Thursday, March 31, 2016 9:32 AM

In the previous lecture you learned about a few new concepts and notations:

- $v_p : \mathbb{Z}^+ \to \mathbb{Z}$ s.t. $n = \prod p^{v_p(n)}$ (the p-adic valuation).
- $\mathcal{M} := \{ f : \mathbb{Z} \to \mathbb{C} \mid f(1)=1 , \ f(mn)=f(m)f(n) \text{ if } \gcd(m,n)=1 \}$

(Multiplicative functions)

Thm $(\mathcal{M}, *)$ is a group.

- $\mathbb{1}^{-1} = \mu$ Möbius function.

Recall. Euler ϕ-function: $\phi(n) := \left|\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\right| = |\{0<r<n \mid \gcd(r,n)=1\}|$

Thm (1) $\phi \in \mathcal{M}$.

(2) $\phi * \mathbb{1} = id$.

Pf. (1) We need to understand $\phi(mn) = \left|\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times\right|$.

By Chinese Remainder Theorem, $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

, as two rings, if $\gcd(m,n)=1$.

So $\left(\mathbb{Z}/mn\mathbb{Z}\right)^\times \simeq \left(\mathbb{Z}/m\mathbb{Z}\right)^\times \times \left(\mathbb{Z}/n\mathbb{Z}\right)^\times \Rightarrow \phi(mn) = \phi(m)\phi(n)$.

(2) We would like to prove $\sum_{d \mid n} \phi(d) = n$.

Proof 1. $\{1,2,\dots,n\} = \bigsqcup_{d \mid n} \{k \mid 1 \le k \le n, \ \gcd(k,n)=d\}$

$$= \bigsqcup_{d \mid n} \{ dk' \mid 1 \le k' \le n/d, \ \gcd(k', \tfrac{n}{d})=1 \}$$

$$\Rightarrow n = \sum_{d \mid n} \left| \{ dk' \mid 1 \le k' \le n/d, \ \gcd(k', \tfrac{n}{d})=1 \} \right|$$

$$= \sum_{d \mid n} \phi(n/d) = (\mathbb{1} * \phi)(n).$$

Proof 2. For a prime factor p of n let

$$A_p := \{ k \mid 1 \le k \le n \text{ and } p \mid n \}.$$

then $\{k \mid 1 \le k \le n,\ \gcd(k,n)=1\}$

$$= \{1,2,\dots,n\} \setminus \bigcup_{p \mid n} A_p .$$

$\Rightarrow$ By inclusion-exclusion,

$$\phi(n) = n - \sum_{p \mid n} |A_p| + \sum_{\substack{p_1,p_2 \mid n \\ p_1 \neq p_2}} \underbrace{|A_{p_1} \cap A_{p_2}|}_{A_{p_1 p_2}} - \sum_{\substack{p_1,p_2,p_3 \mid n \\ p_i \neq p_j}} |\underbrace{A_{p_1} \cap A_{p_2} \cap A_{p_3}}_{A_{p_1 p_2 p_3}}| + \cdots$$

$$= n + \sum_{\substack{q \mid n \\ \text{square-free}}} \mu(q)\,|A_q|$$

$$= \sum_{d \mid n} \mu(d)\,\underbrace{|A_d|}_{n/d} = (\mu * \mathrm{id})(n)$$

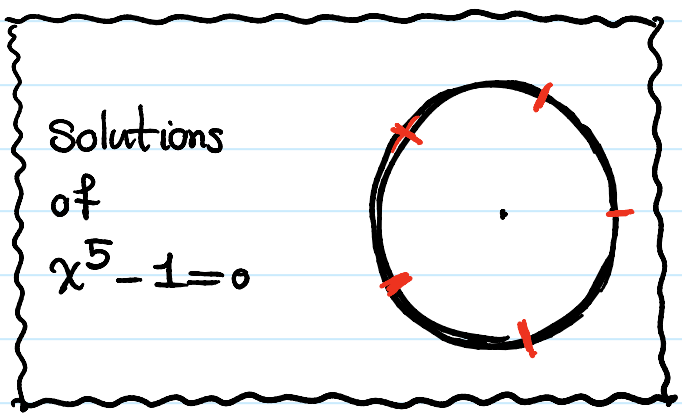
$\Rightarrow \quad \phi = \mu * \mathrm{id} \quad \Rightarrow \quad \mathbb{1} * \phi = \mathrm{id}$ ■

Cyclotomic Polynomials

Let's start with $x^n - 1 = 0$. Can you tell me its solutions?

Recall the Euler equation

$$e^{i\theta} = \cos\theta + i \sin\theta$$



In fact, one defines

$$e^z := 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \cdots$$

. For any $z \in \mathbb{C}$, the right hand side is absolutely convergence. So we are allowed to reorder its terms, and get the same limit:

$$e^{i\theta} = 1 + i\theta - \frac{\theta^2}{2!} - i\frac{\theta^3}{3!} + \frac{\theta^4}{4!} + i\frac{\theta^5}{5!} - \cdots$$

$$= \left(1 - \frac{\theta^2}{2!} + \frac{\theta^4}{4!} - \cdots\right) + i\left(\theta - \frac{\theta^3}{3!} + \cdots\right)$$

$= \cos\theta + i \sin\theta$.

$e^{x+iy} = e^x(\cos y + i \sin y) \Rightarrow |e^z| = e^{\mathrm{Re}(z)}$.

Let $\zeta_n = e^{\frac{2\pi i}{n}}$. Then $\zeta_n, \zeta_n^2, \cdots, \zeta_n^{n-1}, \zeta_n^n - 1$ are distinct roots of $x^n - 1$. So

$$x^n - 1 = (x-1)(x-\zeta_n)\cdots(x-\zeta_n^{n-1}).$$

Let $\Phi_n(x) = \prod_{\gcd(i,n)=1} (x-\zeta_n^i)$. Then Φ_n is called the n^{th} cyclotomic polynomial.

Basic facts. $\deg \Phi_n = \phi(n)$.

. Φ_n is a monic polynomial (the coeff. of the highest degree is 1.)

Theorem. $\prod_{d|n} \Phi_d(x) = x^n - 1$.

Proof. $x^n - 1 = \prod_{1 \le i \le n} (x - \zeta_n^i)$

$$= \prod_{d|n} \prod_{\substack{1 \le i \le n \\ \gcd(i,n)=d}} (x - \zeta_n^i)$$

$$= \prod_{d|n} \prod_{1 \le k \le n/d \atop \gcd(k, n/d)=1} (x - \zeta_n^{dk})$$

$$= \prod_{d|n} \underbrace{\prod_{1 \le k \le n/d \atop \gcd(k,n/d)=1} (x - \zeta_{n/d}^k)}_{\Phi_{n/d}(x)}$$

$$= \prod_{d|n} \Phi_{n/d}(x). \quad \blacksquare$$

$n/$ $\mu(d)$

Corollary. $\Phi_n(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}$.

Proof. (A little bit of cheating)

$$\sum_{d \mid n} \log \Phi_d(x) = \log(x^n - 1)$$

By Möbius inversion, $\log \Phi_n(x) = \sum_{d \mid n} \mu(d) \log(x^{n/d} - 1)$

$$\Rightarrow \quad \Phi_n(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)}. \qquad \blacksquare$$

Lemma. $P_1(x), P_2(x) \in \mathbb{Z}[x]$ monic polynomials. $\left.\begin{array}{l} \\ \\ \end{array}\right\} \Rightarrow Q(x) \in \mathbb{Z}[x]$.

$P_1(x) = Q(x) P_2(x)$ for some $Q(x) \in \mathbb{C}[x]$

Proof. Since $P_2(x)$ is monic, one can apply the long division algorithm. So there are $q(x), r(x) \in \mathbb{Z}[x]$ such that

① $P_1(x) = q(x) P_2(x) + r(x)$.

② $0 \le \deg r < \deg q$

On the other hand, the division over $\mathbb{C}$ has unique quotient and remainder. Since $P_1(x) = Q(x) P_2(x)$ over $\mathbb{C}$, we have $Q(x) = q(x) \in \mathbb{Z}[x]$ and $r(x) = 0$. $\blacksquare$

Corollary $\Phi_n(x) \in \mathbb{Z}[x]$.

Proof. $\Phi_n(x) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)} \Rightarrow \Phi_n(x)$ is ratio of two monic integral polynomials $\Rightarrow$ by the above lemma, $\Phi_n(x) \in \mathbb{Z}[x]$. $\blacksquare$

Our next goal is to prove the following theorem:

Theorem. Suppose p is prime and $p \nmid n$. Then $\Phi_n(x) \equiv 0 \pmod p$ has a solution

$\Uparrow$

$$\Updownarrow$$

$$p \equiv 1 \pmod{n}.$$

- $\Phi_n(a) \overset{p}{\equiv} 0 \Rightarrow a^n \overset{p}{\equiv} 1 \Rightarrow \operatorname{ord}_p(a) \mid n.$
- By Euler's theorem, $\operatorname{ord}_p(a) \mid p-1$. So it is enough to prove:

<u>Proposition</u>. $\Phi_n(a) \overset{p}{\equiv} 0$ and $p \nmid n \Rightarrow \operatorname{ord}_p(a) = n$.

<u>Pf.</u> Since $p \mid \Phi_n(a)$, we have

$$0 < v_p(\Phi_n(a)) = \sum_{d \mid n} \mu(d)\, v_p(a^{n/d} - 1).$$

So we need to understand $v_p(a^{n/d} - 1)$.

<u>Lemma</u>. $v_p(a^m - 1) \neq 0 \iff \operatorname{ord}_p(a) \mid m$

<u>Pf.</u> $v_p(a^m - 1) > 0 \iff a^m \equiv 1 \pmod{p}$

$\iff \operatorname{ord}_p(a) \mid m$. ■

<u>Lemma</u>. Suppose $p \nmid m$. Then

$$v_p(a^{\operatorname{ord}_p(a)\cdot m} - 1) = v_p(a^{\operatorname{ord}_p(a)} - 1).$$

<u>Proof.</u> Let $t = \operatorname{ord}_p(a)$.

$$a^{tm} - 1 = (a^t - 1)\left[(a^t)^{m-1} + (a^t)^{m-2} + \cdots + (a^t) + 1\right],$$

and $(a^t)^{m-1} + (a^t)^{m-2} + \cdots + a^t + 1 \overset{p}{\equiv} \underbrace{1 + 1 + \cdots + 1}_{m} \overset{p}{\not\equiv} 0.$

Hence

$$v_p(a^{tm} - 1) = v_p(a^t - 1). \quad ■$$

$$0 < \sum_{d \mid n} \mu(n/d)\, v_p(a^d - 1) = \sum_{\substack{d \mid n \\ t \mid d}} \mu(n/d)\, v_p(a^d - 1) \quad (1^{\text{st}} \text{ Lemma})$$

$$= \sum_{d' \mid n/t} \mu\left(\frac{n/t}{d'}\right) v_p(a^{td'} - 1)$$

$$= \sum_{1' \mid n/} \mu\left(\frac{n/t}{d'}\right) v_p(a^t - 1) \quad (2^{\text{nd}} \text{ Lemma})$$

$$= \underbrace{\sum_{d' \mid n/t}} \mu(d') \, v_p(a^{\frac{t}{d'}} - 1) \quad \cdots$$

$$= v_p(a^t - 1) \; I(n/t)$$

$\Rightarrow \quad n/t = 1 \Rightarrow n = t.$ ■

Proof of Theorem. ($\Downarrow$) by Proposition, $\operatorname{ord}_p a = n$.

Hence $n \mid p-1$.

($\Uparrow$) Suppose $p \overset{n}{\equiv} 1$. Let g be a primitive element* of p, i.e. $\left(\mathbb{Z}/p\mathbb{Z}\right)^\times = \langle g \rangle$ or equivalently $\operatorname{ord}_p g = p-1$.

Claim $\quad \Phi_n(g^{\frac{p-1}{n}}) \overset{p}{\equiv} 0.$

Proof. Let $a = g^{\frac{p-1}{n}}$. Then $\operatorname{ord}_p a = \dfrac{\operatorname{ord}_p g}{\gcd\left(\operatorname{ord}_p g, \frac{p-1}{n}\right)}$

$$= n.$$

$$v_p(\Phi_n(a)) = \sum_{d \mid n} \mu(n/d) \; v_p(a^d - 1)$$

$$= \sum_{\substack{d \mid n \\ n \mid d}} \mu(n/d) \, v_p(a^d - 1) = v_p(a^n - 1) > 0.$$

So $\quad \Phi_n(a) \equiv 0 \pmod{p}$. ■

* we will see later why there is such element (if you have not seen it already.)

Theorem (Special case of Dirichlet's theorem)

There are infinitely many primes of the form $nk+1$.

Proof. Suppose there are only finitely many such primes $p_1, \ldots, p_r$. Consider the polynomial $f(x) := \Phi_n(n p_1 p_2 \cdots p_r \, x)$.

Since it is a degree $\varphi(n) \geq 1$ poly. and the leading

Since Φ_n is a degree $\varphi(n) \geq 1$ poly. and the leading coeffi. is positive, for large enough $x \in \mathbb{Z}$, $f(x)$ has a prime factor p. So

$$\Phi_n(\overbrace{n p_1 p_2 \cdots p_r x_0}^{a}) \overset{p}{\equiv} 0 .$$

$$\Rightarrow \left(n p_1 p_2 \cdots p_r \cdot x_0\right)^n \overset{p}{\equiv} 1 \Rightarrow p \nmid n \text{ and } p \notin \{p_1, \cdots, p_r\}.$$

$$\left.\begin{array}{l} \Phi_n(a) \overset{p}{\equiv} 0 \\ p \nmid n \end{array}\right\} \Rightarrow p \overset{n}{\equiv} 1 .$$

$\Rightarrow$ p is a new prime of the form $nk+1$, which contradicts our assumption. ■