# Modular arithmetic and division

## Quotient-remainder theorem

Given positive integers $a$ and $d$, there exist unique integers $q$ (the **quotient**) and $r$ (the **remainder**) such that:

$$a = dq + r, \qquad 0 \leq r < d$$

$q = a$ **div** $d$ the integer quotient (whole part of $a \div d$)

$r = a$ **mod** $d$ the non-negative remainder

Example: $a = 30$, $d = 7$: $30 = 7(4) + 2$, so $30$ **div** $7 = 4$ and $30$ **mod** $7 = 2$.

## Five equivalent statements

For integers $a$, $q$, $r$, and $d > 0$, the following are all equivalent:

1. $a = dq + r$
2. $a \equiv r \pmod{d}$
3. $a \bmod d = r \bmod d$
4. $d \mid (a - r)$
5. $a$ and $r$ have the same non-negative remainder when divided by $d$

## Congruence

$a \equiv b \pmod{n}$ means $a$ and $b$ have the same remainder when divided by $n$ (equivalently, $n \mid (a - b)$).

Examples: $30 \equiv 2 \pmod{7}$, $9 \equiv 1 \pmod{2}$, $21 \equiv 5 \pmod{8}$, $-8 \equiv 2 \pmod{5}$

Note: Remainders are always **non-negative**. For negatives: $-8 = -2(5) + 2$, so $-8 \bmod 5 = 2$.

## Greatest common divisor and the Euclidean algorithm

The **GCD** of integers $a$ and $b$ is the largest integer that divides both. Use the Euclidean algorithm, based on two lemmas:

1. $\gcd(r, 0) = r$
2. If $a = dq + r$, then $\gcd(a, d) = \gcd(d, r)$

Repeatedly replace the larger number with the remainder until the remainder is 0.

Example: Find $\gcd(408, 120)$.

**Student Learning Support, Teaching and Learning Centre**
studentlearning@ontariotechu.ca
ontariotechu.ca/studentlearning

OntarioTech UNIVERSITY

| Reduction | Division step |
|---|---|
| $\gcd(408, 120)$ | $408 = 3 \times 120 + 48$ |
| $= \gcd(120, 48)$ | $120 = 2 \times 48 + 24$ |
| $= \gcd(48, 24)$ | $48 = 2 \times 24 + 0$ |
| $= \gcd(24, 0) = \mathbf{24}$ | |

Practice: Find $\gcd(5280, 1360)$ using the Euclidean algorithm. *Answer:* 80

## Modular arithmetic properties

Let $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then:

1. $ab \equiv \big[(a \bmod n)(b \bmod n)\big] \bmod n$
2. $(a + b) \equiv (c + d) \pmod{n}$
3. $a^k \equiv c^k \pmod{n}$ for all integers $k$
4. $a^k \bmod n = (a \bmod n)^k \bmod n$

**Fermat's Little Theorem:** If $p$ is prime and $p \nmid a$, then

$$\boxed{a^{p-1} \equiv 1 \pmod{p}}$$

This is powerful for reducing large exponents: since $a^{p-1} \equiv 1$, write the exponent in terms of $p - 1$ and cancel.

Tip: To compute $a \bmod n$ on a calculator:

$$a \bmod n = a - n \left\lfloor \frac{a}{n} \right\rfloor$$

Example: $103 \bmod 12 = 103 - 12 \left\lfloor \frac{103}{12} \right\rfloor = 103 - 12(8) = 103 - 96 = 7$

## Worked examples

Example 1: Compute $(3 - 20) \bmod 5$.

**Solution:** $3 \bmod 5 = 3$ and $20 \bmod 5 = 0$, so $(3 - 20) \bmod 5 = 3 - 0 = 3$.

*Check:* $-17 = -4(5) + 3$, confirming the remainder is 3. □

Example 2: Compute $(12 + 8) \bmod 5$.

**Solution:** $12 \bmod 5 = 2$ and $8 \bmod 5 = 3$, so $(12 + 8) \bmod 5 \equiv (2 + 3) \bmod 5 = 0$. □

Example 3: Find $26^{25} \bmod 4$.

**Solution:** First reduce the base: $26 \bmod 4 = 2$, so $26^{25} \equiv 2^{25} \pmod{4}$.

Since $2^2 = 4 \equiv 0 \pmod{4}$, any power $2^k$ with $k \geq 2$ satisfies $2^k \equiv 0 \pmod{4}$.

$$26^{25} \equiv 2^{25} \equiv 0 \pmod{4}$$

□

Example 4 (Fermat's Little Theorem): Find $4^{17}$ mod $11$.

**Solution:** Since 11 is prime and $11 \nmid 4$, Fermat gives $4^{10} \equiv 1 \pmod{11}$. Write the exponent as $17 = 10 + 7$:

$$4^{17} = 4^{10} \cdot 4^7 \equiv 1 \cdot 4^7 \pmod{11}$$

Now reduce $4^7$. Note $4^2 = 16 \equiv 5 \pmod{11}$, so:

$$4^7 = 4^2 \cdot 4^2 \cdot 4^2 \cdot 4 \equiv 5 \cdot 5 \cdot 5 \cdot 4 = 125 \cdot 4 \pmod{11}$$

Since $125 = 11(11) + 4$, we have $125 \equiv 4 \pmod{11}$, giving:

$$4^{17} \equiv 4 \cdot 4 = 16 \equiv 5 \pmod{11}$$

□

Practice: Show that $3^{26}$ mod $5 = 4$. *Hint: use Fermat with* $p = 5$.