Función de Euler

$$\varphi : \mathbb{Z}^+ \longrightarrow \mathbb{Z}^+$$

$$\varphi(n) = \#\{a \in \{1, \dots, n\} : \text{mcd}(a, n) = 1\}$$

= la cantidad de naturales menores que n y coprimos con n

* si p es primo: $\varphi(p) = p - 1$

* si $n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ $\quad p_1, \dots, p_k$ primos

$$\Rightarrow \varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

* Teorema de Euler:

sean $n, a \in \mathbb{Z}$ tq $\text{mcd}(n, a) = 1$ entonces

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ejercicio 5

a. Los últimos dos dígitos de 7^{42}

buscamos el resto de 7^{42} al dividir entre 100

$$7^{42} \equiv r \pmod{100} \quad \text{con } 0 \leq r \leq 99$$

$\text{mcd}(7, 100) = 1$ ⇒ podemos aplicar el teorema de Euler

$100 = 4 \cdot 25 = 2^2 \cdot 5^2$

$$\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 10 \cdot 4 = 40$$

entonces por el teorema de Euler:

$$7^{\varphi(100)} \equiv 1 \pmod{100}$$

$$7^{40} \equiv 1 \pmod{100}$$

$$\Rightarrow 7^{40} \cdot 7^2 \equiv 7^2 \pmod{100}$$

$$\Rightarrow 7^{42} \equiv 49 \pmod{100}$$

↑ los últimos dos dígitos de 7^{42} son 49

b. 2^{61} (mód 77) y 13^{31} (mód 77).

* resto de dividir 2^{61} entre 77

$$2^{61} \equiv r \pmod{77} \quad \text{donde} \quad 0 \leq r \leq 76$$

$\text{mcd}(2,77) = 1 \Rightarrow$ podemos aplicar el teorema de Euler

$77 = 7 \cdot 11$

$$\varphi(77) = 77\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right) = 77\ \frac{6}{7}\ \frac{10}{11} = 60$$

por el teorema de Euler:

$$2^{\varphi(77)} \equiv 1 \pmod{77}$$

$$2^{60} \equiv 1 \pmod{77}$$

$$\Rightarrow 2^{60} \cdot 2 \equiv 2 \pmod{77}$$

$$\Rightarrow 2^{61} \equiv 2 \pmod{77}$$

el resto de dividir 2^{61} entre 77 es 2.

* resto de dividir 13^{31} entre 77

$$13^{31} \equiv r \pmod{77} \quad \text{con} \quad 0 \leq r \leq 76$$

$\text{mcd}(13,77) = 1$, entonces podemos aplicar el teorema de Euler

$$13^{60} \equiv 1 \pmod{77}$$

$77 = 7 \cdot 11$

$$\left.\begin{array}{l} 13^{31} \equiv r \pmod{77} \\ 7 \mid 77 \end{array}\right] \Rightarrow 13^{31} \equiv r \pmod{7}$$

$$13^{31} \equiv r \pmod{77} \Rightarrow 13^{31} - r = 77k \text{ con } k \in \mathbb{Z}$$

$$\Rightarrow 13^{31} - r = 7(11k) \text{ con } k \in \mathbb{Z}$$

$$\Rightarrow 13^{31} \equiv r \pmod{7}$$

$$\left.\begin{array}{l} 13^{31} \equiv r \pmod{77} \\ 11 \mid 77 \end{array}\right\} \Rightarrow 13^{31} \equiv r \pmod{77}$$

$13^{31} \equiv r \pmod{77} \Rightarrow 13^{31} - r = 77k$ con $k \in \mathbb{Z}$

$\Rightarrow 13^{31} - r = 11(7k)$

$\Rightarrow 13^{31} \equiv r \pmod{11}$

$13^{31} \equiv r \pmod{77}$ $\Longleftrightarrow$ (por TCR) $\begin{cases} 13^{31} \equiv r \pmod{7} \\ 13^{31} \equiv r \pmod{11} \end{cases}$

porque $7 \mid 77$ y $11 \mid 77$

* $13^{31} \equiv r \pmod{7}$

$\text{mcd}(13, 7) = 1$ ⇝ podemos aplicar el teorema de Euler

$\varphi(7) = 6$

entonces por el teorema de Euler: $13^6 \equiv 1 \pmod{7}$

$31 = 6 \cdot 5 + 1$

$13^{31} = 13^{6 \cdot 5 + 1} = (13^6)^5 \cdot 13$

$13^{31} \equiv \underbrace{(13^6)^5}_{\equiv 1 \pmod{7}} \cdot 13 \pmod{7}$

$\Rightarrow 13^{31} \equiv 13 \pmod{7}$

$\Rightarrow \boxed{r \equiv 13 \pmod{7}}$

* $13^{31} \equiv r \pmod{11}$

$\text{mcd}(13, 11) = 1$ ⇝ podemos aplicar el teorema de Euler

$\varphi(11) = 10$

entonces por Euler: $13^{10} \equiv 1 \pmod{11}$

$31 = 10 \cdot 3 + 1$

$13^{31} = 13^{10 \cdot 3 + 1} = (13^{10})^3 \cdot 13$

$13^{31} \equiv \underbrace{(13^{10})^3}_{\equiv 1 \pmod{11}} \cdot 13 \pmod{11}$

$\Rightarrow 13^{31} \equiv 13 \pmod{11}$

$\Rightarrow \boxed{r \equiv 13 \pmod{11}}$

$$13^{31} \equiv r \pmod{77} \iff \begin{cases} 13^{31} \equiv r \pmod{7} \\ 13^{31} \equiv r \pmod{11} \end{cases} \iff \begin{cases} r \equiv 13 \pmod{7} \\ r \equiv 13 \pmod{11} \end{cases}$$

$$\iff r \equiv 13 \pmod{77}$$

el resto de dividir 13^{31} entre 77 es 13.

c) $2^{38} \pmod{55}$

buscamos r tal que $\begin{cases} 2^{38} \equiv r \pmod{55} \\ 0 \leq r < 54 \end{cases}$

$\text{mcd}(2, 55) = 1 \rightarrow$ podemos aplicar el teorema de Euler

$55 = 5 \cdot 11$

$\varphi(55) = 55\left(1 - \frac{1}{5}\right)\left(1 - \frac{1}{11}\right) = 55 \cdot \frac{4}{5} \cdot \frac{10}{11} = 40$

entonces por Euler: $2^{40} \equiv 1 \pmod{55}$

$2^{40} = 2^{38+2} = 2^{38} \cdot 2^2 = 2^{38} \cdot 4$

$2^{40} \equiv 1 \pmod{55}$

$\underbrace{2^{38}}_{\text{inverso de 4 modulo 55}} \cdot 4 \equiv 1 \pmod{55}$

→ vamos a calcular el inverso de 4 modulo 55 usando la igualdad de Bezout:

$$4 \cdot 14 + 55 \cdot (-1) = 1$$

$$4 \cdot 14 + \overbrace{55(-1)}^{\equiv 0 \pmod{55}} \equiv 1 \pmod{55}$$

$$4 \cdot 14 \equiv 1 \pmod{55}$$

↑ inverso de 4 modulo 55

entonces $2^{38} \equiv 14 \pmod{55}$

el resto de dividir 2^{38} entre 55 es 14.

d. 123^{253} (mód 490).

buscamos r tal que $\begin{cases} 123^{253} \equiv r \pmod{490} \\ 0 \leq r \leq 489 \end{cases}$

* 123 y 490 coprimos?

$490 = 49 \cdot 2 \cdot 5 = 2 \cdot 5 \cdot 7^2$

$2 \nmid 123$
$5 \nmid 123$
$7 \nmid 123$

$\Big\}$ $\text{mcd}(123, 490) = 1 \Rightarrow$ podemos aplicar Euler

$$\varphi(490) = 490\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right) = 490 \cdot \frac{1}{2} \cdot \frac{4}{5} \cdot \frac{6}{7} = 7 \cdot 4 \cdot 6 = 168$$

por Euler: $123^{168} \equiv 1 \pmod{490}$

*

$$123^{253} \equiv r \pmod{490} \xleftrightarrow{\text{TCR}} \begin{cases} 123^{253} \equiv r \pmod{2} \\ 123^{253} \equiv r \pmod{5} \\ 123^{253} \equiv r \pmod{49} \end{cases}$$

$2 \mid 490,\ 5 \mid 490$
$49 \mid 490$

* $123^{253} \equiv r \pmod{2}$

$123 \equiv 1 \pmod{2} \Rightarrow 123^{253} \equiv 1 \pmod{2}$

$\Big\} \Rightarrow \boxed{r \equiv 1 \pmod{2}}$

* $123^{253} \equiv r \pmod 5 \Rightarrow 3^{253} \equiv r \pmod 5$

$123 \equiv 3 \pmod 5$

$\text{mcd}(3,5) = 1 \Rightarrow$ podemos aplicar el teorema de Euler

$\varphi(5) = 4$

por Euler: $3^4 \equiv 1 \pmod 5$

$253 = 4 \cdot 63 + 1$

$3^{253} = 3^{4 \cdot 63 + 1} = (3^4)^{63} \cdot 3$

$3^{253} \equiv \underbrace{(3^4)^{63}}_{\equiv 1 \pmod 5} \cdot 3 \pmod 5$

$3^{253} \equiv 3 \pmod 5$

$\Rightarrow \boxed{r \equiv 3 \pmod 5}$

* $123^{253} \equiv r \pmod{49} \Rightarrow 25^{253} \equiv r \pmod{49}$

$123 \equiv 25 \pmod{49}$

$\text{mcd}(25, 49) = 1 \Rightarrow$ podemos aplicar el teorema de Euler

$49 = 7^2$

$\varphi(49) = 49\left(1 - \frac{1}{7}\right) = 49 \cdot \frac{6}{7} = 7 \cdot 6 = 42$

entonces por Euler: $25^{42} \equiv 1 \pmod{49}$

$253 = 42 \cdot 6 + 1$

$25^{253} = 25^{42 \cdot 6 + 1} = (25^{42})^6 \cdot 25$

$25^{253} \equiv \underbrace{(25^{42})^6}_{\equiv 1 \pmod{49}} \cdot 25 \pmod{49}$

$\equiv 25 \pmod{49}$

$\Rightarrow \boxed{r \equiv 25 \pmod{49}}$

$$\begin{cases} 123^{253} \equiv r \pmod 2 \\ 123^{253} \equiv r \pmod 5 \\ 123^{253} \equiv r \pmod{49} \end{cases} \iff \begin{cases} r \equiv 1 \pmod 2 \\ r \equiv 3 \pmod 5 \\ r \equiv 25 \pmod{49} \end{cases}$$

$r \equiv 1 \pmod 2 \iff r \equiv 3 \pmod 2$

$$\begin{cases} r \equiv 1 \pmod 2 \\ r \equiv 3 \pmod 5 \end{cases} \iff r \equiv 3 \pmod{2 \cdot 5}$$

↑ 3 es solución particular

Vamos a resolver:

$$\begin{cases} r \equiv 3 \pmod{10} \\ r \equiv 25 \pmod{49} \end{cases}$$

* buscamos inverso de 10 modulo 49 y el inverso de 49 modulo 10

$10 \cdot 5 + 49(-1) = 1$ igualdad de Bezout

módulo 10: $5 \cdot 10 + 49(-1) \equiv 1 \pmod{10}$

$\boxed{49(-1) \equiv 1 \pmod{10}}$

módulo 49: $5 \cdot 10 + 49(-1) \equiv 1 \pmod{49}$

$\boxed{5 \cdot 10 \equiv 1 \pmod{49}}$

* solución particular

$x_0 = \underbrace{3 \cdot 49(-1)}_{\equiv 0 \pmod{49}} + \underbrace{25 \cdot 5 \cdot 10}_{\equiv 25 \pmod{49}} \equiv 25 \pmod{49}$

$\equiv 3 \pmod{10}$ $\quad \equiv 5 \pmod{10}$

$x_0 = 3 \cdot 49(-1) + 25 \cdot 5 \cdot 10 = 1103$

$$\begin{cases} r \equiv 3 \pmod{10} \\ r \equiv 25 \pmod{49} \end{cases} \iff r \equiv 1103 \pmod{490}$$

$r \equiv 123 \pmod{490}$

↑ resto