# Modular Arithmetic, Floor & the Quotient-Remainder Theorem

## Table of contents



### Floor and ceiling

For a real number $x$:

- $\lfloor x \rfloor$ — the **floor**: move **left** on the number line to the nearest integer.
- $\lceil x \rceil$ — the **ceiling**: move **right** on the number line to the nearest integer.

So $\lfloor -3.2 \rfloor = -4$ and $\lceil -3.2 \rceil = -3$; $\lfloor 3.2 \rfloor = 3$ and $\lceil 3.2 \rceil = 4$. **Negative numbers are where this goes wrong most often** — floor of $-3.2$ is $-4$, not $-3$.

To use floor or ceiling in a proof, it is usually easiest to rewrite the expression as **an integer plus an amount between 0 and 1**. For instance, in proving "if $n$ is an odd integer then $\lceil \frac{n}{2} \rceil = \lfloor \frac{n}{2} \rfloor + 1$", write

$$\frac{n}{2} = \frac{2k+1}{2} = k + \frac{1}{2}$$

for some integer $k$; then $k + \frac{1}{2}$ sits strictly between $k$ and $k+1$, so the floor is $k$ and the ceiling is $k+1$. The same move handles things like $\lfloor (p^3 + 4p^2 + 5) + \frac{1}{4} \rfloor$ where $p \in \mathbb{Z}$.

Two ways to compute $\lfloor \frac{-32}{5} \rfloor$:

- *Fraction approach*: $\lfloor \frac{-32}{5} \rfloor = \lfloor \frac{-30}{5} - \frac{2}{5} \rfloor = \lfloor -6 - \frac{2}{5} \rfloor = -7$ (something smaller than $-6$).
- *Decimal approach*: $\lfloor -6.4 \rfloor = \lfloor -6 - 0.4 \rfloor = -7$.

And $\lceil \frac{-32}{5} \rceil = -6$.

$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$ **is false** — take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$.

## The quotient-remainder theorem

Given any integer $n$ and positive integer $d$, there exist **unique** integers $q$ and $r$ such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

$q$ is the **quotient** ($n \operatorname{div} d$) and $r$ is the **remainder** ($n \bmod d$). Explicitly:

$$q = \left\lfloor \frac{n}{d} \right\rfloor \qquad r = n - d \left\lfloor \frac{n}{d} \right\rfloor$$

With $d = 6$:

| $n$ | $n = dq + r$ | $q$ | $r$ |
|---|---|---|---|
| 53 | $6 \cdot 8 + 5$ | 8 | 5 |
| 20 | $6 \cdot 3 + 2$ | 3 | 2 |
| $-19$ | $6 \cdot (-4) + 5$ | $-4$ | 5 |

**Negative $n$ is the case to watch**: the remainder is still required to be non-negative, so $-19 \bmod 6 = 5$, not $-1$. Likewise $-95 = 11(-9) + 4$, so $-95 \operatorname{div} 11 = -9$ and $-95 \bmod 11 = 4$. And $58 = 11 \cdot 5 + 3$, so $58 \operatorname{div} 11 = 5$, $58 \bmod 11 = 3$.

## mod versus $\equiv$ — take care with notation

These are different statements and the difference is examinable.

- $n \bmod d = r$ — an *equality between numbers*: the remainder when $n$ is divided by $d$ is $r$, with $0 \leq r < d$.
- $m \equiv n \pmod{d}$ — a *relation between $m$ and $n$*: they leave the same remainder when divided by $d$.

Example: $5 \bmod 4 = 1$ and $9 \bmod 4 = 1$, so $9 \equiv 5 \pmod 4$ — but $9 \bmod 4 \neq 5$.

### Two equivalent definitions of congruence

For $m, n, d \in \mathbb{Z}$ with $d > 0$:

- **Definition 1**: $m \equiv n \pmod{d}$ iff $m$ and $n$ have the same remainder under the quotient-remainder theorem.
- **Definition 2**: $m \equiv n \pmod{d}$ iff $d \mid (m - n)$.

Definition 2 is usually the faster one to check, and the one to reach for in proofs (see divisibility-and-factorisation[1]).

Worked both ways — is $-50 \equiv 22 \pmod{8}$?

- *Definition 1*: $-50 = -56 + 6 = 8(-7) + 6$, so $-50 \bmod 8 = 6$; and $22 = 16 + 6$, so $22 \bmod 8 = 6$. Same remainder, so yes.
- *Definition 2*: $22 - (-50) = 72 = 8 \cdot 9$, so $8 \mid (22 - (-50))$, so yes.

Similarly $53 \equiv -19 \pmod{6}$ (both leave remainder 5; and $53 - (-19) = 72$ is divisible by 6), while $53 \not\equiv 20 \pmod{6}$.

## Arithmetic with congruences

**Lemma**: if $a \equiv b \pmod{d}$ and $m \equiv n \pmod{d}$, then

$$a + m \equiv b + n \pmod{d} \qquad \text{and} \qquad am \equiv bn \pmod{d}$$

That is, you may substitute any number for a congruent one *before* adding or multiplying — which is what makes modular arithmetic cheap.

For example, $8 \equiv 2 \pmod{3}$ and $46 \equiv 1 \pmod{3}$, so $8 \cdot 46 \equiv 2 \cdot 1 \equiv 2 \pmod{3}$ and $8 + 46 \equiv 2 + 1 \equiv 0 \pmod{3}$.

**Worked**: suppose $x \bmod 6 = 4$ and $y \bmod 6 = 3$.

- $(x + y) \bmod 6$: $x + y \equiv 4 + 3 \equiv 7 \equiv 1 \pmod{6}$, so the answer is 1.
- $(5x^2 + 4y) \bmod 6$: $5x^2 + 4y \equiv 5(4)^2 + 4(3) \equiv 5(16) + 12 \equiv 5(4) \equiv 20 \equiv 2 \pmod{6}$ — applying the lemma at each step.

**Worked**: if $m \bmod 6 = 4$, what is $35m \bmod 6$? Since $35 \bmod 6 = 5$, $35m \equiv 5 \cdot 4 \equiv 20 \equiv 2 \pmod{6}$. And $3m^2 + 2m + 1 \equiv 3(16) + 8 + 1 \equiv 48 + 9 \equiv 0 + 9 \equiv 3 \pmod{6}$.

**Worked**: an integer $n$ leaves remainder 4 on division by 7 — what is the remainder of $3n$? Write $n = 7k + 4$; then $3n = 21k + 12 = 7(3k) + 5$, so the remainder is 5.

[1] courses/math1061/divisibility-and-factorisation.pdf

**Worked**: $m$ leaves remainder 9 on division by 11 — what remainder does $4m$ leave on division by **22**? Write $m = 11k + 9$; then $4m = 44k + 36 = 22(2k + 1) + 14$, so the remainder is 14. (Note the modulus changed, so you cannot just reduce mod 11.)

## Divisibility tests

Modular arithmetic explains the familiar tests. **A positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3**, because $10 \equiv 1 \pmod 3$ and hence $10^k \equiv 1 \pmod 3$ for every $k \in \mathbb{Z}^+$ (apply the multiplication half of the lemma repeatedly: $10^2 \equiv 1$ from $a = m = 10$, $b = n = 1$; then $10^3 \equiv 1$ from $a = 10^2$, $m = 10$; and so on).

$$254 \equiv 2 \cdot 100 + 5 \cdot 10 + 4 \cdot 1 \equiv 2 + 5 + 4 \equiv 11 \equiv 2 \pmod 3$$

so 254 is not divisible by 3 and leaves remainder 2 (checking: $254 = 3 \cdot 84 + 2$). Whereas

$$3252 \equiv 3 + 2 + 5 + 2 \equiv 12 \equiv 0 \pmod 3$$

so $3 \mid 3252$.

## Worked proofs

**For any odd integer $n$, $n^2 \bmod 4 = 1$.**

> Suppose $n$ is odd, so $n = 2k + 1$ for some $k \in \mathbb{Z}$. Then
>
> $$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$
>
> Since $k^2 + k \in \mathbb{Z}$ and $0 \leq 1 < 4$, the quotient-remainder theorem gives $n^2 \bmod 4 = 1$. □

**Hence for any odd integer $n$, $\left\lfloor \frac{n^2}{4} \right\rfloor = \frac{n^2-1}{4}$.** Two routes:

- *Method 1 — expand both sides.* With $n = 2k + 1$: LHS $= \lfloor \frac{4k^2+4k+1}{4} \rfloor = \lfloor (k^2 + k) + \frac{1}{4} \rfloor = k^2 + k$. RHS $= \frac{(2k+1)^2-1}{4} = \frac{4k^2+4k}{4} = k^2 + k$. Equal.
- *Method 2 — use $r = n - d\lfloor \frac{n}{d} \rfloor$.* With number $n^2$, divisor 4, remainder 1: $1 = n^2 - 4\lfloor \frac{n^2}{4} \rfloor$, so $4\lfloor \frac{n^2}{4} \rfloor = n^2 - 1$ and $\lfloor \frac{n^2}{4} \rfloor = \frac{n^2-1}{4}$.

**For all odd integers $n$, $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$** — true, since with $n = 2k + 1$ the right-hand side is $\frac{2k}{2} \cdot \frac{2k+2}{2} = k(k + 1)$, matching the $k^2 + k$ above.

**If $y$ is any integer, then $y^2$ divided by 5 leaves remainder 0, 1 or 4 — never 2 or 3.**

Fix $y \in \mathbb{Z}$. By the quotient-remainder theorem, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

$$y^2 = 25m^2 + 10mr + r^2 \equiv r^2 \pmod 5.$$

Checking each case: $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 4$, $3^2 \equiv 9 \equiv 4$, $4^2 \equiv 16 \equiv 1 \pmod 5$. So $y^2 \equiv 0, 1$ or $4 \pmod 5$. $\square$

This "split into cases by remainder" move is the standard way to prove something about *every* integer using modular arithmetic.

## See also

- divisibility-and-factorisation[2] · gcd-lcm-and-euclidean-algorithm[3] · proof-techniques[4]
- practice-problems[5] — §14 Modular Arithmetic, with full worked solutions

[2] courses/math1061/divisibility-and-factorisation.pdf
[3] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[4] courses/math1061/proof-techniques.pdf
[5] courses/math1061/practice-problems.pdf