Quadrats a $(\mathbb{Z}/N\mathbb{Z})^*$

Problema 33.
Siguin p un primer senar i $r \geq 1$ un enter.

(i) Demostreu que el conjunt dels elements de $(\mathbb{Z}/p^r\mathbb{Z})^*$ que són quadrats és un subgrup d'índex 2.

(ii) Demostreu que si $a \in \mathbb{Z}$ no és divisible per p, i si $b \in (\mathbb{Z}/p^r\mathbb{Z})^*$ és tal que $b^2 \equiv a \pmod{p^r}$, llavors existeix un únic element $c \in (\mathbb{Z}/p^{r+1}\mathbb{Z})^*$ tal que $c \equiv b \pmod{p^r}$ i $c^2 \equiv a \pmod{p^{r+1}}$.

(iii) Deduïu que si $a \in \mathbb{Z}$ és un nombre no divisible per p, llavors l'equació $X^2 = a$ o bé no té solucions en $(\mathbb{Z}/p^r\mathbb{Z})^*$, per a cap valor de $r \geq 1$, o bé en té exactament dues per a tot valor de $r \geq 1$.

Solució.

(i)

Lema. Sigui a un quadrat en $(\mathbb{Z}/p^r\mathbb{Z})^*$ aleshores té com a mínim 2 arrels (x i $-x$).

Prova. Suposem que en tingués només una, és a dir, que $x = -x$. Això és equivalent a dir que $2x \equiv 0 \pmod{p^r}$, cosa que implicaria que, o bé $p = 2$ o bé $x = 0$, consa que no pot ser per pertanyer x al grup multiplicatiu i ser p senar. Per tant arribem a contradicció i el lema queda provat. □

Observació 1. Donat que si a és un quadrat té com a mínim dues arrels, i que pel Teorema fonamental de l'Àlgebra en té com a molt dues, sabem que en té exactament dues.

Ara considerem l'aplicació seguent:

$$\begin{array}{rccc} f: & (\mathbb{Z}/p^r\mathbb{Z})^* & \longrightarrow & (\mathbb{Z}/p^r\mathbb{Z})^* \\ & x & \mapsto & x^2 \end{array}$$

A partir dels lemes anteriors podem veure a partir d'aquí que el cardinal de la imatge és el cardinal del domini dividit entre 2 i que la imatge és precisament el subconjunt de $(\mathbb{Z}/p^r\mathbb{Z})^*$ format pels seus quadrats.

A més a més, aquest subconjunt hereda la estructura de grup de $(\mathbb{Z}/p^r\mathbb{Z})^*$ i la operació és interna, ja que $x^2(y^2)^{-1} = x^2(y^{-1})^2 = (xy^{-1})^2$ i com $xy^{-1} \in (\mathbb{Z}/p^r\mathbb{Z})^*$ és clar que $(xy^{-1})^2$ pertany al subconjunt dels quadrats.

Per definició d'índex, sabent que el cardinal del subgrup és el cardinal del grup entre dos, i aplicant el teorema de Lagrange obtenim que el subgrup dels quadrats té index 2. □

(ii) En primer lloc es recomanable reescriure alguns punts del problema, no per tenir un punt de vista diferent sino per evitar confusions que puguin induir-nos a cometre errors.

Els elements x de $\mathbb{Z}$ els denotarem amb la forma usual, y els elements de $(\mathbb{Z}/p^r\mathbb{Z})^*$ els denotarem amb x_r, de forma que $x \in \mathbb{Z}$ i serà un representant de la classe $x_r \in (\mathbb{Z}/p^r\mathbb{Z})^*$. Notem que coneixer x_r determina quins seran $x_{r-1}, x_{r-2}, \ldots, x_1$ però no quins seran els x_s per $s > r$ ni quin nombre serà $x \in \mathbb{Z}$ (òbviament conèixer x ens diu quin element és x_r per tot $r \in \mathbb{N}$).

El que voldrem veure és que donat a tal que existeix b_r complint $b_r^2 = a_r$ aleshores es existeix un únic c_{r+1} tal que $c_r = b_r$ i $c_{r+1}^2 = a_{r+1}$.

Sabem que si escollim α_{r+1} arrel primitiva del grup al que pertany, aleshores α_r serà també arrel multiplicativa del seu respectiu grup.

Com α_r és arrel primitiva, aleshores podem escriure b_r com una potència de α_r. Així doncs tenim $b_r = \alpha^s$ i que $a_r = b_r^2 = \alpha_r^{2s}$ per algún $s \in \mathbb{N}$ menor que $\frac{\varphi(p^r)}{2}$ (la cota ve donada per l'ordre del grup, que és $\varphi(p^r)$ i perquè no considerem el cas trivial $a = 1$ on $b_r = \alpha_r^{\frac{\varphi(p^r)}{2}}$ i $c_{r+1} = \alpha_{r+1}^{\frac{\varphi(p^{r+1})}{2}}$).

Anem a veure com hauria de ser c_{r+1}, clarament hauria de ser de la forma $c_{r+1} = \alpha_{r+1}^{s+k\varphi(p^r)}$ per algun $k \in \mathbb{N}$ doncs és la única forma de que quan el fem "baixar"quedi $c_r = \alpha_r^{s+k\varphi(p^r)} = \alpha_r^s = b_r$.

Queda veure que existeix algún $k \in \mathbb{N}$ tal que $a_{r+1} = c_{r+1}^2 = \alpha^{2(s+k\varphi(p^r))}$ i que a més a més és únic mòdul p, el que ens dona de forma directa la unicitat de c_{r+1} (fem anar k de 0 a $p-1$ ja que per $k = p$ tindriem que $k\varphi(p^r) = p\varphi(p^r) = \varphi(p^{r+1})$, que és l'ordre del grup).

Per altra banda tenim que a té classe a_{r+1} de la forma $a_{r+1} = \alpha_{r+1}^{2s+k'\varphi(p^r)}$ per un cert $k' \in \mathbb{N}$ complint també que $0 \geq k' > p$. Això últim és clar ja que a ha de tenir una classe $a_{r+1} \in (\mathbb{Z}/p^{r+1}\mathbb{Z})^*$ tal que quan baixi sigui $a_r \in (\mathbb{Z}/p^r\mathbb{Z})^*$.

Podem veure clarament que a_{r+1} és un quadrat al seu grup multiplicatiu, ja que $\varphi(p^r)$ és parell, i sumat amb $2s$ segueix éssent parell. Ara podem reescriure:

$$a_{r+1} = \alpha_{r+1}^{2s+k'\varphi(p^r)} = \alpha_{r+1}^{2(s+k'\frac{\varphi(p^r)}{2})}$$

A més a més volem que c_{r+1} sigui una arrel quadrada de a_{r+1}, per tant hem d'escriure

$$c_{r+1} = \alpha_{r+1}^{s+k'\frac{\varphi(p^r)}{2}}$$

En aquest punt ja gairebé estem, doncs falta molt poc per determinar unívocament k.

En cas que k' sigui parell k només pot ser $\frac{k'}{2}$.

En cas que k' fos senar n'hi haurà prou amb agafar k com el representant positiu més petit de la classe $k'_1 \cdot 2_1^{-1}$. (Multipliquem per l'invers de 2 mòdul p per "dividir" entre 2)

Per acabar hem de fixar-nos en un petit detall: hem escollit una arrel quadrada de a_{r+1}, però hem de veure que l'altra arrel (recordem que n'hi ha només dues per estar treballant en un cos), que és l'element oposat a la primera, no baixa a b_r sino a un altre element.

Convenim en dir c_{r+1} a la primera arrel, aleshores la segona és

$$-c_{r+1} = \alpha_{r+1}^{s+k\varphi(p^r)} \cdot \alpha_{r+1}^{\frac{\varphi(p^{r+1})}{2}}$$

Si ara fem baixar aquest element, tindrem:

$$\alpha_r^s \cdot \alpha_r^{\frac{\varphi(p^{r+1})}{2}} = \alpha_r^s \cdot \alpha_r^{\frac{\varphi(p^r)}{2}p} = \alpha_r^s \cdot \left(\alpha_r^{\frac{\varphi(p^r)}{2}}\right)^p = \alpha_r^s \cdot (-1_r)^p = -b_r \neq b_r$$

Per tant c_{r+1} existeix i és únic. □

(iii) Que existeixi solució per a l'equació $X^2 = a$ en $(\mathbb{Z}/p^r\mathbb{Z})^*$ és equivalent a dir que a és un quadrat en aquell grup multiplicatiu. Si a és un quadrat en $(\mathbb{Z}/p^r\mathbb{Z})^*$, aplicant l'apartat (ii) tenim que hi ha un únic quadrat c congruent amb a mòdul p^{r+1}, és a dir, que l'equació tindrà també només dues solucions (pels apartats anteriors) en $(\mathbb{Z}/p^{r+1}\mathbb{Z})$, i per inducció, per tot $r \geq 1$.

A més a més, sabem que si α és arrel primitiva de $(\mathbb{Z}/p\mathbb{Z})$ també ho serà de $(\mathbb{Z}/p^r\mathbb{Z})$ per tot $r \geq 1$, i que si a és un quadrat dins $(\mathbb{Z}/p^r\mathbb{Z})$, aleshores podem escriure $a = \alpha^{2k} = (\alpha^k)^2$ per algún natural k, de manera que a també ha de ser un quadrat a $(\mathbb{Z}/p\mathbb{Z})$. □