

1776

Antistralia Titus

Claim.

$$R_n(x + \frac{1}{x}) = x^n + x^{n-1} + \dots + x + 1 + \frac{1}{x} + \dots + \frac{1}{x^n}.$$

Pf. Inducció.

$$\begin{aligned} R_{n+1}(x + \frac{1}{x}) &= (x + \frac{1}{x}) \left(x^n + \dots + 1 + \dots + \frac{1}{x^n} \right) - \left(x^{n-1} + \dots + 1 + \dots + \frac{1}{x^{n-1}} \right) \\ &= x^{n+1} + \dots + x + 1 + \frac{1}{x} + \dots + \frac{1}{x^{n+1}}. \end{aligned}$$

Per tant

$$\boxed{x^n R_n(x + \frac{1}{x}) = \frac{x^{2n+1} - 1}{x - 1}}.$$

Farem els casos $p = 4n+1$ i $p = 4n+3$ per separat.

$p = 4n+3$

Tenim $x^n R_n(x + \frac{1}{x}) = \frac{x^{\frac{p-1}{2}} - 1}{x - 1}.$

Mirat a $\mathbb{F}_p$, si $\langle g \rangle = (\mathbb{F}_p)^*$ és un generador, llavors si $x = g^{2k}$ $1 \leq k \leq \frac{p-3}{2} = 2n$ tenim RHS és $\frac{g^{2k(\frac{p-1}{2})} - 1}{g^{2k} - 1} = 0.$

Com $g^{2kn} \neq 0$ i $\mathbb{F}_p$ és íntegre, tenim

$$R_n(g^{2k} + \frac{1}{g^{2k}}) = 0.$$

Veiem que $\{g^2 + \frac{1}{g^2}, \dots, g^{2k} + \frac{1}{g^{2k}}, \dots, g^{p-3} + \frac{1}{g^{p-3}}\}$ són
 n valors diferents a $\mathbb{F}_p$. Això demostrarà que hem
 trobat n arrels
 diferent i que per tant $P_n(x)$ es descomposa completament
 a $\mathbb{F}_p$.

Per això, nota que si $x, y \neq 0$ llavors

$$\begin{aligned} x + \frac{1}{x} = y + \frac{1}{y} &\Leftrightarrow x - y + \frac{1}{x} - \frac{1}{y} = 0 \\ &\Leftrightarrow (x - y) \left(1 - \frac{1}{xy}\right) = 0 \\ &\Leftrightarrow x = y \quad \text{ó} \quad x = \frac{1}{y}. \end{aligned}$$

Per tant $g^{2k} + \frac{1}{g^{2k}} = g^{2j} + \frac{1}{g^{2j}} \Leftrightarrow 2k = 2j \pmod{p-1}$. Per

tant, dels $2n$ valors $g^{2k} + \frac{1}{g^{2k}}$, $1 \leq k \leq 2n$, només
 ens apareixen residus repetits 2 cops. Per tant,
 efectivament hem trobat n arrels.

$$\boxed{p=4n+1} \text{ Tenim}$$

$$x^n R_n\left(x + \frac{1}{x}\right) = \frac{x^{\frac{p+1}{2}} - 1}{x - 1}.$$

Ara considera $\mathbb{F}_{p^2}$ com a extensió de $\mathbb{F}_p$, i considera el generador $\langle g \rangle = (\mathbb{F}_{p^2})^*$. Nota que per a tot $1 \leq s \leq \frac{p-1}{2} = 2n$ tenim que si $x = g^{2(p-1)s}$ llavors el RHS és

$$\frac{g^{(p^2-1)s} - 1}{g^{2(p-1)s} - 1} = 0 \quad \left(g \text{ té ordre } p^2-1, \text{ perquè } \left| (\mathbb{F}_{p^2})^* \right| = p^2-1 \right).$$

Per tant $g^{2(p-1)s} + g^{-2(p-1)s}$, $1 \leq s \leq \frac{p-1}{2}$ és arrel de

$R \quad \forall s$. Pel mateix argument d'abans $\left(x + \frac{1}{x} = y + \frac{1}{y} \right) (\mathbb{F}_{p^2})$
 $\begin{matrix} \uparrow \\ x=y \end{matrix}$ o $x = \frac{1}{y} (\mathbb{F}_{p^2})$,

tenim que el conjunt

$$\left\{ g^{2(p-1)s} + g^{-2(p-1)s} \right\}_{s=1, \dots, \frac{p-1}{2} = 2n} \text{ són } n$$

valors diferents de $\mathbb{F}_{p^2}$. Si veïssim que tots aquests pertanyen a $\mathbb{F}_p$ hauríem acabat.

Per això recorda que $\mathbb{F}_{p^2}/\mathbb{F}_p$ és Galois al ser extensió de cossos finits, i $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ ve generat per l'automorfisme de Fröbenius, $(x \mapsto x^p)$. Per tant, si veièssim que $g^{2(p-1)s} + g^{-2(p-1)s}$ queda fix per l'automorfisme de Fröbenius això implicaria que queda fix $\forall \sigma \in \text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$. Però és ben conegut que els únics elements fixos per tot automorfisme de $\text{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ són els del cos base, que implicaria que $g^{2(p-1)s} + g^{-2(p-1)s} \in \mathbb{F}_p$. Per tant, hem acabat, doncs efectivament fent

$$\begin{aligned} \left(g^{2(p-1)s} + g^{-2(p-1)s} \right)^p &= g^{2(p-1)sp} + g^{-2(p-1)s \cdot p} \\ &= g^{2(p^2-p)s} + g^{-2(p^2-p)s} = g^{2(-p+1)s} + g^{-2(-p+1)s} \\ &= g^{-2(p-1)s} + g^{2(p-1)s} \end{aligned}$$

Fix per Fröbenius!!
Hem guanyat.

