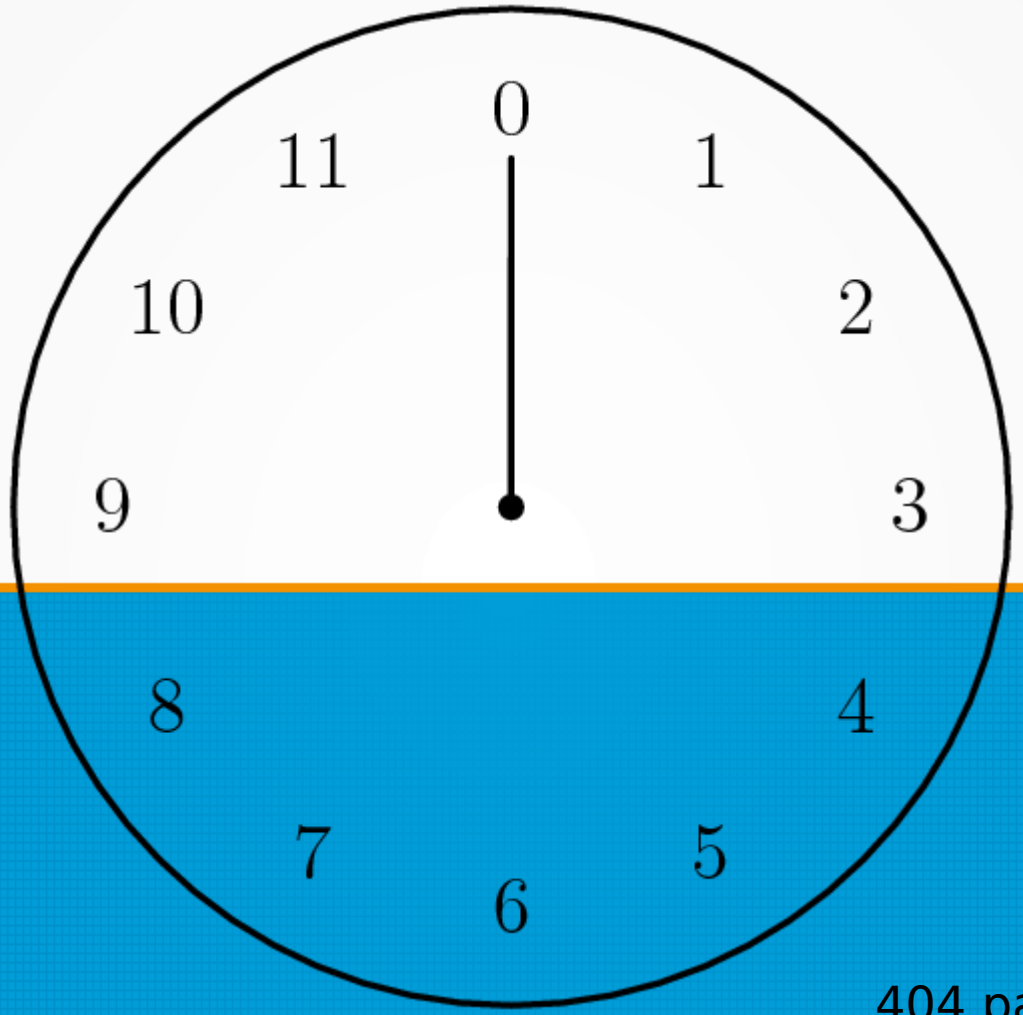
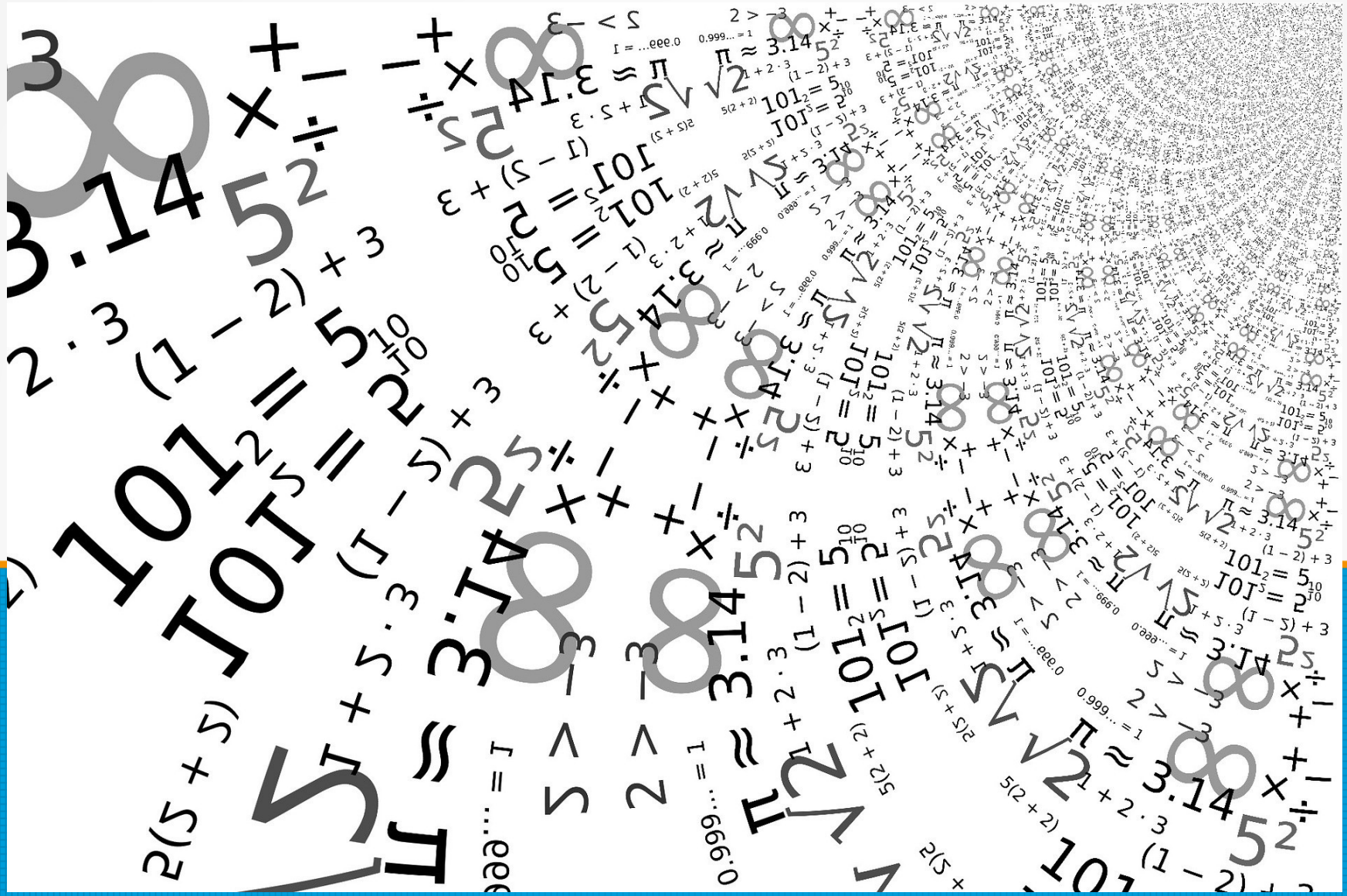
Sesión 21 (Z)
Aritmética modular



404 pasos hacia adelante

Motivación



El módulo

R = A mod B

En algunos lenguajes de programación:

R = A % B

$$\frac{A}{B} = Q \text{ residuo } R.$$

A es el dividendo

B es el divisor

Q es el cociente

R es el residuo

Visualización (1/2)

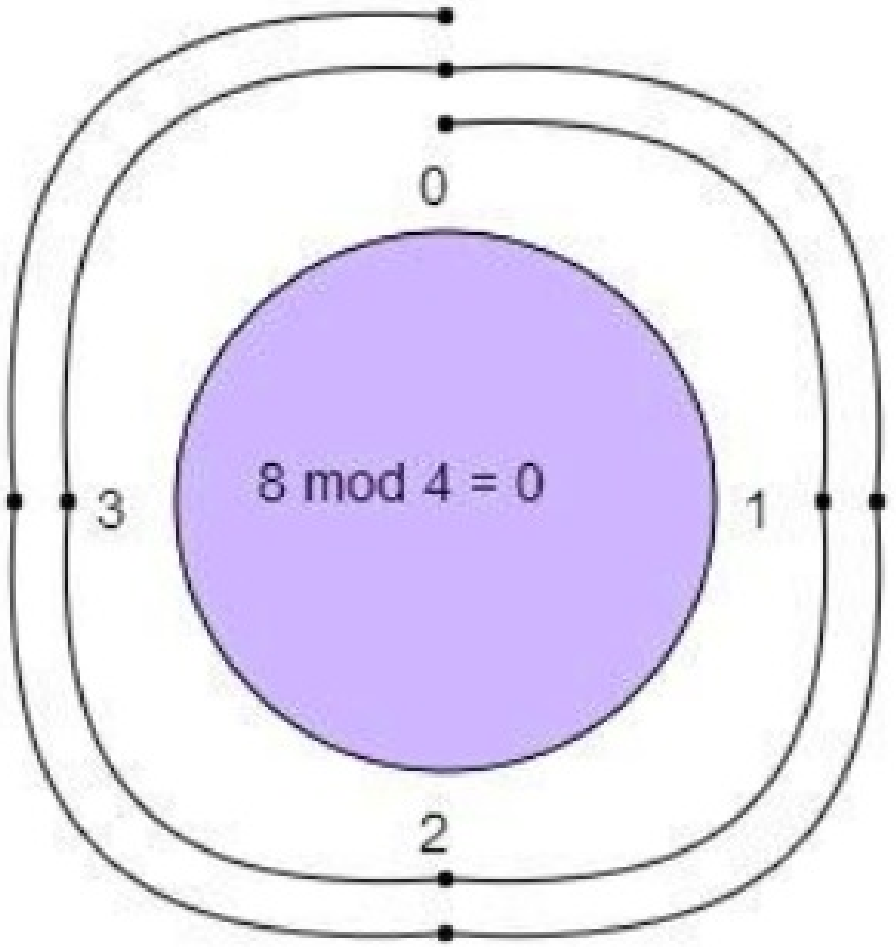
$$\frac{0}{3} = 0 \text{ residuo } \mathbf{0}$$
$$\frac{1}{3} = 0 \text{ residuo } \mathbf{1}$$
$$\frac{2}{3} = 0 \text{ residuo } \mathbf{2}$$
$$\frac{3}{3} = 1 \text{ residuo } \mathbf{0}$$
$$\frac{4}{3} = 1 \text{ residuo } \mathbf{1}$$
$$\frac{5}{3} = 1 \text{ residuo } \mathbf{2}$$
$$\frac{6}{3} = 2 \text{ residuo } \mathbf{0}$$

X / 3 = Q residuo R

Visualización (2/2)

8 mod 4 = ?

Practicar



Congruencia módulo

Puede que veas una expresión como:

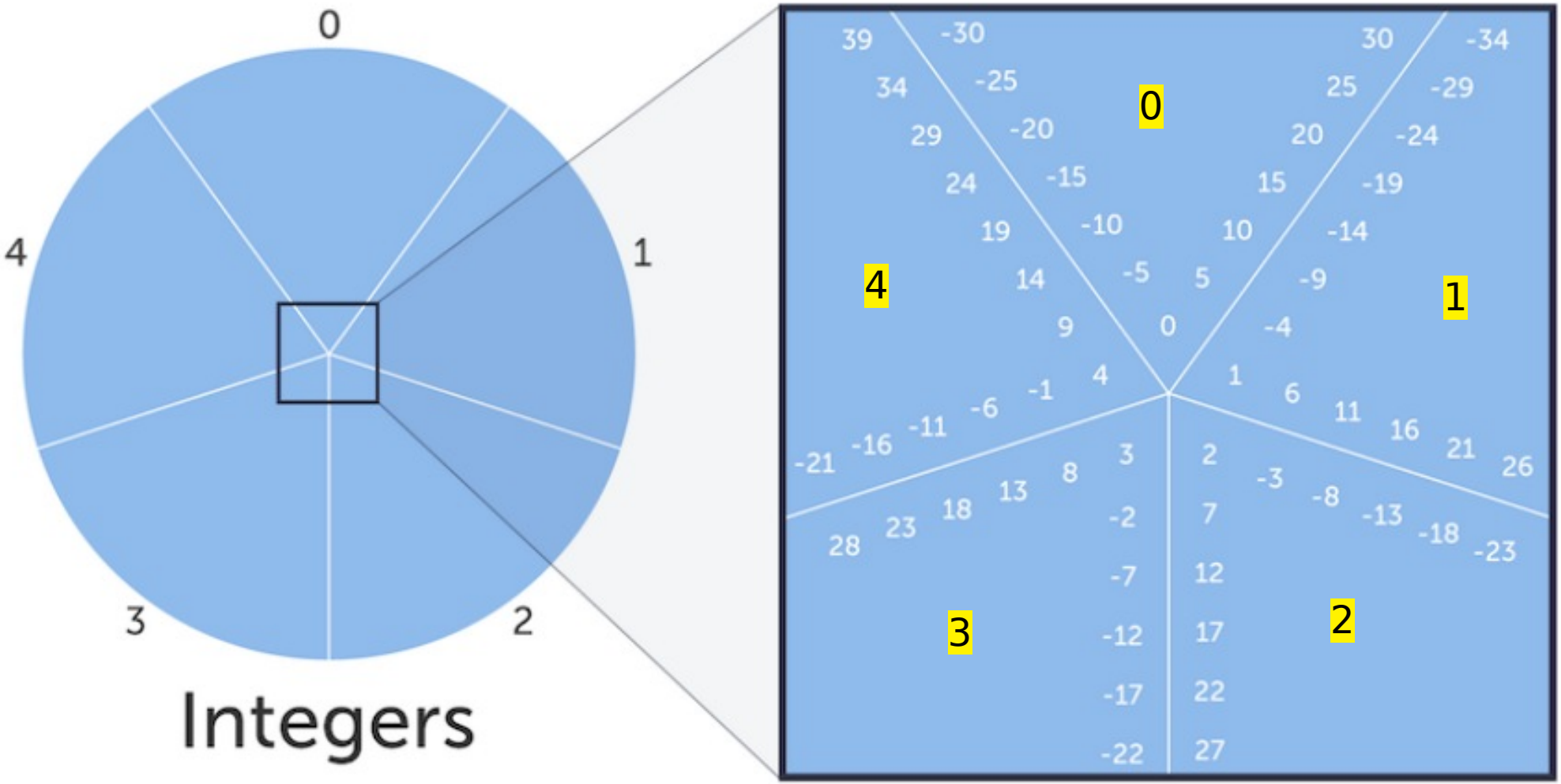
$$A \equiv B \pmod{C}.$$

Esto dice que A es congruente con B módulo C.

Congruencia módulo

Práctica

Imaginemos que estamos calculando mod 5 para todos los enteros:



Suma y resta modular (1/2)

$$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$$

Ejemplo:

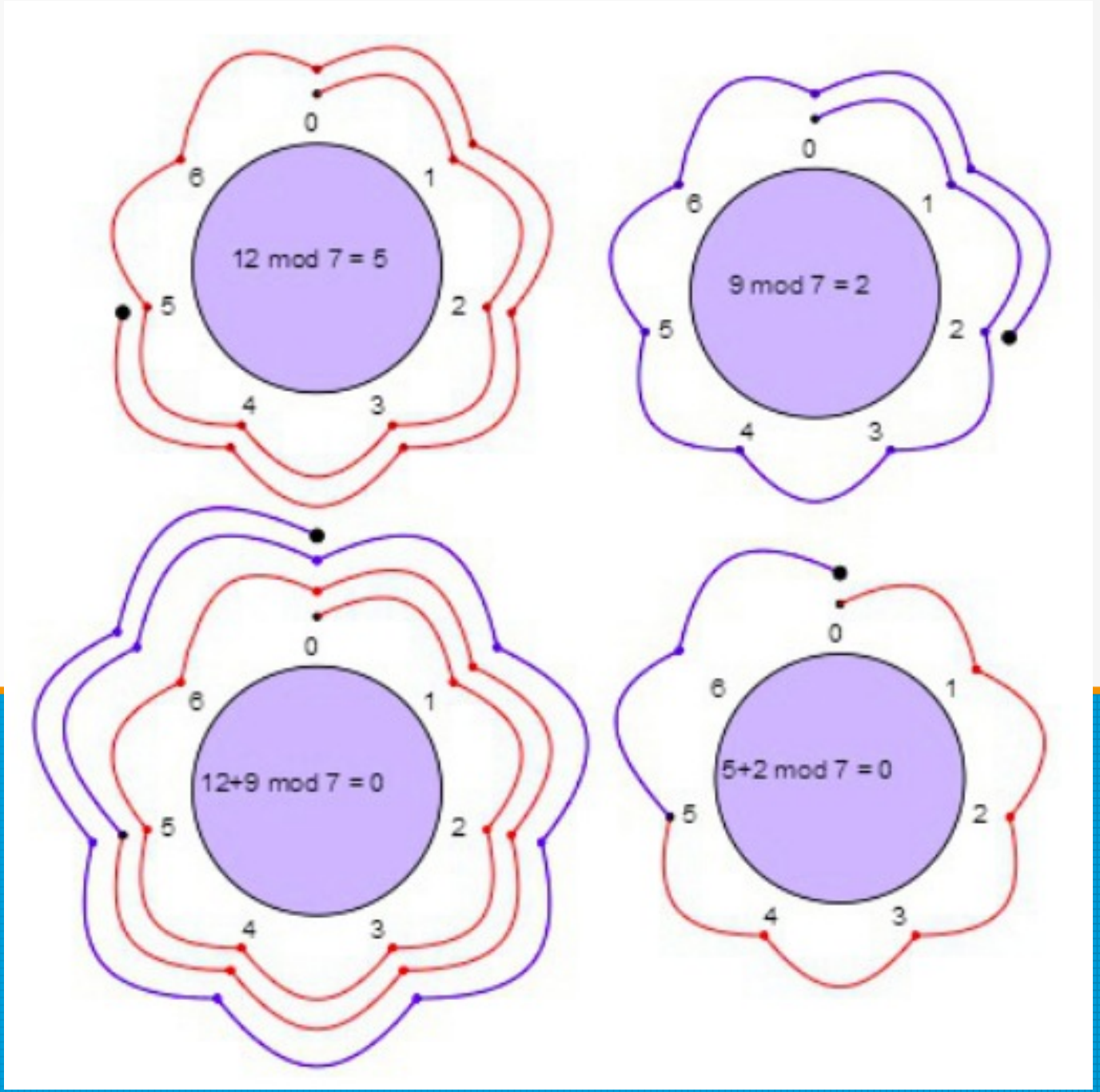
$(12 + 9) \bmod 7 = 0$

Es igual a:

$((12 \bmod 7) + (9 \bmod 7)) \bmod 7 =$
$(5 + 2) \bmod 7 = 0$

Suma y resta modular (1/2)

Practicar



Multiplicación modular

$$(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$$

Ejemplo:

(4 * 9) mod 7 = (36) mod 7 = 1

Es igual a:

((4 mod 7) * (9 mod 7)) mod 7 =
(4 * 2) mod 7 =
8 mod 7 = 1

Resolver – Factoriales extremos (OmegaUp)