

Exponenciación modular

La **exponenciación modular** es un tipo de exponenciación realizada en un módulo específico. Esta se utiliza especialmente en el campo de la criptografía.

El objetivo es calcular el residuo de un número entero positivo b (la base) que se eleva a la e -ésima potencia (el exponente) al ser dividido por un entero positivo n (el módulo)


Ejemplo 1. Calcule el residuo de 5^6 al ser dividido por 13.

🚫 Evitamos calcular la potencia.

La exponenciación modular basa su funcionamiento en la *elevación sucesiva al cuadrado* de la base.


Primero, escribimos la representación binaria del exponente: $6 = (110)_2$.

Luego construimos la siguiente tabla:

		Bin.	b^{2^n}	$b^{2^n} \pmod{13}$
 Escribimos la representación binaria del exponente desde el dígito menos significativo	$n=0$	0	5^1	5
	$n=1$	1	5^2	$5^2 = 12$
	$n=2$	1	$5^4 \equiv 12^2$	$5^4 \equiv 1$

⚠️ Luego de cada exponenciación se calcula el residuo mod m

Finalmente, $5^6 = 5^4 \cdot 5^2 \equiv 1 \cdot 12 \equiv 12 \pmod{13}$

 Podemos verificar el resultado al calcular 5^6 (porque es un número *pequeño*) y determinar el residuo al dividir por 13.

$$5^6 = 15625 = 1201 \cdot 13 + 12$$

Ejemplo 2. Calcule el residuo de 7^{45} al ser dividido por 17.

Si calculamos 7^{45} en una calculadora obtenemos: $1.07006904 \times 10^{38}$.

[Extended Keyboard](#)
[Upload](#)
[Examples](#)
[Random](#)

Input:

 7^{45}

Result:

 $107006904423598033356356300384937784807$

Scientific notation:

 $1.07006904423598033356356300384937784807 \times 10^{38}$

Number names:

[Full name](#)

107 undecillion ...

107 billion billion billion billion ...

Number length:

39 decimal digits

Vemos que hay 8 dígitos después del punto, eso quiere decir que la calculadora *perdió* 30 dígitos de información (los que están tachados de rojo).

Primero escribimos la representación binaria del exponente: $45 = (101101)_2$

Luego construimos la tabla:

	Bin.	7^{2^n}	$7^{2^n} \pmod{17}$	
$n=0$	1	7	7 ✓	
$n=1$	0	7^2	15 ✗	$49 = 2 \cdot 17 + 15$
$n=2$	1	$7^4 \equiv 15^2$	4 ✓	$225 = 13 \cdot 17 + 4$
$n=3$	1	$7^8 \equiv 4^2$	16 ✓	
$n=4$	0	$7^{16} \equiv 16^2$	1 ✗	$256 = 15 \cdot 17 + 1$
$n=5$	1	$7^{32} \equiv 1^2$	1 ✓	

Finalmente $7^{45} = 7^{32} \cdot 7^8 \cdot 7^4 \cdot 7^1 \equiv 1 \cdot 16 \cdot 4 \cdot 7 \equiv 16 \cdot 11 \equiv 6 \pmod{17}$