^\times| = p^f - 1$.
Thus $p^f \equiv 1 \bmod n$, and $f_p \mid f$. Since is cyclic, in fact $\mathcal{O}_L/\mathfrak{p} = \mathbb{F}_{p^{f_p}}$. Thus $\overline{\Phi}_n \in \mathbb{F}_p[X]$ factors into $\overline{\varphi}_1(x)^e \cdot \ldots \cdot \overline{\varphi}_r(x)^e$ all of deg $f_p$.
As $X^n - 1$ has distinct roots in $\mathcal{O}_L/\mathfrak{p}$, must have $e = 1$, completing the proof in this case.

General Case: Set $m$ by $n = p^{v_p} m$. Consider

$\eta_i$ - primitive $(p^{v_p})^{th}$ roots of unity

$\xi_j$ - primitive $m^{th}$ roots of unity.

Then $\{\eta_i \xi_j\}$ are exactly the primitive $n^{th}$ roots of unity.

Thus $\Phi_n(x) = \prod_{i,j} (x - \eta_i \xi_j)$

Now $x^{p^{\nu_p}} - 1 \equiv (x-1)^{p^{\nu_p}} \bmod p$, so if $\mathfrak{p}$ is a prime of $\mathcal{O}_L$ above $p$, we have $\eta_i \equiv 1 \bmod \mathfrak{p}$.

Thus

$$\Phi_n(x) \equiv \prod_{i,j} (x - \xi_j) \equiv \Phi_m(x)^{\varphi(p^{\nu_p})} \bmod \mathfrak{p}$$

As this is true for some prime above $p$, we get $\Phi_n(x) \equiv \Phi_m(x)^{\varphi(p^{\nu_p})} \bmod p$ ✪ and we've reduced to the earlier case. ▨

[✪ The point is just $\mathfrak{p} \cap \mathbb{Z} = (p)$.]

<u>Next time</u>: Quadratic Reciprocity

<u>Special Case</u>: $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

<u>Proof</u>:

Since $(1+i)^2 = 2i$, we have

$$(1+i)^p = (1+i)\left((1+i)^2\right)^{\frac{p-1}{2}} = (1+i)\, i^{\frac{p-1}{2}}\, 2^{\frac{p-1}{2}}$$

Now $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \bmod p$, since $\mathbb{F}_p^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \supseteq (\mathbb{F}_p^\times)^2$.

Combining

$$(1+i)^p \equiv 1 + i^p \equiv 1 + i(-1)^{\frac{p-1}{2}} \equiv (1+i)\, i^{\frac{p-1}{2}} \left(\frac{2}{p}\right) \bmod p$$

If $\frac{p-1}{2}$ is even, we have $(1+i) \equiv (1+i)(-1)^{\frac{p-1}{4}}\left(\frac{2}{p}\right) \bmod p$

$\Rightarrow \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{4}}$. (Note $(1+i)$ is invert mod $p$; take $(1+i)^{-1} = (1-i)2^{-1}$.)

A similar calculation shows $\left(\frac{2}{p}\right) = (-1)^{\frac{p+1}{4}}$

if $\frac{p-1}{2}$ is odd.

Since $\frac{p^2-1}{8} = \left(\frac{p-1}{4}\right)\left(\frac{p+1}{2}\right) = \left(\frac{p+1}{4}\right)\left(\frac{p-1}{2}\right)$

we're done. $\blacksquare$