Lecture 19: Cyclotomic fields

$\mathbb{Q}(\zeta_n)$ with $\zeta_n = e^{2\pi i/n}$

$\Phi_n = \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta)$. Then $x^n - 1 = \prod_{d \mid n} \Phi_d(x)$.

Thm: For any n, $\Phi_n(x) \in \mathbb{Z}[x]$ and is irreducible.

Hence $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

Proof: Suppose Φ_n factors as $f(x)g(x)$ for $f, g \in \mathbb{Z}[x]$ and f is irred.

Claim: ζ a root of f. If p is prime, $p \nmid n$, then ζ^p is also a root of f.

If so, let ζ be a fixed root of f. Then any prim. n^{th} root is ζ^m where $m = p_1 \cdots p_k$ and no $p_i \mid n$.

As $\zeta^m = (((\zeta^{p_1})^{p_2})^{p_3} \cdots)^{p_n}$ applying the claim repeatedly gives ζ^m is a root of $f(x)$. So $f(x) = \Phi_n(x)$.

Pf of claim: Suppose instead $g(\zeta^p) = 0$. ↙ in $\mathbb{Z}[x]$.

Thus ζ is a root of $g(x^p) \Rightarrow g(x^p) = f(x)h(x)$

Let's look in $\mathbb{F}_p[x]$. Some observations

(1) $x^n - 1$ is separable, since der is $nx^{n-1} \neq 0$.
So $\overline{\Phi}_n(x)$ has distinct roots.

(2) The Frob. map $\mathbb{F}_p \to \mathbb{F}_p$ is trivial, since
$a^{p-1} - 1 = 0$ for $\forall a \in \mathbb{F}_p \Rightarrow a^p = a$ for all $a \in \mathbb{F}_p$.
Hence

$$\bar{g}(x^p) = \bar{g}(x)^p \quad \text{for any } \bar{g} \in \mathbb{F}_p[x]$$

(3) As $\bar{g}(x)^p = \bar{f}(x)\bar{h}(x)$, then $\bar{g}$ and $\bar{f}$ have a common root.

But then $\overline{\Phi}_n(x) = \bar{g}(x)\bar{f}(x)$ has a mult. root, a contradiction. ▨

Thm: $m \in \mathbb{N}$. There exist ∞-many primes $p \equiv 1 \bmod m$, i.e. $p = cm + 1$.

[Special case of Dirichlet Thm on Primes in Arithmetic Progressions.]

Proof: Consider $\Phi_m(a)$ for $a \in \mathbb{N}$. Then

① There are infinitely many primes dividing some $\Phi_m(a)$.

② Any $p \mid \Phi_m(a)$ with $p \nmid m$ has $p \equiv 1 \bmod m$.

[One is true for all monic in $\mathbb{Z}[x]$, so focus on ②]

Pf of ②: In $\mathbb{F}_p$ we have

$$a^m - 1 = \Phi_m(a) \cdot \prod_{\substack{d \mid m \\ d < m}} \Phi_d(a) = 0$$

Claim: The order of a in $\mathbb{F}_p^\times$ is m.

Suppose $a^d = 1$ for $d < m$. Now $d \mid m$ and so a is the root of some $\Phi_{d'}$ for $d' \mid m$.

But then $a^m - 1$ has a mult root, which isn't poss since the der of $x^m - 1$ is $mx^{m-1} \neq 0$.

So the order of a in $\mathbb{F}_p$ is m.

Thus $m \mid p-1 \Rightarrow p \equiv 1 \bmod m$ as needed.

Proof of ①: More gen, let $f(x) \in \mathbb{Z}[x]$ be monic.

Suppose $\{f(a) \mid a \in \mathbb{N}\}$ have only finitely many prime divisors $p_1, \dots, p_k$. Choose a so that $f(a) = c \neq 0$

Consider y

$$g(x) = c^{-1} f(a + c p_1 \cdots p_k x) \qquad n = \deg f.$$

$$= c^{-1}\left(f(a) + f'(a) c y + \frac{f''(a)}{2} c^2 y^2 + \cdots \frac{f^{(n)}(a)}{n!} c^n y^n \right)$$

$$= 1 + f'(a) y + \frac{f''(a)}{2} c\, y^2 + \cdots + \underbrace{\frac{f^{(n)}(a)}{n!}}_{\text{in } \mathbb{Z}} c^{n-1} y^n$$

which is in $\mathbb{Z}[x]$.

For any b, have $g(b) \equiv 1 \bmod p_1 \cdots p_k$.

Pick b large so that $|g(b)| > 1$. Let p be any prime factor of $g(b)$. Then $p \neq$ any p_i, and $p \mid f(a + c p_1 \cdots p_k b)$. ▨