Cuando queremos hallar r tal que $a^k \equiv r \pmod{n}$ nos puede resultar útil tener b tal que $a^b \equiv 1 \pmod{n}$.

Cuidado: para que exista el exponente b a debe ser invertible porque $a \cdot a^{b-1} \equiv 1 \pmod{1}$.

Teoremas de Euler y Fermat:

Def: $\varphi(n) = \#\{a \in \{1, \dots, n\} : mcd(a,n) = 1\}$ (es la cant. de coprimos con n menores a n)

Ejemplo: Si p es primo $\begin{cases} \varphi(p) = p-1 \\ \varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1) \end{cases}$

Si $mcd(m,n) = 1 \Rightarrow \varphi(m \cdot n) = \varphi(m)\varphi(n)$.

T. Euler: si $mcd(a,n) = 1 \Rightarrow \boxed{a^{\varphi(n)} \equiv 1 \pmod{n}}$

T. Fermat: p primo $\Rightarrow a^{p-1} \equiv 1 \pmod{p}$.
$a \not\equiv 0$.

Ejercicio 5. Cuando pedimos calcular $a \pmod{m}$ nos referimos a hallar el entero $0 \leq x < m$ tal que $a \equiv x \pmod{m}$, en particular $a^{-1} \pmod{m}$ denota al inverso de a módulo m. En los siguientes casos, calcular:

- **a.** los últimos dos dígitos de 7^{42} y de 23^{41};
- **b.** $2^{61} \pmod{77}$ y $13^{31} \pmod{77}$ (sug. en el último caso descomponer módulo 7 y módulo 11);
- **c.** $2^{-1} \pmod{55}$ y $2^{38} \pmod{55}$;
- **d.** $123^{253} \pmod{490}$ (sug. descomponer módulo 2, 5 y 49).

(a) Calcular los últimos dos dígitos es lo mismo que hallar r tal que

(1) $0 \leq r < 99$

(2) $7^{42} \equiv r \pmod{100}$

Sabemos que $\varphi(100) = \varphi(5^2) \cdot \varphi(2^2) = (25-5) \cdot (4-2) = 40$, por T. Euler si $mcd(a,100) = 1$ $a^{40} \equiv 1 \pmod{100}$.

Tomando $a = 7$: $7^{42} \equiv 7^{40} \cdot 7^2 \equiv 1 \cdot 7^2 \equiv 49 \pmod{100}$

Entonces $r = 49$ cumple (1) y (2), como queríamos.

(b) De nuevo usamos T. Euler:

$\varphi(77) = \varphi(7)\varphi(11) = 6 \cdot 10 = 60.$

Entonces $2^{61} \equiv 2^{60} \cdot 2 \pmod{77}$

$\equiv 2 \pmod{77}$

$13^{31} \equiv 13^{30} \cdot 13 \equiv 13^{60/2} \cdot 13$, como $13^{60} \equiv 1 \Rightarrow 13^{30} \equiv \pm 1$, pero hay que hallar el signo.

Entonces estudiamos la congruencia módulo 11 y 7.

$$* \begin{cases} 13^{31} \equiv (13^{10})^3 \cdot 13 \equiv 13 \pmod{11} & (\text{pues } 3^{10} \equiv 1 \pmod{11}) \\ 13^{31} \equiv (13^6)^5 \cdot 13 \equiv 13 \pmod{7} & (\text{pues } 3^6 \equiv 1 \pmod{7}) \end{cases}$$

Por el Teorema Chino 13 es solución de $*$, y todas las sols. son $13 \pmod{77}$.

Esto quiere decir que el signo es $+$, por lo tanto $13^{31} \equiv 13^{30} \cdot 13 \equiv +1 \cdot 13 \equiv 13 \ (77)$.

(c) Nosotros vimos que si el módulo es impar $\Rightarrow$ 2 es invertible y el inverso es $2^{-1} \equiv coc(m,2) + 1 \pmod{m}$. En este caso $2^{-1} \equiv coc(55,2) + 1 \equiv 27 + 1 \equiv 28 \ (55)$.

Para calcular 2^{38} usemos T. Euler y el inverso de 2:

$\varphi(55) = \varphi(5)\varphi(11) = 4 \cdot 10 = 40$

$2^{38} \equiv \underbrace{2^{40}}_{1} \cdot (2^{-1})^2 \equiv 1 \cdot (2^{-1})^2 \equiv 28^2 \equiv 14 \pmod{55}.$