2/07

Recordar: Criterio de Eisenstein

Si $f \in \mathbb{Z}[x]$, $f = \sum_{j=0}^{n} a_j x^j$ si $\exists p$ primo tq $p \mid a_i \ \forall 0 \le i < n$ $p \nmid a_n$ y $p^2 \nmid a_0 \Rightarrow f$ es irreducible en $\mathbb{Z}[x]$ (y por ende en $\mathbb{Q}[x]$)

Dem: supongamos f reducible en $\mathbb{Z}[x]$

$f = g \cdot h$; $g, h \in \mathbb{Z}[x]$; $g = \sum_{i=0}^{l_1} b_i x^i$, $h = \sum_{j=0}^{l_2} c_j x^j$

$l_1 + l_2 = gr(f) = n$, $b_{l_1} \cdot a_{l_2} = a_n$, $b_0 \cdot a_0 = a_0$

Tomando congruencia mod p queda $\overline{f} = \sum_{j=0}^{n} \overline{a_j} x^j \in \mathbb{Z}/p\mathbb{Z}[x]$

$\overline{a_j}$ es la clase de congruencia de a_j en $\mathbb{Z}/p\mathbb{Z}$. Idem con g, h

$\overline{g} = \sum_{0}^{l_1} \overline{b_i} x^i \in \mathbb{Z}/p\mathbb{Z}[x]$

$\overline{h} = \sum_{0}^{l_2} \overline{c_j} x^j$.

Además $\overline{f} = \overbrace{\overline{g \cdot h}}^{\text{en } \mathbb{Z}[x]} = \overline{g} \cdot \overline{h}$ (en $\mathbb{Z}/p\mathbb{Z}[x]$)

Como por hipótesis $p \mid a_j \ \forall\ 0 \le j < n$, entonces:

$\overline{f} = \overline{a_n} x^n \in \mathbb{Z}/p\mathbb{Z}[x]$

Entonces $\overline{g} = \overline{b_{l_1}} x^{l_1}$ y $\overline{h} = \overline{c_{l_2}} x^{l_2}$. Veamos esto en (*)

(*) Como en $\mathbb{Z}/p\mathbb{Z}[x]$ vale el TF Aritmética, y el poli $\overline{f}$ es irreducible y el único poli que aparece en la factorización de $\overline{f}$, como $\overline{g} \cdot \overline{h} = \overline{f}$ es una factorización de $\overline{f}$ debe ocurrir que el único divisor irreducible de $\overline{g}$ es x o sea $\overline{g} = \overline{b_{l_1}} x^{l_1}$ (Idem con $\overline{h}$)

(Usamos también que $\overline{a_n} = \overline{b_{l_1}} \cdot \overline{c_{l_2}}$ como $\overline{a_n} \neq 0 \Rightarrow \overline{b_{l_1}} \neq 0$ y $\overline{c_{l_2}} \neq 0$)

Como $\overline{g} = \overline{b_{l_1}} x^{l_1}$, $\overline{h} = c_{l_2} x^{l_2}$, esto quiere decir que:

$p \mid b_i \ \forall\ 0 \le i < l_1$, $p \mid c_j \ \forall\ 0 \le j < l_2$

En particular $p \mid b_0$ y $p \mid c_0 \Rightarrow p^2 \mid b_0 \cdot c_0$ como $b_0 \cdot c_0 = a_0 \Rightarrow p^2 \mid a_0$ Abs!

Entonces f es irreducible.

Como ejemplo vimos que:

$\frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \dots + X + 1 = \sum_0^{p-1} X^j$ es irreducible.

Raíces de la unidad (Visto como polinomios)

$X^n - 1 \in \mathbb{C}[x]$. Las raíces de la unidad $G_n = \{w \in \mathbb{C},\ w^n = 1\}$ son la raíces del poli $X^n - 1$

$G_n = \langle w^j : j = 0, \dots, n-1 \rangle$

$w = e^{\frac{2\pi i}{n}}$ $\quad G_n^* = \{w^j \cdot (j:n) = 1\}$

$X^n - 1 = \prod_{j=0}^{n-1} (x - w^j)$ es una factorización en $\mathbb{C}[x]$.

Podemos intentar factorizarlo en $\mathbb{Q}[x]$ (o $\mathbb{Z}[x]$)

Recordad.

$G_n^* = \{w \in \mathbb{C}\ w$ es raíz n-ésima primitiva$\}$

$= \{w \in \mathbb{C},\ w^n = 1$ y además n es el menor natural tq $w^n = 1\}$

$= \{w \in G_n,\ w$ genera $G_n\}$

$w \in G_n \wedge w^k = 1$ con $k \le n \Rightarrow k \mid n$ Esto es clave

Si $w \in \mathbb{C}$ $|w| = 1$, $\mathrm{ord}(w) = \min\{k,\ w^k = 1\}$, o sea que w es raíz $\mathrm{ord}(w)$-ésima primitiva.

Lema: $G_n = \bigcup_{d \mid n}^{\text{disjunta}} G_d^*$

Antes de la Dem

Ej: $G_6 = G_1^* \cup G_2^* \cup G_3^* \cup G_6^* =$

$= \{1\} \cup \{-1\} \cup \{e^{\frac{2\pi i}{3}}, e^{\frac{2\pi i}{3}\cdot 2}\} \cup \{e^{\frac{2\pi i}{6}}, e^{\frac{2\pi i}{6}\cdot 5}\}$

a) La unión es disjunta por definición de primitiva. Si $x \in G_d^* \Rightarrow \mathrm{ord}(x) = d$

$\Rightarrow x \notin G_\ell^*$ porque si no $\mathrm{ord}(x) = \ell \Rightarrow \ell = d$.

b) Veamos la igualdad de los conjuntos.

b1) Como $d \mid n$, $G_d^* \subset G_d \subset G_n \Rightarrow \bigcup_{d \mid n}^{dis} G_d^* \subset G_n$

Si $w \in G_n \Rightarrow w^n = 1$ y si $w^k = 1 \Rightarrow k \mid n$. $\Rightarrow \operatorname{ord}(w) \mid n \Rightarrow w \in G_{\operatorname{ord}(w)}^* \subset \bigcup_{d \mid n}^{dis} G_d^*$

Corolario:

$$n = \sum_{d \mid n} \phi(d)$$

Dem

$n = |G_n|$ (cardinal), $\phi(d) = |G_d^*|$

Como $G_n = \bigcup_{d \mid n}^{dis} G_d^*$.

Porque la unión es disjunta

Tomando cardinal ambos: $|G_n| \overset{\downarrow}{=} \sum_{d \mid n} |G_d^*| \Rightarrow n = \sum_{d \mid n} \phi(d)$

Polinomios ciclotómicos

Sea $n \in \mathbb{N}$, $\Psi_n = \prod_{z \in G_n^*} (X - z)$

Para hacerlo concreto: $\Psi_n = \prod_{(j,n)=1} (X - w^j)$ con $w = e^{\frac{2\pi i}{n}}$

Prop

1) $\Psi_n \mid X^n - 1$
2) $\operatorname{gr}(\Psi) = |G_n^*| = \varphi(n)$
3) Ψ_n es mónico.
4) $X^n - 1 = \prod_{d \mid n} \Psi_d$
5) Si p primo $\Psi_p = \sum_{j=0}^{p-1} X^j$, $\Psi_p \in \mathbb{Z}[X]$, es mónico e irreducible (Eisenstein)
6) $\Psi_n \in \mathbb{Z}[X]$ $\forall n$
7) $\Psi_n \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Q}[X]$ (o en $\mathbb{Z}[X]$)

Vamos 6) en el caso p^2 $\quad X^{p^2} - 1 = \underbrace{\Psi_1 \Psi_p \Psi_{p^2}}_{\in \mathbb{Z}[X] \text{ mónico}}$ $\quad \Psi_1, \Psi_p \in \mathbb{Z}[X]$ mónicos

$\Rightarrow \Psi_{p^2} \in \mathbb{Z}[X]$ mónico

Vamos 6) en el caso p^n: $\underbrace{X^{p^n} - 1}_{\in \mathbb{Z}[X] \text{ mónico}} = \underbrace{\Psi_1 \Psi_p \Psi_{p^2} \cdots \Psi_{p^{n-1}}}_{\in \mathbb{Z}[X] \text{ mónico}} \Psi_{p^n}$

$\Rightarrow \Psi_{p^n} \in \mathbb{Z}[X]$, mónico

Ej Calcular Ψ_{49}

$gr(\Psi_{49}) = \varphi(49) = P(P-1) = 42$

$X^{49}-1 = \underbrace{\Psi_1 \Psi_7}_{x^7-1} \Psi_{49}$

$x^{49}-1 \;\big|\; x^7-1$

$0 \;\; \Psi_{49}$

$\Psi_{3.5.7}$ de $gr(2.4.6) = 48$.

Es el primero que tiene algún coef $\neq 1, -1, 0$.