7) p primo impar, a raíz primitiva mód p^α

a) Si a es impar, probar que a es raíz primitiva mód $2p^\alpha$

Ideas: Teo. Chino del Resto: $U(2p^\alpha) \simeq U(2) \times U(p^\alpha)$

porque p impar $\Rightarrow p^\alpha$ impar $\Rightarrow \text{mcd}(p^\alpha, 2) = 1$

$$U(p^\alpha) = \bar{a}^0, \bar{a}^1, \bar{a}^2, \dots, \bar{a}^{\varphi(p^\alpha)}$$

$$\varphi(2p^\alpha) = \varphi(2)\,\varphi(p^\alpha)$$

$$\| \quad 1$$

$1, a, a^2, \dots, a^{\varphi(p^\alpha)}$ son todos impares

dado $\bar{x} \in U(2p^\alpha)$, queremos

probar que $\exists k$ tal que $\bar{x} = \bar{a}^k$ en $U(2p^\alpha)$

o sea,

$$x \equiv a^k \pmod{2p^\alpha}$$

$$\Updownarrow \text{ TchR}$$

y $\begin{cases} x \equiv a^k \pmod 2 \\ x \equiv a^k \pmod{p^\alpha} \end{cases}$

Si encontramos un k que verifique las dos congruencias de abajo, ese k va a verificar la congruencia de arriba

Como a es raíz primitiva mód p^α,

$\exists k : x \equiv a^k \pmod{p^\alpha}$ ✓

Para resolver la cong mód 2:

a es impar $\Rightarrow$ a^k es impar

$\bar{x} \in U(2p^\alpha) \Rightarrow x$ coprimo con $2p^\alpha \Rightarrow x$ es impar

$x \equiv a^k \pmod 2$

Entonces probamos lo que queríamos

b) si a es par, probar que $a+p^\alpha$ es raíz primitiva mód $2p^\alpha$

Ideas: ¿Será que lo que hicimos en la parte anterior puede servir acá también?

$\bar{x} \in U(2p^\alpha)$ queremos encontrar k tal que $x \equiv (a+p^\alpha)^k \pmod{2p^\alpha}$

$\Updownarrow$ TCh R

$$\begin{cases} x \equiv (a+p^\alpha)^k \pmod 2 \\ x \equiv (a+p^\alpha)^k \pmod{p^\alpha} \end{cases}$$

Como a es r.p. mód p^α, $\exists k: x \equiv a^k \pmod{p^\alpha}$

$a+p^\alpha \equiv a \pmod{p^\alpha}$

$(a+p^\alpha)^k \equiv a^k \equiv x \pmod{p^\alpha}$

Para el k que encontramos.

$a + p^\alpha$ es impar $\Rightarrow (a+p^\alpha)^k$ es impar

a: par; p^α: impar

$\overline{x} \in U(2p^\alpha) \Rightarrow \text{mcd}(x, 2p^\alpha) = 1 \Rightarrow x$ es impar

$x \equiv (a+p^\alpha)^k \pmod 2$ ✓

Igual que en la parte anterior.

Probamos lo que queríamos.

d) Hallar una r.p. mód 162

$162 = 2 \cdot 3^4$

Si encontramos una r.p. mód 81, ya está, usamos la parte a) ó b)

Para hallar una r.p. mód 3^4, alcanza con hallar una r.p. mód $3^2 = 9$

Recordar: $\varphi(9) = 6$. $U(9) = \{\bar{1}, \bar{2}, \bar{4}, \bar{5}, \bar{7}, \bar{8}\}$

Probamos con potencias de 2.

$\bar{2}^1 = \bar{2}$, $\bar{2}^2 = \bar{4}$, $\bar{2}^3 = \bar{4}\,\bar{2} = \bar{8}$ $\Rightarrow o(\bar{2}) > 3$

$*_{\bar{1}}$ $*_{\bar{1}}$ $*_{\bar{1}}$

como $o(\bar{2}) \mid 6 = |U(9)|$

$\Rightarrow o(\bar{2}) = 6 \Rightarrow \langle \bar{2} \rangle = U(9)$

Si no me acuerdo de este argumento, como 6 es chico hago hasta $\bar{2}^6$

Recién probamos que 2 es r.p mód $9=3^2$

Por el teorema visto en teórico, 2 es rp mód 3^k $\forall k \geq 2$

$\Rightarrow$ 2 es r.p. mód 3^4

Ahora, como 2 es par, usamos la parte b)

$2+3^4$ es rp de $2 \cdot 34$

83 es r.p. de 162