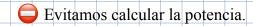
Exponenciación modular

La **expoenenciación 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)

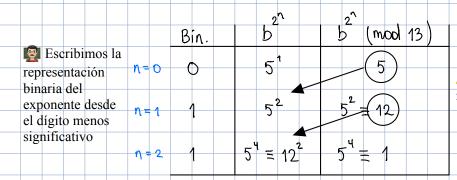
Ejemplo 1. Calcule el residuo de 56 al ser dividido por 13.



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:



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 5⁶ (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 7⁴⁵ al ser dividido por 17.

Si calculamos 7⁴⁵ en una calculadora obtenemos: 1.07006904×10³⁸.



