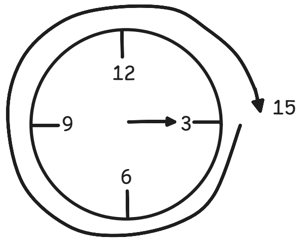
3 - Modular arithmetic

Clock points the same way at these hours:

-9 ≡ 3 ≡ 15 ≡ 27 (mod 12)



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

a ≡ b (mod 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 ≡ 5 (mod 3) because 17−5 = 12 = 3 x 4 is a multiple of 3.
15 ≢ 2 (mod 3) because 3 does not divide 15−2 = 13.
32 ≡ 21 ≡ 10 ≡ -1 ≡ -12 ≡ -23 (mod 11)

Example 2. All even numbers are ≡ 0 (mod 2)
All odd numbers are ≡ 1 (mod 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 ≡ a+b (mod n). Similar computation shows xy ≡ ab (mod n).

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

(a) M = 11, N = 10^2 + 111 x 12 ≡ $(-1)^2$ + 1 x 1 = 2 (mod 11)

(b) M = 3, N = 1234

(c) M = 11, N = 1234

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

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

Divisibility Rules.

- N÷3 has remainder ≡ the sum of the digits of N (mod 3).
- N÷9 has remainder ≡ the sum of the digits of N (mod 9).
- N÷11 has remainder ≡ the reversed alternating sum of the digits of N (mod 11).

In-class exercises. Without a calculator, find the remainder of N÷M if:

1. (a) N = 24680, M = 11 ... 24680 ≡ 2-4+6-8+0 ≡ -4 ≡ 7 (mod 11)

   (b) N = 35 x 16 + 180, M = 17 ... 35 x 16 + 180 ≡ 1 x (-1) + 10 ≡ 9 (mod 17)

   (c) N = 6! = 6·5·4·3·2·1, M = 7 ... 6·(-1)·(-2)·(3·2) ≡ 6·2·6 ≡ (-1)·2·(-1) ≡ 2 (mod 7)

   (d) N = 123456789, M = 101

   (e) N = 111111_2 (binary), M = 3

2. Find gcd(123456, 33) by hand.

Application: error correcting code.

UPC (Universal product code) is a 12-digit code, the last digit is a check digit that checks if the cashier typed the previous digits correctly. The digits satisfy the congruence relation:

$$x_1 + x_3 + x_5 + x_7 + x_9 + x_{11} \equiv 3(x_2 + x_4 + x_6 + x_8 + x_{10} + x_{12}) \pmod{10}$$

Example 5. Check the bar code shown above is valid:

$$0+6+0+2+1+5 \stackrel{?}{\equiv} 3(3+0+0+9+4+2) \pmod{10}$$
$$14 \stackrel{?}{\equiv} 3(18) \pmod{10} \quad \Rightarrow \quad \text{Yes.}$$

Example 6. Find the missing last digit of the UPC code (right).

$$0+7+0+0+0+1 \equiv 3(3+0+0+0+0+x_{12}) \pmod{10}$$
$$8 \equiv 9 + 3x_{12} \pmod{10}$$
$$-1 \equiv 3x_{12} \pmod{10} \quad \Rightarrow \quad x_{12} = 3$$

Example 7. Is 1234567 a square number? What about 2615441?

Square numbers end in digits 0,1,4,5,6,9 only so 1234567 is not a square. Checking units digit is the same as computing mod 10. To see 2615441 is not a square, work mod 3: $n^2 \bmod 3$ can only be $0^2 \equiv 0 \pmod 3$, $1^2 \equiv 1 \pmod 3$, or $2^2 \equiv 1 \pmod 3$ but 1234567≡1+2+3+4+5+6+7≡2 (mod 3) so 2615441 is not a square.