Arrels primitives

Problema 79. Comproveu les afirmacions següents:

(i) Els divisors primers senars d'un enter de la forma n^2+1 són de la forma $4k+1$. (Indicació: $n^2 \equiv -1 \pmod{p}$, on $p \neq 2$ és un primer, implica que $4 \mid \varphi(p)$)

(ii) Els divisors primers senars d'un enter de la forma n^4+1 són de la forma $8k+1$.

(iii) Els divisors primers senars d'un enter de la forma n^2+n+1 que són diferents de 3 són de la forma $6k+1$.

Solució. Anem a veure com demostrar les anteriors proposicions:

(i) En primer lloc demostrarem la indicació que ens donen per resoldre el problema. Introduirem un lema que ens facilitarà la feina.

Lema. Sigui $(\mathbb{Z}/p\mathbb{Z})^*$ amb p primer, i α una arrel primitiva qualsevol d'aquest grup multiplicatiu, aleshores l'element $\overline{-1} = \overline{p-1}$ és igual a $\alpha^{\frac{\varphi(p)}{2}}$.

Prova. Sabem que $\left(\alpha^{\frac{\varphi(p)}{2}}\right)^2 \equiv 1 \pmod{p}$ i que a més $\alpha^{\frac{\varphi(p)}{2}}$ també és diferent de 1 ja que si fos 1 això contradiuria que $\varphi(p)$ fos l'ordre del grup multiplicatiu $(\mathbb{Z}/p\mathbb{Z})^*$. Sabem a més a més que, com estem treballant en un cos, 1 només té dues arrels quadrades, i que com en particular també estem en un anell, es compleix que $(-1)\cdot(-1) = 1$. Com estem treballant amb $p > 2$ és clar que $1 \neq -1$, i per tant, donat que no hi ha més possibilitats, la igualtat que hem presentat s'ha de donar forçosament. □

Lema. (Indicació)

Prova. Suposem que $n^2 \equiv -1 \pmod{p}$, si considerem α arrel primitiva aleshores ho podem reescriure com $\alpha^{2s} \equiv \alpha^{\frac{\varphi(p)}{2}} \pmod{p}$ per certa $s \in \mathbb{N}$. Es més, agafant un representant $\tilde{\alpha}$ de la classe de α podem establir una igualtat a $\mathbb{Z}$ (això ho podem fer suposant que $2s < \varphi(p)$ ja que $\varphi(p)$ és l'ordre del grup multiplicatiu). Així podem passar a la equació $\tilde{\alpha}^{2s} = \tilde{\alpha}^{\frac{\varphi(p)}{2}}$.

Ara podem prendre logaritmes en base $\tilde{\alpha}$ i arribem a la igualtat $2s = \frac{\varphi(p)}{2}$, només ens queda aïllar $\varphi(p)$:

$$\varphi(p) = 4s$$

i per tant la indicació queda provada. □

Ara fixem-nos en el primer problema que ens ocupava. Podem establir les següents congruencies:

$$n^2 + 1 \equiv 0 \pmod{p} \ \forall p \in \mathbb{P} \text{ tal que } p \mid (n^2+1)$$

En particular això passa pels divisors primers senars. Escollim qualsevol d'aquests primers i transformem la congruencia en una que tingui la forma donada a la indicació:

$$n^2 \equiv -1 \pmod{p}$$

D'aquí podem extreure que $4 \mid \varphi(p)$, és a dir, podem escriure $\varphi(p) = 4k$ per algun $k \in \mathbb{N}$. Ara aplicant que si p és primer aleshores $\varphi(p) = p - 1$ arribem on volíem $p = \varphi(p) + 1 = 4k + 1$. □

(ii) Aplicarem el mateix procediment que hem fet anar per provar la indicació de l'apartat anterior.

Lema. $n^4 \equiv -1 \pmod{p}$, on $p \neq 2$ és un primer, implica que $8 \mid \varphi(p)$.

Prova. Igual que la de la indicació de l'apartat anterior, canviant $2s$ per $4s$ (respectivament $2s'$ i $4s'$).

Per tot p divisor primer senar podem establir la congruencia $n^4 + 1 \equiv 0 \pmod{p}$, fent un petit canvi arribem a $n^4 \equiv -1 \pmod{p}$, aplicant el lema immediatament anterior arribem a que $8 \mid \varphi(p) = p - 1$. I finalment

$$p = \varphi(p) + 1 = 8k + 1 \quad \text{per cert} \quad k \in \mathbb{N}$$

□

(iii) Aquest és potser el cas més interessant ja que ens obliga a jugar una mica amb les expressions. Sabem que si tenim un divisor primer p senar diferent de 3 complirà la congruencia $n^2 + n + 1 \equiv 0 \pmod{p}$ (per ser divisors, no per ser primers o diferents de 2 i 3). Podem transformar aquesta congruencia així:

$$n^2 + n + 1 + n \equiv n \pmod{p} \;\Rightarrow\; (n+1)^2 \equiv n \pmod{p} \; (\Delta)$$

També podem fer la transformació:

$$n(n+1) \equiv n^2 + n \equiv -1 \pmod{p}$$

Si ara apliquem (Δ) per substituïr n a la segona congruencia que hem obtingut tenim:

$$(n+1)^3 \equiv -1 \pmod{p}$$

Ara podem tornar a aplicar la tècnica anterior, escrivim $-1 = \alpha^{\frac{\varphi(p)}{2}}$ i $(n+1)^3 = \alpha^{3s}$, podem considerar que $3s < \varphi(p)$ (aquí es on fem servir que hem de deixar de banda el cas $p = 3$) sense pèrdua de generalitat ja que $\varphi(p)$ és l'ordre del grup multiplicatiu, així doncs podem transformar la congruencia en una identitat a $\mathbb{Z}$ per un cert representant $\tilde{\alpha}$ de α (ara entesa com una classe):

$$\begin{aligned} \tilde{\alpha}^{3s} &= \tilde{\alpha}^{\frac{\varphi(p)}{2}} \\ 3s &= \frac{\varphi(p)}{2} \\ 6s &= \varphi(p) \end{aligned}$$

Només ens queda veure que $p = \varphi(p) + 1 = 6s + 1$, tal com volíem demostrar. □