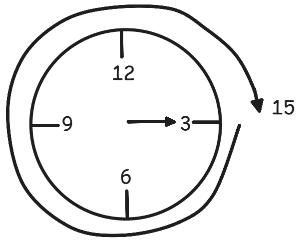
3 - Modular arithmetic

Clock points the same way at these hours:

$$-9 \equiv 3 \equiv 15 \equiv 27 \pmod{12}$$



Definition. For integers n, a, b with n≠0, we write

$$a \equiv b \pmod{n},$$

read "a is congruent to b mod n", if n divides a-b or equivalently, a÷n and b÷n give the same remainder.

Example 1. $17 \equiv 5 \pmod{3}$ because 17–5 = 12 = 3 x 4 is a multiple of 3.
$15 \not\equiv 2 \pmod{3}$ because 3 does not divide 15–2 = 13.
$32 \equiv 21 \equiv 10 \equiv -1 \equiv -12 \equiv -23 \pmod{11}$

Example 2. All even numbers are $\equiv 0 \pmod{2}$
All odd numbers are $\equiv 1 \pmod{2}$

Example 3. My birthday is Tuesday in 2026 and ??? in 2027.

Answer. Say Sunday = 0, Monday = 1, ..., Saturday = 6. Then:

$$\underset{\text{(in 2026)}}{\text{Tuesday}} + 365 = 2 + 365 = 367 = \underbrace{350 + 14 +}_{\text{divisible by 7}} 3 \equiv 3 \pmod{7} = \underset{\text{(in 2027)}}{\text{Wednesday.}}$$

Theorem. $$\begin{cases} x \equiv a \\ y \equiv b \end{cases} \pmod{n} \quad \Rightarrow \quad \begin{cases} x + y \equiv a + b \\ xy \equiv ab \end{cases} \pmod{n}$$

Why? Know a and b are the remainders of some division of $x \div n$ and $y \div n$:

$$x = j \cdot n + a$$
$$y = k \cdot n + b$$

Add these two equations. We get:

$$x + y = \underbrace{(j+k)}_{\text{quotient of } (x+y)\div n} \cdot n + \underbrace{(a+b)}_{\text{remainder of } (x+y)\div n}$$

So $x+y \equiv a+b \pmod{n}$. Similar computation shows $xy \equiv ab \pmod{n}$.

Example 4. Find the remainder of N÷M if:

(a) M = 11, N = $10^2 + 111 \times 12 \equiv (-1)^2 + 1 \times 1 = 2 \pmod{11}$

(b) M = 3, N = 1234

(c) M = 11, N = 1234

Answer (b): $$\begin{aligned} 1234 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \\ &\equiv 1 \cdot (1)^3 + 2 \cdot (1)^2 + 3 \cdot (1) + 4 \pmod{3} \\ &\equiv 1 + 2 + 3 + 4 \equiv 10 \equiv 1 \pmod{3}. \end{aligned}$$

Answer (c): $$\begin{aligned} 1234 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 3 \cdot 10 + 4 \\ &\equiv 1 \cdot (-1)^3 + 2 \cdot (-1)^2 + 3 \cdot (-1) + 4 \pmod{11} \\ &\equiv 1 - 2 - 3 + 4 \equiv 2 \pmod{11}. \end{aligned}$$