Lecture 11 — Modular Arithmetic

Table of contents

Learning goals . . . 1
Common questions . . . 2
Floor and ceiling . . . 2
Quotient-remainder theorem and "mod" . . . 3
Take care with notation . . . 4
Worked: -32 divided by 5 . . . 4
Worked: n^2 mod 4 for odd n . . . 5
Modular arithmetic — the congruence lemma . . . 5
Remainders and divisibility tests . . . 6
See also . . . 7

Pre-work: Video 014 (Modular Arithmetic). See modular-arithmetic[1] for the reference definitions, the quotient-remainder theorem and the congruence lemma this lecture builds on.

Learning goals

1. Understand the proof that there are an infinite number of primes. *(See 2026-08-17-divisibility[2].)*
2. Understand the definition of floor and ceiling.
3. Understand the quotient-remainder theorem.
4. Gain fluency in applying modular arithmetic.

[1] courses/math1061/modular-arithmetic.pdf
[2] courses/math1061/2026-08-17-divisibility.pdf

Common questions

How does the quotient-remainder theorem work with negative integers? The remainder is still required to satisfy $0 \le r < d$, so it stays non-negative: $-19 = 6 \cdot (-4) + 5$, giving $-19 \bmod 6 = 5$.

What is the difference between using mod with an equal sign and with an equivalence sign? See "Take care with notation" below, and "$\bmod$ versus $\equiv$" in modular-arithmetic[3] — this is the notational trap of the topic.

Floor and ceiling

For the floor you move **left** on the number line, so $\lfloor -3.2 \rfloor = -4$. For the ceiling you move **right**, so $\lceil -3.2 \rceil = -3$. (And $\lfloor 3.2 \rfloor = 3$, $\lceil 3.2 \rceil = 4$.) **Watch out** for the negatives.

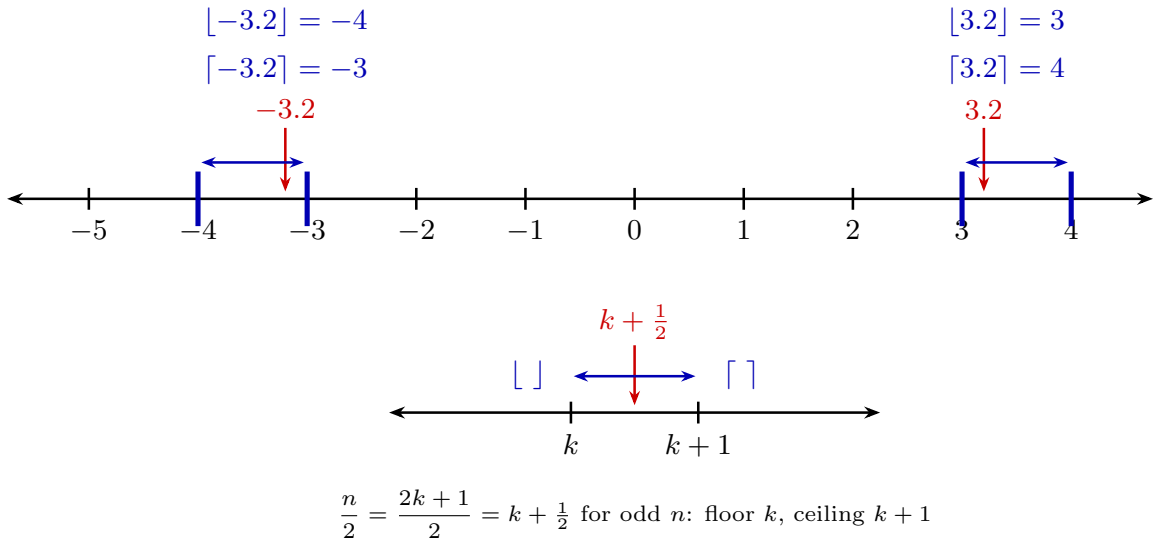

Figure 1: Floor and ceiling on the number line. Floor hops left to the nearest integer, ceiling hops right; it is that *direction* — not the differing arrow lengths — that the negative case gets wrong, giving $\lfloor -3.2 \rfloor = -4$ rather than -3. The lower line is the proof trick: for odd n, $n/2$ lands strictly between the integers k and $k+1$, so the floor and ceiling can be read straight off.

The awkward case can be rewritten as *an integer plus a bit*: $-3.2 = -4 + 0.8$, so $\lfloor -3.2 \rfloor = \lfloor -4 + 0.8 \rfloor = -4$ with no thinking required. That is the same manoeuvre as the $k + \frac{1}{2}$ line in Figure 1, and it is the one to reach for in a proof.

[3] courses/math1061/modular-arithmetic.pdf

To use floor or ceiling in a proof, it is often helpful to write an expression as **an integer plus an amount between 0 and 1**. For example, to prove that "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 — and $k + \frac{1}{2}$ sits between k and $k+1$, so the floor is k and the ceiling is $k+1$. The same trick handles $\left\lfloor (p^3 + 4p^2 + 5) + \frac{1}{4} \right\rfloor$ where $p \in \mathbb{Z}$.

Quotient-remainder theorem and "mod"

> Given any integer n and positive integer d, there exist **unique** integers q and r such that $n = dq + r$ and $0 \leq r < d$.

The quotient is $q = \lfloor \frac{n}{d} \rfloor$ and the remainder is $r = n - d\lfloor \frac{n}{d} \rfloor$. We define $n \bmod d = r$.

With $d = 6$: $53 = 6 \cdot 8 + 5$, $20 = 6 \cdot 3 + 2$, $-19 = 6 \cdot (-4) + 5$.

This is primary-school long division: $3 \overline{)\,122}$ giving 40 remainder 2 is the same statement as $122 = 3 \cdot 40 + 2$, and in general $d \overline{)\,n}$ gives q remainder r. The one thing school long division does not tell you is what happens when n is negative, which is what the $0 \leq r < d$ clause settles. See modular-arithmetic[4] for that case drawn on the number line.

Two equivalent ways of defining $m \equiv n \pmod{d}$

- **Definition 1**: m and n are congruent modulo d iff they have **the same remainder** according to the quotient-remainder theorem.
- **Definition 2**: $m \equiv n \pmod{d}$ iff $d \mid (m - n)$.

In the examples above, 53 and -19 are congruent modulo 6: $53 \equiv -19 \pmod{6}$. Checking with Definition 2: does $6 \mid (53 - (-19))$? We have $53 + 19 = 72$ and $6 \mid 72$, so yes.

However 53 and 20 have different remainders on division by 6, so $53 \not\equiv 20 \pmod{6}$.

[4] courses/math1061/modular-arithmetic.pdf

Take care with notation

- For $n, d \in \mathbb{Z}$, $d > 0$: $n \bmod d = r$ indicates that the remainder when n is divided by d is r, with $0 \leq r < d$.
- For $m, n, d \in \mathbb{Z}$, $d > 0$: $m \equiv n \pmod{d}$ indicates that m and n have the same remainder when divided by d — equivalently $d \mid (m - n)$.

E.g. $5 \bmod 4 = 1$ and $9 \bmod 4 = 1$, so $9 \equiv 5 \pmod{4}$ — **but** $9 \bmod 4 \neq 5$**.**

Q4 from the pre-class multiple choice questions

True or false? $-50 \equiv 22 \pmod{8}$. **True**, both ways:

- *Definition 1*: $-50 = -48 - 2 = -56 + 6 = 8(-7) + 6$, so $-50 \bmod 8 = 6$; and $22 = 16 + 6$, so $22 \bmod 8 = 6$. Same remainder.
- *Definition 2*: $22 - (-50) = 72 = 8 \times 9$, so $8 \mid (22 - (-50))$.

Worked: -32 divided by 5

(a) $\lfloor \frac{-32}{5} \rfloor$ and $\lceil \frac{-32}{5} \rceil$:

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

So $\lfloor \frac{-32}{5} \rfloor = -7$ and $\lceil \frac{-32}{5} \rceil = -6$.

$\lceil x \rceil = \lfloor x \rfloor + 1$ only when x is **not** an integer; when $x \in \mathbb{Z}$ the two are equal. That's exactly why the result $\lceil n/2 \rceil = \lfloor n/2 \rfloor + 1$ is stated only for **odd** n.

(b) Quotient and remainder for $n = -32$, $d = 5$: $-32 = -7 \cdot 5 + 3$, so $q = -7$ and $r = 3$.

(c) $-32 \bmod 5 = 3$.

(d) Is $-32 \equiv 32 \pmod{5}$? By Definition 2: $32 - (-32) = 64$, and $5 \nmid 64$, so **no** — $32 \not\equiv -32 \pmod{5}$.

(e) Integers between 10 and 20 congruent to -32 modulo 5: those leaving remainder 3, i.e. **13 and 18**.

On a number line: mark 10 (which is $\equiv 0$, since $5 \mid 10$), count 3 to the right to reach the first member 13, then hop $+5$ to 18 and $+5$ again to 23 — which has overshot 20, so the hunt stops. A congruence class is an arithmetic progression of step d, and finding its members inside a range is just walking it.

Worked: $n^2 \bmod 4$ **for odd** n

(a) Prove that for any odd integer n, $n^2 \bmod 4 = 1$.

Direct proof. Suppose n is odd. Then $\exists k \in \mathbb{Z}$ such that $n = 2k + 1$. So

$$n^2 = (2k+1)^2 = 4k^2 + 4k + 1 = 4(k^2 + k) + 1.$$

Since $k^2 + k \in \mathbb{Z}$, this gives by the QR theorem: $n^2 \bmod 4 = 1$. □

What licenses reading the remainder straight off that last line is the theorem's **uniqueness** clause together with the range check $0 \le r < d$ — here $0 \le 1 < 4$. Without the range check, $n^2 = 4(k^2 + k - 1) + 5$ would be an equally valid rearrangement.

Four marks are accepted for "end of proof" in this course: //, □, ■, or **QED**.

(b) Use this fact to show that for any odd integer n, $\left\lfloor \frac{n^2}{4} \right\rfloor = \frac{n^2-1}{4}$.

Method 1 — show LHS = RHS using $n = 2k + 1$:

$$\text{LHS} = \left\lfloor \frac{(2k+1)^2}{4} \right\rfloor = \left\lfloor \frac{4k^2 + 4k + 1}{4} \right\rfloor = \left\lfloor (k^2 + k) + \frac{1}{4} \right\rfloor = k^2 + k$$

$$\text{RHS} = \frac{(2k+1)^2 - 1}{4} = \frac{4k^2 + 4k + 1 - 1}{4} = k^2 + k$$

so LHS = RHS.

Method 2 — use the rule $r = n - d\lfloor \frac{n}{d} \rfloor$ with number n^2, divisor 4, remainder 1:

$$1 = n^2 - 4\left\lfloor \frac{n^2}{4} \right\rfloor \implies 4\left\lfloor \frac{n^2}{4} \right\rfloor = n^2 - 1 \implies \left\lfloor \frac{n^2}{4} \right\rfloor = \frac{n^2 - 1}{4}$$

Modular arithmetic — the congruence lemma

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

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

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 $8 + 46 \equiv 2 + 1 \equiv 0 \pmod 3$.

$$\text{If } \overset{4}{a} \equiv \overset{x}{b} \pmod{\overset{6}{d}} \text{ and } \overset{3}{m} \equiv \overset{y}{n} \pmod{\overset{6}{d}}, \text{ then } \overset{4+3}{a+m} \equiv \overset{x+y}{b+n} \pmod{\overset{6}{d}}.$$

and $am \equiv bn \pmod{d}$. (the half that 3(b) needs)

4, **3**: known remainders **x**, **y**: the unknown integers **6**: the modulus, fixed throughout

Activity 3(a): $x \bmod 6 = 4$ and $y \bmod 6 = 3$, so $x + y \equiv 4 + 3 \equiv 7 \equiv 1 \pmod{6}$.

Figure 2: How the lemma is actually used: the numbers of the worked example below sit directly above the lemma's slots. Reading down a column tells you what to substitute — the known remainders 4 and 3 go into the a and m slots, the unknown integers x and y into b and n, and the modulus 6 is the same in every slot. The multiplication half is stated with nothing substituted.

Worked: sums and products mod 6

Suppose $x \bmod 6 = 4$ and $y \bmod 6 = 3$.

(a) $(x + y) \bmod 6$**:**

$$x + y \equiv 4 + 3 \equiv 7 \equiv 1 \pmod{6}$$

so the answer is **1**.

(b) $(5x^2 + 4y) \bmod 6$**:**

$$5x^2 + 4y \equiv 5(4)^2 + 4(3) \equiv 5(16) + 12 \equiv 5(16) \equiv 5(4) \equiv 20 \equiv 2 \pmod{6}$$

The lemma licenses each step: the first substitution, then its $+$ half for dropping the 12 (since $12 \equiv 0 \pmod{6}$), and its $\times$ half for replacing 16 by 4. The answer is **2**.

Reducing at every step is what keeps the numbers small.

Remainders and divisibility tests

Modular arithmetic explains the common divisibility tests.

A positive integer is divisible by 3 if and only if the sum of its digits is divisible by 3.

Example: 254 is not divisible by 3 — the sum of its digits is $2 + 5 + 4 = 11$, not divisible by 3.

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

so the remainder is 2 (confirming with the quotient-remainder theorem: $254 = 3 \cdot 84 + 2$).

Example: 3252 **is** divisible by 3, because $3 + 2 + 5 + 2 = 12$ is.

$$3252 \equiv 3 \cdot 1 + 2 \cdot 1 + 5 \cdot 1 + 2 \cdot 1 \equiv 12 \equiv 0 \pmod 3 \implies 3 \mid 3252$$

The test works because $\forall a \in \mathbb{Z}^+$, $10^a \equiv 1 \pmod 3$. To see $10^2 \equiv 1 \pmod 3$, use the lemma with $a = m = 10$ and $b = n = 1$; to see $10^3 \equiv 1 \pmod 3$, use the lemma with $a = 10^2$, $m = 10$, $b = n = 1$; and so on.

See also

- modular-arithmetic[5] · divisibility-and-factorisation[6]
- 2026-08-20-euclidean-algorithm[7] — Lecture 12
- practice-problems[8] — §14 Modular Arithmetic, with full worked solutions

[5] courses/math1061/modular-arithmetic.pdf
[6] courses/math1061/divisibility-and-factorisation.pdf
[7] courses/math1061/2026-08-20-euclidean-algorithm.pdf
[8] courses/math1061/practice-problems.pdf