3.7.33. *Considérese la congruencia* $x^2 \equiv p^t b \mod p^s$ *con* p *primo impar,* $s \geq 1$, $(b, p) = 1$. *Probar que*

1. *si* $t \geq s$, *la congruencia tiene solución.*

2. *si* $t < s$, *la congruencia tiene solución si y sólo si* t *es par y* b *es un residuo cuadrático módulo* p.

Solución: El apartado 1 es simple, si $t \geq s$ entonces $p^t \equiv 0 \mod p^s$ y la congruencia que hay que resolver es $x^2 \equiv 0 \mod p^s$. Está claro que tiene solción, $x \equiv 0 \mod p^s$ por ejemplo.

Para el apartado 2 vamos a demostrar las dos implicaciones, empecemos probando

$\Longleftarrow$: Pongamos $t = 2k$ y b que sea un resíduo cuadrático módulo p, por tanto existe x_0 tal que $b \equiv x_0^2 \mod p$. Nos gustaría tener esa última congruencia módulo p^s por tanto vamos a intentar subirla. Sea $q(x) = x^2 - b$ que tiene solución en $\mathbb{Z}_p$. Desarrollando por Taylor:

$$q(x_0 + hp) = q(x_0) + q'(x_0)hp + \underbrace{\frac{q''(x_0)}{2}(hp)^2 + ...}_{\text{términos en } p^2.}$$

Mirándo esto módulo p^2 si queremos subir x_0, tiene que ocurrir que $q(x_0) + q'(x_0)hp \equiv 0 \mod p^2$ y como $q(x_0) = pz$ esa congruencia se transforma en $z + q'(x_0)h \equiv 0 \mod p$.

Si $q'(x_0)$ es invertible $\mod p$ entonces podré subir la solución de manera única. Como $q'(x) = 2x$ tenempos que $q'(x_0) \equiv 2x_0 \not\equiv 0 \mod p$. Esto último sale de que como $x_0^2 \equiv b \mod p$ con b una unidad eso implica que x_0 es también una unidad y como p es un primo impar, 2 también es unidad en $\mathbb{Z}_p$. Por tanto puedo subir la solución a módulo p^2 y en general (la cuenta es exáctamente la misma) puedo subirla hasta p^s, así que existe un $y_0 \in \mathbb{Z}_{p^s}$ tal que $y_0^2 \equiv b \mod p^s$.

Con toda esta información junta está claro que ya podemos construir una solución a la congruencia $x^2 \equiv p^t b \mod p^s$, una solución es $x \equiv y_0 p^k \mod p^s$ (recordemos que $t = 2k$).

$\Longrightarrow$: Supongamos ahora que tengo una solución, $x_0^2 \equiv p^t b \mod p^s$. El caso $t = 0$ es trivial, ya que lo que tengo es $x_0^2 \equiv b \mod p^s$ y mirando esto módulo p tenemos que b es resíduo cuadrático módulo p.

Para $t \geq 1$ vamos a escribir la solución x_0 (como número entero, un representante) como $x_0 = p^k a$ donde $(p, a) = 1$ para algún $k \geq 0$ ($x_0 \neq 0$ ya que si no $p|b$ y esto no ocurre). Por tanto ahora tenemos la igualdad $p^{2k}a^2 \equiv p^t b \mod p^s$. Queremos ver que $t = 2k$. Para empezar, podemos mirar la igualdad anterior módulo p^t y tendríamos $p^{2k}a^2 \equiv 0 \mod p^t$ y por tanto $p^t | p^{2k}a^2$. Como $(a, p) = 1$ eso implica que $2k \geq t$. Sabiendo esto, en la ecuación $p^{2k}a^2 \equiv p^t b \mod p^s$ podemos *dividir* todo entre p^t para llegar a $p^{2k-t}a^2 \equiv b \mod p^{s-t}$ (recordemos que esto es lícito por la definición de congruencia). Como $s - t \geq 1$ podemos mirar la ecuación anterior módulo p y por tanto llegamos a $p^{2k-t}a^2 \equiv b \mod p$. Y ahora tenemos a la derecha una unidad y por tanto lo de la izquierda debe ser necesariamente una unidad también, lo que implica que $2k \leq t$. Esto concluye que efectivamente $2k = t$.

Con esto ya casi hemos acabado, ahora, partiendo de $p^t a^2 \equiv p^t b \mod p^s$ dividimos entre p^t todo para llegar a $a^2 \equiv b \mod p^{s-t}$. Como $s - t \geq 1$ podemos mirar la ecuación anterior módulo p y llegamos a $a^2 \equiv b \mod p$, lo que nos dice que b es residuo cuadrático módulo p.

Problema escrito por Diego González Sánchez.