3 Ciclotomia (raíces de la unidad)

$q \geq 2$ primo $\quad \zeta^q = 1, \ \zeta \neq 1$ (raíz primitiva de 1)

ζ raíz de $\Phi_q(x) = 1 + x + \cdots + x^{q-1} = \dfrac{x^q - 1}{x - 1}$

($\zeta = e_q(1)$) $\qquad$ ↳ irreducible

Todas las raíces primitivas $\{\zeta, \zeta^2, \ldots, \zeta^{q-1}\}$ $\qquad \sum = -1$

$\mathbb{Z}[\zeta] \ni a \rightsquigarrow a = a_1\zeta + a_2\zeta^2 + \cdots + a_{q-1}\zeta^{q-1} \quad a_i \in \mathbb{Z}$

↳ a_i únicos (Φ_q irred)

i.e. $\{\zeta, \zeta^2, \ldots, \zeta^{q-1}\}$ es base de $\mathbb{Z}[\zeta]$

Recuerdo: g raíz primitiva mód q $\quad \nu(n)$ t.q. $g^{\nu(n)} = n$

$n = 1, \ldots, q-1 \qquad \nu(n) = 1, \ldots, q-1$ (en otro orden)

Sup: $q - 1 = e \cdot f$ $\qquad (e = 2)$

$$\eta_j = \sum_{n=1}^{q-1} \zeta^n \qquad (j = 0, \ldots, e-1)$$

$\nu(n) \equiv j \ (e)$ $\qquad \left(\sum \eta_i = -1\right)$

$e = 2$ $\quad \eta_0 = \sum_{\substack{n=1 \\ \nu(n) \equiv 0 \ (2)}}^{q-1} \zeta^n = \sum_R \zeta^R$ $\qquad \eta_1 = \sum_N \zeta^N$

↳ Fijamos $\varphi = e_g(1)$

$$\begin{cases} \eta_0 - \eta_1 = \sum \left(\frac{n}{g}\right) e_g(n) = G = \varepsilon q^{1/2} \\ \eta_0 + \eta_1 = -1 \end{cases}$$

$$\eta_0 = \frac{1}{2}\left(-1 + \varepsilon q^{1/2}\right) \qquad \eta_1 = \frac{1}{2}\left(-1 - \varepsilon q^{1/2}\right).$$

$$\left(\text{general: } \varphi = e(1/q) \rightsquigarrow \eta_0 = e^{-1} \sum_{x=1}^{q-1} e_g(x^e) \right)$$

para η_j depende de g.

Consideramos: $F(\xi) = \sum_{r=1}^{q-1} A_r \xi^r$

Sup: $F(\xi^m) = F(\xi)$ siempre que $v(m) \equiv 0 \pmod{e}$

$v(r) \equiv v(s) + v(m) \ (q)$

$\Leftrightarrow$ $A_r = A_s$ si $r \equiv s m \ (q-1)$

para algún m con $v(m) \equiv 0 \ (q)$

$\Leftrightarrow v(r) \equiv v(s) \pmod{e}$

$$F(\xi) = A_1 \eta_1 + \cdots + A_e \eta_e \quad (A_i \text{ son } A_0 \text{ reordenados})$$

Obs: A_i pueden ser polinomios en $\mathbb{Z}[x]$.

$$F(\xi) = \prod_R (x - \xi^R)$$

Si $v(m) \equiv 0 (2)$ $\rightarrow$ $F(\xi^m) = \prod_R (x - \xi^{mR})$

$\left(\frac{m}{q}\right) = +1$ $\qquad = \prod_R (x - \xi^R) = F(\xi)$

Luego $F(\xi) = A_0(x) \cdot \eta_0 + A_1(x) \eta_1$

$$= \frac{1}{2} A_0(x) \left(-1 + \varepsilon q^{1/2}\right) + \frac{1}{2} A_1(x) \left(-1 - \varepsilon q^{1/2}\right)$$

$$= \frac{1}{2}\left[\varphi(x) - \varepsilon q^{1/2} z(x)\right] \qquad \varphi(x), z(x) \in \mathbb{Z}[x]$$

$$F(\xi^q) = \prod_R (x - \xi^{qR}) = \prod_N (x - \xi^N)$$

$$= A_0(x) \eta_1 + A_1(x) \eta_0$$

$$= \frac{1}{2}\left[\varphi(x) + \varepsilon q^{1/2} z(x)\right]$$

$q \equiv 1 (4) \rightarrow \varepsilon = 1$ demostrar

Teo $\prod (x - e_q(R)) = \frac{1}{2}\left[\varphi(x) - q^{1/2} z(x)\right]$ $\qquad \varphi, t \in \mathbb{Z}[x]$

$\prod (x - e_q(N)) = \frac{1}{2}\left[\varphi(x) + q^{1/2} z(x)\right]$