$$Cop(n) = \{ i < n : mcd(i,n) = 1 \}$$

$$\varphi(n) = \#Cop(n)$$

Enumeramos los elementos $i_1, i_2, \ldots, i_{\varphi(n)}$

sea a: $mcd(a,n) = 1$

Probar que los restos de dividir

$a i_1, a i_2, \ldots, a i_{\varphi(n)}$ entre n,

son $i_1, i_2, \ldots, i_{\varphi(n)}$ en algún orden.

Para empezar

Si $ai_j \equiv ai_k \pmod m$,

como a es coprimo con m, es invertible mód m, se puede "cancelar"

$\Rightarrow i_j \equiv i_k \pmod m \Rightarrow i_j = i_k$ (los dos son menores que m)

Entonces los restos de $ai_1, ai_2 \dots, ai_{\varphi(m)}$ al dividir entre m, son todos distintos

Falta ver que $\forall j$, el resto de (resto$(ai_j, m) \in Cop(m)$) dividir ai_j entre m es coprimo con m

$$\left.\begin{array}{l} mcd(a, m) = 1 \\ mcd(i_j, m) = 1 \end{array}\right\} \Rightarrow mcd(a\,i_j, m) = 1$$

(por ejemplo, porque ni a ni i_j tienen factores primos en comun con m, entonces el producto entre ellos tampoco)

Dividimos $a\,i_j$ entre m por el razonamiento del alg. de Euclides

$$a\,i_j = q\,m + r$$

$$mcd(a\,i_j, m) = mcd(m, r)$$

$$\| \quad , \text{entonces } mcd(m, r) = 1$$

$$1 \quad , \text{entonces } r \in Cop(m)$$

Como $res(a_{i_1}, m), res(a_{i_2}, m), \dots res(a_{i_{\varphi(m)}}, m)$

son menores que m y coprimos con m,
son elementos de $Cop(m)$.

Como son todos distintos entre sí,
son $\varphi(m)$ elementos,

entonces son todos los elementos
de $Cop(m)$ (en algún orden)

Sea n compuesto tal que $\varphi(n) \mid n-1$

Probar que n es libre de cuadrados e impar

Escribimos n como producto de primos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right) \quad \Big| \quad n-1$$

lo pueb expresar descompuesto

"

$$\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

hacer cuentas. $1 - \frac{1}{p_i} = \frac{(p_i - 1)}{p_i}$

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ $\quad \alpha_i \geq 1$

$\varphi(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot \frac{(p_1 - 1)}{p_1} \cdot \frac{(p_2 - 1)}{p_2} \cdots \frac{(p_k - 1)}{p_k}$

(cancelo) ≥ 0

$= p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1)(p_2 - 1) \cdots (p_k - 1)$

todo este producto divide a $n - 1$

¿Qué quiere decir que n sea libre de cuadrados, en términos de $p_1, \dots, p_k, \alpha_1, \dots, \alpha_k$?

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ es libre de cuadrados si todos los $\alpha_i = 1$

($p_1, \dots, p_k$ son primos que aparecen)

Consideremos el primo p_i. $p_i \mid n \Rightarrow p_i \nmid n-1$

$\Rightarrow p_i^{\alpha_i - 1} = 1 = p_i^0$ (si no, es absurdo)

$\Rightarrow \alpha_i - 1 = 0 \Rightarrow \alpha_i = 1$

Como esto vale $\forall i$, $n = p_1^1 p_2^1 \cdots p_k^1$ es libre de cuadrados

¿Qué quiere decir que n sea impar?

n es impar $\Leftrightarrow$ 2 no está en la descomp. en f. primos de n

$\Leftrightarrow p_i \neq 2 \ \forall i$

Idea: Si p_i es impar, $p_i - 1$ es par, entonces $n-1$ es par

Como n es compuesto, $k \geq 2$, o sea alguno de los p_i es distinto de 2.

(Está 2 y al menos hay otro distinto) $\Rightarrow n-1$ es par $\Rightarrow$ n es impar

Probar que n es "pseudo primo de Carmichael" o sea $a^n \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$

$n = p_1 \cdots p_k$, $p_i \neq 2$

Queremos probar $a^n \equiv a \pmod{n}$ $\forall a \in \mathbb{Z}$

Por el TChR:

$$a^n \equiv a \pmod{n} \iff \begin{cases} a^n \equiv a \pmod{p_1} \\ a^n \equiv a \pmod{p_2} \\ \vdots \\ a^n \equiv a \pmod{p_k} \end{cases}$$

separo en casos según si $p_i \mid a$ o no...