MATH1061 — Week 6 Notes

Table of contents

Lecture 15 — Mathematical Induction and Recursive Definitions **3**
- Learning goals . . . 3
- Worked: what is wrong with this 'proof' that all numbers are equal? . . . 3
- Recursively defined sequences . . . 4
- A recursively defined set . . . 8
- Worked: $F_n < 2^n$ for the Fibonacci sequence . . . 9
- See also . . . 10

Lecture 16 — Solving Recurrence Relations **10**
- Learning goals . . . 11
- Why the second goal is worth having . . . 11
- Calculating terms gives a guess, not a proof . . . 11
- Arithmetic and geometric sequences . . . 11
- From a recursive definition to an explicit formula . . . 13
- Q3 of the pre-class questions . . . 13
- Worked: a recurrence with two initial conditions . . . 14
- Worked: a recurrence with a fraction . . . 15
- The Tower of Hanoi . . . 16
- Worked: proving the Tower of Hanoi formula . . . 17
- See also . . . 18

Lecture 18 — Proving Properties of Sets and Intro to Functions **18**
- Learning goals . . . 18
- Common questions . . . 19
- Worked: Q1 from video 23 — a proper subset . . . 19
- Worked: Q3 from video 23 — a Venn diagram is not a proof . . . 19
- The element method of proof . . . 20
- Worked: complementation reverses containment . . . 20
- Methods of proof for properties of sets . . . 21
- The laws of logical equivalence method . . . 22

Set identities . . . 22
Worked: the same equality by set identities . . . 23
Russell's paradox . . . 23
Definition of a function . . . 24
Worked: Q1 from video 24 — which set of pairs is a function? . . . 24
Q2 from video 24 — co-domain versus range . . . 25
Image and preimage . . . 26
Worked: images and preimages . . . 26
See also . . . 27

Lecture 17 — Set Theory Definitions and Examples **27**
Learning goals . . . 27
Element, subset, proper subset . . . 27
Q2 from the pre-class questions . . . 28
Worked: is it an element? . . . 28
Subsets and proper subsets . . . 30
Worked: prove one set is a subset of another . . . 30
When are two sets equal? . . . 31
The empty set . . . 31
Unions and intersections . . . 32
Worked: an infinite union and an infinite intersection . . . 32
The power set . . . 33
Worked: element or subset of a power set? . . . 33
Worked: write down each power set . . . 33
Cartesian products . . . 34
Partitions . . . 34
Worked: partitions . . . 35
See also . . . 36

Reference material **36**
Conditional & Biconditional Statements . . . 36
The Examination Formula Page . . . 41
Functions on General Sets . . . 45
Logical Equivalence & Laws . . . 50
Mathematical Induction . . . 54
Modular Arithmetic, Floor & the Quotient-Remainder Theorem . . . 60
Practice Problems — the Semester-wide Set . . . 65
Proof Techniques — Direct, Counterexample, Contradiction, Contraposition . . . 190
Proving Properties of Sets . . . 199
Recursive Definitions . . . 206
Sequences and Summations . . . 210
Sets and Set Notation . . . 214
Solving Recurrence Relations . . . 226

Strong Induction and the Well-Ordering Principle 235

Lecture 15 — Mathematical Induction and Recursive Definitions

Pre-work: Video 019 (Recursive Definitions). See recursive-definitions[1] for the reference material — what a recursive definition of a sequence or a set consists of, and the worked examples — and mathematical-induction[2] / strong-induction-and-the-well-ordering-principle[3] for the proof machinery used below.

Learning goals

1. Continue to become more comfortable with **mathematical induction**.
2. Become more familiar with **recursive definitions of sequences and sets**.

Worked: what is wrong with this 'proof' that all numbers are equal?

Proof. Let $P(n)$ be the predicate "for any collection of n numbers, $x_1, x_2, \ldots, x_n$, it is always the case that $x_1 = x_2 = \cdots = x_n$."

Basis step: $P(1)$ is true, since the collection is just x_1.

Inductive step: Suppose that k is a positive integer and that $P(k)$ is true. This means that in each collection of k numbers, all the numbers are equal.

Now consider a collection of $k+1$ numbers, say $x_1, x_2, \ldots, x_k, x_{k+1}$.

The sub-collection $x_1, x_2, \ldots, x_k$ contains k numbers, and so $x_1 = x_2 = \cdots = x_k$ by the inductive hypothesis.

The sub-collection $x_2, x_3, \ldots, x_{k+1}$ also contains k numbers, and so $x_2 = x_3 = \cdots = x_{k+1}$ by the inductive hypothesis.

Therefore $x_1 = x_2 = \cdots = x_k = x_{k+1}$ and so $P(k+1)$ is true.

By mathematical induction, $P(n)$ is true for each integer $n \geq 1$, and so we have proven that all numbers are equal.

[1] courses/math1061/recursive-definitions.pdf
[2] courses/math1061/mathematical-induction.pdf
[3] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

The conclusion is **false**, so something in the argument must fail.

The basis step is fine. So are "now consider a collection of $k+1$ numbers" and the first sub-collection's conclusion. The trouble is with the *second* sub-collection, $x_2, \ldots, x_{k+1}$. There are two readings of where it goes wrong; both turn on that sub-collection and they differ only over which line is at fault.

One reading puts the fault at the **second use of the inductive hypothesis**: if $P(k)$ is a statement about $x_1, \ldots, x_k$, i.e. $x_1 = x_2 = \cdots = x_k$, then concluding $x_2 = x_3 = \cdots = x_{k+1}$ carries $P(k)$ over to a *different* k numbers.

The other puts it one line later. $P(n)$ as stated is about *any* collection of n numbers, and both sub-collections genuinely do contain k of them, so each conclusion is defensible taken alone; what cannot be defended is the **"Therefore" line, at** $k = 1$. Gluing $x_1 = \cdots = x_k$ to $x_2 = \cdots = x_{k+1}$ into one chain requires the two sub-collections to **overlap** — you need some number that appears in both, to carry the equality across. For $k \geq 2$ they share $x_2, \ldots, x_k$ and the step is sound. For $k = 1$ the collection is just x_1, x_2, the two sub-collections are $\{x_1\}$ and $\{x_2\}$, and they share nothing: each says only that a single number equals itself, and there is no reason at all that $x_1 = x_2$.

Put the two sub-collections on one row and the overlap is visible: $x_1, \ldots, x_k$ (orange in the figure) and $x_2, \ldots, x_{k+1}$ (yellow), the second leaving out x_1. What matters is what the two share.

So $P(1) \to P(2)$ is false. The chain of implications never gets off the basis step, and the "proof" proves nothing beyond $P(1)$.

The lesson: the inductive step has to hold for *every* k from the basis value on — including the very first one. An inductive step that is valid for all large k but fails at the bottom leaves a gap the induction cannot cross.

Recursively defined sequences

A recursive definition needs **initial conditions** and a **recurrence relation** — and the same recurrence relation with different initial conditions can give a completely different sequence ($a_1 = 2$, $a_k = 3a_{k-1}$ gives $2, 6, 18, 54, \ldots$; $b_1 = 7$ with the same recurrence gives $7, 21, 63, 189, \ldots$). See recursive-definitions[4].

Number the two parts in the order you *use* them: **(i) initial conditions, (ii) recurrence relation**. The numbering comes back in 2026-08-31-solving-recurrence-relations[5], where the two things Method 1 checks are labelled (i) and (ii) because they are exactly these two halves.

[4] courses/math1061/recursive-definitions.pdf
[5] courses/math1061/2026-08-31-solving-recurrence-relations.pdf

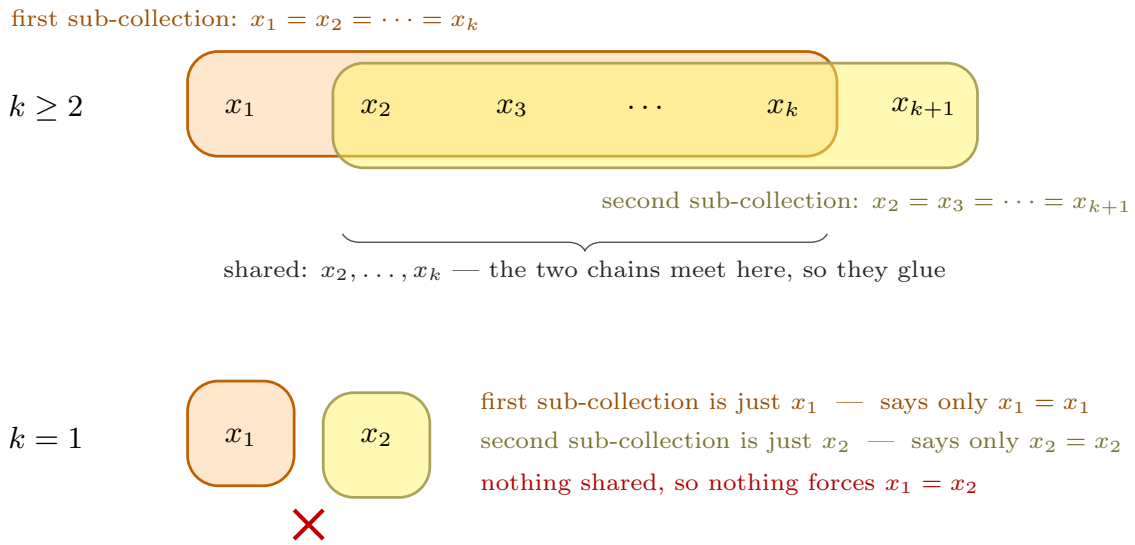


Figure 1: Why the inductive step fails at $k = 1$. The two sub-collections of the $k + 1$ numbers are drawn as overlapping rings on a single row, the first in orange and the second in yellow, so the shared elements can be seen at once. For $k \geq 2$ they overlap on $x_2, \ldots, x_k$, and that shared block is exactly what lets the two equality chains be joined into one. For $k = 1$ the rings shrink to x_1 and x_2, they share nothing, and nothing in the argument forces $x_1 = x_2$.

Worked: which recurrence does $b_n = 4n + 3$ satisfy? (pre-class Q2)

Which of the following recurrence relations is satisfied by the sequence $b_n = 4n + 3$ for each integer $n \geq 1$?

b. $b_k = 4 + b_{k-1}$ for each integer $k \geq 2$.

The method: **assume $b_{k-1} = 4(k-1)+3$, check what b_k equals** — that is, $P(k-1) \Rightarrow P(k)$ — for each candidate in turn. The target is $b_k = 4k + 3$.

Option	Substituting $b_{k-1} = 4(k-1) + 3$
a. $b_k = 4b_{k-1}$	$4(4(k-1)+3) =$ $16k - 16 + 3 = 16k - 13$
b. $b_k = 4 + b_{k-1}$	$4 + 4(k-1) + 3 = 4k + 3$
c. $b_k = 3 + b_{k-1}$	$3 + 4(k-1) + 3 = 4k + 2$
d. $b_k = 3b_{k-1}$	$3(4(k-1)+3) = 12k - 3$

Worked: the recursive definition of $c_n = 3^n - 2^n$ (pre-class Q3)

The sequence $c_n = 3^n - 2^n$ for each integer $n \geq 1$ satisfies the recurrence relation $c_k = 5c_{k-1} - 6c_{k-2}$ for each integer $k \geq 3$. What is the recursive definition for this sequence?

c. $c_1 = 1$, $c_2 = 5$, $c_k = 5c_{k-1} - 6c_{k-2}$ for each integer $k \geq 3$.

Two things pin it down: the values of the initial conditions, and the indexing.

The **initial conditions** come from evaluating the explicit formula:

$$c_1 = 3^1 - 2^1 = 3 - 2 = 1 \qquad c_2 = 3^2 - 2^2 = 9 - 4 = 5$$

Option c has those two values. Option **b** has the clashing $c_1 = 0$ — so b goes out on values. Options **a and d** go out on *indexing* instead: they define c_0 and start the recurrence at $k \geq 2$, whereas the sequence was given as starting at $n = 1$, so c_0 lies outside its domain. Option d fails on values too — it puts $c_1 = 5$.

Option a is the subtle one. Its arithmetic is entirely correct — $c_0 = 3^0 - 2^0 = 0$, $c_1 = 1$, and $c_2 = 5(1) - 6(0) = 5$, $c_3 = 5(5) - 6(1) = 19 = 3^3 - 2^3$ — so it does generate the right sequence for every $n \geq 1$. It is wrong only because it defines a term the given sequence does not have. That is the difference between a wrong sequence and a right sequence with the wrong domain.

Worked: a recursive definition for $a_n = (-1)^n/n!$

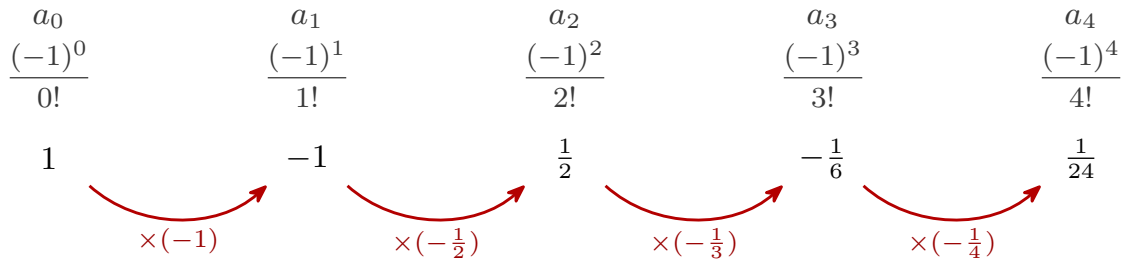
Consider the sequence defined by the explicit formula $a_n = \dfrac{(-1)^n}{n!}$ for each integer $n \geq 0$. (Recall that for $n \in \mathbb{Z}^+$, $n! = n(n-1)\cdots(2)(1)$, and that $0! = 1$ **by definition**. Memorise that clause: it is what makes a formula built out of $n!$ work at $n = 0$ with no special case, which is exactly what this sequence needs.)

(a) Determine the first five terms of this sequence and guess a suitable recurrence relation.

$$a_0 = \frac{(-1)^0}{0!} = \frac{1}{1} = 1 \qquad a_1 = \frac{(-1)^1}{1!} = \frac{-1}{1} = -1 \qquad a_2 = \frac{(-1)^2}{2!} = \frac{1}{2}$$

$$a_3 = \frac{(-1)^3}{3!} = \frac{-1}{3\times 2} = -\frac{1}{6} \qquad a_4 = \frac{(-1)^4}{4!} = \frac{1}{4\times 3\times 2} = \frac{1}{24}$$

The guess does not come from staring at the five values; it comes from asking **what multiplies each one to give the next**. Write those multipliers in as curved arrows between consecutive terms:



$$\text{the multiplier at step } n \text{ is } -\frac{1}{n}, \quad \text{so } a_n = -\frac{1}{n}\, a_{n-1}$$

Figure 2: Reading the recurrence off the terms. Each curved arrow carries the factor taking one term to the next, and the four factors $-1, -\frac{1}{2}, -\frac{1}{3}, -\frac{1}{4}$ are read as one pattern, $-\frac{1}{n}$ at step n. The pattern is the guess; part (b) is where it gets proved.

$$a_n = -\frac{1}{n} a_{n-1}$$

(b) Show that this sequence satisfies your recurrence relation.

Suppose $a_{n-1} = \dfrac{(-1)^{n-1}}{(n-1)!}$. Then

$$a_n = -\frac{1}{n} \cdot a_{n-1} = \frac{(-1)(-1)^{n-1}}{n \cdot (n-1)!} = \frac{(-1)^n}{n!} \qquad \square$$

(c) Write down a recursive definition of this sequence.

- *initial condition*: $a_0 = 1$
- *recurrence relation*: $a_n = -\dfrac{1}{n} a_{n-1}$ for all $n \geq 1$

A recursively defined set

Three parts — **Base**, **Recursion** and **Restriction** — spelled out in recursive-definitions[6] along with the set of all binary strings B, in which the string 011 is built up as $\varepsilon \to 0 \to 01 \to 011$. The worked question below is practice with step II, the Recursion: what its rules do and do not generate.

Worked: which strings are in S?

Let the subset S of the set of all binary strings be defined recursively as follows. Base: the empty string is in S. Recursion: if $s \in S$, then $s1 \in S$ and $s01 \in S$. Restriction: nothing is in S other than objects defined by the Base and the Recursion.

So there are two rules, named by what they append: **rule `1`** (append `1`) and **rule `01`** (append `01`). Naming them matters, because a membership argument is a chain of rule applications and each link has to say which rule was used. The rule's bare name goes above the arrow, and nothing else:

(a) Is the string 1101 $\in S$?

Yes — it has a build history:

$$\varepsilon \xrightarrow{1} 1 \xrightarrow{1} 11 \xrightarrow{01} 1101 \in S$$

(b) Is the string 0110 $\in S$?

No — S contains no strings ending in 0. Both rules append a string ending in `1`, so every non-empty member of S ends in `1`, and by the Restriction there is nothing else in S.

(c) Is the string 1001 $\in S$?

[6] courses/math1061/recursive-definitions.pdf

No — S contains no strings with two or more consecutive 0s. A `0` can only ever enter as the first character of an appended `01`, so every `0` is immediately followed by a `1`.

(d) State a property that all strings in S must have and explain why.

The number of 1s is greater than or equal to the number of 0s.

The empty string has zero of each, so the property holds at the Base. Each rule preserves it: appending `1` adds one 1 and no 0s, and appending `01` adds one of each. So no application of the Recursion can ever make the 0s outnumber the 1s, and by the Restriction every member of S is reached by some finite chain of these rules.

Worked: $F_n < 2^n$ for the Fibonacci sequence

Recall the Fibonacci sequence: $F_0 = 1$, $F_1 = 1$, $F_k = F_{k-1} + F_{k-2}$ for every integer $k \geq 2$. Use (strong) mathematical induction to prove that $F_n < 2^n$ for every integer $n \geq 1$.

The first thing to settle is the number of base cases. The recurrence $F_k = F_{k-1} + F_{k-2}$ points to **2 base cases**; the "$n \geq 1$" in the claim points to **1 base case**. The recurrence settles it. $F_k = F_{k-1} + F_{k-2}$ reaches back **two** terms, so producing $P(k+1)$ needs $P(k)$ *and* $P(k-1)$: that is strong induction, and it needs two base cases to start from.

The same reasoning fixes the range of the inductive step: it is $\forall k \geq 2$, not $\forall k \geq 1$. At $k = 1$ the step would reach for $P(0)$, which is not one of the base cases. This is not merely an indexing nicety, because with $F_0 = 1$ the statement $P(0)$ is **false** — it would say $F_0 < 2^0$, i.e. $1 < 1$. So the claim could not have been extended down to $n = 0$ in any case.

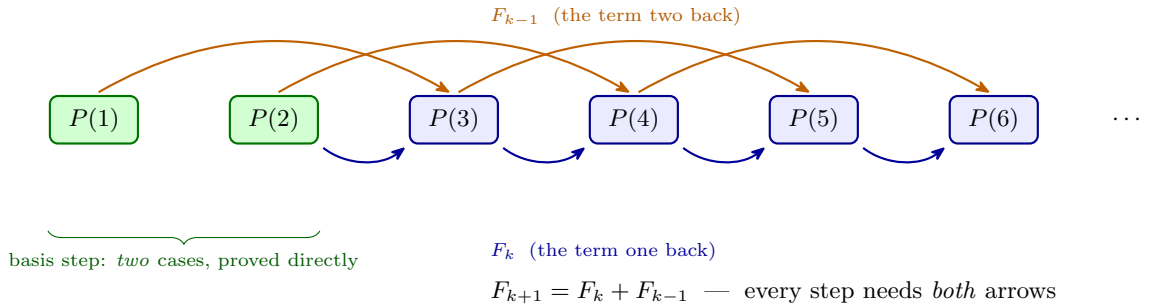


Figure 3: The shape of the strong induction, drawn out. Each $P(k+1)$ is reached from the term one back (blue) and the term two back (orange), because the recurrence $F_{k+1} = F_k + F_{k-1}$ names both; that is why the inductive hypothesis has to be the strong one, and why two cases have to be proved outright before the chain can start.

Let $P(n)$ be the predicate $F_n < 2^n$.

Basis step — $P(1)$ and $P(2)$.

LHS of $P(1)$: $F_1 = 1$. RHS of $P(1)$: $2^1 = 2$. Since $1 < 2$, $P(1)$ is true.

LHS of $P(2)$: $F_2 = F_1 + F_0 = 1 + 1 = 2$. RHS of $P(2)$: $2^2 = 4$. Since $2 < 4$, $P(2)$ holds.

Inductive step — $(P(1), \dots, P(k)) \to P(k+1)$ for all $k \geq 2$.

LHS of $P(k+1)$:

$$F_{k+1} = F_k + F_{k-1} < 2^k + 2^{k-1} \qquad \text{(by the inductive hypothesis } P(k) \text{ and } P(k-1)\text{)}$$
$$= 2(2^{k-1}) + 2^{k-1} = 3(2^{k-1}) < 2^2(2^{k-1}) \qquad (3 < 4 = 2^2)$$
$$= 2^{k+1}$$

which is the RHS of $P(k+1)$. Therefore $(P(1), \dots, P(k)) \to P(k+1)$. $\square$

The trick in the middle is rewriting 2^k as $2(2^{k-1})$ so that both terms carry the same power and can be collected — turning $2^k + 2^{k-1}$ into $3(2^{k-1})$, which is then bounded by $4(2^{k-1}) = 2^{k+1}$.

See also

- recursive-definitions[7] · mathematical-induction[8] · strong-induction-and-the-well-ordering-principle[9] · sequences-and-summations[10]
- 2026-08-27-strong-induction-and-well-ordering[11] — Lecture 14
- practice-problems[12] — §19 Recursive Definitions, with full worked solutions

Lecture 16 — Solving Recurrence Relations

Pre-work: Video 020 (Solving Recurrence Relations). See solving-recurrence-relations[13] for the reference material — arithmetic and geometric sequences, the two proof methods and the Tower of Hanoi — and recursive-definitions[14] for the definitions this lecture starts from.

[7] courses/math1061/recursive-definitions.pdf
[8] courses/math1061/mathematical-induction.pdf
[9] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[10] courses/math1061/sequences-and-summations.pdf
[11] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf
[12] courses/math1061/practice-problems.pdf
[13] courses/math1061/solving-recurrence-relations.pdf
[14] courses/math1061/recursive-definitions.pdf

Learning goals

1. Become more familiar with **recursive definitions of sequences**.
2. Gain fluency in **moving between a recursive definition and an explicit formula**.

Why the second goal is worth having

Put the two forms side by side and ask for the same thing from each, say the term at $n = 1000$:

Form	Example	Getting a_{1000}
Explicit formula	$a_n = 7n^2$ for all $n \in \mathbb{Z}^+$	substitute: $7(1000)^2$ — one step
Recursive definition	$a_0 = 4$ and $a_n = 5a_{n-1} + 3$	compute $a_1, a_2, ...$ all the way up — a thousand steps

That gap is the motivation for the whole topic. A recursive definition is often the easy thing to *write down* (it is how the Tower of Hanoi and the Fibonacci numbers naturally arise), and an explicit formula is the thing you want to *compute with*. The topic is converting the first into the second.

Calculating terms gives a guess, not a proof

To show that a recursive definition is the same as an explicit formula, it is **not** enough to calculate values and show they give the same terms. Calculating terms produces a **guess**, never a proof. Any finite run of terms is consistent with infinitely many formulas (see sequences-and-summations[15]), so agreement on the first five terms says nothing about the sixth. Terms are calculated to have something to prove. In the two methods below, "write out the first few terms and guess" is a separate step from "prove that your guess is correct".

Question 3 of the pre-class work asks whether such a claim is true or false. It is worked below, twice, once by each method.

Arithmetic and geometric sequences

For a sequence $a_0, a_1, a_2, ...$:

[15] courses/math1061/sequences-and-summations.pdf

	Recurrence relation	Explicit formula
Arithmetic	$a_k = a_{k-1} + d$ for integers $k \geq 1$	$a_n = a_0 + dn$ for integers $n \geq 0$
Geometric	$a_k = r \cdot a_{k-1}$ for integers $k \geq 1$	$a_n = a_0 \cdot r^n$ for integers $n \geq 0$

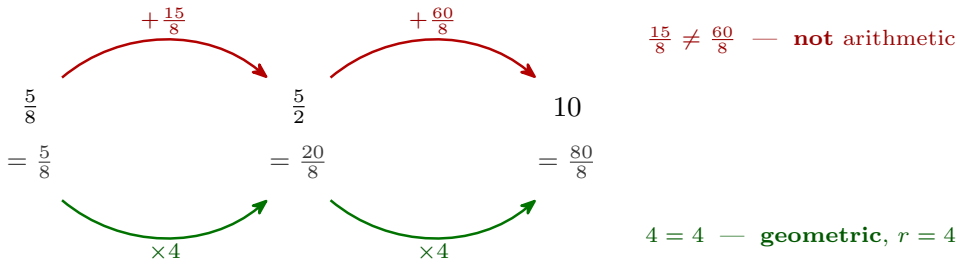
The four formulas look alike. **The two written in k with a_{k-1} on the right are the recurrence relations; the two written in n are the explicit formulas.**

For example, $2, 6, 18, 54, \ldots$ multiplies by 3 each step, so $r = 3$, and with $a_0 = 2$ the explicit formula is $a_n = 2 \cdot 3^n$.

Worked: geometric but not arithmetic

The three terms $\frac{5}{8}, \frac{5}{2}, 10$ could be three consecutive terms of what type of sequence?

A geometric sequence. Putting them over a common denominator, $\frac{5}{8}, \frac{20}{8}, \frac{80}{8}$, makes both tests quick. Run both on the same three terms, with the differences above the row and the ratios below it:



both tests are run on the same three terms; passing one says nothing about the other

Figure 4: Both tests, run on the same three terms. Rewriting over the common denominator 8 makes each test one subtraction or one division. The differences $\frac{15}{8}$ and $\frac{60}{8}$ disagree, so the terms are not arithmetic; the ratios are both 4, so they are geometric with $r = 4$. Neither verdict is evidence about the other, which is what the answer *both* gets wrong.

The answer "both" is the trap. Passing the ratio test earns nothing on the difference test. The two conditions are independent.

Worked: both arithmetic and geometric

The three terms $2, 2, 2$ could be three consecutive terms of what type of sequence?

Both. The differences are all 0 (arithmetic, $d = 0$) and the ratios are all 1 (geometric, $r = 1$).

This is **a constant sequence**, $a_n = c$ for all $n \in \mathbb{Z}^+$. The constant sequences are not just *examples* of the overlap but the whole of it — $a_n = a_0 + dn$ and $a_n = a_0 r^n$ can agree for every n only when $d = 0$ and the sequence is constant.

From a recursive definition to an explicit formula

Given a recursive definition, write out the first few terms and **guess** an explicit formula. To prove the guess correct, either:

> **Method 1.** Check that your guess gives the correct initial conditions and satisfies the recurrence relation.
>
> **Method 2.** Use (strong) mathematical induction to prove that if $a_0, a_1, a_2, ...$ is the sequence defined by [the recursive definition], then [your guess].

Method 1 is the **quicker** one and Method 2 the **rigorous** one. Both are complete proofs; Method 1 leans on the fact that a recursive definition determines its sequence uniquely, which solving-recurrence-relations[16] spells out.

Q3 of the pre-class questions

> **True or false?** The sequence defined recursively as $c_1 = 1$ and $c_k = c_{k-1} + 2^k$ for each integer $k \geq 2$ can be defined using the explicit formula $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$.

True.

By Method 1

Label the two checks (i) and (ii). They are the two halves of the recursive definition.

(i) Initial conditions ($n = 1$): $c_1 = 2^{1+1} - 3 = 2^2 - 3 = 4 - 3 = 1$

(ii) Recurrence relation:

$$\text{LHS} = c_k = 2^{k+1} - 3$$

[16] courses/math1061/solving-recurrence-relations.pdf

$$\text{RHS} = c_{k-1} + 2^k = 2^{(k-1)+1} - 3 + 2^k = 2^k + 2^k - 3 = 2(2^k) - 3 = 2^{k+1} - 3$$

so the explicit formula satisfies the given recurrence relation. Therefore the statement is true.

By Method 2

To prove that *if* $c_1, c_2, c_3, ...$ is the sequence defined by $c_1 = 1$ and $c_k = c_{k-1} + 2^k$ for each integer $k \geq 2$, *then* $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$ — by mathematical induction (PMI).

Let $P(n)$ be the predicate $c_n = 2^{n+1} - 3$.

Basis step. $c_1 = 1$ by the recursive definition, and $2^{1+1} - 3 = 4 - 3 = 1$, so the statement is true for $n = 1$.

Inductive hypothesis. Suppose $P(k)$ is true for some integer $k \geq 1$. This means $c_k = 2^{k+1} - 3$. Then

$$c_{k+1} = c_k + 2^{k+1} = 2^{k+1} - 3 + 2^{k+1} = 2(2^{k+1}) - 3 = 2^{k+2} - 3$$

Therefore $P(k+1)$ is true. Hence by mathematical induction the sequence with the given recursive definition is defined explicitly as $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$. ■

The recurrence is stated for $k \geq 2$, so the substitution $c_{k+1} = c_k + 2^{k+1}$ is legitimate for $k \geq 1$ — the indices line up exactly with the basis step.

Worked: a recurrence with two initial conditions

> Consider the sequence $b_0 = 0$, $b_1 = 1$ and $b_k = \frac{1}{2}(b_{k-1} + b_{k-2} + 1) + 3(k-1)$ for each integer $k \geq 2$.

(a) Calculate a few more terms and guess an explicit formula

$$b_2 = \tfrac{1}{2}(b_1 + b_0 + 1) + 3(1) = \tfrac{1}{2}(0 + 1 + 1) + 3 = 1 + 3 = 4$$
$$b_3 = \tfrac{1}{2}(4 + 1 + 1) + 3(2) = 3 + 6 = 9$$
$$b_4 = \tfrac{1}{2}(9 + 4 + 1) + 3(3) = 7 + 9 = 16$$

giving $0, 1, 4, 9, 16, ...$ — **guess $b_n = n^2$ for all integers $n \geq 0$.**

(b) Prove the guess by Method 1

Initial conditions ($n = 0$ and $n = 1$): $b_0 = 0^2 = 0$ and $b_1 = 1^2 = 1$ — so the explicit formula satisfies the initial conditions. **Two** initial conditions means **two** checks.

Recurrence relation. Suppose $b_n = n^2$ for all n:

$$\text{LHS} = b_k = k^2$$

$$\begin{aligned}\text{RHS} &= \tfrac{1}{2}\big((k-1)^2 + (k-2)^2 + 1\big) + 3(k-1) \\ &= \tfrac{1}{2}(k^2 - 2k + 1 + k^2 - 4k + 4 + 1) + 3k - 3 \\ &= (k^2 - 3k + 3) + 3k - 3 \\ &= k^2\end{aligned}$$

$\therefore$ LHS = RHS, so the explicit formula satisfies the recurrence relation. ■

The same result can be proved by **strong** induction — strong because the recurrence reaches back two terms, so $P(k)$ alone would not be enough. See solving-recurrence-relations[17] for that proof written out.

(c) Find a different recursive definition of the sequence

Look for a one-step recurrence $b_n = b_{n-1} + p$ and solve for the step:

$$n^2 = (n-1)^2 + p \implies p = 2n - 1 \implies b_n = b_{n-1} + (2n - 1)$$

Completed into a recursive definition, $b_0 = 0$ with $b_n = b_{n-1} + (2n - 1)$ for $n \geq 1$ gives the same sequence — the squares as running totals of the odd numbers. Two things to take from the exercise: **a sequence does not have a unique recursive definition**, and this one needs only one initial condition where the original needed two.

Worked: a recurrence with a fraction

Consider the sequence defined as $d_0 = 1$ and $d_k = \dfrac{d_{k-1}}{1 + d_{k-1}}$ for each integer $k \geq 1$.

[17] courses/math1061/solving-recurrence-relations.pdf

(a) Calculate a few more terms and guess an explicit formula

The trick used throughout is "$\times 1$": multiply top and bottom by the denominator of the inner fraction to clear the compound fraction in one move.

$$d_1 = \frac{1}{1+1} = \frac{1}{2} \qquad d_2 = \frac{\frac{1}{2}}{1+\frac{1}{2}} \cdot \frac{2}{2} = \frac{1}{2+1} = \frac{1}{3} \qquad d_3 = \frac{\frac{1}{3}}{1+\frac{1}{3}} \cdot \frac{3}{3} = \frac{1}{3+1} = \frac{1}{4}$$

giving $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ — **guess** $d_n = \dfrac{1}{n+1}$**.**

(b) Prove the guess by Method 1

Initial condition ($d_0 = 1$): $d_0 = \dfrac{1}{0+1} = \dfrac{1}{1} = 1$

Recurrence relation. Suppose $d_n = \dfrac{1}{n+1}$:

$$\text{LHS} = d_k = \frac{1}{k+1} \qquad \text{RHS} = \frac{d_{k-1}}{1+d_{k-1}} = \frac{\frac{1}{k}}{1+\frac{1}{k}} \cdot \frac{k}{k} = \frac{1}{k+1}$$

$\therefore$ LHS = RHS, so the explicit formula satisfies the recurrence relation. ■

The same result can be proved by ordinary induction (**MI**) — ordinary this time, since the recurrence reaches back only one term.

The Tower of Hanoi

> Given a tower of 8 discs in decreasing size on one of three pegs, transfer the entire tower to one of the other pegs, subject to: **(a)** move only one disc at a time; **(b)** never move a larger disc onto a smaller disc. Is there a solution? If so, what is the fewest number of moves?

For $n \geq 1$ let m_n be the minimum number of moves to transfer a tower of n discs from one pole to another. Work up to the recurrence through three cases:

- $n = 1$: one move, so $m_1 = 1$.
- $n = 2$: small disc to the spare peg, large disc across, small disc back on top — so $m_2 = 3$.
- the general case: the whole transfer takes m_n moves and passes through four board positions, with the $n-1$ smaller discs treated as one group. For four discs, $m_4 = m_3 + 1 + m_3$.

The first two are shown below as sequences of board positions, each a transfer that takes that many moves. The recurrence is read off the general case.

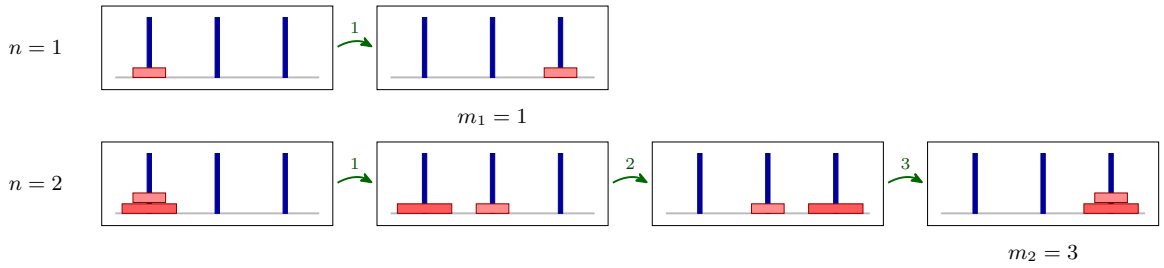


Figure 5: The two small cases. One disc goes left peg to right peg in one move, and two discs take three, numbered $1, 2, 3$, with the small disc parked on the middle peg in between. Each position is boxed and the green arrows are the moves. **The middle move is forced**: the large disc cannot move until the small one is off it and cannot land on the small one, so the spare peg has to be used, and that is what generalises to $m_k = 2m_{k-1} + 1$.

In general:

$$m_1 = 1 \qquad \text{and} \qquad m_k = 2m_{k-1} + 1 \ \text{ for all integers } k \geq 2$$

The three stages between the four board positions take m_{n-1}, $m_1 = 1$ and m_{n-1} moves (drawn out in solving-recurrence-relations[18]). The largest disc has to move at some point, and it can only move onto an empty peg — so the other $k-1$ discs must first be stacked on the spare peg, and then moved back on top afterwards. Two sub-transfers plus one move.

Worked: proving the Tower of Hanoi formula

> On page 310 (4th edition) or page 346 (5th edition) the textbook guesses $m_n = 2^n - 1$ for all integers $n \geq 1$. Prove the guess is correct by checking that it gives the correct initial conditions and satisfies the recurrence relation.

Suppose $m_n = 2^n - 1$ for all $n \in \mathbb{Z}^+$.

Initial condition ($m_1 = 1$): $m_1 = 2^1 - 1 = 2 - 1 = 1$

Recurrence relation ($m_k = 2m_{k-1} + 1$):

$$\text{LHS} = m_k = 2^k - 1$$

[18] courses/math1061/solving-recurrence-relations.pdf

$$\text{RHS} = 2m_{k-1} + 1 = 2(2^{k-1} - 1) + 1 = 2 \cdot 2^{k-1} - 2 + 1 = 2^k - 1$$

So LHS = RHS $\therefore$ the explicit formula satisfies the recurrence relation. ■

The textbook proves the same result by mathematical induction (**PMI**) instead — so this is Method 1 versus Method 2 on the same problem one more time.

The eight-disc puzzle of the problem statement needs $2^8 - 1 = 255$ moves, and "is there a solution?" is answered constructively, because the recurrence *is* the algorithm.

See also

- solving-recurrence-relations[19] — the reference note for all of the above
- recursive-definitions[20] · sequences-and-summations[21] · mathematical-induction[22] · strong-induction-and-the-well-ordering-principle[23]
- 2026-08-31-recursive-definitions[24] — Lecture 15
- 2026-09-03-set-theory-definitions[25] — Lecture 17
- practice-problems[26] — §20 Solving Recurrence Relations, with full worked solutions

Lecture 18 — Proving Properties of Sets and Intro to Functions

Pre-work: Video 023 (Properties of sets) and Video 024 (Functions defined on general sets). See proving-set-properties[27] for the three proof methods and the set identities, and functions-on-general-sets[28] for the function material in the second half.

Learning goals

1. Be comfortable with notation for sets including $x \in A$, $A \subseteq B$, $A \subset B$, $A \cap B$, $A \cup B$, $A - B$, A^c, $\mathcal{P}(A)$, $A \times B$.
2. Be able to use the **element method** to prove set properties.
3. Be able to use the **laws of logical equivalence** to prove that two sets are equal.
4. Be able to use **set identities** to prove that two sets are equal.

[19] courses/math1061/solving-recurrence-relations.pdf
[20] courses/math1061/recursive-definitions.pdf
[21] courses/math1061/sequences-and-summations.pdf
[22] courses/math1061/mathematical-induction.pdf
[23] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[24] courses/math1061/2026-08-31-recursive-definitions.pdf
[25] courses/math1061/2026-09-03-set-theory-definitions.pdf
[26] courses/math1061/practice-problems.pdf
[27] courses/math1061/proving-set-properties.pdf
[28] courses/math1061/functions-on-general-sets.pdf

5. Understand **what a function is**, and associated concepts and definitions.

Goal 1 carries over from 2026-09-03-set-theory-definitions[29]. For **goal 2**, the element method, the operational point is that $A = B$ means ($A \subseteq B$ and $B \subseteq A$) — the shape every equality proof below takes.

Common questions

Q1 and Q3 from video 23, and Q1 and Q2 from video 24, are all worked below.

What is the difference between co-domain and range, and how do you distinguish between them? The co-domain is declared, the range is computed. See the functions section.

Worked: Q1 from video 23 — a proper subset

Let $S = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\}$ and let $T = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod 6\}$.

$$S = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} \qquad T = \{\dots, -7, -1, 5, 11, \dots\}$$

Prove that $T \subset S$. The proof splits into the two things $\subset$ demands, (i) and (ii):

(i) $T \subseteq S$**.** Suppose $t \in T$. Then $t = 6k+5$ for some integer k. Thus $t = 3(2k+1)+2$, and since $2k + 1 \in \mathbb{Z}$, we have $t \in S$. Therefore $T \subseteq S$.

(ii) $T \neq S$ and $\exists s \in S - T$. Furthermore, $2 \in S$ but $2 \notin T$, so $T \subset S$. ■

Part (i) is the general argument — "suppose $t \in T$", nothing assumed beyond membership. Part (ii) is a single witness. **A universal claim needs a general argument; an existential claim needs one example**, and mixing up which is which is the usual way this proof goes wrong.

Worked: Q3 from video 23 — a Venn diagram is not a proof

For all sets A, B, C: $(A - B) \cap (B - A) = \emptyset$. **True.**

[29] courses/math1061/2026-09-03-set-theory-definitions.pdf

Three Venn diagrams — A and B; then $A - B$ shaded; then $B - A$ shaded — show the result, but they are **not a proof**. The figure is in proving-set-properties[30].

Worth taking seriously, because the diagrams are so convincing. A Venn diagram shows **one** configuration; the claim is about **all** sets, including the cases the picture does not draw — $A = B$, either set empty, one contained in the other. And the regions are drawn non-empty when the statement has to survive them being empty.

The proof takes two lines: suppose $x \in (A - B) \cap (B - A)$; then $x \in A$ and $x \notin B$, and also $x \in B$ and $x \notin A$; so $x \in B$ and $x \notin B$, a contradiction. Hence no such x, and the intersection is empty. ■

Diagrams to **find** the answer; the element method to **justify** it.

The element method of proof

To prove that $S \subseteq T$, you consider an arbitrary element $x \in S$ and show that $x \in T$.

To prove that $S \subset T$, you prove that $S \subseteq T$ and then prove $\exists\, t \in T$ such that $t \notin S$.

To prove that $S = T$, you prove that $S \subseteq T$ and also prove that $T \subseteq S$.

Worked: complementation reverses containment

Prove that for all sets A and B in some universe U, if $A \subseteq B$ then $B^c \subseteq A^c$.

Proof. Let $x \in B^c$. Then $x \in U - B$ (by definition of complement). Thus $x \in U$ and $x \notin B$ (by definition of set difference).

Since $A \subseteq B$ we have: every element in A is also an element of B. Taking the contrapositive,

$$x \notin B \;\longrightarrow\; x \notin A$$

Since $x \in U$ and $x \notin A$, then by the definition of complement, $x \in A^c$. ■

The step to notice is the **contrapositive**. $A \subseteq B$ gives you "$x \in A \to x \in B$", which is the wrong way round for what you have; flipping it to "$x \notin B \to x \notin A$" is what makes the hypothesis usable. See proof-techniques[31] for why that flip is free.

The result itself is worth remembering as a fact: **complementation reverses containment.** The smaller set has the bigger complement.

[30] courses/math1061/proving-set-properties.pdf
[31] courses/math1061/proof-techniques.pdf

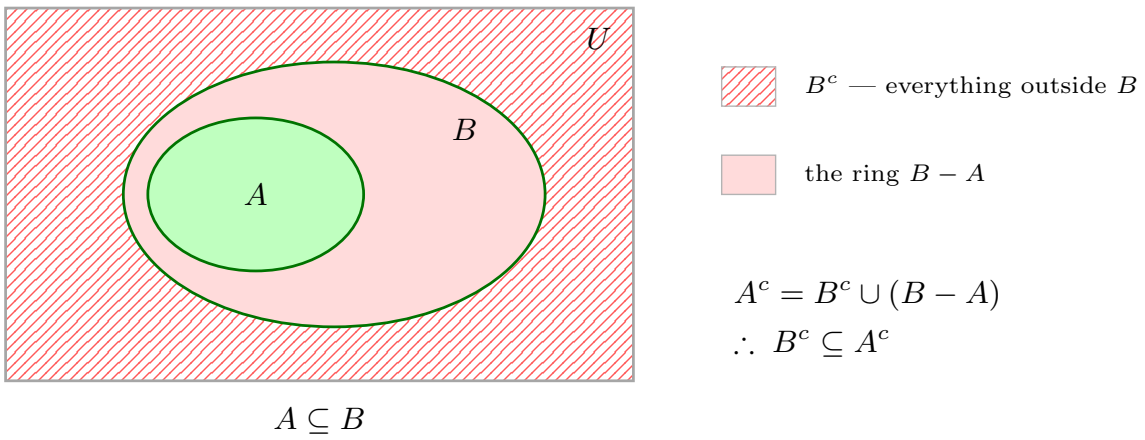


Figure 6: The universe as a rectangle, A inside B, and B-complement hatched in red. The shading of the ring B − A is what makes the result readable off the picture: A-complement is the hatched region plus the ring, so it contains B-complement. A picture like this is a check on the answer, not a substitute for the element proof above.

Methods of proof for properties of sets

Three methods, and when each is useful:

Method	Useful for	Note
The element method	a **variety** of results about sets	the only one that can prove a containment, not just an equality
Laws of logical equivalence	proving two sets are **equal**	quicker
Set identities	proving two sets are **equal**	quicker

The element method has three sub-forms, the second of which does not mention a second set at all:

1. To prove $S \subseteq T$, suppose $x \in S$ and then prove that $x \in T$.
2. To prove that **all elements in a set** S **have property** P, suppose $x \in S$, and then prove that x has property P.
3. To prove that $S = T$, first prove that $S \subseteq T$, and then prove that $T \subseteq S$.

The laws of logical equivalence method

Example. Prove that for all sets A and B, $A - (A - B) = A \cap B$.

$$
\begin{aligned}
x \in A - (A - B) &\equiv (x \in A) \wedge (x \notin (A - B)) && \text{by definition of set difference} \\
&\equiv (x \in A) \wedge \sim (x \in (A - B)) && \text{by definition of } \notin \\
&\equiv (x \in A) \wedge \sim ((x \in A) \wedge (x \notin B)) && \text{by definition of set difference} \\
&\equiv (x \in A) \wedge (\sim (x \in A) \vee \sim (x \notin B)) && \text{by De Morgan's law} \\
&\equiv (x \in A) \wedge ((x \notin A) \vee (x \in B)) && \text{by definition of } \in \text{ and } \notin \\
&\equiv ((x \in A) \wedge (x \notin A)) \vee ((x \in A) \wedge (x \in B)) && \text{by the distributive law} \\
&\equiv \mathbf{c} \vee ((x \in A) \wedge (x \in B)) && \text{by the negation law} \\
&\equiv (x \in A) \wedge (x \in B) && \text{by the identity law} \\
&\equiv x \in A \cap B && \text{by the definition of } \cap
\end{aligned}
$$

The justifications are of two kinds, and the grouping is the lesson. **Four** of the nine lines are **laws of logical equivalence** doing the actual work — De Morgan, distributive, negation, identity. The other **five** are **definitions of set symbols**, translating in and out of logic: the three at the top, the last one, and — easy to miss — the "$\in$ and $\notin$" line sitting in the middle of the chain, so the two kinds do not fall into neat blocks. Every line is named; the naming is where the marks are.

Because the chain is all $\equiv$, this proves the equality **in one pass** rather than the element method's two containments.

Set identities

The full table is in proving-set-properties[32] and appears on the exam formula page (see formula-sheet[33]). The ones used below:

3(b)	Distributive	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4(a)	Identity	$A \cup \emptyset = A$
5(b)	Complement	$A \cap A^c = \emptyset$
6	Double Complement	$(A^c)^c = A$
9(b)	De Morgan's	$(A \cap B)^c = A^c \cup B^c$
12	Set Difference	$A - B = A \cap B^c$

[32] courses/math1061/proving-set-properties.pdf
[33] courses/math1061/formula-sheet.pdf

Worked: the same equality by set identities

Using the set identities, prove that for all sets A and B, $A - (A - B) = A \cap B$.

The same result as the worked example, by the third method:

$$\begin{aligned}
A - (A - B) &= A - (A \cap B^c) && \text{by the set difference law (12)} \\
&= A \cap (A \cap B^c)^c && \text{by the set difference law (12)} \\
&= A \cap (A^c \cup (B^c)^c) && \text{by De Morgan (9b)} \\
&= A \cap (A^c \cup B) && \text{by the double complement law} \\
&= (A \cap A^c) \cup (A \cap B) && \text{by the distributive law (3b)} \\
&= \emptyset \cup (A \cap B) && \text{by the complement law (5b)} \\
&= A \cap B && \text{by the identity law (4a)}
\end{aligned}$$

Seven lines against the previous method's nine, with no logic notation. Two things worth pulling out:

- **Law 12 is applied twice** — to the inner difference, then the outer one. Clearing every minus sign first is what makes the rest routine, since none of the other identities mention set difference at all.
- The final step cites identity law (4a), $A \cup \emptyset = A$, but is applied to $\emptyset \cup (A \cap B)$ — the operands reversed. **Commutativity (1a) is being used silently.** Standard practice, but the step is really two.

Russell's paradox

When mathematicians wanted to show that all of mathematics could be built on set theory, **Bertrand Russell** discovered a problem.

Let S be the set of all sets that are not elements of themselves, $S = \{A \mid A \text{ is a set and } A \notin A\}$. Is S an element of itself?

If $S \in S$, then $S \notin S$. If $S \notin S$, then $S \in S$. So we conclude that both $S \in S$ and $S \notin S$, which is impossible.

The natural objection — that a set is never an element of itself — is the right instinct but is not an escape, because nothing in "a set is any collection of objects" rules self-membership out. The contradiction is not that S is strange; it is that **the assumption that every describable collection is a set** cannot be maintained.

Several ways to define the basic concepts of set theory were found so that Russell's paradox does not arise. For more detail, read pages 419–421 (5th ed.) or 378–380 (4th ed.) of the textbook. For more set theory, take **MATH3306 Set Theory and Logic**.

Definition of a function

> A function $f : X \to Y$ is a subset $f \subseteq X \times Y$ such that for each $x \in X$, there is a **unique** $y \in Y$ such that $(x, y) \in f$.

So a function **is** a set of ordered pairs, and the notations are names for the same object:

$$y = 2x + 1 \qquad \text{or} \qquad f(x) = 2x + 1 \qquad \text{or} \qquad f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x + 1\}$$

with $f(x) = y$ meaning exactly $(x, y) \in f$, which is the bridge between the two styles.

Three graphs: the plot of $y = 2x + 1$ through $(-5, -9)$, $(0, 1)$ and $(5, 11)$; a curve that **is not a function**, because a vertical line meets it twice; and a wiggly curve that **is a function**, despite taking the same value more than once. The asymmetry is the definition: **repeated y-values are fine, repeated x-values are not.** The plots are in functions-on-general-sets[34].

Worked: Q1 from video 24 — which set of pairs is a function?

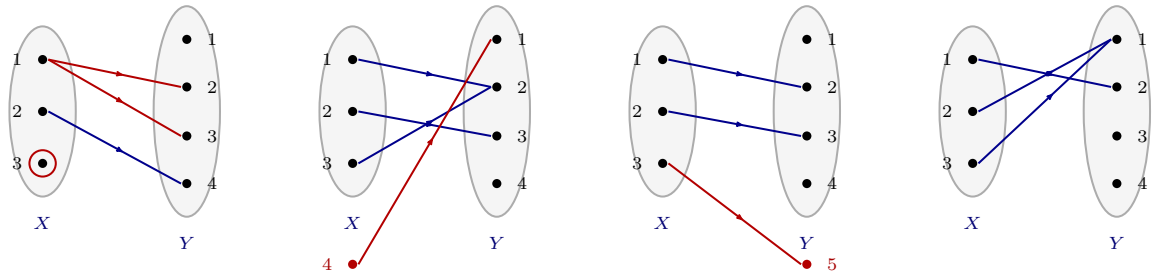
> Let $X = \{1, 2, 3\}$ and $Y = \{1, 2, 3, 4\}$. Which one of the following is a function from X to Y?

There are three conditions to check — $x \in X$, $y \in Y$, and $f(x)$ unique for all $x \in X$:

	Candidate	Why
(a)	$\{(1, 2), (1, 3), (2, 4)\}$	$f(1) = 2$ and $f(1) = 3$ — $f(1)$ **is not unique**
(b)	$\{(1, 2), (2, 3), (3, 2), (4, 1)\}$	$4 \notin X$
(c)	$\{(1, 2), (2, 3), (3, 5)\}$	$5 \notin Y$
(d)	$\{(1, 2), (2, 1), (3, 1)\}$	$1, 2, 3 \in X$, values $1, 2 \in Y$, and $f(1) = 2$, $f(2) = 1$, $f(3) = 1$ all unique

Each wrong option breaks a **different one** of the three conditions — which is what makes the question worth the time. In (d), $f(2) = f(3) = 1$; two inputs sharing a value is not a problem.

(a) fails twice over. As well as sending 1 to two places, it never gives 3 a value at all, so it breaks the "for each $x \in X$" half of the definition too.



(a) $\{(1,2),(1,3),(2,4)\}$
× $f(1)$ is not unique (and 3 gets no value)

(b) $\{(1,2),(2,3),(3,2),(4,1)\}$
× $4 \notin X$

(c) $\{(1,2),(2,3),(3,5)\}$
× $5 \notin Y$

(d) $\{(1,2),(2,1),(3,1)\}$
✓ a function
range $f(X) = \{1,2\}$

Figure 7: The four candidates drawn out, one panel each, with the offending pairs in red. (a) sends 1 to two places and leaves 3 with no value at all; (b) has a pair starting outside X; (c) has a pair landing outside Y; (d) satisfies all three conditions. Each panel is an arrow diagram: domain left, co-domain right, elements as labelled dots, the two bags named beneath in blue, and each mapping a line carrying a small arrowhead partway along pointing from X to Y.

Drawn out in Figure 7, the three failures are visibly different shapes of mistake: a fan-out from one point of X, a line starting outside X, and a line landing outside Y. Only (d) has exactly one line leaving each of 1, 2, 3, and both endpoints of every line in the right bag.

Q2 from video 24 — co-domain versus range

> For a function $f : X \to Y$ the **co-domain** is Y and the **range** is $f(X) = \{f(x) : x \in X\}$, which is a subset of Y.

For option (d) above:

$$\text{co-domain} = Y = \{1,2,3,4\} \qquad \text{range} = \{1,2\} \subseteq Y$$

The distinction in one line: **the co-domain is declared when you write $f : X \to Y$; the range is computed from the pairs.** 3 and 4 are permitted values that this function never takes.

[34] courses/math1061/functions-on-general-sets.pdf

Image and preimage

> If $f : X \to Y$ is **any** function and A is any subset of X, then the **image** of A is defined by $f(A) = \{f(x) : x \in A\}$.
>
> If $f : X \to Y$ is **any** function and B is any subset of Y, then the **inverse image** or **preimage** of B is defined by $f^{-1}(B) = \{x \in X : f(x) \in B\}$.

Both take a set and return a set: $f(A)$ and $f^{-1}(B)$ are themselves **sets**. The emphasis on **any** matters too: $f^{-1}(B)$ is defined for every function, invertible or not. It is not an inverse function.

Worked: images and preimages

> Let $X = \{1, 2, 3\}$ and $Y = \{1, 2, 3, 4\}$. From Q1 of video 24 above, $\{(1, 2), (2, 1), (3, 1)\}$ is a function from X to Y.

So $f(1) = 2$, $f(2) = 1$, $f(3) = 1$.

	Asked for	Working	Answer
(a)	image of $\{1\}$	$f(1) = 2$	$f(\{1\}) = \{2\}$
(b)	image of $\{2, 3\}$	$f(2) = 1$, $f(3) = 1$	$f(\{2, 3\}) = \{1\}$
(c)	inverse image of $\{2\}$	only 1 maps to 2	$f^{-1}(\{2\}) = \{1\}$
(d)	preimage of $\{1\}$	both 2 and 3 map to 1	$f^{-1}(\{1\}) = \{2, 3\}$
(e)	preimage of $\{3, 4\}$	nothing maps to 3 or 4	$f^{-1}(\{3, 4\}) = \emptyset$

On an arrow diagram, the images follow the arrows forwards and the preimages follow them backwards. Both diagrams are in functions-on-general-sets[35].

The three things this set of answers is built to show: an **image can shrink** (b), a **preimage can grow** (d), and a **preimage can be empty** (e) when the set sits outside the range. All three are ordinary, not failures — and every answer is a **set**, so the braces are not optional. In part (c), write $\{1\}$, not 1.

[35] courses/math1061/functions-on-general-sets.pdf

See also

- proving-set-properties[36] — the reference note for the three methods and the set identities
- functions-on-general-sets[37] — the reference note for the second half
- sets-and-set-notation[38] — the definitions from Lecture 17 that this builds on
- logical-equivalence-laws[39] · proof-techniques[40] · formula-sheet[41]
- 2026-09-03-set-theory-definitions[42] — Lecture 17
- practice-problems[43] — §23 Properties of Sets, with full worked solutions
- practice-problems[44] — §24 Functions Defined on General Sets

Lecture 17 — Set Theory Definitions and Examples

Pre-work: Video 021 (Set Theory Definitions) and Video 022 (More definitions and examples of sets). See sets-and-set-notation[45] for the reference material — every definition below, with the worked examples and the diagrams.

Learning goals

1. Understand the distinction between **"is an element of"** $x \in A$ and **"is a subset of"** $A \subseteq B$.
2. Be comfortable with notation for sets including

$$x \in A, \quad A \subseteq B, \quad A \subset B, \quad A \cap B, \quad A \cup B, \quad A - B, \quad A^c, \quad \mathcal{P}(A), \quad A \times B$$

Element, subset, proper subset

What is the difference between "is a subset of" $\subseteq$ and "is a proper subset of" $\subset$? A four-way comparison settles it:

[36] courses/math1061/proving-set-properties.pdf
[37] courses/math1061/functions-on-general-sets.pdf
[38] courses/math1061/sets-and-set-notation.pdf
[39] courses/math1061/logical-equivalence-laws.pdf
[40] courses/math1061/proof-techniques.pdf
[41] courses/math1061/formula-sheet.pdf
[42] courses/math1061/2026-09-03-set-theory-definitions.pdf
[43] courses/math1061/practice-problems.pdf
[44] courses/math1061/practice-problems.pdf
[45] courses/math1061/sets-and-set-notation.pdf

	$\subseteq$	$\subset$
$\mathbb{Z}$ against $\mathbb{R}$	$\mathbb{Z} \subseteq \mathbb{R}$	$\mathbb{Z} \subset \mathbb{R}$
$\mathbb{Z}$ against itself	$\mathbb{Z} \subseteq \mathbb{Z}$	$\mathbb{Z} \not\subset \mathbb{Z}$

A set is always a subset of itself, and never a **proper** subset of itself. That single row is the entire difference — exactly parallel to $\leq$ against $<$.

What is the difference between "is a subset of" and "is an element of"? A concrete universe shows it better than a symbol:

> Let $L :=$ {everyone in the lecture theatre}, and let $m :=$ *me* and $y :=$ *you*.

Four memberships hold: $m \in L$, $y \in L$, $\{m\} \subseteq L$, $\{m, y\} \subseteq L$. The two braced objects are sets. A person is an **element**; a *group* of people is a **subset**. One is a person, the other is a collection of people. Just as $2 \neq \{2\}$ (below), $m \neq \{m\}$ — a person is not a group containing one person.

The other people in the room are drawn into Figure 8 for a reason: $\{m, y\}$ is *a* subset of L, not *the* subset. Every group you can pick out of the room is one, and there are a great many of them — how many exactly is the power set fact further down this page.

Why isn't $\mathbb{Z} \in \mathbb{Q}$ — aren't all integers rational numbers? They are, and that is exactly the claim $\mathbb{Z} \subseteq \mathbb{Q}$. But $\mathbb{Z} \in \mathbb{Q}$ says $\mathbb{Z}$ is *one of the rational numbers*, and $\mathbb{Z}$ is a **set of numbers**, not a number. The instinct is right; the symbol is wrong.

Set difference — do the backslash and the minus sign mean the same thing? Yes. $A - B$ can be written $A \setminus B$. Purely a matter of which textbook you are reading.

Q2 from the pre-class questions

> **True or false?** $\mathbb{Z} \in \mathbb{Q}$

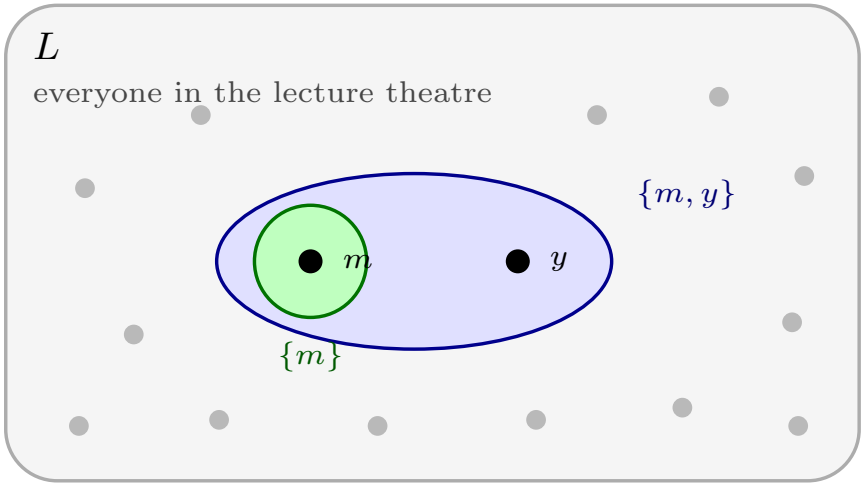
False. $\mathbb{Z}$ is a set of numbers, so it is not an element of $\mathbb{Q}$; the true statement is $\mathbb{Z} \subseteq \mathbb{Q}$.

Take care with the distinction between "is an element of" and "is a subset of".

And one level down: **a single element is not the same as the set containing a single element**, so $2 \neq \{2\}$.

Worked: is it an element?

> Determine whether each of the following is true or false.



elements — a *person*:
$m \in L$ $\quad y \in L$

subsets — a *group* of people:
$\{m\} \subseteq L$ $\quad \{m, y\} \subseteq L$

$m \neq \{m\}$ — a person is not a group of one person

Figure 8: The lecture theatre example drawn out. A person in the room is an element of L; any group of people in the room is a subset of L. The two symbols relate different kinds of thing, which is why m and {m} are not the same object even though the group has exactly one member.

	Statement		Reasoning
a)	$4 \in \{4\}$	**True**	$\{4\}$ contains 4 as an element
b)	$4 \in \{\{4\}\}$	**False**	$\{\{4\}\}$ does **not** contain 4 as an element — it does contain $\{4\}$ as an element
c)	$\{4\} \in \{2, 3, 4\}$	**False**	$\{2, 3, 4\}$ does **not** contain $\{4\}$ as an element — it does contain 4 as an element

(b) and (c) are parallel: in each case the set contains *something*, just not the thing being asked about. $\{4\} \subseteq \{2, 3, 4\}$ **is** true — (c) fails on the symbol, not on the containment.

The reliable technique is to write the set's elements out as a list and ask whether the left-hand object is literally one of them. For $\{\{4\}\}$ that list has one entry, the set $\{4\}$, and 4 is not it.

Subsets and proper subsets

A set S is a **subset** of a set T, denoted $S \subseteq T$, if every element that is in S is also in T. Formally we say $\forall x$, if $x \in S$ then $x \in T$.

A set S is a **proper subset** of a set T, denoted $S \subset T$, if $S \subseteq T$ **and** there is an element in T that is not in S.

Examples: $\mathbb{Z} \subseteq \mathbb{Q}$ and $\mathbb{Z} \subseteq \mathbb{Z}$; $\mathbb{Z} \subset \mathbb{Q}$ but $\mathbb{Z} \not\subset \mathbb{Z}$.

For sets S and T, to prove that $S \subseteq T$, you consider an **arbitrary** element of S and show that it is also in T. That is, we suppose $x \in S$ and prove that $x \in T$.

Worked: prove one set is a subset of another

(a) Let $D = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and let E be the set of even integers. Prove that $D \subseteq E$.

Writing out both sets first makes the shape of the proof obvious:

$$D = \{\dots, 2, 10, 18, \dots\} \qquad E = \{\dots, 2, 4, 6, 8, \dots\} = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 2\}$$

Rewriting E as a congruence class is the move that makes the two sets comparable — both are now "$\equiv$ something", and the proof is arithmetic.

Proof. Let $x \in D$. Then $x \equiv 2 \pmod 8$, so $\exists k \in \mathbb{Z}$ such that

$$x = 8k + 2 = 2(4k + 1) + 0$$

$\therefore x \equiv 0 \pmod 2$, $\therefore x \in E$. Thus $D \subseteq E$. ■

(b) Is $D \subset E$?

Yes. $4 \in E$ but $4 \notin D$, so $D \subseteq E$ is proper. One witness is all a proper containment needs.

When are two sets equal?

For sets S and T, saying $S = T$ means $\forall x$, $x \in S$ **if and only if** $x \in T$.

Recall that $S \subseteq T$ means $\forall x$, if $x \in S$ then $x \in T$. Since $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, it follows that $S = T$ is logically equivalent to $(S \subseteq T) \wedge (T \subseteq S)$.

So to prove two sets S and T are equal you do **two separate proofs**: suppose $x \in S$ and prove $x \in T$ (giving $S \subseteq T$), then suppose $x \in T$ and prove $x \in S$ (giving $T \subseteq S$). Together these show $S = T$.

This is a **consequence**, not a convention — it is the biconditional law of logical-equivalence-laws[46] read through the definition of $\subseteq$.

The empty set

$\emptyset = \{\ \}$

Why is $\emptyset \subseteq A$ for every set A? Because "$\forall x$, if $x \in \emptyset$ then $x \in A$" is true for every set A. The hypothesis is never satisfied, so the conditional is **vacuously true** — the F-hypothesis row of the truth table in conditional-statements[47] is doing all the work.

Take the two halves of the conditional separately: $x \in \emptyset$ is **F** — always false, whatever x is — and $x \in A$ is **F/T**, because it could go either way. A conditional with a false hypothesis is true regardless of the conclusion, so the implication holds for every x and every A.

Do not confuse this with $\emptyset \in A$. There are some sets that do contain the empty set, but there are lots of sets that do not.

Why is $A \subseteq A$ for every set A? Because "$\forall x$, if $x \in A$ then $x \in A$" is true for every set A — this time because the conclusion restates the hypothesis.

[46] courses/math1061/logical-equivalence-laws.pdf
[47] courses/math1061/conditional-statements.pdf

Lemma. There is only one empty set.

Proof (by contradiction). Suppose that $\emptyset_1$ and $\emptyset_2$ are distinct sets each having no elements, so $\emptyset_1 \neq \emptyset_2$. Since $\emptyset_1$ has no elements, it is a subset of $\emptyset_2$, that is, $\emptyset_1 \subseteq \emptyset_2$. Also since $\emptyset_2$ has no elements, we have $\emptyset_2 \subseteq \emptyset_1$. Thus $\emptyset_1 = \emptyset_2$ by definition of set equality, and we have reached a contradiction. ■

Hence $\emptyset_1 = \emptyset_2 = \emptyset$ — *the* empty set, which is why it gets a symbol of its own.

Unions and intersections

Let $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 4\}$ and $A_3 = \{3, 4, 5\}$.

$$A_1 \cup A_2 = \{1, 2, 3, 4\} \qquad A_1 \cap A_2 = \{1, 2\} \qquad A_1 \cap A_3 = \{3\} \qquad A_2 \cap A_3 = \{4\}$$

$$\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 = \{1, 2, 3, 4, 5\}$$

$$\bigcap_{i=1}^{3} A_i = (A_1 \cap A_2) \cap A_3 = \{1, 2\} \cap \{3, 4, 5\} = \emptyset$$

All three pairwise intersections are non-empty, and the triple intersection is still empty. Pairwise overlap does not propagate to the whole family.

Worked: an infinite union and an infinite intersection

Determine the following sets, recalling the interval notation $[a, b] = \{x \in \mathbb{R} \mid a \leq x \leq b\}$.

$$\bigcup_{i=0}^{\infty} \{i, -i\} = \{0, -0\} \cup \{1, -1\} \cup \{2, -2\} \cup \cdots = \{\dots, -2, -1, 0, 1, 2, \dots\} = \mathbb{Z}$$

$$\bigcap_{i=0}^{\infty} [-i,\, i] = \{0\}$$

For the intersection, the intervals **grow** with i — $[0, 0] \subseteq [-1, 1] \subseteq [-2, 2] \subseteq \cdots$ — so the intersection is pinned by the smallest, the $i = 0$ term $[0, 0] = \{0\}$. The nested intervals are drawn on a number line in sets-and-set-notation[48].

[48] courses/math1061/sets-and-set-notation.pdf

The power set

Let $S = \{1, 2, 3\}$. Then $\mathcal{P}(S) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$

The elements of a power set are **sets**, which resets the $\in/\subseteq$ trap one level up:

$\{1, 2\} \in \mathcal{P}(S)$	it is one of the eight things listed
$\{1, 2\} \nsubseteq \mathcal{P}(S)$	that would need 1 and 2 to be elements of $\mathcal{P}(S)$
$\{\{1, 2\}\} \subseteq \mathcal{P}(S)$	its one element, $\{1, 2\}$, is in $\mathcal{P}(S)$

Since $\emptyset \subseteq A$ for every set A, it follows that $\emptyset \in \mathcal{P}(A)$ for every set A.

Fact. If T is a **finite** set that contains n elements, then $|\mathcal{P}(T)| = 2^n$.

This fact is **important**. The **finite** qualifier is part of it, and the 2^n comes from building a subset by making n independent in-or-out choices.

Worked: element or subset of a power set?

True or false? $\{1, 3, -1\} \subset \mathcal{P}(\mathbb{Z})$

False, by walking the levels carefully:

$$1, 3, -1 \in \mathbb{Z} \ \therefore \{1, 3, -1\} \subseteq \mathbb{Z} \ \therefore \{1, 3, -1\} \in \mathcal{P}(\mathbb{Z}) \ \text{ so } \ \{1, 3, -1\} \nsubseteq \mathcal{P}(\mathbb{Z})$$

It is an **element** of the power set, not a subset of it. For it to be a subset, its own elements 1, 3, -1 would have to be subsets of $\mathbb{Z}$ — and they are integers, not sets. The statement is off by exactly one level.

Worked: write down each power set

Number the elements while writing them and then check each answer against 2^n, which is the cheapest way to catch a dropped brace:

Power set	Value	Check
$\mathcal{P}(\{a\})$	$\{\emptyset,\ \{a\}\}$	$\lvert\{a\}\rvert = 1$, so $2^1 = 2$
$\mathcal{P}(\emptyset)$	$\{\emptyset\}$	$\lvert\emptyset\rvert = 0$, so $2^0 = 1$
$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$	$\{\emptyset,\ \{\emptyset\}\}$	$\lvert\{\emptyset\}\rvert = 1$, so $2^1 = 2$
$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset, \{\emptyset\}\})$	$\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\}\}$	$\lvert\{\emptyset, \{\emptyset\}\}\rvert = 2$, so $2^2 = 4$

The line to get right is $\mathcal{P}(\emptyset) = \{\emptyset\}$: the empty set has exactly one subset — itself — so its power set has **one** element and is **not** empty.

Cartesian products

Let $A_1 = \{1, 2\}$, $A_2 = \{3, 4, 5\}$ and $A_3 = \{6\}$.

$$A_1 \times A_2 = \{(1,3), (1,4), (1,5), (2,3), (2,4), (2,5)\}$$
$$A_1 \times A_2 \times A_3 = \{(1,3,6), (1,4,6), (1,5,6), (2,3,6), (2,4,6), (2,5,6)\}$$

with $|A_1 \times A_2| = |A_1| \cdot |A_2| = 2 \times 3 = 6$. The product is drawn as a grid of points in sets-and-set-notation[49].

Let $S = \{a, b, c\}$ and $T = \{c, d\}$.

- $(d, c) \notin S \times T$ since $d \notin S$ — **order matters**.
- $(c, d) \in S \times T$ since $c \in S$ and $d \in T$.
- $S \times T$ contains $3 \times 2 = 6$ elements.

The familiar case is $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$, often denoted $\mathbb{R}^2$.

Two more facts: if $A = \emptyset$ or $B = \emptyset$ then $A \times B = \emptyset$; and for finite sets, $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

> **Notation issue to be aware of.** (a, b) can be used for an **ordered pair**. (a, b) can also be used as an **interval**, representing the real numbers x where $a < x < b$. Only context distinguishes them.

Partitions

> A finite or infinite collection of **non-empty** sets $\{A_1, A_2, A_3, \dots\}$ is a **partition** of a set A if and only if
>
> $$A = A_1 \cup A_2 \cup A_3 \cup \cdots \qquad \text{and} \qquad A_i \cap A_j = \emptyset \text{ for each } i, j \geq 1,\ i \neq j$$

Examples. A partition of $\mathbb{Z}$ is given by $\{E, O\}$ where E is the even integers and O the odd integers. Another partition of $\mathbb{Z}$ is $\{\{0\}, \mathbb{Z}^+, \mathbb{Z}^-\}$ — the same set, partitioned two different ways.

[49] courses/math1061/sets-and-set-notation.pdf

Worked: partitions

(a) Let $S = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\}$, let $T = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4\}$, and let $R = S \cup T$. Is $\{S, T\}$ a partition of the set R? Explain why or why not.

No. The covering condition $R = S \cup T$ holds by definition, but disjointness fails:

$$10 \equiv 1 \pmod 3 \;\Rightarrow\; 10 \in S \qquad \text{and} \qquad 10 \equiv 2 \pmod 4 \;\Rightarrow\; 10 \in T$$

So $10 \in S \cap T$, hence $S \cap T \neq \emptyset$, and $\{S, T\}$ is **not** a partition of R. Stripe the two congruence classes along a number line — pink for S, green for T — and a tick carrying both colours is a point of $S \cap T$.

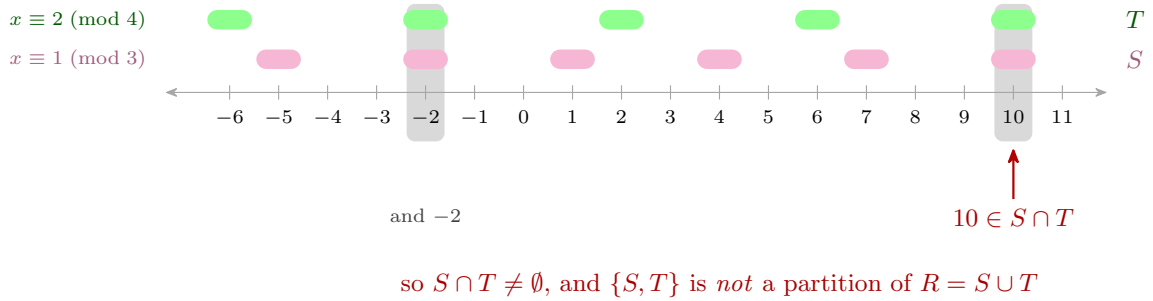


Figure 9: Finding the counterexample: the two congruence classes striped along the integers — S every third integer (pink row), T every fourth (green row) — and read off for a tick that both stripes cover. The grey capsules mark those ticks, which are the overlap.

The grey capsules mark every tick both stripes cover in the range drawn — 10 is the witness above, and -2 works equally well. Two witnesses are no better than one here: disjointness is a *universal* claim, so a single overlap kills it.

(b) State two different partitions of the set $\mathbb{Z} \times \mathbb{Z}$.

By the sign of the first coordinate:

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \geq 0\} \qquad L = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a < 0\}$$

$\{L, R\}$ is a partition of $\mathbb{Z} \times \mathbb{Z}$.

By the parity of the second coordinate:

$$E = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 0 \pmod 2\} \qquad O = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 1 \pmod 2\}$$

$\{E, O\}$ is another partition of $\mathbb{Z} \times \mathbb{Z}$.

Picture $\mathbb{Z} \times \mathbb{Z}$ as a lattice of dots carrying **both** partitions at once: a block over the right half of the lattice against a block over the left half for $\{L, R\}$, and horizontal stripes alternating row by row for the parity split $\{E, O\}$ — the same "cut the whole thing up and check nothing is covered twice" picture as Figure 9, one dimension up.

The general recipe: **any property that every element either has or lacks splits the set into two parts that partition it**, provided neither part is empty. Made exact later in the course by equivalence relations.

See also

- sets-and-set-notation[50] — the reference note for all of the above
- proving-set-properties[51] · functions-on-general-sets[52] — where Lecture 18 takes this
- modular-arithmetic[53] — the congruence classes in the subset proof and the partition question
- conditional-statements[54] · logical-equivalence-laws[55] — vacuous truth, and the biconditional behind set equality
- 2026-08-31-solving-recurrence-relations[56] — Lecture 16
- 2026-09-03-set-properties-and-functions[57] — Lecture 18
- practice-problems[58] — §21 Set Theory Definitions, with full worked solutions
- practice-problems[59] — §22 More Definitions and Examples of Sets

Reference material

Conditional & Biconditional Statements

Conditional ($\rightarrow$)

p	q	$p \rightarrow q$
T	T	T
T	F	F

[50] courses/math1061/sets-and-set-notation.pdf
[51] courses/math1061/proving-set-properties.pdf
[52] courses/math1061/functions-on-general-sets.pdf
[53] courses/math1061/modular-arithmetic.pdf
[54] courses/math1061/conditional-statements.pdf
[55] courses/math1061/logical-equivalence-laws.pdf
[56] courses/math1061/2026-08-31-solving-recurrence-relations.pdf
[57] courses/math1061/2026-09-03-set-properties-and-functions.pdf
[58] courses/math1061/practice-problems.pdf
[59] courses/math1061/practice-problems.pdf

p	q	$p \to q$
F	T	T
F	F	T

Only one row makes a conditional false: the row where the hypothesis p is true and the conclusion q is false. Everything else is true, including both rows where p is false.

$p \to q$ is true when p is false **because that is how it is defined.** There is no deeper intuition to recover; $\to$ is a truth-functional connective fixed by the table above, and arguing with the bottom two rows is arguing with a definition. The standard name for those two rows is **vacuous truth**. It does real work later: it is why $\emptyset \subseteq A$ for every set A (see sets-and-set-notation[60]).

The picture behind the table is containment:

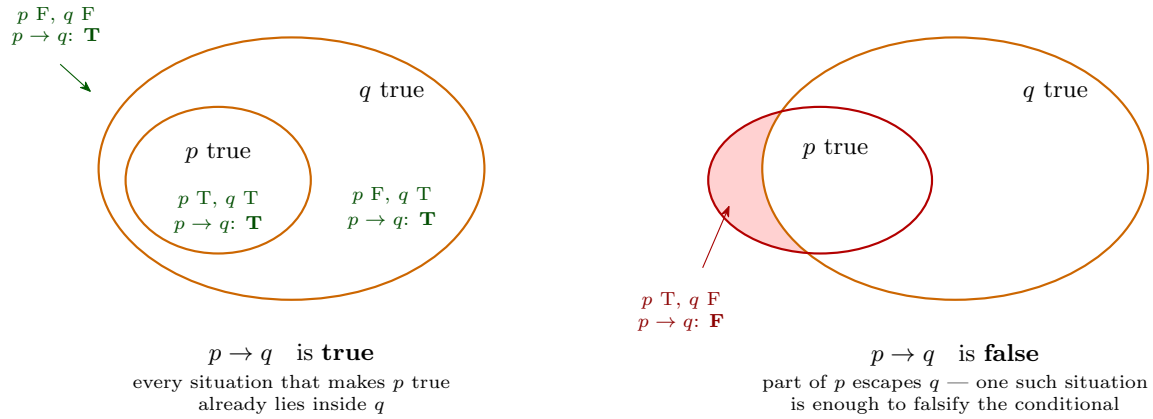


Figure 10: Why the truth table has the shape it does. Left: p $\to$ q asserts that the situations making p true all lie inside the situations making q true, so every region carries T. Right: the conditional fails exactly when part of p escapes q, which is the single F row of the table.

Disjunctive form

By definition,

$$p \to q \equiv \sim p \vee q$$

[60] courses/math1061/sets-and-set-notation.pdf

The right-hand side is the **disjunctive form** of the conditional, and it is the single most useful fact in the topic: the laws of logical equivalence (see logical-equivalence-laws[61]) are stated only for $\sim$, $\wedge$ and $\vee$, so they say nothing about $\rightarrow$ directly. To use the laws on a conditional:

> **Replace $p \rightarrow q$ with $\sim p \vee q$ and then use the laws.**

Every worked proof about conditionals in this course starts and (usually) ends with that substitution.

$p \rightarrow q$ can be phrased: "p implies q", "if p then q", "q if p", "p is sufficient for q", "p only if q", "q is necessary for p".

Warning: $p \rightarrow q \not\equiv q \rightarrow p$.

Contrapositive, converse, inverse

Name	Form	Equivalent to
Conditional	$p \rightarrow q$	Contrapositive
Contrapositive	$\sim q \rightarrow \sim p$	Conditional
Converse	$q \rightarrow p$	Inverse
Inverse	$\sim p \rightarrow \sim q$	Converse

The conditional and its **contrapositive** are always logically equivalent. The **converse** and **inverse** are always logically equivalent to each other — but *not* to the original conditional.

Both equivalences fall straight out of the disjunctive form. For the first: $p \rightarrow q \equiv \sim p \vee q$ and $\sim q \rightarrow \sim p \equiv \sim(\sim q) \vee \sim p \equiv q \vee \sim p$, which is the same disjunction commuted. The converse/inverse pair is the same computation with p and q interchanged.

Necessary and sufficient conditions

- p is a **necessary condition** for q means "if $\sim p$ then $\sim q$", or equivalently "if q then p", or "q **only if** p". In symbols, $q \rightarrow p$.
- p is a **sufficient condition** for q means "if p then q", or equivalently "q **if** p". In symbols, $p \rightarrow q$.

The two phrasings of "necessary" are contrapositives of each other, which is why they say the same thing: $\sim p \rightarrow \sim q$ and $q \rightarrow p$.

The reliable reading is: **"if" introduces the sufficient condition; "only if" introduces the necessary one.**

[61] courses/math1061/logical-equivalence-laws.pdf

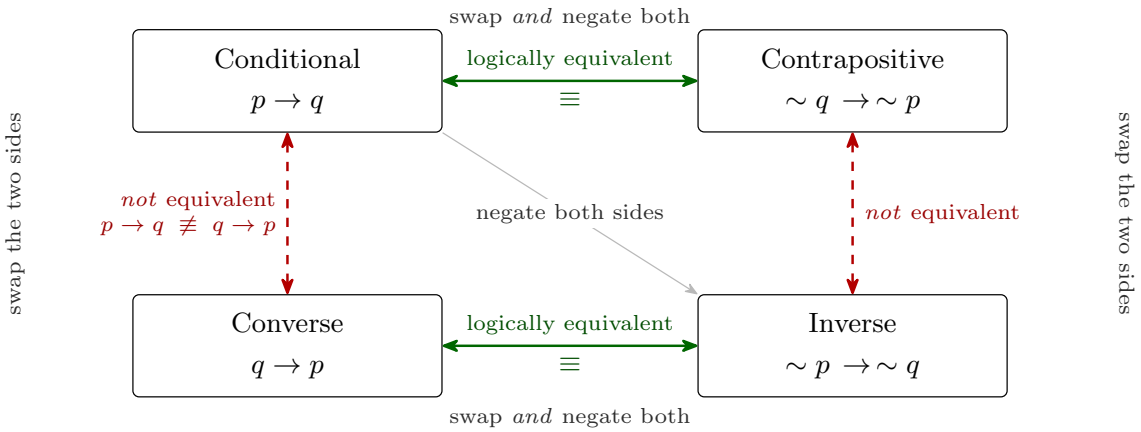


Figure 11: The four forms and the only equivalences among them. The conditional and the contrapositive are one logically equivalent pair, the converse and the inverse are the other, and p → q q → p. Swapping the two sides gives the converse, negating both gives the inverse, and doing both gives the contrapositive — the only one of the three that preserves meaning.

Worked: necessary but not sufficient

Being a non-negative integer is necessary for a number to be the square of an integer, but it is not sufficient.

- *Necessary*: if a number is the square of an integer, then it is non-negative. So −9 cannot be the square of an integer — failing the condition rules the number out.
- *Not sufficient*: 7 is a non-negative integer but it is not the square of an integer. Meeting the condition does not settle it.

Worked: sufficient but not necessary

Being an integer that is divisible by 4 is sufficient for being an even integer, but it is not necessary.

- *Sufficient*: if an integer is divisible by 4, then it is even. 8 is divisible by 4, so we know 8 is even without checking anything else.
- *Not necessary*: 10 is an even integer but 10 is not divisible by 4. The condition can fail while the conclusion still holds.

The two shapes are exactly opposite in how they are refuted: a claimed **sufficient** condition is killed by something satisfying the condition but not the conclusion; a claimed **necessary** condition is killed by something satisfying the conclusion but not the condition.

Biconditional ($\leftrightarrow$)

$$a \leftrightarrow b \equiv (a \to b) \wedge (b \to a)$$

A biconditional is the two one-way conditionals conjoined, and each of the standard English phrasings splits along the same seam:

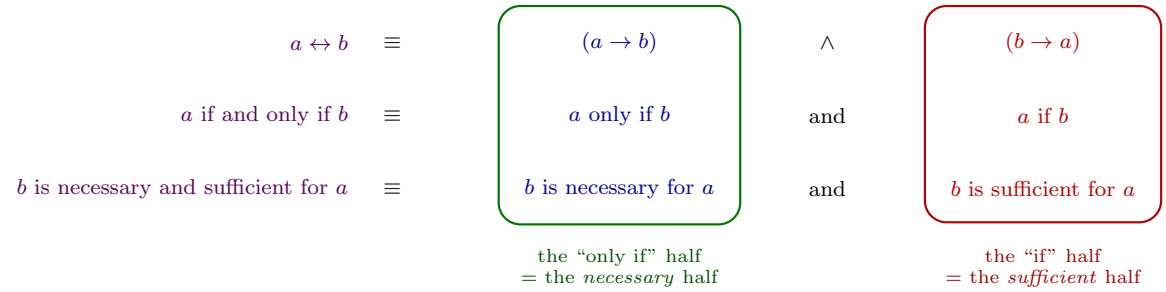


Figure 12: The biconditional decomposed three ways, with each half in its own ringed column. Reading down the left column: a → b, 'a only if b', 'b is necessary for a' are three names for the same half. Reading down the right: b → a, 'a if b', 'b is sufficient for a'. The whole necessary/sufficient vocabulary is just this correspondence — 'only if' is the necessary half, 'if' is the sufficient half.

Negating a conditional

$$\sim (p \to q) \equiv \sim (\sim p \vee q) \equiv p \wedge \sim q$$

by the definition of →, then De Morgan's law, then the double negative law.

The negation of a conditional is not a conditional — it's an *and*. "If it rains, the match is cancelled" is negated by "it rains **and** the match is not cancelled", not by "if it rains, the match is not cancelled".

The classic error is to answer $\sim p \to \sim q$ (that's the *inverse*) or $q \to p$ (the *converse*). Neither is the negation, and neither is even equivalent to the original — see Figure 11 above.

Worked: $\sim (p \to q) \not\equiv \sim p \to \sim q$**.** Let p be **true** and q be **true**. Then $p \to q$ is true, so $\sim (p \to q)$ is **false**. But $\sim p \to \sim q$ is F → F, which is **true**. The two differ on this row, so they are not equivalent.

Sanity check on the shapes: $\sim (p \to q)$ is a conjunction and is true on exactly **one** of the four rows; $\sim p \to \sim q$ is a conditional and is true on **three**. They could hardly be equivalent.

Order of operations

1. $\sim$
2. $\wedge, \vee$ (equal)
3. $\rightarrow, \leftrightarrow$ (equal)

Within a tier, work left to right if no parentheses are given. So $p \rightarrow \sim q \vee r$ means $p \rightarrow ((\sim q) \vee r)$ — but parenthesise explicitly rather than relying on the tie-breaking rule.

Notation, not to be blurred: the biconditional $\leftrightarrow$ is a connective used to **combine** statements (like $+$, $-$, $\times$, $\div$ with numbers). Logical equivalence $\equiv$ is used when **comparing** two statements (like $=$ with numbers). $a \leftrightarrow b$ is a statement; $a \equiv b$ is a claim *about* two statements.

See also

- logical-connectives[62]
- logical-equivalence-laws[63]
- sets-and-set-notation[64] — vacuous truth doing real work, in $\emptyset \subseteq A$
- 2026-07-30-conditional-statements[65] — Lecture 3
- practice-problems[66] — §3 Conditional Statements, with full worked solutions

The Examination Formula Page

The *MATH1061/MATH7861 Examination Formula Page* is **provided in both exams**, which are otherwise closed book with no written materials permitted (see math1061[67]). Knowing what is on it — and what is not — is what decides whether a fact needs memorising.

It has **seven blocks**.

1. Logical equivalences

Eleven named laws, given any statement variables p, q, r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$. Reproduced in full in logical-equivalence-laws[68].

[62] courses/math1061/logical-connectives.pdf
[63] courses/math1061/logical-equivalence-laws.pdf
[64] courses/math1061/sets-and-set-notation.pdf
[65] courses/math1061/2026-07-30-conditional-statements.pdf
[66] courses/math1061/practice-problems.pdf
[67] courses/math1061/math1061.pdf
[68] courses/math1061/logical-equivalence-laws.pdf

Commutative · Associative · Distributive · Identity · Negation · Double negative · Idempotent · Universal bound · De Morgan's · Absorption · Negations of **t** and **c**.

2. Valid argument forms

Nine forms. Reproduced in full in valid-argument-forms[69].

Modus Ponens · Modus Tollens · Generalization (a)(b) · Specialization (a)(b) · Conjunction · Elimination (a)(b) · Transitivity · Proof by division into cases · Contradiction Rule.

3. Set identities

Twelve numbered laws, for all sets A, B, C that are subsets of a universal set U:

	Law	
1	Commutative	$A \cup B = B \cup A$ · $A \cap B = B \cap A$
2	Associative	$(A \cup B) \cup C = A \cup (B \cup C)$ · $(A \cap B) \cap C = A \cap (B \cap C)$
3	Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ · $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4	Identity	$A \cup \emptyset = A$ · $A \cap U = A$
5	Complement	$A \cup A^c = U$ · $A \cap A^c = \emptyset$
6	Double complement	$(A^c)^c = A$
7	Idempotent	$A \cup A = A$ · $A \cap A = A$
8	Universal bound	$A \cup U = U$ · $A \cap \emptyset = \emptyset$
9	De Morgan's	$(A \cup B)^c = A^c \cap B^c$ · $(A \cap B)^c = A^c \cup B^c$
10	Absorption	$A \cup (A \cap B) = A$ · $A \cap (A \cup B) = A$
11	Complement of U and $\emptyset$	$U^c = \emptyset$ · $\emptyset^c = U$
12	Set difference	$A - B = A \cap B^c$

Reproduced with worked proofs in proving-set-properties[70].

Note the one-to-one correspondence with the logical equivalences in block 1 — laws 1–11 are those same eleven laws in the same order, plus set difference at 12. The names are not quite identical: *negation* becomes **complement** (5), *double negative* becomes **double complement**

[69] courses/math1061/valid-argument-forms.pdf
[70] courses/math1061/proving-set-properties.pdf

(6), and *negations of* **t** *and* **c** becomes **complement of** U **and** $\emptyset$ (11). That correspondence is not a coincidence: $\cup$ behaves as $\vee$, $\cap$ as $\wedge$, and complement as $\sim$. Law 12 is the one with no counterpart in block 1.

The numbering is not decoration — it is how the course expects you to cite. The worked identity proof in Lecture 18 justifies its lines by the number on this page: *by set diff law (12)*, *by de Morgan (9b)*, *dist. law (3b)*, *complement law (5b)*, *identity law (4a)* — only the double complement step goes uncited there, by name alone. Naming and numbering the law is where the marks are, and this page is in front of you while you do it.

4. The Quotient-Remainder Theorem

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

See modular-arithmetic[71]. The uniqueness clause and the range $0 \leq r < d$ are what let you read a remainder off a rearranged expression.

5. Unique Factorisation Theorem

> Given any integer $n > 1$, there exists a positive integer k, distinct prime numbers $p_1, p_2, \ldots, p_k$, and positive integers $e_1, e_2, \ldots, e_k$ such that
>
> $$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$
>
> and **any other expression for n as a product of prime numbers is identical to this except perhaps for the order** in which the factors are written.

See divisibility-and-factorisation[72]. The second half is the "unique" part, and it is the half students leave out when asked to state the theorem.

6. Schröder-Bernstein Theorem

> For all sets A and B, if $|A| \leq |B|$ and $|A| \geq |B|$ then $|A| = |B|$.

See cardinality[73]. In use it means two injections, one each way, in place of one bijection, and the two must point in opposite directions between the same two sets.

[71] courses/math1061/modular-arithmetic.pdf
[72] courses/math1061/divisibility-and-factorisation.pdf
[73] courses/math1061/cardinality.pdf

7. Binomial Theorem

Given any real numbers a and b, and any nonnegative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$$

Belongs to the counting material (L30–L31). The coefficient $\binom{n}{k}$ is "n choose k", the number of k-element subsets of an n-element set (counting-selections[74]). The theorem, with its proof by counting a, b-sequences and the method for picking one coefficient out of an expansion, is in binomial-coefficients[75].

What this means for revision

Blocks 1 and 2 are the bulk of the page and are reproduced in the vault, so for the logic material the assessed skill is **recognising and naming** which law or form applies — not recalling the list.

Block 3 works the same way: the set identities are given, so the assessed skill is choosing and **citing by number**, not reciting the twelve laws — see proving-set-properties[76] for both worked methods that use them.

Blocks 4 and 5 are covered by modular-arithmetic[77] and divisibility-and-factorisation[78]. Block 6 is covered by cardinality[79]. Block 7 is covered by binomial-coefficients[80], and its $\binom{n}{k}$ by counting-selections[81].

Nothing else is provided. In particular the whole of set theory apart from block 3 — the definitions of $\subseteq$, $\subset$, $\mathcal{P}(A)$, $A \times B$, partition, function, image and preimage — is **not** on the page, and neither is any proof technique, nor anything about sequences, induction and recursion. Nor is anything about relations, groups or fields: the definitions of reflexive, symmetric, transitive and antisymmetric, of an equivalence relation (equivalence-relations[82]) and a partial order (partial-order-relations[83]), the four group properties (groups[84]), the subgroup checks (subgroups-and-cyclic-groups[85]) and the conditions for a field (fields[86]). Nor are the counting

[74] courses/math1061/counting-selections.pdf
[75] courses/math1061/binomial-coefficients.pdf
[76] courses/math1061/proving-set-properties.pdf
[77] courses/math1061/modular-arithmetic.pdf
[78] courses/math1061/divisibility-and-factorisation.pdf
[79] courses/math1061/cardinality.pdf
[80] courses/math1061/binomial-coefficients.pdf
[81] courses/math1061/counting-selections.pdf
[82] courses/math1061/equivalence-relations.pdf
[83] courses/math1061/partial-order-relations.pdf
[84] courses/math1061/groups.pdf
[85] courses/math1061/subgroups-and-cyclic-groups.pdf
[86] courses/math1061/fields.pdf

rules and selection formulas of counting-principles[87] and counting-selections[88], Pascal's formula, inclusion/exclusion (inclusion-exclusion[89]), the pigeonhole principle (pigeonhole-principle[90]) or the Handshake Theorem (graphs[91]). Nor is any of the rest of the graph theory: the definitions of walk, trail, circuit and connected (walks-trails-and-circuits[92]), the Euler circuit and trail theorem (euler-circuits-and-trails[93]), adjacency and incidence matrices (adjacency-matrices[94], incidence-matrices[95]), or the theorem that a tree with n vertices has $n-1$ edges (trees[96]). All of that has to come from memory.

Functions on General Sets

The set-theoretic definition of a function — not "a rule" or "a formula", but a particular kind of **subset of a Cartesian product**. See sets-and-set-notation[97] for the Cartesian products this is built on.

The definition

> A **function** $f : X \to Y$ is a subset $f \subseteq X \times Y$ such that for each $x \in X$, there is a **unique** $y \in Y$ such that $(x, y) \in f$.

The function *is* the set of pairs. There is no separate "rule" object — the familiar notations are all names for the same set:

$$y = 2x + 1 \qquad \text{or} \qquad f(x) = 2x + 1 \qquad \text{or} \qquad f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x + 1\}$$

and the bridge between the two styles is

$$f(x) = y \quad \iff \quad (x, y) \in f$$

Defining a function this way costs a little intuition and buys a great deal of precision: **the definition applies to any sets at all**, not just sets of numbers, and questions like "are these two functions equal?" become ordinary questions about set equality.

[87] courses/math1061/counting-principles.pdf
[88] courses/math1061/counting-selections.pdf
[89] courses/math1061/inclusion-exclusion.pdf
[90] courses/math1061/pigeonhole-principle.pdf
[91] courses/math1061/graphs.pdf
[92] courses/math1061/walks-trails-and-circuits.pdf
[93] courses/math1061/euler-circuits-and-trails.pdf
[94] courses/math1061/adjacency-matrices.pdf
[95] courses/math1061/incidence-matrices.pdf
[96] courses/math1061/trees.pdf
[97] courses/math1061/sets-and-set-notation.pdf

Three conditions hidden in one sentence

Unpacking "for each $x \in X$ there is a unique $y \in Y$ with $(x, y) \in f$" gives three separate things to check:

1. **Every** $x \in X$ is used — no element of the domain is left without a value. ("for each $x \in X$")
2. Every value lands **in** Y — no pair points somewhere outside the codomain.
3. Each x has **only one** value — no x appears as the first coordinate of two different pairs. ("unique")

Checking a candidate means checking all three, and a candidate can fail each one separately.

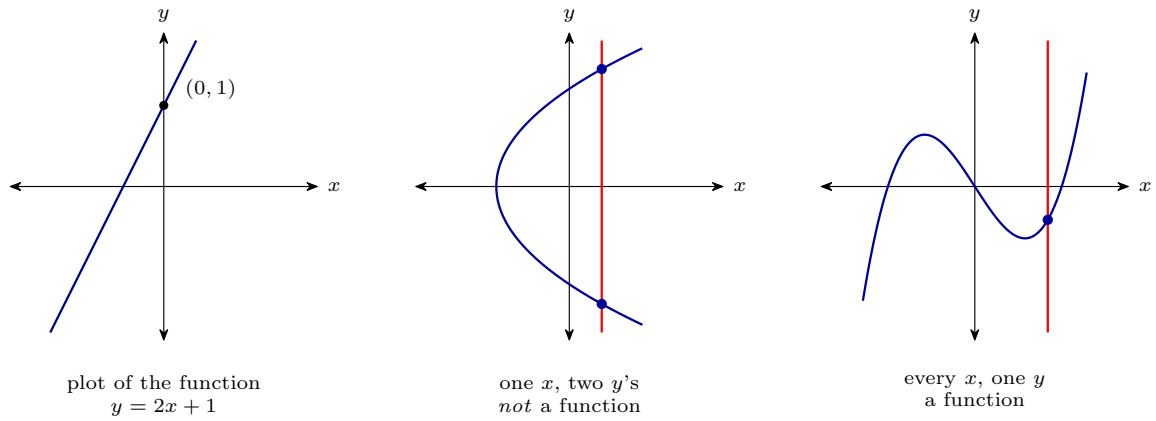


Figure 13: The uniqueness condition, seen graphically. A subset of the plane is a function of x exactly when every vertical line meets it at most once: the middle curve fails because one input is paired with two outputs, while the right-hand curve passes despite repeating output values, which the definition never forbids. The red vertical line in the middle and right-hand panels is the test.

The asymmetry in that picture is the whole definition: **repeated y-values are fine, repeated x-values are not.** The right-hand curve takes the same value three times over and is still a function.

Worked: which of these is a function?

Let $X = \{1, 2, 3\}$ and $Y = \{1, 2, 3, 4\}$. Which one of the following is a function from X to Y?

	Candidate	Why
(a)	$\{(1,2),(1,3),(2,4)\}$	$f(1)=2$ *and* $f(1)=3$ — the value at 1 is **not unique**. (Also 3 is unused.)
(b)	$\{(1,2),(2,3),(3,2),(4,1)\}$	$4 \notin X$ — a pair whose first coordinate is outside the domain
(c)	$\{(1,2),(2,3),(3,5)\}$	$5 \notin Y$ — a value outside the codomain
(d)	$\{(1,2),(2,1),(3,1)\}$	all first coordinates in X, all second in Y, each of $1,2,3$ used exactly once

Each wrong answer breaks a **different** one of the three conditions, which is what makes this a good question: the three failures are not variations on one mistake.

For (d): $f(1)=2$, $f(2)=1$, $f(3)=1$. Note $f(2)=f(3)$ — two inputs sharing a value is not a problem, for exactly the reason the picture above shows.

Codomain and range

The two are constantly confused, and the difference is one word:

> For a function $f : X \to Y$, the **co-domain** is Y, and the **range** is $f(X) = \{f(x) : x \in X\}$, which is a **subset of** Y.

	Is	Determined by
Co-domain	Y — where values are *allowed* to land	the declaration $f : X \to Y$
Range	$f(X)$ — where values *actually* land	the pairs in f

So the codomain is a choice you make when you write down the function, and the range is a fact you compute. Always $f(X) \subseteq Y$, and the containment is often proper.

For the function (d) above, $f = \{(1,2),(2,1),(3,1)\}$:

$$\text{co-domain} = Y = \{1,2,3,4\} \qquad \text{range} = f(X) = \{1,2\} \subseteq Y$$

3 and 4 are in the codomain and not in the range — they are permitted values that this particular function never takes.

Image and preimage

The two definitions generalise "range" to any subset, in each of the two directions:

> If $f : X \to Y$ is **any** function and A is any subset of X, then the **image** of A is
>
> $$f(A) = \{f(x) : x \in A\}$$
>
> If $f : X \to Y$ is **any** function and B is any subset of Y, then the **inverse image** or **preimage** of B is
>
> $$f^{-1}(B) = \{x \in X : f(x) \in B\}$$

Both take a **set** and return a **set** — $A \subseteq X$ gives $f(A) \subseteq Y$, and $B \subseteq Y$ gives $f^{-1}(B) \subseteq X$. The range is then just the image of the whole domain, $f(X)$.

> **The notation f^{-1} here does not mean an inverse function.** $f^{-1}(B)$ is defined for **any** function, invertible or not — the emphasis on *any* in both definitions is the point. It is a set-to-set operation that always exists; an inverse function is a different thing that usually does not.

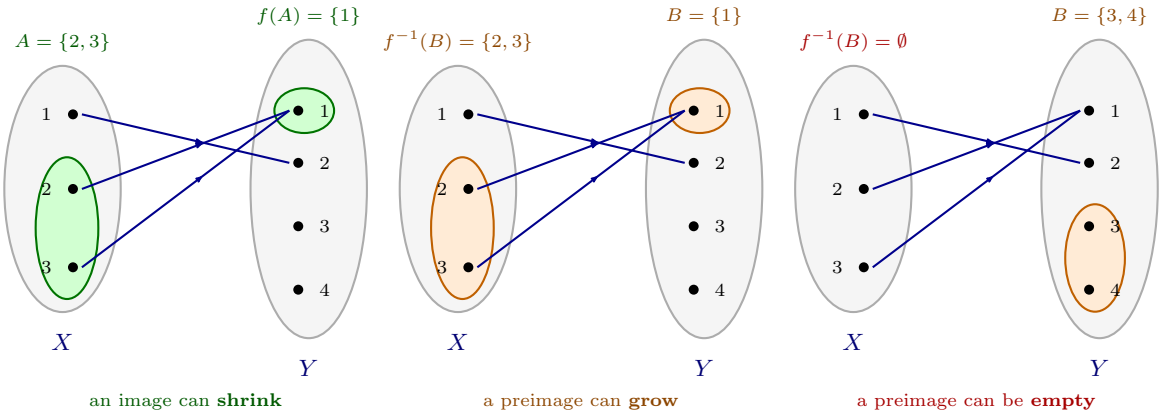


Figure 14: Image and preimage of the same function, read in opposite directions. Following the lines forward from a subset of X collects a subset of Y; following them backwards from a subset of Y collects every x that lands in it — which can be several elements, or none at all. In each panel the domain is on the left and the co-domain on the right, each line runs from an element of X to its value in Y, and the subset under discussion is outlined in colour with its expression in the same colour.

Worked

Let $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$ and $f = \{(1, 2), (2, 1), (3, 1)\}$, the function from the question above. So $f(1) = 2$, $f(2) = 1$, $f(3) = 1$.

	Asked for	Working	Answer
(a)	image of $\{1\}$	$f(1) = 2$	$f(\{1\}) = \{2\}$
(b)	image of $\{2, 3\}$	$f(2) = 1$, $f(3) = 1$	$f(\{2, 3\}) = \{1\}$
(c)	inverse image of $\{2\}$	which x have $f(x) = 2$? only $x = 1$	$f^{-1}(\{2\}) = \{1\}$
(d)	preimage of $\{1\}$	which x have $f(x) = 1$? $x = 2$ and $x = 3$	$f^{-1}(\{1\}) = \{2, 3\}$
(e)	preimage of $\{3, 4\}$	no x maps to 3 or 4	$f^{-1}(\{3, 4\}) = \emptyset$

Three things this table is designed to show — they are the three panels of Figure 14:

- **(b): an image can be smaller than the set you started with.** $\{2, 3\}$ has two elements, $f(\{2, 3\})$ has one, because f sends both to the same place.
- **(d): a preimage can be larger than the set you started with.** One element of Y pulls back to two of X.
- **(e): a preimage can be empty.** $\{3, 4\}$ lies outside the range entirely. Note this is a perfectly good answer, not a failure — $\emptyset$ is a subset of X like any other, and it is the reason f^{-1} needs no invertibility to be defined.

Always write the answers as **sets**: $f^{-1}(\{2\}) = \{1\}$, not $= 1$. The operation returns a subset, and dropping the braces is the standard slip.

See also

- sets-and-set-notation[98] — Cartesian products, and the $\in$ / $\subseteq$ distinction these definitions lean on
- proving-set-properties[99] — the proof methods, for arguing about images and preimages
- relations-on-sets[100] — functions as the relations with exactly one arrow out of each element
- 2026-09-03-set-properties-and-functions[101] — Lecture 18
- practice-problems[102] — §24 Functions Defined on General Sets, with full worked solutions

[98] courses/math1061/sets-and-set-notation.pdf
[99] courses/math1061/proving-set-properties.pdf
[100] courses/math1061/relations-on-sets.pdf
[101] courses/math1061/2026-09-03-set-properties-and-functions.pdf
[102] courses/math1061/practice-problems.pdf

Logical Equivalence & Laws

Two statement forms are **logically equivalent** ($\equiv$) if they have the same truth value for every combination of truth values of their variables — shown via a truth table, or by chaining the laws below. To show two forms are **not equivalent** ($\not\equiv$), exhibit one combination of truth values where they differ.

$\equiv$ *compares* statements (like $=$ compares numbers); it's not a connective itself. The connective that *combines* two statements into one is the biconditional $\leftrightarrow$ — see conditional-statements[103].

Tautologies and contradictions

> A **tautology t** is a statement that is **always true**. A **contradiction c** is a statement that is **always false**.

Both are written in bold upright lower case on the formula sheet, and both appear as *values* inside the laws — $p \vee \sim p \equiv \mathbf{t}$ produces one, $p \wedge \mathbf{t} \equiv p$ consumes one. A chain of laws that reaches $\mathbf{t}$ or $\mathbf{c}$ has proved the original form is always true or always false, which is usually the point of the exercise.

Laws of logical equivalence

> **Provided in the exam.** These laws are printed on the *MATH1061/MATH7861 Examination Formula Page*, so they don't need memorising. What the exercises ask for is choosing and applying them, and naming the one used at each step. The same page also carries the valid-argument-forms[104] and the set identities of proving-set-properties[105].

Given statement variables p, q, r, a tautology $\mathbf{t}$, and a contradiction $\mathbf{c}$:

Law	Form 1	Form 2
Commutative	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
Associative	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
Distributive	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
Identity	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
Negation	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
Double negative	$\sim (\sim p) \equiv p$	
Idempotent	$p \wedge p \equiv p$	$p \vee p \equiv p$
Universal bound	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$

[103] courses/math1061/conditional-statements.pdf
[104] courses/math1061/valid-argument-forms.pdf
[105] courses/math1061/proving-set-properties.pdf

Law	Form 1	Form 2
De Morgan's	$\sim (p \wedge q) \equiv \sim p \vee \sim q$	$\sim (p \vee q) \equiv \sim p \wedge \sim q$
Absorption	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
Negations of $\mathbf{t}/\mathbf{c}$	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

De Morgan's Laws are especially important for negating "and"/"or" statements — e.g. the negation of "5 is divisible by 2 **and** 6 is divisible by 2" is "5 is **not** divisible by 2 **or** 6 is **not** divisible by 2". Note what changes: the connective flips from *and* to *or*, and **both** halves get negated. Negating only one half, or leaving the connective alone, is the standard error.

How to write a law chain

The layout expected in your own work:

- the **first line is the starting expression**, on its own;
- **every later line begins with** $\equiv$, vertically aligned down the page;
- the **name of the law** used to get there sits in its own **right-hand column** on that line.

Two or more laws may be cited on one line if they act on the same step (e.g. "by De Morgan's law and the double negative law"). Name a law on every line that *changes* the expression. The one kind of line that goes unnamed is a pure re-labelling that asserts nothing new, like the "where $r = (p \wedge \sim q)$" line in the first worked example below.

Treat a compound expression as a single letter

The laws are stated for variables p, q, r, but they hold with **any statement form** substituted in. Spotting that turns a long expression into a short one:

$$(p \wedge \sim q) \wedge \ \sim (p \wedge \sim q)$$

is $r \wedge \sim r$ with $r = (p \wedge \sim q)$, so the negation law applies directly and it is $\mathbf{c}$. This is exactly the move in the first worked example below.

Worked: reaching a contradiction

Show that $(p \wedge \sim q) \wedge (\sim p \vee q) \equiv \mathbf{c}$**.**

$$\begin{aligned}
(p \wedge \sim q) \wedge (\sim p \vee q) &\equiv (p \wedge \sim q) \wedge \ \sim (p \wedge \sim q) && \text{by De Morgan's law and the double negative law} \\
&\equiv r \wedge \sim r \quad \text{where } r = (p \wedge \sim q) \\
&\equiv \mathbf{c} && \text{by the negation law}
\end{aligned}$$

The whole proof is the first line: recognising that $\sim p \vee q$ is $\sim (p \wedge \sim q)$ in disguise. Read De Morgan's backwards — $\sim p \vee q \equiv \sim p \vee \sim (\sim q) \equiv \sim (p \wedge \sim q)$ — and the two conjuncts are a statement and its own negation.

Worked: absorbing a conjunction

Show that $\sim p \vee (p \wedge q) \equiv \sim p \vee q$**.**

$$\begin{aligned}
\sim p \vee (p \wedge q) &\equiv (\sim p \vee p) \wedge (\sim p \vee q) && \text{by the distributive law} \\
&\equiv \mathbf{t} \wedge (\sim p \vee q) && \text{by the negation law} \\
&\equiv \sim p \vee q && \text{by the identity law}
\end{aligned}$$

The pattern *distribute, collapse the tautology or contradiction, drop it with the identity law* is the most common three-step shape in this topic, and it recurs in both routes below.

Worked: two routes to the same answer

Show that $\sim \big((\sim p \wedge q) \vee (\sim p \wedge \sim q)\big) \equiv p$**.**

There is no unique chain. Here are two, and both are complete proofs:

Neither route is "the" answer, and nothing turns on finding the short one. What matters is that every line follows from the one above by a **named** law. The shorter route is found by looking for a **common factor** before doing anything else: both disjuncts inside the brackets contain $\sim p$, so the distributive law pulls it out and the rest collapses.

The same equivalence can also be established with a truth table — see the worked table in 2026-07-30-logical-form-and-equivalence[106], where the column for $\sim \big((\sim p \wedge q) \vee (\sim p \wedge \sim q)\big)$ comes out identical to the column for p.

[106] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf

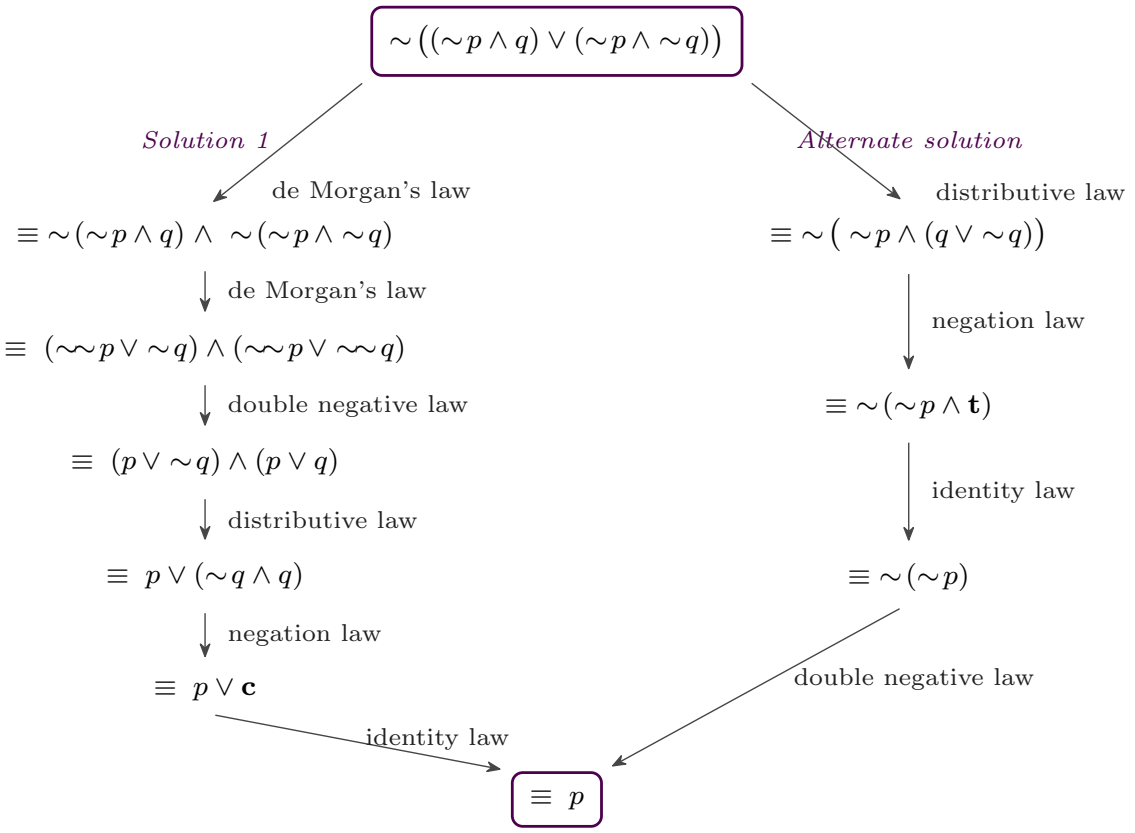


Figure 15: The same equivalence proved two ways. Starting from the same expression and ending at the same p, the left route pushes the negation inward with De Morgan's first and takes six steps; the right route factors out the common ~p with the distributive law first and takes four. Every edge names the law that licenses it — that naming is what the chain is for.

Showing two forms are *not* equivalent

To show $\not\equiv$ you do **not** need a full truth table. Find **one** assignment of truth values on which the two forms disagree, and say what each evaluates to.

Worked. Show that $\sim(p \vee q) \not\equiv \sim p \vee \sim q$.

Take p **false** and q **true**. Then

- LHS: $p \vee q$ is $\mathrm{F} \vee \mathrm{T} = \mathrm{T}$, so $\sim(p \vee q)$ is **false**.
- RHS: $\sim p \vee \sim q$ is $\mathrm{T} \vee \mathrm{F} = \mathrm{T}$, so it is **true**.

One row on which they differ is a complete disproof, so the two forms are **not** logically equivalent.

The correct partner for $\sim(p \vee q)$ is of course $\sim p \wedge \sim q$ — this is precisely the De Morgan trap of changing the sign but not the connective.

See also

- logical-connectives[107]
- conditional-statements[108]
- formula-sheet[109] — what else is provided in the exam, and what is not
- proving-set-properties[110] — the same eleven laws as set identities, and the two set-equality proof methods built on them
- 2026-07-30-logical-form-and-equivalence[111] — Lecture 2, where these laws were introduced and applied
- practice-problems[112] — §2 Logical Equivalence, with full worked solutions

Mathematical Induction

The principle of mathematical induction, the four-step shape every induction proof takes, and the extra care inequalities need. See sequences-and-summations[113] for the summation manipulations these proofs run on, and proof-techniques[114] for the other proof methods in the course.

[107] courses/math1061/logical-connectives.pdf
[108] courses/math1061/conditional-statements.pdf
[109] courses/math1061/formula-sheet.pdf
[110] courses/math1061/proving-set-properties.pdf
[111] courses/math1061/2026-07-30-logical-form-and-equivalence.pdf
[112] courses/math1061/practice-problems.pdf
[113] courses/math1061/sequences-and-summations.pdf
[114] courses/math1061/proof-techniques.pdf

Why it works

Let $P(n)$ be a predicate written in terms of some integer n. Suppose you know two statements are true:

1. $P(2)$
2. $\forall k \in \mathbb{Z}$ with $k \geq 2$, if $P(k)$ then $P(k+1)$

Can you conclude $P(5)$? Yes — statement 2 is a general implication, so instantiate it repeatedly and apply modus ponens. The conclusion of one step is the premise of the next, which is what turns two facts into a chain (Figure 16).

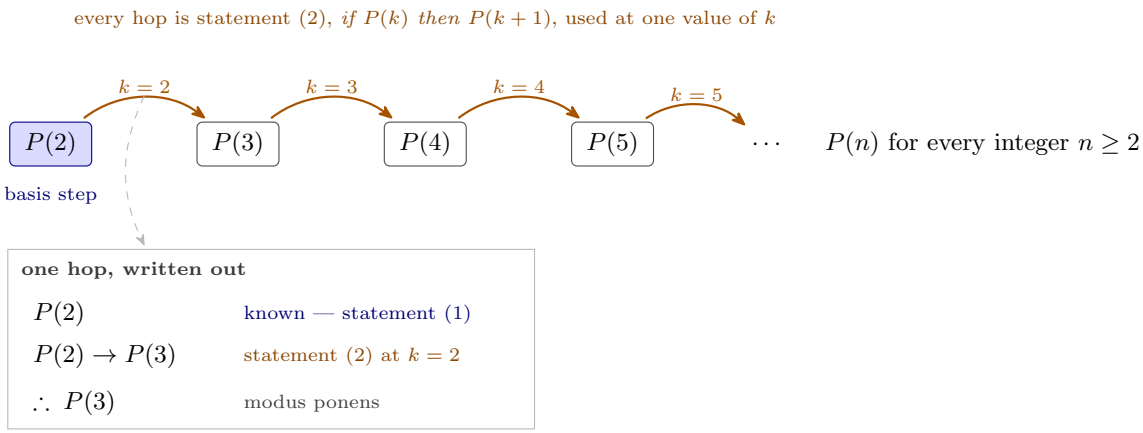


Figure 16: Why those two statements are enough. The basis step pins one statement true; every hop after it is the *same* general implication used at one more value of k, so each conclusion becomes the next premise. The panel writes one hop out in full — it is a single modus ponens, nothing more.

Nothing here is special to 5. $P(5)$ is reached in three hops, but the chain never stops, so $P(n)$ is true for **each** integer $n \geq 2$.

Both statements are needed. Statement 2 alone gives nothing: an implication $P(k) \to P(k+1)$ is true in three of the four rows of its truth table — including both rows where $P(k)$ is false. Without the basis step pinning P true somewhere, the chain has nothing to start from and every link stays vacuously true while every $P(n)$ stays false.

The shape of an induction proof

Four steps, and it is worth naming each one explicitly in the write-up so the reader can follow the argument:

1. **Define the predicate.** Let $P(n)$ denote *(the statement, with n free).*
2. **Basis step.** Prove the predicate is true at the smallest value of n in the claim — evaluate the two sides separately and observe they agree.
3. **Inductive hypothesis.** Suppose k is an integer at or above the basis value, and that the predicate is true for $n = k$. Write out what $P(k)$ actually says.
4. **Inductive step.** Prove $P(k+1)$ follows, i.e. $\forall k \in \mathbb{Z}$ with $k \geq$ *(basis)*, if $P(k)$ is true then $P(k+1)$ is true. Start from the LHS of $P(k+1)$, use the inductive hypothesis somewhere (say where), and arrive at the RHS of $P(k+1)$.

Then conclude: *therefore, by the principle of mathematical induction, …* for each integer $n \geq$ *(basis).*

One thing about the order. In the write-up, the inductive step's goal — *prove that $\forall k \in \mathbb{Z}$ with $k \geq$ (basis), if $P(k)$ is true then $P(k+1)$ is true* — goes on the line **above** the inductive hypothesis, and the assumption is made underneath it: goal first, assumption second. The numbering above counts the four actions; the goal line itself is not numbered. Write the goal down, then assume, then work.

Worked example — a summation

Prove that for each integer $n \geq 1$, $\displaystyle\sum_{i=1}^{n}(3i+2) = \frac{3n^2+7n}{2}$.

Proof. Let $P(n)$ denote the predicate $\displaystyle\sum_{i=1}^{n}(3i+2) = \frac{3n^2+7n}{2}$.

Basis step. Prove the predicate is true for $n = 1$.

LHS of $P(1)$: $\displaystyle\sum_{i=1}^{1}(3i+2) = 3 \cdot 1 + 2 = 5$. RHS of $P(1)$: $\dfrac{3(1^2)+7(1)}{2} = \dfrac{3+7}{2} = 5$. Therefore $P(1)$ is true.

Inductive step. Prove that $\forall k \in \mathbb{Z}$ with $k \geq 1$, if $P(k)$ is true then $P(k+1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and the predicate is true for $n = k$ — that is, $\displaystyle\sum_{i=1}^{k}(3i+2) = \frac{3k^2+7k}{2}$.

LHS of $P(k+1)$:

$$\sum_{i=1}^{k+1}(3i+2) = \sum_{i=1}^{k}(3i+2) + \big(3(k+1)+2\big)$$

$$= \frac{3k^2+7k}{2} + 3k + 5 \qquad \text{(by the inductive hypothesis } P(k)\text{)}$$

$$= \frac{3k^2+13k+10}{2} = \frac{3(k^2+2k+1)+7k+7}{2} = \frac{3(k+1)^2+7(k+1)}{2}$$

which is the RHS of $P(k+1)$.

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n}(3i+2) = \frac{3n^2+7n}{2}$ for each integer $n \geq 1$.

The move at the first line is splitting off the last term (see sequences-and-summations[115]) — that is what exposes the $P(k)$ sum so the hypothesis can be applied to it. Figure 17 tracks that one expression through the chain.

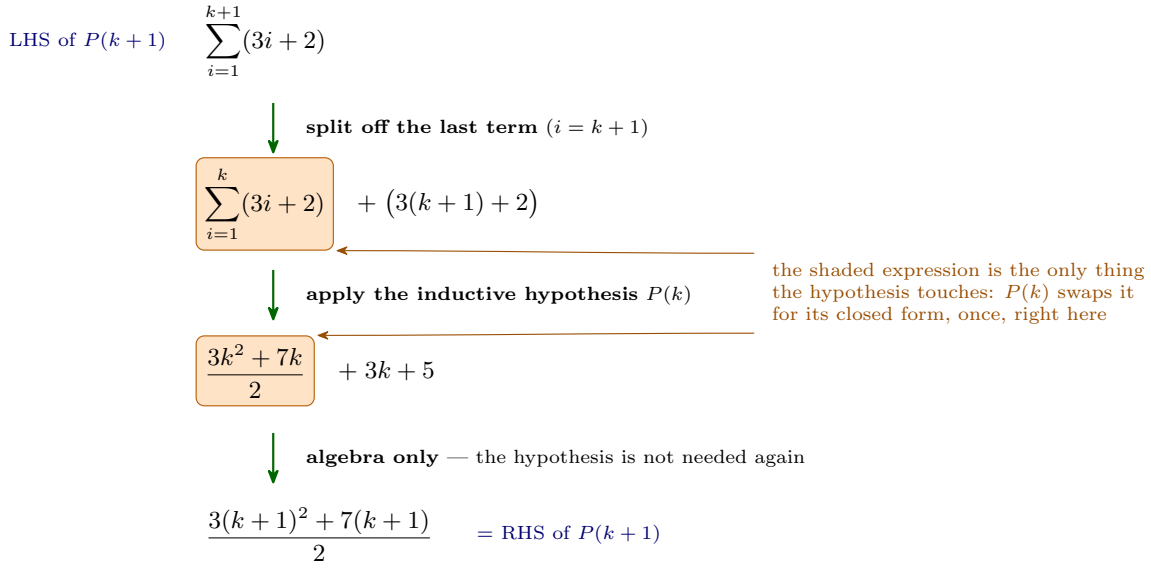


Figure 17: Where the inductive hypothesis actually enters. Splitting off the last term turns the LHS of $P(k+1)$ into *the LHS of $P(k)$, plus one more term*; the hypothesis is then spent exactly once, swapping that sum for its closed form; everything below is algebra. The shading follows that one expression from line to line.

Before starting the chain, write down what the RHS of $P(k+1)$ actually is — here $\frac{3(k+1)^2+7(k+1)}{2}$. Without it you are simplifying with no idea what counts as finished; with it, the last algebraic step is obvious, because you already know the shape you are steering the numerator into.

Induction with inequalities

Be careful when manipulating inequalities. The rules that hold:

[115] courses/math1061/sequences-and-summations.pdf

Given	Conclusion
$a < b$	$a + x < b + x$, regardless of the sign of x
$a < b$, x positive	$ax < bx$
$a < b$, x negative	$ax > bx$ — *the direction flips*
$a < b$, x zero	$ax = bx$
$a < b$ and $x < y$	$a + x < b + y$
$a < b$ and $x > y$	**nothing** can be concluded about $a + x$

All of these still hold with $<$ and $>$ replaced by $\leq$ and $\geq$.

Worked example — $n^2 < 2^n$

Prove that for each integer $n \geq 5$, $n^2 < 2^n$.

> *Proof.* Let $P(n)$ be the predicate $n^2 < 2^n$.
>
> **Basis step.** Consider $n = 5$. Then $n^2 = 25$ and $2^n = 32$. Since $25 < 32$, $P(5)$ is true.
>
> **Inductive hypothesis.** Suppose $k \geq 5$ is an integer and $P(k)$ is true. Thus $k^2 < 2^k$, and hence $2k^2 < 2 \cdot 2^k$.
>
> **Inductive step.** Consider $n = k + 1$; the goal is $(k+1)^2 < 2^{k+1} = 2 \cdot 2^k$.
>
> $$(k+1)^2 = k^2 + 2k + 1 < k^2 + 2k + k = k^2 + 3k < k^2 + k^2 = 2k^2 < 2(2^k) = 2^{k+1}$$
>
> The first inequality uses $1 < k$ (since $k \geq 5$); the second uses $3k < k \cdot k$, which holds because $5 \leq k$; the last uses the inductive hypothesis. Thus $P(k+1)$ is true.
>
> Therefore, by PMI, for each integer $n \geq 5$, $n^2 < 2^n$.

The pattern for an inequality is a **chain**: start at the LHS of $P(k+1)$ and relax it one step at a time — each step justified by a rule from the table or by the inductive hypothesis — until it reaches the RHS of $P(k+1)$. Every step must be an inequality in the *same* direction, or the chain says nothing.

The inductive step must hold at every k

Including the first one. An inductive step that is sound for all large k but fails at the basis value leaves a gap the chain cannot cross, and the induction proves nothing beyond the basis case — even though every individual line of the argument can look correct.

The classic demonstration is the 'proof' that all numbers are equal, whose inductive step is valid for every $k \geq 2$ and false at $k = 1$; it is picked apart in 2026-08-31-recursive-definitions[116]. When checking an induction proof, run the inductive step at the smallest k it claims to cover and see whether it still says anything.

Strong induction

When the inductive step needs more than just the immediately preceding case — typically because a recurrence reaches back several terms, or because the step splits a number into two smaller ones it cannot control — ordinary induction is not enough. See strong-induction-and-the-well-ordering-principle[117] for the stronger form, how many base cases it demands, and the well-ordering principle it is equivalent to.

See also

- sequences-and-summations[118] · strong-induction-and-the-well-ordering-principle[119] · proof-techniques[120]
- solving-recurrence-relations[121] — induction used to prove an explicit formula for a recursively defined sequence
- inclusion-exclusion[122] — the rule for n sets, from the rule for two by splitting off the last set, an induction on n
- 2026-08-24-sequences-and-mathematical-induction[123] — Lecture 13
- practice-problems[124] — §17 Mathematical Induction, with full worked solutions

[116] courses/math1061/2026-08-31-recursive-definitions.pdf
[117] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[118] courses/math1061/sequences-and-summations.pdf
[119] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[120] courses/math1061/proof-techniques.pdf
[121] courses/math1061/solving-recurrence-relations.pdf
[122] courses/math1061/inclusion-exclusion.pdf
[123] courses/math1061/2026-08-24-sequences-and-mathematical-induction.pdf
[124] courses/math1061/practice-problems.pdf

Modular Arithmetic, Floor & the Quotient-Remainder Theorem

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

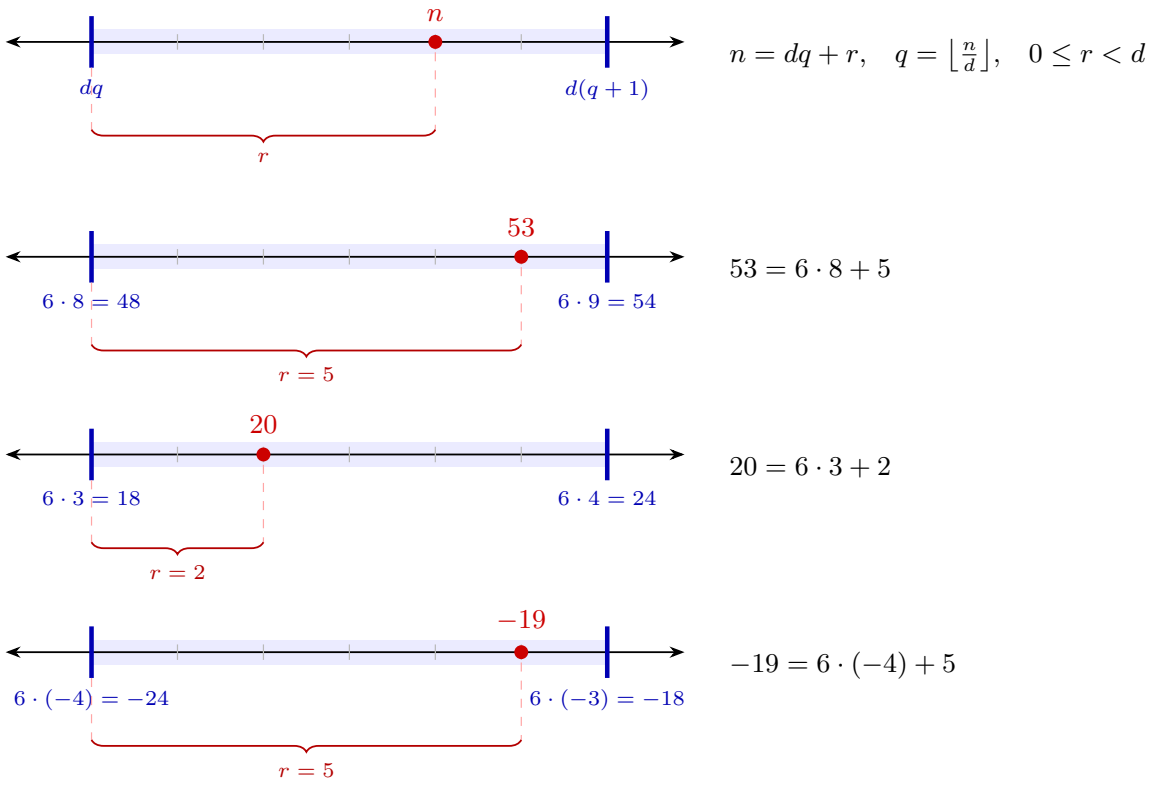
$$n = dq + r \quad \text{and} \quad 0 \leq r < d$$

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



The shaded band is the half-open block $[\,dq,\ d(q+1)\,)$ that n lands in. The quotient q names the multiple of d at or *below* n, so the remainder r is always measured rightwards — which is why -19 has remainder 5 and not -1.

Figure 18: Why the remainder is never negative: the general case and the three $d = 6$ examples on the number line. Each shaded band is one block $[dq, d(q+1))$ of width d; the quotient names the multiple of d at or below n, so r is always the rightward gap from that multiple, and -19 therefore has remainder 5 rather than -1.

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.

- $n \bmod d = r$ — 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[125]).

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 $y \bmod 6 = 3$.

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

- $(x + y) \bmod 6$: $x + y \equiv 4 + 3 \equiv 7 \equiv 1 \pmod 6$, 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 $3m^2 + 2m + 1 \equiv 3(4)^2 + 2(4) + 1 \equiv 12(4) + 8 + 1 \equiv 8 + 1 \equiv 3 \pmod 6$ — $3 \cdot 4^2$ is $12 \cdot 4$, and that term drops out whole, since $6 \mid 12$.

Worked: an integer n leaves remainder 4 on division by 7 — what is the remainder of $3n$? Write $n = 7k + 4$; then $3n = 21k + 12 = 7(3k + 1) + 5$, so the remainder is 5. (The course's solutions PDF has this step as $7(3k) + 5$, which is $21k + 5$, not $21k + 12$; the quotient is $3k + 1$. The answer of 5 is unaffected — see practice-problems[126].)

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 $n^2 \bmod 4 = 1$. □

[126] courses/math1061/practice-problems.pdf

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 $= \left\lfloor \frac{4k^2+4k+1}{4} \right\rfloor = \lfloor (k^2+k) + \frac{1}{4} \rfloor = k^2 + k$. 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 $4 \pmod 5$. □

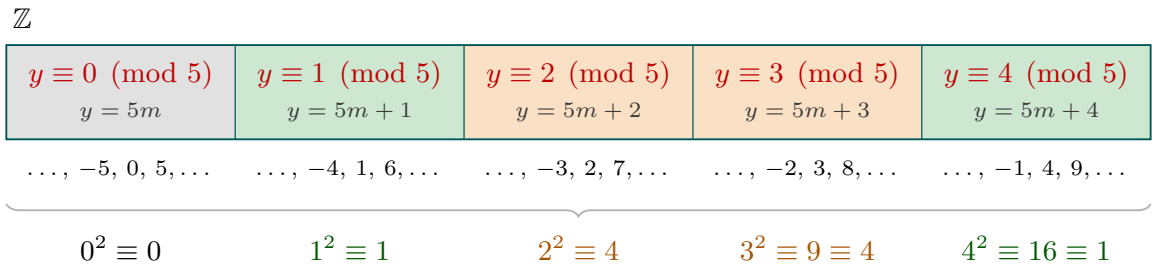


Figure 19: The case split the proof above runs on: $\mathbb{Z}$ cut into the five residue classes mod 5. The tints group the classes by the remainder their square leaves, which is what makes 2 and 3 unreachable.

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[127] · gcd-lcm-and-euclidean-algorithm[128] · proof-techniques[129]
- sets-and-set-notation[130] — congruence classes as sets, and the partitions of $\mathbb{Z}$ they give
- equivalence-relations[131] · integers-modulo-n[132] — congruence as an equivalence relation, and its classes as the number system $\mathbb{Z}_n$
- pigeonhole-principle[133] — the n remainders as pigeonholes: among any $n+1$ integers, two differ by a multiple of n
- practice-problems[134] — §14 Modular Arithmetic, with full worked solutions

Practice Problems — the Semester-wide Set

This is the course's one problem set for the whole semester — a single document rather than a per-week handout. 46 sections, one per pre-work video, each with the relevant textbook pages, a set of practice problems and full worked solutions. Everything is reproduced here in full, so you never need to open the PDF.

Applied Classes start in **Week 2** and run to Week 13 — twelve of them, matching the "best 8 of 12" Applied Classes component worth 30% (see math1061[135]). Each week's class applies the *previous* week's lecture content, so the material a class covers runs roughly one week behind the lecture column below. Which sections a given Applied Class draws on is not stated in any of the source material.

These problems belong to the roughly three hours of individual study each week, which are for revising the videos, readings and classes **and completing the Practice Problems**. They are the out-of-class half of the course, and they are *not* the same thing as the Assessed Exercises, which are done and submitted inside the class itself. (That class goes by two names, the **Active Class** and the **Applied Class**. They are one session.)

How each section is laid out

1. Relevant textbook pages for Epp 4th edition and 5th (metric) edition
2. **Practice problems**

[127] courses/math1061/divisibility-and-factorisation.pdf
[128] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[129] courses/math1061/proof-techniques.pdf
[130] courses/math1061/sets-and-set-notation.pdf
[131] courses/math1061/equivalence-relations.pdf
[132] courses/math1061/integers-modulo-n.pdf
[133] courses/math1061/pigeonhole-principle.pdf
[134] courses/math1061/practice-problems.pdf
[135] courses/math1061/math1061.pdf

3. **Solutions** — full worked solutions, not just answers
4. Occasionally a non-assessable **Application** block (see the table below)

Errata

The source document carries an errata page listing corrections made during semester. **Last update: 24 August 2026**, with two entries:

- On page 195, the solution to 1(b) was corrected (the note in brackets had previously copied the note from 1(a)) — already applied in §45 below.
- **Question 2 in section 30 has been updated, and the original version moved to section 32** (because it refers to antisymmetry) — applied in §30 and §32 below.

If something looks wrong, post on the Ed Discussion board.

Section index

Every section is below, with its topic and textbook page ranges. Each section goes with one pre-work video (§1 with *Video 001*, and so on up to *Video 046*), and the Lecture (week) column places it in the schedule of math1061[136] by that video number. The Notes column links to the concept note covering that material where one exists; the rest are still ahead in the semester.

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
1	Logical Form	L2 (wk 1)	023–029	037–043	logical-connectives[137]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[138]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[139]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[140]

[136] courses/math1061/math1061.pdf
[137] courses/math1061/logical-connectives.pdf
[138] courses/math1061/logical-equivalence-laws.pdf
[139] courses/math1061/conditional-statements.pdf
[140] courses/math1061/valid-argument-forms.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[141]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[142]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[143]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[144]
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[145]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[146]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[147]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[148]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[149]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[150]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[151]

[141] courses/math1061/determining-argument-validity.pdf
[142] courses/math1061/quantified-statements.pdf
[143] courses/math1061/quantified-statements.pdf
[144] courses/math1061/quantified-statements.pdf
[145] courses/math1061/proof-techniques.pdf
[146] courses/math1061/proof-techniques.pdf
[147] courses/math1061/proof-techniques.pdf
[148] courses/math1061/rational-and-irrational-numbers.pdf
[149] courses/math1061/divisibility-and-factorisation.pdf
[150] courses/math1061/modular-arithmetic.pdf
[151] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[152]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[153]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[154]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[155]
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[156]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[157]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[158]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[159]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[160]
25	one-to-one, Onto, and Inverse Functions	L19 (wk 7)	397–416	439–461	

[152] courses/math1061/sequences-and-summations.pdf
[153] courses/math1061/mathematical-induction.pdf
[154] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[155] courses/math1061/recursive-definitions.pdf
[156] courses/math1061/solving-recurrence-relations.pdf
[157] courses/math1061/sets-and-set-notation.pdf
[158] courses/math1061/sets-and-set-notation.pdf
[159] courses/math1061/proving-set-properties.pdf
[160] courses/math1061/functions-on-general-sets.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
26	Composition of Functions	L20 (wk 7)	416–427	461–472	
27	Cardinalities	L21 (wk 8)	428–441	473–486	
28	Countable and Uncountable Sets	L22 (wk 8)	428–441	473–486	
29	Relations on Sets	L23 (wk 8)	442–449	487–494	
30	Reflexivity, Symmetry, Transitivity	L23 (wk 8)	449–459	495–505	
31	Equivalence Relations	L24 (wk 9)	459–478	505–523	
32	Partial Order Relations	L25 (wk 9)	498–515	546–563	
33	Definitions and Examples of Groups	L26 (wk 9)	—	—	
34	Elementary Properties of Groups	L27 (wk 10)	—	—	
35	Group Isomorphisms	*not scheduled*	—	—	
36	Definitions and Examples of Fields	L28 (wk 10)	—	—	
37	Introduction to Counting	L29 (wk 11)	516–553	564–604	
38	Counting Selections	L30 (wk 11)	516–553	564–604	
39	Introduction to Probability	L31 (wk 12)	516–553	564–604	
40	Binomial Coefficients	L31 (wk 12)	565–591	617–641	
41	Inclusion Exclusion	L32 (wk 12)	545–549	595–599	

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
42	The Pigeonhole Principle	L33 (wk 12)	554–565	604–616	
43	Introduction to Graph Theory	L33 (wk 12)	625–660	677–697	
44	Walks, Trails and Circuits	L34 (wk 12)	625–660	677–697	
45	Matrix Representations of Graphs	L35 (wk 13)	661–675	698–712	
46	Trees	L36 (wk 13)	683–701	720–742	

§35 Group Isomorphisms has no lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36). The section itself carries no practice problems and is marked *optional and will not be assessed*, so the gap is deliberate.

§28 Countable and Uncountable Sets carries its own note in the source: *this content will not be assessed in MATH1061.* It still has a full set of problems and solutions.

Sections 33–36 (groups and fields) list no textbook page ranges.

Non-assessable application blocks

Eight sections carry an extra block of problems, **not assessable for MATH1061**, mostly drawn from K. Rosen, *Discrete Mathematics and its Applications*, 7th ed. (1991), with two from Epp. They connect the pure material to computer science, and are reproduced in full alongside their sections.

After §	Block	Source
2	Applications to Computer Science — bit strings and logic circuits	Rosen pp. 20–24
5	Applications of Valid and Invalid Arguments	Rosen pp. 48–68
9	Applications of Proofs to Computer Science — resolution and automated theorem proving	Rosen pp. 74–80

After §	Block	Source
15	Trace Tables for Algorithms — the Division and Euclidean algorithms	Epp §4.8 (4th ed.) / §4.10 (5th ed.)
21	Computer Representations of Sets	Rosen pp. 134–138
28	Computability of Functions	Rosen pp. 170–177
31	Identifiers — C identifiers as an equivalence-relation example	Rosen pp. 608–618
37	Runtime — counting basic instructions	Epp 5th ed. pp. 787–799

A note on the diagrams: the source PDF draws logic circuits, graphs and Hasse diagrams as figures. Those are reproduced here as explicit gate netlists and edge lists, which carry the same information in a form that renders everywhere.

§1 — Logical Form

Epp 4th ed. pp. 023–029 · 5th ed. (metric) pp. 037–043. Lecture 2 (week 1). Notes: logical-connectives[161].

Problems

1. Write a truth table for the statement form $p \wedge (\sim q \vee r)$.
2. Suppose you know that $(\sim p \wedge q) \vee p$ is false. What can you conclude about the truth values of each of the two variables?
3. Let p be the statement "DATAENDFLAG is off," q the statement "ERROR equals 0," and r the statement "SUM is less than 1,000." Express the following sentences in symbolic notation.
   (a) DATAENDFLAG is off, ERROR equals 0, and SUM is less than 1,000.
   (b) DATAENDFLAG is off but ERROR is not equal to 0.
   (c) DATAENDFLAG is off; however, ERROR is not 0 or SUM is greater than or equal to 1,000.
   (d) DATAENDFLAG is on and ERROR equals 0 but SUM is greater than or equal to 1,000.

[161] courses/math1061/logical-connectives.pdf

(e) Either DATAENDFLAG is on or it is the case that both ERROR equals 0 and SUM is less than 1,000.

Solutions

1. The truth table is

p	q	r	$\sim q$	$\sim q \vee r$	$p \wedge (\sim q \vee r)$
T	T	T	F	T	T
T	T	F	F	F	F
T	F	T	T	T	T
T	F	F	T	T	T
F	T	T	F	T	F
F	T	F	F	F	F
F	F	T	T	T	F
F	F	F	T	T	F

2. We know $(\sim p \wedge q) \vee p$ is false. A disjunction is false only when both parts are false, so we must have

$$p \text{ is false} \quad \text{and} \quad (\sim p \wedge q) \text{ is false.}$$

From p being false, it follows that $\sim p$ is true. Now $(\sim p \wedge q)$ can be false only if q is false (since $\sim p$ is already true). Hence q is false.

Therefore p **is false and** q **is false**.

3. (a) $p \wedge q \wedge r$.

   (b) $p \wedge \sim q$.

   (c) $p \wedge (\sim q \vee \sim r)$.

   (d) $\sim p \wedge q \wedge \sim r$.

   (e) $\sim p \vee (q \wedge r)$.

§2 — Logical Equivalence

Epp 4th ed. pp. 030–038 · 5th ed. (metric) pp. 043–053. Lecture 2 (week 1). Notes: logical-equivalence-laws[162].

[162] courses/math1061/logical-equivalence-laws.pdf

Problems

1. (a) Use the laws of logical equivalence to show that $p \wedge q \equiv \sim (\sim p \vee \sim q)$.

   (b) Use the laws of logical equivalence to show that $\sim (p \vee \sim q) \vee (\sim p \wedge \sim q) \equiv \sim p$.

2. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

   (a) $((p \wedge q) \vee (q \wedge r)) \vee \sim q$

   (b) $(\sim p \vee q) \vee (p \wedge \sim q)$

3. Use De Morgan's laws to write sentences equivalent to the following:

   (a) It is not true that I am studying Computer Science and I am studying Engineering.

   (b) I am not going to the movies this weekend or I am not going swimming this weekend.

4. Let $\oplus$ denote **exclusive or**, which means '… or … but not both'. The truth table for $p \oplus q$ is as follows:

p	q	$p \oplus q$
T	T	F
T	F	T
F	T	T
F	F	F

   (a) Use a truth table to show that $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

   (b) Use a truth table to show that $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

   (c) Use the laws of logical equivalence and the equivalence $p \oplus q \equiv (p \vee q) \wedge \sim (p \wedge q)$ (which is the definition of $\oplus$) to show that

$$(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r).$$

Solutions

1. (a) We have

$$\begin{aligned} \sim (\sim p \vee \sim q) &\equiv \sim (\sim p) \wedge \sim (\sim q) && \text{by De Morgan's law} \\ &\equiv p \wedge q && \text{by the double negative law (used twice).} \end{aligned}$$

   (b) We have

$$
\begin{aligned}
\sim (p \vee \sim q) \vee (\sim p \wedge \sim q) &\equiv (\sim p \wedge \sim\sim q) \vee (\sim p \wedge \sim q) && \text{by De Morgan's law} \\
&\equiv (\sim p \wedge q) \vee (\sim p \wedge \sim q) && \text{by the double negative law} \\
&\equiv \sim p \wedge (q \vee \sim q) && \text{by the distributive law} \\
&\equiv \sim p \wedge \mathbf{t} && \text{by the negation law} \\
&\equiv \sim p && \text{by the identity law.}
\end{aligned}
$$

2. (a) We have

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \vee (q \wedge r)$	$\sim q$	$((p \wedge q) \vee (q \wedge r)) \vee \sim q$
T	T	T	T	T	T	F	T
T	T	F	T	F	T	F	T
T	F	T	F	F	F	T	T
T	F	F	F	F	F	T	T
F	T	T	F	T	T	F	T
F	T	F	F	F	F	F	F
F	F	T	F	F	F	T	T
F	F	F	F	F	F	T	T

Thus the statement is **neither a tautology nor a contradiction**.

(b) We have

p	q	$\sim p$	$\sim p \vee q$	$\sim q$	$p \wedge \sim q$	$(\sim p \vee q) \vee (p \wedge \sim q)$
T	T	F	T	F	F	T
T	F	F	F	T	T	T
F	T	T	T	F	F	T
F	F	T	T	T	F	T

Hence the statement is a **tautology**.

3. (a) Let C be the statement "I am studying Computer Science" and E be the statement "I am studying Engineering." The given statement is $\sim (C \wedge E)$. By De Morgan's law,

$$\sim (C \wedge E) \equiv (\sim C) \vee (\sim E).$$

So an equivalent statement is: "I am not studying Computer Science or I am not studying Engineering."

(b) Let M be the statement "I am going to the movies this weekend" and S be the statement "I am going swimming this weekend." The given sentence is $(\sim M) \vee (\sim S)$. By De Morgan's law (in reverse),

$$(\sim M) \vee (\sim S) \equiv \sim (M \wedge S).$$

So an equivalent statement is: "It is not the case that I am both going to the movies this weekend and going swimming this weekend."

4. (a) We have

p	q	$p \vee q$	$\sim p$	$(p \vee q) \wedge \sim p$	$q \wedge \sim p$
T	T	T	F	F	F
T	F	T	F	F	F
F	T	T	T	T	T
F	F	F	T	F	F

Since the last two columns agree on every row, we have $(p \vee q) \wedge \sim p \equiv q \wedge \sim p$.

(b) We have

p	q	r	$p \oplus q$	$(p \oplus q) \wedge r$	$p \wedge r$	$q \wedge r$	$(p \wedge r) \oplus (q \wedge r)$
T	T	T	F	F	T	T	F
T	T	F	F	F	F	F	F
T	F	T	T	T	T	F	T
T	F	F	T	F	F	F	F
F	T	T	T	T	F	T	T
F	T	F	T	F	F	F	F
F	F	T	F	F	F	F	F
F	F	F	F	F	F	F	F

The columns for $(p \oplus q) \wedge r$ and $(p \wedge r) \oplus (q \wedge r)$ match on all rows, hence $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$.

(c) To save space, multiple laws have been applied in some steps. There are many different ways to apply the laws to prove this, so your proof may look different to this one. We have

$(p \wedge r) \oplus (q \wedge r)$

$\equiv ((p \wedge r) \vee (q \wedge r)) \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by the given equivalence (def of $\oplus$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	by distributive and commutative laws (for $\wedge r$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge (r \wedge r))$	by associative and commutative laws (for $\wedge$)
$\equiv (p \vee q) \wedge r \wedge \sim ((p \wedge q) \wedge r)$	by idempotent law
$\equiv (p \vee q) \wedge r \wedge (\sim (p \wedge q) \vee \sim r)$	by De Morgan's law
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee (r \wedge \sim r) \Big)$	by distributive law (for $r \wedge$)
$\equiv (p \vee q) \wedge \Big((r \wedge \sim (p \wedge q)) \vee \mathbf{c} \Big)$	by negation law
$\equiv (p \vee q) \wedge r \wedge \sim (p \wedge q)$	by identity law
$\equiv (p \vee q) \wedge \sim (p \wedge q) \wedge r$	by associative and commutative laws (for $\wedge$)
$\equiv (p \oplus q) \wedge r$	by the given equivalence (def of $\oplus$)

Application — Applications to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 20–24.*

Information is often represented using binary or **bit strings**, which are sequences consisting of zeros and ones. The **length** of a string is the total number of bits in it — for example 0110110 is a string of length 7. The logical operators $\wedge$, $\vee$ and $\oplus$ extend to binary strings. The operators AND, OR and XOR are:

p	q	$p \vee q$	$p \wedge q$	$p \oplus q$
0	0	0	0	0
0	1	1	0	1
1	0	1	0	1
1	1	1	1	0

Propositional logic also applies to the design of computer hardware. A **digital logic circuit** receives input signals (either 0, the wire being off, or 1, on) and produces output signals which are also bits. Complicated digital logic circuits can be constructed from three basic gates: the **OR gate**, the **NOT gate** and the **AND gate**.

A **combinational circuit** uses these gates and obeys the following rules.

1. Two input wires cannot be combined without a gate.
2. A single input wire can be split partway and directed into two separate gates.
3. An output wire from a gate can be used as input for another gate.

4. No output wire from a gate can eventually feed back into that gate.

For example, the logical expression $(p \wedge \sim q) \vee \sim r$ has the combinational circuit

- NOT$(q) \to n_1$
- AND$(p, n_1) \to a_1$
- NOT$(r) \to n_2$
- OR$(a_1, n_2) \to$ output $(p \wedge \sim q) \vee \sim r$

Application problems

1. Find the bitwise OR, bitwise AND and bitwise XOR of each of these pairs of binary strings.

   (a) 1011110, 0100001

   (b) 11110000, 10101010

2. Construct a combinational circuit using the NOT, OR and AND gates that produces the outputs:

   (a) $(\sim p \vee \sim r) \wedge q$

   (b) $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. Find the output of the following combinational circuit, simplify the expression using logical laws and construct a new circuit for the simplified expression. The circuit is

   - NOT$(p) \to n_1$
   - NOT$(q) \to n_2$
   - OR$(p, n_2) \to o_1$
   - OR$(n_1, n_2) \to o_2$
   - AND$(o_1, o_2) \to a_1$
   - OR$(a_1, r) \to$ output

   (both p and q have their wires split, feeding two gates each).

4. The logical binary operation NAND, denoted $|$, is defined by

$$p \mid q \equiv \sim (p \wedge q).$$

   (a) Write down the truth table for $\sim (p \mid q)$. Show all working.

   (b) Prove, using truth tables or otherwise, that $(p \mid p) \equiv (\sim p)$. Show all working.

   (c) Prove, using truth tables or otherwise, that $((p \mid p) \mid (q \mid q)) \equiv p \vee q$. Show all working.

Application solutions

1. (a)
$$1011110 \text{ OR } 0100001 = 1111111,$$
$$1011110 \text{ AND } 0100001 = 0000000,$$
$$1011110 \text{ XOR } 0100001 = 1111111.$$

   (b)
$$11110000 \text{ OR } 10101010 = 11111010,$$
$$11110000 \text{ AND } 10101010 = 10100000,$$
$$11110000 \text{ XOR } 10101010 = 01011010.$$

2. (a) The circuit is
   - NOT$(p) \to n_1$
   - NOT$(r) \to n_2$
   - OR$(n_1, n_2) \to o_1$
   - AND$(o_1, q) \to$ output $(\sim p \vee \sim r) \wedge q$

   (b) The circuit is
   - NOT$(r) \to n_1$
   - AND$(p, n_1) \to a_1$
   - NOT$(q) \to n_2$
   - AND$(n_2, r) \to a_2$
   - OR$(a_1, a_2) \to$ output $(p \wedge \sim r) \vee (\sim q \wedge r)$

3. The given digital logic circuit has output $((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r$. Using laws of logical equivalence we have

$$\begin{aligned} ((p \vee \sim q) \wedge (\sim p \vee \sim q)) \vee r &\equiv (\sim q \vee (p \wedge \sim p)) \vee r && \text{by distributive and commutative laws} \\ &\equiv (\sim q \vee \mathbf{c}) \vee r && \text{by negation law} \\ &\equiv \sim q \vee r && \text{by identity law} \end{aligned}$$

   The simplification is $\sim q \vee r$. The simplified logic circuit is
   - NOT$(q) \to n_1$
   - OR$(r, n_1) \to$ output $\sim q \vee r$

4. (a) We have

p	q	$p \wedge q$	$p \mid q$	$\sim (p \mid q)$
T	T	T	F	T
T	F	F	T	F
F	T	F	T	F
F	F	F	T	F

Hence $\sim (p \mid q)$ has the same truth values as $p \wedge q$ (it is true exactly when both p and q are true).

(b) Since $p \mid p \equiv \sim (p \wedge p)$, we have

$$p \mid p \equiv \sim (p \wedge p) \equiv \sim p$$

because $p \wedge p \equiv p$ (idempotent law). Alternatively, by truth table:

p	$p \wedge p$	$p \mid p$	$\sim p$
T	T	F	F
F	F	T	T

The last two columns agree, so $p \mid p \equiv \sim p$.

(c) First note from part (b) that $p \mid p \equiv \sim p$ and $q \mid q \equiv \sim q$. Therefore

$$\begin{aligned} (p \mid p) \mid (q \mid q) &\equiv (\sim p) \mid (\sim q) && \text{by part (b)} \\ &\equiv \sim ((\sim p) \wedge (\sim q)) && \text{by def of NAND} \\ &\equiv p \vee q && \text{by De Morgan's law.} \end{aligned}$$

Alternatively, by truth table:

p	q	$p \mid p$	$q \mid q$	$(p \mid p) \mid (q \mid q)$	$p \vee q$
T	T	F	F	T	T
T	F	F	T	T	T
F	T	T	F	T	T
F	F	T	T	F	F

The last two columns match, hence $(p \mid p) \mid (q \mid q) \equiv p \vee q$.

§3 — Conditional Statements

Epp 4th ed. pp. 039–050 · 5th ed. (metric) pp. 053–066. Lecture 3 (week 1). Notes: conditional-statements[163].

Problems

1. Let p, q and r be statements. Use the laws of logical equivalence to show that

$$p \to (q \vee r) \equiv (p \wedge \sim q) \to r.$$

2. Let p and q be statement variables. Are the following statements logically equivalent? Justify your answer.

   - **Statement A:** $(p \to q) \wedge \sim q$
   - **Statement B:** $\sim (p \wedge q)$

3. Write each of the following statements in the form 'if … then …'.

   (a) A sufficient condition for the warranty to be good is that you bought the computer less than a year ago.

   (b) Jane gets seasick whenever she is on a boat.

4. For each of the following, write down a truth table for the statement, and determine whether the statement is a tautology, a contradiction, or neither.

   (a) $(\sim p \wedge (p \to q)) \to \sim q$

   (b) $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$

5. Negate the following two statements.

   (a) If it rains, then Sue takes her umbrella.

   (b) The cakes burn if the oven temperature is too high.

6. Recall "a sufficient condition for s is r" means r is a sufficient condition for s, and that "a necessary condition for s is r" means r is a necessary condition for s. Rewrite the following statements in 'if … then …' form:

   (a) A sufficient condition for John's team to win the championship is that it wins the rest of its games.

   (b) A necessary condition for this computer program to be correct is that it not produce error messages during translation.

[163] courses/math1061/conditional-statements.pdf

Solutions

1. We have

$$\begin{aligned} p \to (q \vee r) &\equiv \sim p \vee (q \vee r) && \text{by definition of implication} \\ &\equiv (\sim p \vee q) \vee r && \text{by the associative law} \\ &\equiv \sim (p \wedge \sim q) \vee r && \text{by De Morgan's law and double negative law} \\ &\equiv (p \wedge \sim q) \to r && \text{by definition of implication.} \end{aligned}$$

2. Let A be the statement $(p \to q) \wedge \sim q$ and let B be the statement $\sim (p \wedge q)$. Then

$$\begin{aligned} A &\equiv (\sim p \vee q) \wedge \sim q && \text{by definition of implication} \\ &\equiv (\sim p \wedge \sim q) \vee (q \wedge \sim q) && \text{by distributive and commutative laws} \\ &\equiv (\sim p \wedge \sim q) \vee \mathbf{c} && \text{by negation law} \\ &\equiv \sim p \wedge \sim q && \text{by identity law,} \end{aligned}$$

   while

$$B \equiv \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \text{by De Morgan's law.}$$

   Thus Statement A and Statement B are **not** logically equivalent because, for example, if p is false and q is true, then A is false and B is true. Hence $A \not\equiv B$.

3. (a) If you bought the computer less than a year ago, then the warranty is good.

   (b) If Jane is on a boat, then Jane gets seasick.

4. (a) **Solution Option 1.** The truth table for the statement is

p	q	$\sim p$	$p \to q$	$\sim p \wedge (p \to q)$	$\sim q$	$(\sim p \wedge (p \to q)) \to \sim q$
T	T	F	T	F	F	T
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T

   The statement is **neither a tautology nor a contradiction**.

   Solution Option 2. The same truth table, written under the parts of the statement:

p	q	$\sim p$	$\wedge$	$(p \to q)$	$\to$	$\sim q$
T	T	F	F	T	T	F
T	F	F	F	F	T	T
F	T	T	T	T	F	F
F	F	T	T	T	T	T
order						

The small numbers show the order in which the columns were completed. Column comes from comparing columns and . Column comes from comparing columns and , and shows the truth values for the entire statement. This shows that this statement is neither a tautology nor a contradiction. (You don't have to number the columns — this is just to help your understanding!)

(b) **Solution Option 1.** The truth tables for the LHS and RHS are:

p	q	r	$q \vee r$	$p \to (q \vee r)$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \to r$
T	T	T	T	T	F	F	T
T	T	F	T	T	F	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	F	F	T
F	T	F	T	T	F	F	T
F	F	T	T	T	T	F	T
F	F	F	F	T	T	F	T

Therefore the truth table for the statement is:

p	q	r	$(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$
T	T	T	T
T	T	F	T
T	F	T	T
T	F	F	T
F	T	T	T
F	T	F	T
F	F	T	T
F	F	F	T

The statement is a **tautology**.

Solution Option 2. Another way to represent the truth table for $(p \to (q \vee r)) \leftrightarrow ((p \wedge \sim q) \to r)$:

p	q	r	$p \to$	$(q \vee r)$	$\leftrightarrow$	$(p \wedge \sim q)$	$\to r$
T	T	T	T	T	T	F	T
T	T	F	T	T	T	F	T
T	F	T	T	T	T	T	T
T	F	F	F	F	T	T	F
F	T	T	T	T	T	F	T
F	T	F	T	T	T	F	T
F	F	T	T	T	T	F	T
F	F	F	T	F	T	F	T
order							

Here column comes from comparing columns and . We see (from column) that this is a tautology.

5. (a) Let R be the statement "it rains" and U be the statement "Sue takes her umbrella." The given statement is $R \to U$. Its negation is

$$R \wedge \sim U,$$

i.e. "It rains and Sue does not take her umbrella."

(b) Let H be the statement "the oven temperature is too high" and B be the statement "the cakes burn." The given statement is $H \to B$. Its negation is

$$H \wedge \sim B,$$

i.e. "The oven temperature is too high and the cakes do not burn."

6. (a) If John's team wins the rest of its games, then John's team will win the championship.

(b) If this computer program is correct, then it does not produce error messages during translation.

§4 — Valid and Invalid Arguments

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 4 (week 2). Notes: valid-argument-forms[164].

[164] courses/math1061/valid-argument-forms.pdf

Problems

1. State truth values for the statement variables p and q that demonstrate that the following argument is invalid, and justify your answer.

   Premise 1: q Premise 2: $p \to q$ Conclusion: p

2. Find values of the statement variables a, b and c that show that the following argument is invalid.

   1. $a \to b$
   2. $\sim a \to c$
   3. $\sim b \to c \therefore b$

3. Use a truth table to show that the following argument forms are valid.

   (a) **Elimination:**

   1. $p \vee q$
   2. $\sim q \therefore p$

   (b) **Generalisation:**

   1. $p \therefore p \vee q$

4. Use a truth table to show that the following argument is invalid.

   1. $(p \wedge q) \to \sim r$
   2. $p \vee \sim q$
   3. $\sim q \to p \therefore \sim r$

Solutions

1. To show the argument is invalid, we must find truth values for p and q such that the premises are true and the conclusion is false.

   Suppose p is false and q is true. Then Premise 1 (q) is true and Premise 2 ($p \to q$) is true (by definition of implication). However, the conclusion (p) is false. Therefore the argument is invalid.

2. To show the argument is invalid, we must find truth values for a, b and c such that the premises are true and the conclusion is false.

   Let a be false, b be false, and c be true. By definition of implication, all three premises are true, but the conclusion (b) is false, so the argument is invalid.

3. (a)

p	q	premise 1: $p \vee q$	premise 2: $\sim q$	conclusion: p
T	T	T	F	T
T	F	T	T	T
F	T	T	F	F
F	F	F	T	F

There is only one row of the truth table in which all premises are true (the second row), and here the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

(b)

p	q	premise 1: p	conclusion: $p \vee q$
T	T	T	T
T	F	T	T
F	T	F	T
F	F	F	F

There are two rows for which all premises (here just the one premise) are true — the first two rows — and for each of these rows the conclusion is true. Thus, whenever all the premises are true, the conclusion is true, so the argument is **valid**.

4. We compute the truth table:

p	q	r	$(p \wedge q) \rightarrow \sim r$	$p \vee \sim q$	$\sim q \rightarrow p$	Prem. 1 $\wedge$ Prem. 2 $\wedge$ Prem. 3	$\sim r$
T	T	T	F	T	T	F	F
T	T	F	T	T	T	T	T
T	F	T	T	T	T	T	F
T	F	F	T	T	T	T	T
F	T	T	T	F	T	F	F
F	T	F	T	F	T	F	T
F	F	T	T	T	F	F	F
F	F	F	T	T	F	F	T

There are three rows for which all the premises are true, however for one of these rows the conclusion is false. In particular, taking p to be true, q to be false, and r to be true makes all the premises true but the conclusion false, so the argument is **invalid**.

§5 — Methods for Determining Validity

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 5 (week 2). Notes: determining-argument-validity[165].

Problems

1. Determine whether the following arguments are valid. If the argument is valid, prove it using rules of inference. If the argument is invalid, demonstrate it with a choice of truth values for the variables.

   (a)

   $p \to q \; q \to p \therefore p \vee q$

   (b)

   $p \; p \to q \sim q \vee r \therefore r$

   (c)

   $p \vee q \; p \to\sim q \; p \to r \therefore r$

2. Write the following argument in symbolic form. Then determine whether the argument is valid or not.

   > An error message is received if the output is flagged. The system is running normally only if the output is not flagged. An error message is received. Therefore, the system is not running normally.

   Please use the following variables:

p	the output is flagged
q	an error message is received
r	the system is running normally

[165] courses/math1061/determining-argument-validity.pdf

3. Give truth values for the variables p, q, r, s and w which demonstrate that the following argument is invalid.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

Solutions

1. (a) The argument is **invalid**. When p and q are both false, all the premises are true, but the conclusion is false. One could arrive at this example by computing the following truth table:

p	q	$p \to q$	$q \to p$	$p \vee q$
T	T	T	T	T
T	F	F	T	T
F	T	T	F	T
F	F	T	T	F

(In the last row, the premises are true, but the conclusion is false.)

(b) The argument is **valid**, and we prove this with rules of inference:

1.	p	Premise
2.	$p \to q$	Premise
3.	$\sim q \vee r$	Premise
4.	q	from 1 and 2 by Modus Ponens
5.	r	from 3 and 4 by elimination (and the double negative law)

Therefore the argument is valid.

(c) Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is false**. Since r is false but the third premise $(p \to r)$ is true, we must have p **is false**. Since p is false, this means the second premise $(p \to \sim q)$ is also true. Now since p is false but the first premise $(p \vee q)$ is true, we must have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

2. The argument has the symbolic form:

1.	$p \to q$	(An error message is received if the output is flagged.)
2.	$r \to \sim p$	(The system is running normally only if the output is not flagged.)
3.	q	(An error message is received.)
$\therefore$	$\sim r$	(The system is not running normally.)

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have r **is true**. Since r is true, and premise 2 is true, we must have $\sim p$ true, that is p **is false**. Since premise 3 is true, we have q **is true**.

Thus, with these truth values for the three variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

3. The argument being valid is the same as this overall implication statement being a tautology.

$$\big[(p \vee q) \wedge (q \to r) \wedge ((p \wedge s) \to w) \wedge (\sim r) \wedge (q \to s)\big] \to w$$

We can write the argument as follows:

1. $p \vee q$
2. $q \to r$
3. $(p \wedge s) \to w$
4. $\sim r$
5. $q \to s \therefore w$

Suppose the argument is invalid. Then it is possible to find truth values for the statement variables that make all the premises true and the conclusion false. For the conclusion to be false, we have w **is false**. Since premise 4 is true we have r **is false**. Since premise 2 is true and r is false, we must have q **is false**. Since premise 1 is true and q is false we have p **is true**. Since premise 3 is true and w is false, we must have $(p \wedge s)$ false, and since p is true, this means s **is false**. These truth values also mean premise 5 is true.

Thus with these truth values for the variables, we have that all the premises are true, but the conclusion is false. So the argument is **invalid**.

Application — Applications of Valid and Invalid Arguments

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 48–68.*

Application problems

1. Translating English sentences into logical expressions is an essential part of specifying both hardware and software systems. Software engineers must take requirements in English and produce precise, unambiguous specifications that can be used as the basis for system development.

   Consider the following predicates and domains:

   Predicates:

$F(x, y)$	disk x has more than y kilobytes of free space.
$S(m)$	mail message m can be saved.
$A(x)$	alert x is active.
$Q(m)$	message m is queued.
$T(m)$	message m is transmitted.
$D(s)$	the diagnostic monitor tracks the status of system s.

   Domains:

M	the nonempty set of all messages.
X	the set of all disks.
Y	the set of all alerts.
S	the set of all systems.

   Express the system specifications below using quantifiers and logical connectives:

   (a) At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.

   (b) Whenever there is an active alert, all queued messages are transmitted.

   (c) The diagnostic monitor tracks the status of all systems except the main console.

2. System specifications should be **consistent**; that is, they should not contain conflicting requirements that could be used to derive a contradiction. When specifications are not consistent, there would be no way to develop a system that satisfies all specifications. Logically, a system is consistent if it is possible for all the premises to be simultaneously true.

Use logical expressions and methods of logical deduction to determine whether the following specifications are consistent.

(a) The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode.

(b) The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed. The router does not support the new address space.

Application solutions

1. (a) $(\exists x \in X \text{ s.t. } F(x, 10)) \rightarrow (\exists m \in M \text{ s.t. } S(m))$.

   (b) $(\exists y \in Y \text{ s.t. } A(y)) \rightarrow (\forall m \in M,\ (Q(m) \rightarrow T(m)))$.

   (c) Let $c \in S$ denote the main console. $\forall s \in S,\ (s \neq c \rightarrow D(s))$.

2. (a) Define the following variables:

m	the system is in multiuser state
n	the system is operating normally
k	the kernel is functioning
i	the system is in interrupt mode

Now we can express the specifications as follows:

1. $m \leftrightarrow n$
2. $n \rightarrow k$
3. $\sim k \vee i$
4. $\sim m \rightarrow i$
5. $\sim i$

Solution Option 1. If these specifications are consistent, then we must be able to find truth values for each of the variables that makes all of the specifications true. Assume the specifications are consistent (so we assume each specification is true). For specification 5 to be true we know i **is false**. For specification 4 to be true, with i false, we know $\sim m$ is false so m **is true**. For premise 1 to be true, with m true, we have n **is true**. For specification 2 to be true, and since n is true, we have k **is true**. However, now $\sim k$ is

false and i is false, which means specification 3 is false. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

Solution Option 2. Suppose the specifications are all true. Using laws of inference, we have

1.	$m \leftrightarrow n$	specification
2.	$n \rightarrow k$	specification
3.	$\sim k \vee i$	specification
4.	$\sim m \rightarrow i$	specification
5.	$\sim i$	specification
6.	$\sim k$	from 3 and 5 by elimination (and double negative law)
7.	$\sim n$	from 2 and 6 by Modus Tollens
8.	$(m \rightarrow n) \wedge (n \rightarrow m)$	from 1 by definition of $\leftrightarrow$
9.	$m \rightarrow n$	from 8 by specialisation
10.	$\sim m$	from 9 and 7 by Modus Tollens
11.	i	from 4 and 10 by Modus Ponens

But now we have both i and $\sim i$ being true, which is a contradiction. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

(b) Define the following variables:

r	the router can send packets to the edge system
a	the router supports the new address space
s	the latest software release is installed

Now we can express the specifications as follows:

1. $r \rightarrow a$
2. $a \rightarrow s$
3. $s \rightarrow r$
4. $\sim a$

Assume the specifications are consistent, so each specification is true. For specification 4 to be true, $\sim a$ is true, so a **is false**. For specification 1 to be true with a false we must

have r **is false**. Now, since r is false and specification 3 is true, we have s **is false**. We double-check that specification 2 is true, which it is because a is false. Thus, we have found truth values of the statement variables that make all of the specifications true, so the system **is consistent**.

§6 — Quantified Statements

Epp 4th ed. pp. 096–108 · 5th ed. (metric) pp. 108–121. Lecture 5 (week 2). Notes: quantified-statements[166].

Problems

1. Rewrite each of the following in the form "∀__, __." Here, let D be the set of all dinosaurs, and let L be the set of all logicians.
   (a) All dinosaurs are extinct.
   (b) Every real number is positive, negative, or zero.
   (c) No irrational numbers are integers.
   (d) No logicians are lazy.
   (e) The number 2,147,581,953 is not equal to the square of any integer.
   (f) The number -1 is not equal to the square of any real number.
2. Rewrite each of the following in the form "∃__ such that __." Here, let X be the set of all exercises.
   (a) Some exercises have answers.
   (b) Some real numbers are rational.
3. Determine whether the following statements are true or false. Justify your reasoning.
   (a) $\forall x \in \mathbb{R},\ x \geq \frac{1}{x}$.
   (b) $\forall a \in \mathbb{Z},\ \frac{a-1}{a} \notin \mathbb{Z}$.
   (c) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

[166] courses/math1061/quantified-statements.pdf

Solutions

1. (a) $\forall x \in D,\ x$ is extinct.

   (b) $\forall x \in \mathbb{R},\ (x > 0 \vee x < 0 \vee x = 0)$.

   (c) $\forall x \in \mathbb{R},\ (x \text{ is irrational} \to x \notin \mathbb{Z})$.

   (d) $\forall x \in L,\ x$ is not lazy.

   (e) $\forall x \in \mathbb{Z},\ x^2 \neq 2147581953$.

   (f) $\forall x \in \mathbb{R},\ -1 \neq x^2$.

2. (a) $\exists x \in X$ such that x has an answer.

   (b) $\exists x \in \mathbb{R}$ such that $x \in \mathbb{Q}$.

3. (a) **False.** Counterexample: take $x = \frac{1}{2}$. Then $x = \frac{1}{2}$ but $\frac{1}{x} = 2$, so $x \geq \frac{1}{x}$ is false.

   (b) **False.** Counterexample: take $a = 1$. Then $\frac{a-1}{a} = \frac{0}{1} = 0 \in \mathbb{Z}$.

   (c) **False.** Counterexample: take $n = m = 1$. Then $mn = 1$ but $m + n = 2$.

§7 — Negation of Quantified Statements

Epp 4th ed. pp. 108–117 · 5th ed. (metric) pp. 122–131. Lecture 6 (week 2). Notes: quantified-statements[167].

Problems

1. Write the negation of each of the following statements, and then determine whether the original or the negation is true:

   (a) $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$.

   (b) $\forall n \in \mathbb{Z}^+$, n is either prime or composite.

   (c) $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$.

2. Write down the negation of each of the following statements:

   (a) All fire engines are red.

   (b) Some apples are ripe.

   (c) A triangle with equal sides exists.

[167] courses/math1061/quantified-statements.pdf

Solutions

1. (a) **Original:** $\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$. **Negation:** $\exists x \in \mathbb{R}$ such that $x^2 > 9$ and $x < 2$.

   The original statement is **false**. For instance, take $x = -4$. Then $x^2 > 9$ but $x \ngeq 2$.

   (b) **Original:** $\forall n \in \mathbb{Z}^+$, n is either prime or composite. **Negation:** $\exists n \in \mathbb{Z}^+$ such that n is neither prime nor composite.

   The original statement is **false**. For instance, consider $n = 1$, which is neither prime nor composite.

   (c) **Original:** $\exists x, y \in \mathbb{R}$ such that $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ but $xy \in \mathbb{Z}$. **Negation:** $\forall x, y \in \mathbb{R}$, if $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$ then $xy \notin \mathbb{Z}$.

   The original statement is **true**. For instance, take $x = \sqrt{2}$ and $y = \sqrt{2}$. Then $x \notin \mathbb{Z}$ and $y \notin \mathbb{Z}$, but $xy = 2 \in \mathbb{Z}$.

2. (a) **Original:** All fire engines are red. **Negation:** There exists a fire engine which is not red.

   (b) **Original:** Some apples are ripe. **Negation:** All apples are not ripe.

   (c) **Original:** A triangle with equal sides exists. **Negation:** There does not exist a triangle with equal sides.

§8 — Statements with Multiple Quantifiers

Epp 4th ed. pp. 117–131 · 5th ed. (metric) pp. 131–146. Lecture 6 (week 2). Notes: quantified-statements[168].

Problems

1. Write down the negation of each of the following statements. Then determine whether the statement is true, or whether its negation is true.

   (a) $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$.

   (b) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$.

   (c) $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$.

   (d) $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$.

2. For each of the following English sentences:

[168] courses/math1061/quantified-statements.pdf

(a) For any rational number x and any negative integer y there exists a real number that is greater than the product of x and y.

(b) For every real number x, there is a real number y for which $3y = x$.

do the following:

i. Write the statement in symbolic form.

ii. Write the negation of the statement in symbolic form.

iii. Determine which of the statement or its negation is true.

Solutions

1. (a) **Original:** $\forall x, y \in \mathbb{Z}$, $\exists z \in \mathbb{Z}$ such that $z = x - y$. **Negation:** $\exists x \in \mathbb{Z}$ $\exists y \in \mathbb{Z}$ such that $\forall z \in \mathbb{Z}$, $z \neq x - y$.

   The original statement is **true** (and the negation is false). For any given $x, y \in \mathbb{Z}$, choose $z = x - y \in \mathbb{Z}$.

   (b) **Original:** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $x^2 - xy - 2y^2 = 0$. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}$, $x^2 - xy - 2y^2 \neq 0$.

   The original statement is **true** (and the negation is false). For any $x \in \mathbb{R}$, taking $y = \frac{x}{2}$ gives

$$x^2 - x\left(\frac{x}{2}\right) - 2\left(\frac{x}{2}\right)^2 = x^2 - \frac{x^2}{2} - 2 \cdot \frac{x^2}{4} = x^2 - \frac{x^2}{2} - \frac{x^2}{2} = 0.$$

   (c) **Original:** $\exists x \in \mathbb{Z}^+$ such that $\forall y \in \mathbb{Z}^+$, $x \geq y$. **Negation:** $\forall x \in \mathbb{Z}^+$ $\exists y \in \mathbb{Z}^+$ such that $x < y$.

   The **negation** is true (and the original is false). For any $x \in \mathbb{Z}^+$, take $y = x + 1$. Then y is an integer satisfying the inequality $x < y$.

   (d) **Original:** $\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$, then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$. **Negation:** $\exists r, s \in \mathbb{R}$ such that $rs \in \mathbb{Q}$ and ($r \notin \mathbb{Q}$ or $s \notin \mathbb{Q}$).

   The **negation** is true (and the original is false). Take $r = \sqrt{2}$ and $s = \sqrt{2}$. Then $rs = 2 \in \mathbb{Q}$ but $r, s \notin \mathbb{Q}$.

2. (a) i. **Original:** $\forall x \in \mathbb{Q}$, $\forall y \in \mathbb{Z}^{<0}$, $\exists z \in \mathbb{R}$ s.t. $z > xy$.

   ii. **Negation:** $\exists x \in \mathbb{Q}$ $\exists y \in \mathbb{Z}^{<0}$ s.t. $\forall z \in \mathbb{R}$, $z \leq xy$.

   iii. The **original** statement is true. For any given $x \in \mathbb{Q}$ and $y \in \mathbb{Z}^{<0}$, take $z = xy + 1$. This is a real number satisfying the inequality $z > xy$.

(b) i. **Original:** $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}$ s.t. $3y = x$.

ii. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R},\ 3y \neq x$.

iii. The **original** statement is true. Given any $x \in \mathbb{R}$, choose $y = \frac{x}{3}$. This is a real number satisfying the equality $3y = x$.

§9 — Direct Proofs and Counterexamples

Epp 4th ed. pp. 145–163 · 5th ed. (metric) pp. 160–182. Lecture 7 (week 3). Notes: proof-techniques[169].

Problems

1. For each of the following statements, either prove the statement or disprove it using a counterexample.

   (a) The sum of any pair of even integers is even.

   (b) There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.

   (c) There is an even integer n such that $5n - 4$ is prime.

   (d) $\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

   (e) $\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.

2. Find a counterexample that disproves the following statement:

   $$\text{For all } x \in \mathbb{R},\ \lfloor x^2 \rfloor = \lfloor x \rfloor^2.$$

   (Recall that $\lfloor \cdot \rfloor$ denotes the floor function.)

3. Find the errors in the following proofs and rewrite the proof correctly. Here is a list of common errors made when writing proofs:

   - Arguing from examples
   - Using the same variable to mean two different things
   - Jumping to the conclusion
   - Assuming what is to be proved
   - Confusion between what is known and what is to be shown
   - Use of the word *any* instead of *some*
   - Misuse of the word *if*

[169] courses/math1061/proof-techniques.pdf

(a) The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

(b) If a and b are even integers, then $4a + 2b$ is even.

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

(c) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true.

(d) $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that $n^2 + 2n + 1$ is composite, so this means

$$n^2 + 2n + 1 = rs$$

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite.

Solutions

1. (a) **The sum of any pair of even integers is even.**

Proof. Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence

$$m + n = 2k + 2\ell = 2(k + \ell),$$

which is even. Therefore, the sum of any pair of even integers is even. □

(b) **There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.**

Proof. Consider the positive integers $a = 3$, $b = 4$, $c = 5$. Then $a^2 + b^2 = 9 + 16 = 25 = c^2$. □

(c) **There is an even integer n such that $5n - 4$ is prime.** This statement is **false**. We prove the negation: $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

Proof. Suppose that n is an even integer. Thus $n = 2k$ for some integer k. Hence

$$5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2).$$

By definition, this means that $5n - 4$ is even. The only even prime is 2. If $2(5k - 2) = 2$, then $5k - 2 = 1$ and hence $k = \frac{3}{5}$ which is not an integer. Therefore $5n - 4$ is not a prime number. □

(d) **$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.**

Proof. Suppose n is a positive integer and $n \geq 4$. Let us factor

$$2n^2 - 5n + 2 = (2n - 1)(n - 2).$$

Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers > 1. Hence the expression is composite for all $n \geq 4$. □

(e) **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** This statement is **false**. Take $x = 1$ and $y = -2$. Then $y^2 = 4 > x^2 = 1$, but $y = -2 \not> 1 = x$.

2. Take $x = \frac{3}{2}$. Then $\lfloor x^2 \rfloor = \lfloor \frac{9}{4} \rfloor = 2$, while $\lfloor x \rfloor^2 = \lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$. Hence $\lfloor x^2 \rfloor \neq \lfloor x \rfloor^2$, so the statement is false.

3. (a) **Statement.** The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. **[Error: using k for both m and n means that the statement is only proved when $m = n + 1$.]** Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

Correct proof. Let m be any odd integer and let n be any even integer. Then there exist $k, \ell \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2\ell$. Hence

$$m - n = (2k + 1) - 2\ell = 2(k - \ell) + 1,$$

which is an odd integer by definition. □

(b) **Statement.** If a and b are even integers, then $4a + 2b$ is even. **[Error: the proof forgets to state its assumptions.]**

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \quad \textbf{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

Correct proof. Suppose a and b are even integers. Then $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Therefore

$$4a + 2b = 4(2k) + 2(2j) = 8k + 4j = 2(4k + 2j).$$

Since $k, j \in \mathbb{Z}$, we have $(4k + 2j) \in \mathbb{Z}$ and so, by definition, $4a + 2b$ is even. □

(c) **Statement.** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true. **[Error: the proof argues from a single example, which cannot establish a universal statement. Moreover, the statement is false.]**

Correct disproof. The statement is false. As a counterexample, let $x = 0$. We know that $0 \cdot y = 0$ for all $y \in \mathbb{R}$ and so there is no real number y such that $0 \cdot y = 1$. □

(d) **Statement.** $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that n^2+2n+1 is composite, so this means

$n^2+2n+1 = rs$ **[Error: forgets to define r, s — e.g. for some $r, s \in \mathbb{Z}$]**

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite. **[Error: this is jumping to the conclusion without showing what needs to be shown. The expression we need to show (the definition of composite) has been given but it has not been shown.]**

Correct proof. Let $n \in \mathbb{Z}$ with $n > 0$. Then we have

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

Now since $0 < n < n^2 + 2n$, we must have that $1 < n + 1 < n^2 + 2n + 1$. So by letting $r = s = n + 1$ we have shown that

$$n^2 + 2n + 1 = rs$$

for integers $1 < r, s < n^2 + 2n + 1$. By definition this means $n^2 + 2n + 1$ is composite. □

Application — Applications of Proofs to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 74–80.*

Computer programs have been developed to automate the task of reasoning and proving theorems. Many of these programs make use of a rule of inference known as **resolution**. This rule of inference is based on the tautology

$$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r) \tag{1}$$

Resolution can be used to build automatic theorem proving systems.

To construct proofs using resolution as the only rule of inference, the hypotheses and conclusion must be expressed as **clauses**. Clauses are logical expressions which only feature disjunctions of variables or their negations (i.e. expressions which only use $\vee$, $\sim$, so they do not use $\wedge$, $\rightarrow$). To express any statement as a clause, we can use the laws of logical equivalence.

Application problems

1. (a) Using a truth table, show that expression (1) is a tautology.

   (b) Write the following expressions as clauses.

   i. $\sim (\sim r \wedge w)$

   ii. $r \rightarrow u$

   iii. $\sim (u \wedge w)$

   (c) Use resolution only to show that the following argument is valid:

   If it is raining, then Yvette has their umbrella. It is not the case that Yvette has their umbrella and gets wet. It is not the case that Yvette gets wet while it is not raining. Therefore, Yvette does not get wet.

Application solutions

1. (a) The truth table is

p	q	r	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r)$
T	T	T	T	T	T	T	T
T	T	F	T	F	F	T	T
T	F	T	T	T	T	T	T
T	F	F	T	F	F	F	T
F	T	T	T	T	T	T	T
F	T	F	T	T	T	T	T
F	F	T	F	T	F	T	T
F	F	F	F	T	F	F	T

Since the last column is always T, the statement is a tautology.

(b) Clause forms:

i. $\sim (\sim r \wedge w) \equiv r \vee \sim w$ (by De Morgan's law and double negative law).

ii. $r \rightarrow u \equiv \sim r \vee u$ (by definition of implication).

iii. $\sim (u \wedge w) \equiv \sim u \vee \sim w$ (by De Morgan's law).

(c) Define the following variables:

r	it is raining
u	Yvette has their umbrella
w	Yvette gets wet

Then we can express the argument as

1. $r \rightarrow u$
2. $\sim (u \wedge w)$
3. $\sim (\sim r \wedge w) \therefore \sim w$

Using the equivalences in (b), we can rewrite this as

1.	$\sim r \vee u$	
2.	$\sim u \vee \sim w$	
3.	$r \vee \sim w$	
4.	$\sim r \vee \sim w$	From 1 and 2 by Resolution
5.	$\sim w$	From 3 and 4 by Resolution.

§10 — Proof by Contradiction

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 8 (week 3). Notes: proof-techniques[170].

Problems

1. Prove the following statement using a proof by contradiction:

   For integers a and b, if $6a + 3b$ is odd, then b is odd.

2. Use a proof by contradiction to prove the following statement:

   For all positive integers x and y, $x^2 - y^2 \neq 1$.

Solutions

1. **For integers a and b, if $6a + 3b$ is odd, then b is odd.**

   Proof. Suppose the statement is false, that is, suppose that there exist integers a and b for which $6a + 3b$ is odd and b is even.

   Since b is even, $b = 2k$ for some integer k. Thus

   $$6a + 3b = 6a + 3(2k) = 6a + 6k = 2(3a + 3k).$$

   Since $a, k \in \mathbb{Z}$, $3a + 3k \in \mathbb{Z}$ so $6a + 3b$ is even. This contradicts our assumption that $6a + 3b$ is odd, so our assumption was incorrect and hence the original statement is true. □

[170] courses/math1061/proof-techniques.pdf

2. **For all positive integers x and y, $x^2 - y^2 \neq 1$.**

   Proof. Suppose, for contradiction, that x and y are positive integers satisfying $x^2 - y^2 = 1$. Now, by factoring, we have

   $$1 = x^2 - y^2 = (x - y)(x + y).$$

   Since x and y are positive integers, we must have $x - y = 1$ and $x + y = 1$. This means $2x = 2$, so $x = 1$. But then we must have $y = 0$ which is not a positive integer; this is a contradiction. Therefore the original statement is true. □

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[171].

Problems

1. Use proof by contraposition to prove the following statement:

   For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

2. Prove the following statement:

   For any integer n, n^2 is odd if and only if n is odd.

   Use a direct proof for the reverse implication ($\Leftarrow$), and a proof by contraposition for the forward implication ($\Rightarrow$).

3. Use proof by contraposition to prove the following statement:

   For all integers x and y, if $x^2(y^2 - 2y)$ is odd then x and y are odd.

[171] courses/math1061/proof-techniques.pdf

Solutions

1. **For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.**

   Proof. We prove the contrapositive statement, which is:

   > For all integers a and b, if a is even or b is even, then $(ab)^2$ is even.

   Let a and b be integers and suppose a is even or b is even. Without loss of generality, suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ is even, and therefore $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, we know $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even by definition. □

2. **For any integer n, n^2 is odd if and only if n is odd.**

   Proof. To prove this "if and only if" statement, we must prove each of the following two statements:

   > ($\Leftarrow$) For any integer n, if n is odd, then n^2 is odd. ($\Rightarrow$) For any integer n, if n^2 is odd, then n is odd.

   ($\Leftarrow$) Let n be an integer and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Hence $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Since $k \in \mathbb{Z}$, we have $2k^2+2k \in \mathbb{Z}$ and hence n^2 is odd by definition.

   ($\Rightarrow$) The contrapositive is: for any integer n, if n is even, then n^2 is even. Let n be an integer and suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 = 4k^2 = 2(2k^2)$. Since $k \in \mathbb{Z}$, we have $2k^2 \in \mathbb{Z}$, so n^2 is even by definition.

   Therefore, for all integers n, n^2 is odd if and only if n is odd. □

3. **For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.**

   Proof. We will prove the contrapositive statement, which is:

   > For all integers x and y, if x is even or y is even, then $x^2(y^2-2y)$ is even.

   Let $x, y \in \mathbb{Z}$ and suppose x or y is even. We consider the cases of x even or y even individually.

   Case 1. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Hence

   $$x^2(y^2-2y) = (2k)^2(y^2-2y) = 2(2k^2)(y^2-2y).$$

   Since $k, y \in \mathbb{Z}$, we have $(2k^2)(y^2-2y) \in \mathbb{Z}$, and hence $x^2(y^2-2y)$ is even, by definition.

Case 2. Suppose y is even. Then $y = 2\ell$ for some $\ell \in \mathbb{Z}$. Hence

$$x^2(y^2 - 2y) = x^2((2\ell)^2 - 2(2\ell)) = 2(x^2(2\ell^2 - 2\ell)).$$

Since $x, \ell \in \mathbb{Z}$, we have $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$ and thus $x^2(y^2 - 2y)$ is even, by definition. □

§12 — Rational Numbers

Epp 4th ed. pp. 163–170 · 5th ed. (metric) pp. 183–190. Lecture 9 (week 3). Notes: rational-and-irrational-numbers[172].

Problems

1. Prove the following statement:

   For real numbers m and n, if m is irrational and n is rational, then $m - n$ is irrational.

2. Prove the following statement:

   For a real number r, if $2r^2 - 3r$ is irrational, then r is irrational.

3. Prove the following statement:

   For all real numbers r, s, n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrati

4. Recall that $\sqrt{2}$ is irrational. Consider the statement

   For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.

   (a) Write down the negation of the statement.

   (b) Use a proof by contradiction to prove the statement.

[172] courses/math1061/rational-and-irrational-numbers.pdf

Solutions

1. **For real numbers m and n, if m is irrational and n is rational, then $m-n$ is irrational.**

   Proof. Let m and n be real numbers and suppose (for a contradiction) that m is an irrational number and n is rational, but $m-n$ is rational. Since n is rational, we have $n = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Since $m-n$ is rational, we have $m-n = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Notice that $m = (m-n)+n$. Hence

   $$m = (m-n)+n = \frac{c}{d} + \frac{a}{b} = \frac{bc+ad}{bd}.$$

   Since $a, b, c, d \in \mathbb{Z}$ we have $bc+ad \in \mathbb{Z}$ and $bd \in \mathbb{Z}$. Further, since $b \neq 0$ and $d \neq 0$, we have $bd \neq 0$. Thus, by definition, m is rational. But this contradicts the assumption that m is irrational. □

2. **For a real number r, if $2r^2-3r$ is irrational, then r is irrational.**

   Proof. We prove the contrapositive statement: for a real number r, if r is rational, then $2r^2-3r$ is rational.

   Let r be a real number and suppose $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. So

   $$2r^2-3r = 2\left(\frac{a}{b}\right)^2 - 3\left(\frac{a}{b}\right) = \frac{2a^2-3ab}{b^2}.$$

   Since $a, b \in \mathbb{Z}$, we have $2a^2-3ab \in \mathbb{Z}$ and $b^2 \in \mathbb{Z}$. Further, $b^2 \neq 0$ because $b \neq 0$. This means $2r^2-3r$ is rational, by definition. □

3. **For all real numbers r, s, and n, if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrational.**

   Proof. Suppose, for a contradiction, that the statement is false. Then there exist real numbers r, s and n such that r is an irrational number, s is rational, n is a positive integer, but $n(r-s)$ is rational. Since s is rational, $s = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Since $n(r-s)$ is rational, we have $n(r-s) = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

Now,

$$\begin{aligned} r - s &= n(r-s)\left(\frac{1}{n}\right) \quad \text{noting that } n \neq 0 \\ r - s &= \frac{c}{d} \cdot \frac{1}{n} \\ r &= s + \frac{c}{d} \cdot \frac{1}{n} \\ &= \frac{a}{b} + \frac{c}{dn} \\ &= \frac{adn + bc}{bdn} \end{aligned}$$

Since $a, b, c, d \in \mathbb{Z}$, we have $adn + bc \in \mathbb{Z}$ and $bdn \in \mathbb{Z}$. Further, since $b \neq 0$, $d \neq 0$ and $n \neq 0$, we have $bdn \neq 0$. This means r is rational, by definition, which is a contradiction. □

4. **For every rational number r, if $r \neq 0$, then $r\sqrt{2}$ is an irrational number.**

   (a) **Negation:** There exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

   (b)

   Proof. Suppose, for a contradiction, that the original statement is false. Then there exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$. Since r is rational, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and since $r \neq 0$, we have $a \neq 0$. Since we have assumed $r\sqrt{2}$ is rational, $r\sqrt{2} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Now

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \left(r\sqrt{2}\right)\left(\frac{1}{r}\right) = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad}.$$

   Since $a, b, c, d \in \mathbb{Z}$, we know $bc \in \mathbb{Z}$ and $ad \in \mathbb{Z}$. Further, since $a \neq 0$ and $d \neq 0$, we have $ad \neq 0$. Thus, by definition, $\sqrt{2}$ is rational. However, this is a contradiction, as $\sqrt{2}$ is irrational. Thus, the original statement is true. □

§13 — Divisibility

Epp 4th ed. pp. 170–179 · 5th ed. (metric) pp. 190–199. Lecture 10 (week 4). Notes: divisibility-and-factorisation[173].

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

Problems

1. Find the unique factorisation (in standard form) of the integer 27 720.
2. Prove or disprove the statement: for any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.
3. Prove the following statements.
   (a) If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.
   (b) The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.
4. Use proof by contradiction to prove this statement:

$$\text{For all integers } c, d \text{ and } e, \text{ if } c \mid d \text{ and } c \nmid e, \text{ then } c \nmid (d+e).$$

Solutions

1. By repeated division, we have $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.
2. **For any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.** The statement is **true**, and we will prove it.

   Proof. Let m, n, and q be non-zero integers. Assume $m \mid n$ and $n \mid q$. Then, by definition, there exist integers a, b such that

   $$n = ma \quad \text{and} \quad q = nb.$$

   Then observe

   $$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2b).$$

   Since $a^2b \in \mathbb{Z}$, we conclude that $m^2 \mid nq$. □
3. (a) **If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.**

   Proof. Let k be even and m be odd. Then $k = 2a$ and $m = 2b+1$ for some $a, b \in \mathbb{Z}$. Hence

   $$(k+2)^2 = (2a+2)^2 = 4(a+1)^2 \quad \text{and} \quad (m-3)^2 = (2b-2)^2 = 4(b-1)^2.$$

   Therefore

   $$(k+2)^2-(m-3)^2 = 4\big[(a+1)^2-(b-1)^2\big].$$

   Since $a, b \in \mathbb{Z}$ we have $(a+1)^2-(b-1)^2 \in \mathbb{Z}$ so $4 \mid \big[(k+2)^2-(m-3)^2\big]$. □

(b) **The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.**

Proof. Let n and $n+1$ be two consecutive integers. The difference between their cubes is

$$(n+1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n+1) + 1.$$

Now whether n is odd or even (so whatever integer n is), one of n, $n+1$ will be odd and the other one will be even. Thus the product $n(n+1)$ is even.

Since $n(n+1)$ is even, write $n(n+1) = 2t$ for some $t \in \mathbb{Z}$. Then

$$(n+1)^3 - n^3 = 3(2t) + 1 = 6t + 1 \equiv 1 \pmod 6.$$

Hence the remainder is 1 upon division by 6. □

4. **For all integers c, d and e, if $c \mid d$ and $c \nmid e$, then $c \nmid (d+e)$.**

Proof. Suppose for a contradiction that the statement is false. Then there exist integers c, d and e such that $c \mid d$ and $c \nmid e$ and $c \mid (d+e)$.

Now $c \mid d$ means that $d = cx$ for some integer x. And $c \mid (d+e)$ means that $d + e = cy$ for some integer y.

Hence $d + e = cx + e = cy$, so $e = cy - cx = c(y - x)$, and we have $y - x \in \mathbb{Z}$, because x and y are both integers. Thus $c \mid e$, a contradiction. So the original statement is true. □

§14 — Modular Arithmetic

Epp 4th ed. pp. 482–485 · 5th ed. (metric) pp. 528–531. Lecture 11 (week 4). Notes: modular-arithmetic[174].

Problems

1. Prove the following statement:

   If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.

2. (a) Evaluate $58 \operatorname{div} 11$ and $58 \bmod 11$.

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

(b) Find integers q and r, with $0 \leqslant r < d$ and $n = dq + r$, in the case that $n = -95$ and $d = 11$.

3. (a) An integer n, when divided by 7, leaves remainder 4. What is the remainder (between 0 and 6 inclusive) when $3n$ is divided by 7?

   (b) When the integer m is divided by 11, the remainder 9 is left. What remainder is left when $4m$ is divided by 22?

4. Prove or disprove the following statements.

   (a) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

   (b) For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.

Solutions

1. **If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.**

   Proof. Fix $y \in \mathbb{Z}$. By the division algorithm, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

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

   Let us compute the possible values for r^2 mod 5:

   $$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

   Thus $y^2 \equiv 0, 1$, or $4 \pmod 5$, and never 2 or 3. □

2. (a) Since $58 = 11 \cdot 5 + 3$ with $0 \leq 3 < 11$, we have

   $$58 \operatorname{div} 11 = 5 \quad \text{and} \quad 58 \bmod 11 = 3.$$

   (b) We want $-95 = 11q + r$ with $0 \leq r < 11$. Taking $q = -9$ gives

   $$11(-9) = -99 \quad \Rightarrow \quad -95 = -99 + 4 = 11(-9) + 4,$$

   so $q = -9$ and $r = 4$.

3. (a) If n leaves remainder 4 upon division by 7, then $n = 7k + 4$ for some integer k. Hence

$$3n = 21k + 12 = 7(3k + 1) + 5,$$

so the remainder when $3n$ is divided by 7 is **5**. (The source PDF prints this step as $7(3k) + 5$, which equals $21k + 5$, not $21k + 12$ — the quotient is $3k + 1$, as above. The answer of 5 is unaffected.)

(b) If m leaves remainder 9 upon division by 11, then $m = 11k + 9$ for some integer k. Then

$$4m = 44k + 36 = 22(2k + 1) + 14,$$

so the remainder when $4m$ is divided by 22 is **14**.

4. (a) **For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** The statement is **false**. For a counterexample, take $x = \frac{3}{2}$. Then

$$\lfloor x^2 \rfloor = \left\lfloor \frac{9}{4} \right\rfloor = 2 \quad \text{but} \quad \lfloor x \rfloor^2 = \left\lfloor \frac{3}{2} \right\rfloor^2 = 1^2 = 1.$$

(b) **For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.** The statement is **true**.

Proof. Let n be an odd integer, so $n = 2k + 1$ for some integer k. Then

$$\frac{n^2}{4} = \frac{(2k+1)^2}{4} = \frac{4k^2 + 4k + 1}{4} = k(k+1) + \frac{1}{4},$$

so $\left\lfloor \frac{n^2}{4} \right\rfloor = k(k+1)$. Moreover, notice

$$\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = \left(\frac{2k}{2}\right)\left(\frac{2k+2}{2}\right) = k(k+1).$$

Hence $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$ for all odd integers n. □

§15 — The Euclidean Algorithm

Epp 4th ed. pp. 220–224 · 5th ed. (metric) pp. 250–254. Lecture 12 (week 4). Notes: gcd-lcm-and-euclidean-algorithm[175].

[175] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

Problems

1. Use the Euclidean Algorithm to determine $\gcd(14, 3003)$.
2. Compute
   (a) $\operatorname{lcm}(12, 18)$
   (b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
   (c) $\operatorname{lcm}(2800, 6125)$
3. Prove that for all positive integers a and b, we have

$$\gcd(a, b) = \operatorname{lcm}(a, b) \iff a = b.$$

4. Prove that for all positive integers a and b, we have

$$a \mid b \iff \operatorname{lcm}(a, b) = b.$$

5. (a) Use the Euclidean algorithm to determine $\gcd(931, 301)$. Show your working.
   (b) Write down the unique prime factorisation of 931 in standard form.
   (c) How many positive divisors does 931 have? (Hint: use part (b).)
6. (a) Using the Euclidean algorithm, compute $\gcd(116, 88)$. Show your working.
   (b) Using your answer to part (a), compute $\operatorname{lcm}(116, 88)$.

Solutions

1. We apply the Euclidean Algorithm:

$$3003 = 14 \cdot 214 + 7, \qquad 14 = 7 \cdot 2 + 0.$$

   Hence $\gcd(14, 3003) = 7$.

2. (a) We factor $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$ so $\operatorname{lcm}(12, 18) = 2^2 \cdot 3^2 = 36$.
   (b) Using the maximum exponents of each prime, we have

$$\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

   (c) We factor $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$. Thus

$$\operatorname{lcm}(2800, 6125) = 2^4 \cdot 5^3 \cdot 7^2 = 98000.$$

3. **For all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.**

   Proof. Let a and b be positive integers.

   ($\Longleftarrow$) It is clear that if $a = b$ then $\gcd(a, b) = \operatorname{lcm}(a, b)$.

   ($\Longrightarrow$) Assume $\gcd(a, b) = \operatorname{lcm}(a, b)$. Denoting $g = \gcd(a, b)$, we have $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$.

   Now notice gm and gn have no common prime factors beyond those in g, so the least common multiple uses all primes from both m and n. Therefore

   $$\operatorname{lcm}(a, b) = gmn.$$

   Now, we have $g = gmn$. Therefore $mn = 1$, and so $m = n = 1$. This lets us conclude $a = b$. □

4. **For all positive integers a and b, $a \mid b$ if and only if $\operatorname{lcm}(a, b) = b$.**

   Proof. Let us denote $g = \gcd(a, b)$ so that $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$. As explained in the previous question, we have

   $$\operatorname{lcm}(a, b) = gmn.$$

   ($\Longrightarrow$) If $a \mid b$, then $gm \mid gn$, hence $m \mid n$. Since $\gcd(m, n) = 1$, we conclude $m = 1$. Therefore $\operatorname{lcm}(a, b) = gmn = gn = b$.

   ($\Longleftarrow$) If $\operatorname{lcm}(a, b) = b$, then $gmn = gn$ which means $m = 1$. Therefore $a = gm = g$ and so $a \mid b$. □

5. (a) Using the Euclidean Algorithm:

   $$\begin{aligned} 931 &= 301 \cdot 3 + 28 \\ 301 &= 28 \cdot 10 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

   Hence $\gcd(931, 301) = 7$.

   (b) Since $\gcd(931, 301) = 7$, we know $7 \mid 931$, and we have $931 = 7 \cdot 133$. The number 133 has prime factorisation $7 \cdot 19$. Therefore the unique prime factorisation of 931 is $7^2 \cdot 19$.

(c) We have $931 = 7^2 \cdot 19^1$ from part (b). Any divisor of 931 must have a prime factorisation of the form $7^a \cdot 19^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. Thus the number of positive divisors is

$$(2 + 1)(1 + 1) = 6.$$

(There are 3 choices for the exponent a and 2 choices for the exponent b.)

6. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 116 &= 88 \cdot 1 + 28 \\ 88 &= 28 \cdot 3 + 4 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Hence $\gcd(116, 88) = 4$.

(b) Using $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{Z}^+$,

$$\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{\gcd(116, 88)} = \frac{116 \cdot 88}{4} = 116 \cdot 22 = 2552.$$

Application — Trace Tables for Algorithms

Not assessable for MATH1061. For reference, see S. Epp, Discrete Mathematics with Applications, *Section 4.8 (4th edition) or Section 4.10 (5th edition), Brooks/Cole, Belmont, CA.*

The following pseudo-code describes the **Division Algorithm**, with annotations to explain what each step is doing.

Input: a (a non-negative integer), d (a positive integer). This algorithm will take two inputs, a and d, and will find the quotient $a \operatorname{div} d$ and the remainder $a \bmod d$.

Algorithm body:

```
r := a          -- defining our variables
q := 0
                -- starting with a, repeatedly subtract lots of d until we reach
                -- a number less than d; each round adds 1 to the quotient count
while r >= d,
    r := r - d
    q := q + 1
end while
```

Output: q, r. Once we have obtained a number less than d, we are finished. The output q is the quotient ($a \operatorname{div} d$) and the output r is the remainder ($a \bmod d$).

The following pseudo-code describes the **Euclidean Algorithm**, with annotations to explain what each step is doing.

Input: A, B (integers with $A > B \geq 0$).

Algorithm body:

```
a := A          -- defining our variables
b := B
r := B
                -- if b /= 0, compute a mod b (call the algorithm above for this
                -- step) and set r to be this value; replace a with b and b with r
                -- and repeat until b = 0
while b /= 0,
    r := a mod b
    a := b
    b := r
end while
gcd := a
```

Output: gcd (a positive integer).

A **trace table** keeps track of the value of each variable at each step of an algorithm. For example, the trace table for the Division Algorithm with input variables $a = 19$ and $d = 4$ is:

Variable / iteration	0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

Output: $q = 4$, $r = 3$.

Application problems

1. Construct a trace table to trace the action of the Division Algorithm for the following inputs.

   (i) $a = 26$, $d = 7$

(ii) $a = 15$, $d = 6$

2. Construct a trace table to trace the action of the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$.

Application solutions

1. (i) Trace table for the Division Algorithm with $a = 26$, $d = 7$:

Variable / iteration	0	1	2	3
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

Output: $q = 3$, $r = 5$.

(ii) Trace table for the Division Algorithm with $a = 15$, $d = 6$:

Variable / iteration	0	1	2
a	15		
d	6		
r	15	9	3
q	0	1	2

Output: $q = 2$, $r = 3$.

2. Trace table for the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$:

Variable / iteration	0	1	2	3	4	5
A	1001					
B	871					
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Output: gcd = 13.

§16 — Sequences

Epp 4th ed. pp. 227–244 · 5th ed. (metric) pp. 258–275. Lecture 13 (week 5).

Problems

1. Write down the first four terms in the sequence defined by $a_k = \dfrac{k}{10+k}$ for $k = 1, 2, \ldots$.
2. Consider the sequences $a_k = 2k + 1$ and $b_k = (k-1)^3 + k + 2$ where $k = 0, 1, 2, \ldots$. Show that the first three terms of these sequences are identical, but that their fourth terms differ.
3. (a) Find an explicit formula for a sequence c_n whose first six terms are $-1, 1, -1, 1, -1, 1$.
   (b) Find an explicit formula for a sequence d_n whose first six terms are $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$.
4. (a) Write $(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)$ in summation notation.
   (b) Evaluate $\displaystyle\prod_{i=1}^{5}(-1)^i \cdot i$.
   (c) Write $(y-1)(y^2-2)(y^3-3)(y^4-4)$ in product notation.
   (d) Evaluate $\displaystyle\sum_{j=1}^{n}(-1)^j\frac{1}{2^j}$ when $n = 5$.

Solutions

1. We have

$$a_1 = \frac{1}{11}, \qquad a_2 = \frac{2}{12} = \frac{1}{6}, \qquad a_3 = \frac{3}{13}, \qquad a_4 = \frac{4}{14} = \frac{2}{7}.$$

2. We compute

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 5, \quad a_3 = 7;$$

$$b_0 = (-1)^3+0+2 = 1, \quad b_1 = 0^3+1+2 = 3, \quad b_2 = 1^3+2+2 = 5, \quad b_3 = 2^3+3+2 = 13.$$

Hence the first three terms agree ($a_0 = b_0$, $a_1 = b_1$ and $a_2 = b_2$), but the fourth terms differ ($a_3 = 7$ while $b_3 = 13$).

3. (a) One explicit formula is

$$c_n = (-1)^n \qquad n = 1, 2, 3, ...$$

(b) The denominators are square numbers, so an explicit formula is

$$d_n = \frac{n}{(n+1)^2} \qquad n = 1, 2, 3, ...$$

4. (a) We have

$$(x^2 - 1) + (2x^3 - 1) + (3x^4 - 1) + (4x^5 - 1) + (5x^6 - 1) = \sum_{k=1}^{5} \left(kx^{k+1} - 1\right).$$

(b) We have

$$\prod_{i=1}^{5}(-1)^i \cdot i = \left(\prod_{i=1}^{5}(-1)^i\right)\left(\prod_{i=1}^{5} i\right) = (-1)^{1+2+3+4+5} \cdot 5! = (-1)^{15} \cdot 120 = -120.$$

(c) We have

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} \left(y^k - k\right).$$

(d) When $n = 5$, we have

$$\sum_{j=1}^{5}(-1)^j \frac{1}{2^j} = -\frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} = -\frac{11}{32}.$$

§17 — Mathematical Induction

Epp 4th ed. pp. 244–268 · 5th ed. (metric) pp. 275–301. Lecture 13 (week 5).

Problems

1. Use mathematical induction to prove the following statements.

   (a) For every positive integer n, $n(n+1)$ is even.

   (b) For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.

   (c) For all integers $n \geq 7$, $3^n < n!$.

   (d) For each integer $n \geq 1$,

   $$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

   (e) For each integer $n \geq 0$, $1 + 4n \leq 5^n$.

Solutions

1. (a) **For every positive integer n, $n(n+1)$ is even.**

   Proof. Let $P(n)$ be the predicate "$n(n+1)$ is even".

   Basis: when $n = 1$, $n(n+1) = 2$ which is even, so $P(1)$ is true.

   (The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

   Inductive hypothesis: suppose that for some integer $k \geq 1$, $P(k)$ is true. Thus $k(k+1) = 2a$ for some integer a.

   Now consider $n = k + 1$. Then

   $$(k+1)(k+2) = k(k+1) + 2(k+1) = 2a + 2(k+1) = 2(a+k+1).$$

   Since a and k are integers, $a + k + 1$ is an integer, so $(k+1)(k+2)$ is even and $P(k+1)$ is true.

   Thus, by the principle of mathematical induction, $n(n+1)$ is even for every positive integer n. □

   (b) **For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.**

Proof. Let $P(n)$ be the predicate $6 \mid (n^3 - n)$.

Basis: when $n = 2$, $n^3 - n = 8 - 2 = 6$. Since $6 \mid 6$, $P(2)$ is true.

(The inductive step is to show that for all integers $k \geq 2$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose that for some integer $k \geq 2$, $P(k)$ is true. Thus $k^3 - k = 6a$ for some integer a.

Now consider $n = k + 1$. Then

$$(k+1)^3-(k+1) = k^3+3k^2+3k+1-k-1 = k^3-k+3k^2+3k = 6a+3k(k+1).$$

For the integer k, $k(k+1)$ is even from part (a), so let $k(k+1) = 2b$ for some integer b. Hence $(k+1)^3 - (k+1) = 6a + 3(2b) = 6(a+b)$. Thus $6 \mid ((k+1)^3 - (k+1))$ and so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $n^3 - n$ is a multiple of 6 for each integer $n \geq 2$. □

(c) **For all integers $n \geq 7$, $3^n < n!$.**

Proof. Let $P(n)$ be the predicate $3^n < n!$.

Basis: $P(7)$ is the statement $3^7 < 7!$. The left-hand side is $3^7 = 2187$ and the right-hand side is $7! = 5040$, so $P(7)$ holds.

(The inductive step is to show that for all integers $k \geq 7$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: let $k \geq 7$ be an integer and assume that $P(k)$ is true; that is $3^k < k!$. We will now show that $P(k+1)$ holds, so we will show $3^{k+1} < (k+1)!$.

Taking the right-hand side, we have

$$\begin{aligned}(k+1)! &= (k+1) \cdot k! \\ &> (k+1) \cdot 3^k && \text{by the inductive hypothesis} \\ &> 3 \cdot 3^k && \text{since } k \geq 7 \\ &= 3^{k+1}\end{aligned}$$

Hence $P(k+1)$ is true.

Thus by the principle of mathematical induction, for all integers $n \geq 7$, $3^n < n!$. □

(d) **For each integer $n \geq 1$, $\displaystyle\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.**

Proof. Let $P(n)$ be the predicate

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Basis: consider $n = 1$. We have $\sum_{i=1}^{1} i^3 = 1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ so $P(1)$ is true.

(The inductive step is to show that for all integers $k \geq 1$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(k)$ is true. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

Now consider $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 && \text{(splitting off the last term)} \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 && \text{by the inductive hypothesis} \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{(k+1)^2}{4}(k^2 + 4(k+1)) \\
&= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\
&= \frac{(k+1)^2}{4}(k+2)^2
\end{aligned}$$

Thus $P(k+1)$ is true.

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for every integer $n \geq 1$. □

(e) **For each integer $n \geq 0$, $1 + 4n \leq 5^n$.**

Proof. Let $P(n)$ be the predicate $1 + 4n \leq 5^n$.

Basis: when $n = 0$ we have $1 + 4 \cdot 0 \leq 5^0$, so $P(0)$ is true.

(The inductive step is to show that for all integers $k \geq 0$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \geq 0$ is an integer and $P(k)$ is true; that is, $1 + 4k \leq 5^k$.

Now consider $n = k + 1$. Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned} 1 + 4(k+1) &= 1 + 4k + 4 \\ &\leq 5^k + 4 && \text{by the inductive hypothesis} \\ &\leq 5^k + 4 \cdot 5^k && \text{since } k \geq 0 \text{ so } 5^k \geq 1 \\ &= 5(5^k) \\ &= 5^{k+1} \end{aligned}$$

so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $1 + 4n \leq 5^n$ for every integer $n \geq 0$. □

§18 — Strong Induction and the Well Ordering Principle

Epp 4th ed. pp. 268–279 · 5th ed. (metric) pp. 301–314. Lecture 14 (week 5).

Problems

1. Consider the statement

   For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.

   (a) Prove the statement using the well-ordering principle.

   (b) Prove the statement using strong mathematical induction.

2. The Lucas sequence $a_1, a_2, a_3, ...$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Use strong mathematical induction to prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

3. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Use strong mathematical induction to prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.

Solutions

1. **For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.**

   (a)

Proof (using the well-ordering principle). Consider the set of counterexamples

$$S = \{\, n \in \mathbb{Z}^{\geq 2} : \text{there do not exist integers } a, b \geq 0 \text{ with } n = 2a + 3b \,\}.$$

If S is empty, we are done. Otherwise, by the well-ordering principle, S has a least element. Let us call it N.

Notice that $2 \notin S$ because $2 = 2 \cdot 1 + 3 \cdot 0$, and $3 \notin S$ because $3 = 2 \cdot 0 + 3 \cdot 1$. Also $4 \notin S$ because $4 = 2 \cdot 2 + 3 \cdot 0$. Hence $N \geq 5$. By minimality of N, we must have $N - 2 \notin S$. Therefore there exist integers $a, b \geq 0$ such that

$$N - 2 = 2a + 3b.$$

In other words, we have

$$N = 2(a + 1) + 3b.$$

This means $N \notin S$, contradicting the assumption that $N \in S$. Hence S is empty, and the statement holds for all $n \geq 2$. $\square$

(b)

Proof (using strong induction). Let $P(n)$ be the predicate: "there exist integers $a, b \geq 0$ such that $n = 2a + 3b$."

Basis: we have

$$2 = 2 \cdot 1 + 3 \cdot 0, \qquad 3 = 2 \cdot 0 + 3 \cdot 1, \qquad 4 = 2 \cdot 2 + 3 \cdot 0,$$

so $P(2)$, $P(3)$, $P(4)$ are true.

(The inductive step is to show that for every integer $k \geq 4$, if $P(2), P(3), \ldots, P(k)$ are all true then $P(k + 1)$ is true.)

Inductive hypothesis: suppose $k \geq 4$ is an integer and assume $P(m)$ is true for every integer $m = 2, 3, \ldots, k$.

Consider $n = k + 1$. Since $k \geq 4$, we have $k - 1 \geq 3$, so by the inductive hypothesis $P(k - 1)$ is true. Thus there exist $a, b \geq 0$ such that

$$k - 1 = 2a + 3b.$$

Adding 2 gives

$$k + 1 = 2(a + 1) + 3b,$$

so $P(k + 1)$ holds. $\square$

2. **The Lucas sequence** $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $P(n)$ be the predicate $a_n \leqslant \left(\frac{7}{4}\right)^n$.

Basis: when $n = 1$, $a_1 = 1 \leqslant \left(\frac{7}{4}\right)^1 = 1\frac{3}{4}$ is true, so $P(1)$ is true. When $n = 2$, $P(2)$ holds because $a_2 = 3 \leqslant \left(\frac{7}{4}\right)^2 = \frac{49}{16} = 3\frac{1}{16}$.

(The inductive step is to show that for every integer $k \geq 1$, if $P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and that $P(m)$ is true for all m with $1 \leq m \leq k$.

Now consider $P(k+1)$, which we want to prove holds. We have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&\leqslant \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} && \text{by the inductive hypothesis} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right) \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right) \\
&\leqslant \left(\frac{7}{4}\right)^{k-1}\left(\frac{49}{16}\right) && \text{noting } \tfrac{11}{4} = \tfrac{44}{16} < \tfrac{49}{16} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 \\
&= \left(\frac{7}{4}\right)^{k+1}.
\end{aligned}$$

Hence $P(k+1)$ holds. Therefore, by the principle of strong mathematical induction, $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all integers $n \geqslant 1$. □

3. **Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.**

Proof. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Let $P(n)$ be the predicate "a_n is an integer."

Basis: $P(0)$ holds since $a_0 = x^0 + \frac{1}{x^0} = 2$. $P(1)$ holds since $a_1 = x + \frac{1}{x}$, which is an integer by assumption.

(The inductive step is to show that for every integer $k \geq 1$, if $P(0), P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(m)$ holds for all integers $m = 0, 1, \ldots, k$.

We now aim to show that $P(k+1)$ is true. Notice that

$$\begin{aligned} a_1 a_k &= \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) \\ &= \left(x^{k+1} + \frac{1}{x^{k+1}}\right) + \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_{k+1} + a_{k-1}. \end{aligned}$$

Therefore $a_{k+1} = a_1 a_k - a_{k-1}$. By the inductive hypothesis, a_k and a_{k-1} are integers, and a_1 is an integer, so a_{k+1} is an integer. Hence $P(k+1)$ holds.

Therefore, by the principle of strong mathematical induction, a_n is an integer for all $n \geq 0$. □

§19 — Recursive Definitions

Epp 4th ed. pp. 290–304 · 5th ed. (metric) pp. 325–340. Lecture 15 (week 6).

Problems

1. Define the sequence $b_1 = 2$, $b_2 = 6$ and

$$b_k = b_{k-1} + b_{k-2} + \gcd(b_{k-1}, b_{k-2})$$

for all $k \geq 3$. Use strong induction to prove b_n is even for all $n \geq 1$.

2. A sequence is defined by $a_1 = 2$ and

$$a_k = k(a_{k-1} + k - 1)$$

for all integers $k \geq 2$. Use mathematical induction to prove a_n is even for all $n \geq 1$.

3. Recursively define the set S of binary strings as follows.

   (a) *(Base rule)* $1 \in S$.

   (b) *(Recursion rule)* If $s \in S$ then $0s \in S$ and $1s \in S$ (e.g. if $s = 1$ then $0s = 01$).

   (c) *(Restriction rule)* No other strings lie in S besides those given by the rules above.

   What are the strings contained in S arising from the first three applications of the recursive rule?

Solutions

1. *Proof.* Let $P(n)$ be the predicate "b_n is even".

   Base case. The base cases are $n = 1, 2$. We have $b_1 = 2$ and $b_2 = 6$ so $P(1)$ and $P(2)$ are true.

   Inductive hypothesis. Assume $P(m)$ is true for all integers m with $1 \leq m \leq k$, where $k \geq 2$ is an integer. That is, we assume $b_1, b_2, \ldots, b_k$ are all even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. b_{k+1} is even. Using the recursive definition, we have

   $$b_{k+1} = b_k + b_{k-1} + \gcd(b_k, b_{k-1}).$$

   By the inductive hypothesis, b_k and b_{k-1} are even, so $2 \mid b_k$ and $2 \mid b_{k-1}$, hence $2 \mid \gcd(b_k, b_{k-1})$ as well. Therefore each term on the right-hand side is even, so their sum b_{k+1} is even. Thus $P(k+1)$ holds.

   Therefore, b_n is even for all integers $n \geq 1$. □

2. *Proof.* Let $P(n)$ be the predicate "a_n is even".

   Base case. The base case is $n = 1$. We have $a_1 = 2$, which is even, so $P(1)$ is true.

   Inductive hypothesis. Assume $P(k)$ is true for some integer $k \geq 1$. That is, assume a_k is even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. a_{k+1} is even. By the recursive definition, we have

   $$a_{k+1} = (k+1)(a_k + (k+1) - 1) = (k+1)(a_k + k).$$

   Note that a_k is even by the inductive hypothesis. We split into cases:

   - If k is even, then $a_k + k$ is even, hence a_{k+1} is even.
   - If k is odd, then $k+1$ is even, hence a_{k+1} is even.

   In all cases, a_{k+1} is even, so $P(k+1)$ is true.

   Therefore, a_n is even for all integers $n \geq 1$. □

3. By the base rule, we only know $1 \in S$.

   First application of the recursive rule:

   $$01 \in S, \qquad 11 \in S.$$

   Second application of the recursive rule:

$$001 \in S, \quad 101 \in S, \quad 011 \in S, \quad 111 \in S.$$

Third application of the recursive rule:

$$0001 \in S, \quad 1001 \in S, \quad 0101 \in S, \quad 1101 \in S,$$
$$0011 \in S, \quad 1011 \in S, \quad 0111 \in S, \quad 1111 \in S.$$

§20 — Solving Recurrence Relations

Epp 4th ed. pp. 304–328 · 5th ed. (metric) pp. 340–364. Lecture 16 (week 6).

Problems

1. Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that

$$a_n = 5a_{n-1} - 6a_{n-2}$$

for all integers $n \geq 2$.

2. Let $\{b_n\}_{n\geq 0}$ be the sequence defined by

$$b_0 = 2, \qquad b_1 = 5, \qquad \text{and} \qquad b_k = 2b_{k-1} - b_{k-2} \text{ for each integer } k \geq 2.$$

   (a) Write down the values of $b_0, b_1, b_2, b_3, b_4, b_5$.

   (b) Based on your answers for part (a), guess an explicit formula for this sequence.

   (c) Prove that your guess from part (b) is correct.

3. Let T_n be a sequence defined by $T_1 = 1$ and

$$T_{n+1} = 1 + (T_1 \times T_2 \times T_3 \times \cdots \times T_n)$$

for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.

4. Consider the Fibonacci sequence defined recursively by

$$\begin{aligned} a_0 &= 0 \\ a_1 &= 1 \\ a_n &= a_{n-2} + a_{n-1} \qquad \text{for all integers } n \geq 2. \end{aligned}$$

Use strong mathematical induction to prove the explicit formula

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

for all integers $n \geq 0$, where $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. (You may use the fact that $\phi^2 = \phi + 1$ and $\psi^2 = \psi + 1$.)

Solutions

1. **Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$.**

Proof. For $n \geq 2$, we have $n - 2 \geq 0$ so all three terms a_n, a_{n-1} and a_{n-2} are defined in the given formula. Then,

$$\begin{aligned} 5a_{n-1} - 6a_{n-2} &= 5\left(2^{n-1} + 5 \cdot 3^{n-1}\right) - 6\left(2^{n-2} + 5 \cdot 3^{n-2}\right) \\ &= \left(5 \cdot 2^{n-1} - 6 \cdot 2^{n-2}\right) + \left(25 \cdot 3^{n-1} - 30 \cdot 3^{n-2}\right) \\ &= (10 - 6)2^{n-2} + (75 - 30)3^{n-2} \\ &= 4 \cdot 2^{n-2} + 45 \cdot 3^{n-2} \\ &= 2^n + 5 \cdot 3^n \\ &= a_n. \end{aligned}$$

Hence $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. □

2. (a)

$$\begin{aligned} b_0 &= 2 \\ b_1 &= 5 \\ b_2 &= 2(5) - 2 = 8 \\ b_3 &= 2(8) - 5 = 11 \\ b_4 &= 2(11) - 8 = 14 \\ b_5 &= 2(14) - 11 = 17 \end{aligned}$$

(b) Guess that $b_n = 3n + 2$ for each integer $n \geq 0$.

(c)

Proof. The guess gives $b_0 = 3(0) + 2 = 2$ and $b_1 = 3(1) + 2 = 5$ so it gives the correct initial conditions. Now we substitute the guess into the recurrence relation. The LHS of the recurrence relation is $b_k = 3k + 2$. The RHS of the recurrence relation is

$$\begin{aligned} 2b_{k-1} - b_{k-2} &= 2(3(k-1)+2) - (3(k-2)+2) \\ &= 2(3k-1) - (3k-4) \\ &= 6k - 2 - 3k + 4 \\ &= 3k + 2 \end{aligned}$$

So the guess also satisfies the recurrence relation. Thus the guess is correct. □

Alternative proof (by strong induction). Let $P(n)$ be the predicate $b_n = 3n + 2$.

Basis: $b_0 = 2$ from the recursive definition and $3(0) + 2 = 2$ so $P(0)$ is true. $b_1 = 5$ from the recursive definition and $3(1) + 2 = 5$ so $P(1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are true.

Now

$$\begin{aligned} b_{k+1} &= 2b_k - b_{k-1} && \text{by the rec. rel. since } k+1 \geq 2 \\ &= 2(3k+2) - (3(k-1)+2) && \text{since } P(k) \text{ and } P(k-1) \text{ are true} \\ &= 6k + 4 - (3k - 1) \\ &= 3k + 5 \\ &= 3(k+1) + 2 \end{aligned}$$

So $P(k+1)$ is true. Therefore, by the principle of (strong) mathematical induction, the guess is correct for this recursively defined sequence. □

3. **Let T_n be a sequence defined by $T_1 = 1$ and $T_{n+1} = 1 + (T_1 \times \cdots \times T_n)$ for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.**

Proof. We can prove this simply by applying the recursive formula twice, once for T_{n+1} and once for T_n:

$$\begin{aligned} T_{n+1} &= 1 + (T_1 \cdot T_2 \cdot T_3 \cdots T_n) && \text{by the recursive definition} \\ &= 1 + T_n \cdot (T_1 \cdot T_2 \cdot T_3 \cdots T_{n-1}) \\ &= 1 + T_n \cdot (T_n - 1) && \text{since } T_n = 1 + (T_1 \cdots T_{n-1}) \text{ by rec. def.} \\ &= 1 + (T_n)^2 - T_n \\ &= (T_n)^2 - T_n + 1. \end{aligned}$$

Note that both applications of the recursive definition are valid, since $n-1 \geq 1$. $\square$

4. **Fibonacci explicit formula.**

Proof. Let $P(n)$ be the predicate

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}.$$

Basis. The base cases are $n = 0, 1$, which are true because

$$\frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = a_0,$$

and

$$\frac{\phi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = a_1.$$

Inductive hypothesis. Now suppose that for some integer $m \geq 1$, we have that $P(i)$ is true for all $0 \leq i \leq m$. In particular, $P(m)$ and $P(m-1)$ are true, that is,

$$a_m = \frac{\phi^m - \psi^m}{\sqrt{5}} \qquad \text{and} \qquad a_{m-1} = \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}}.$$

We need to show that $P(m+1)$ is true. That is, we aim to show

$$a_{m+1} = \frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}}.$$

Starting with the right-hand side of $P(m+1)$, we have

$$\begin{aligned}
\frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}} &= \frac{\phi^2\phi^{m-1} - \psi^2\psi^{m-1}}{\sqrt{5}} \\
&= \frac{(\phi+1)\phi^{m-1} - (\psi+1)\psi^{m-1}}{\sqrt{5}} && \text{since } \phi^2 = \phi + 1 \text{ and } \psi^2 = \psi + 1 \\
&= \frac{(\phi^m + \phi^{m-1}) - (\psi^m + \psi^{m-1})}{\sqrt{5}} \\
&= \frac{\phi^m - \psi^m}{\sqrt{5}} + \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}} \\
&= a_m + a_{m-1} && \text{by the inductive hypothesis} \\
&= a_{m+1} && \text{by definition.}
\end{aligned}$$

Hence $P(m+1)$ is true. $\square$

§21 — Set Theory Definitions

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Define the sets

$$\begin{aligned} V &= \{x \in \mathbb{Z} \mid 2 \leqslant x \leqslant 11 \text{ and } x \text{ is odd}\}, \\ X &= \{x \in \mathbb{Z} \mid -1 \leqslant x \leqslant 4\}, \\ Y &= \{2, 3, 7, 9\}, \\ Z &= \{x \in \mathbb{Z} \mid x \neq 0\}. \end{aligned}$$

   Write down the following sets, listing their elements and using brackets as appropriate.

   (a) $V \cap X$. (b) $V \cup Y$. (c) $X \cap Z$.

   (b) $X \cap (Z - Y)$. (e) $(X \cup Y) \cap V$. (f) $X \cup (Y \cap V)$.

2. For each of the following sets, write down its elements and then state the size of the set; that is, find $|A|$, $|B|$, $|C|$ and $|D|$.

   (a) $A = \{x \in \mathbb{Z} \mid \exists\, i \in \mathbb{Z} \text{ such that } x = 1 + (-1)^i\}$.

   (b) $B = \{y \in \mathbb{Z} \mid -8 < y \leqslant -5\}$.

   (c) $C = \{s \in \mathbb{Z} \mid s^2 + 1 = 0\}$.

   (d) $D = \{t \in \mathbb{Z} \mid t^4 = 1\}$.

3. Define the sets $A = \{0, 1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ and $C = \{1, 2, 4, 5, 7\}$. List the elements of the set

$$R = ((A - B) \cap (A - C)) \cup (B \cap C \cap A).$$

4. Are the following statements true or false? Justify in one or two sentences.

   (a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{\emptyset\} \in \{\{\emptyset\}\}$

   (b) $\emptyset \subseteq \{x\}$ (e) $\emptyset \in \{x\}$

Solutions

1. (a) $V \cap X = \{3\}$

   (b) $V \cup Y = \{2, 3, 5, 7, 9, 11\}$

   (c) $X \cap Z = \{-1, 1, 2, 3, 4\}$

   (d) $X \cap (Z - Y) = \{-1, 1, 4\}$

   (e) $(X \cup Y) \cap V = \{3, 7, 9\}$

   (f) $X \cup (Y \cap V) = \{-1, 0, 1, 2, 3, 4, 7, 9\}$

2. (a) Note that $(-1)^i$ is either $+1$ or -1 (according as i is even or odd). So x is either $1 + 1$ or $1 - 1$, that is, 2 or 0. So $A = \{2, 0\}$ and $|A| = 2$.

   (b) $B = \{-7, -6, -5\}$, so $|B| = 3$.

   (c) If $s^2 + 1 = 0$, we have $s^2 = -1$, and there are no such real numbers s, let alone integers! So $C = \emptyset$ and $|C| = 0$.

   (d) $D = \{-1, 1\}$, since $t^4 = 1$ with $t \in \mathbb{Z}$ implies $t = \pm 1$. Hence $|D| = 2$.

3. We have $A - B = \{0, 1, 2\}$ and $A - C = \{0, 3\}$, so $(A - B) \cap (A - C) = \{0\}$. Also $B \cap C \cap A = \{4\}$. Thus $R = \{0\} \cup \{4\} = \{0, 4\}$.

4. (a) **True:** $\{x\}$ is the set whose only element is x, so $x \in \{x\}$.

   (b) **True:** every set is a subset of itself, so $\{x\} \subseteq \{x\}$.

   (c) **True:** $\{\{\emptyset\}\}$ has the single element $\{\emptyset\}$, so $\{\emptyset\} \in \{\{\emptyset\}\}$.

   (d) **True:** $\emptyset \subseteq S$ for every set S, in particular $\emptyset \subseteq \{x\}$.

   (e) **False** (in general): $\emptyset \in \{x\}$ would require $\emptyset = x$.

Application — Computer Representations of Sets

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 134–138.*

There are various ways to represent sets using a computer. One such method involves the use of binary strings.

If we fix a finite universal set U with an arbitrary ordering, for example $U = \{a_1, a_2, \ldots, a_n\}$, we can represent subsets of U using binary strings of length n. A 1 in the ith position of the string indicates that element a_i is in the subset and a 0 indicates it is not.

For example if $U = \{1, 2, 3\}$ then the string 000 represents the empty set, 101 represents the subset $\{1, 3\}$ and 111 represents the entire set U.

The set operations union and intersection can be computed at the level of binary strings by utilising the bitwise OR and AND operations. The union of two sets corresponds to the bitwise OR operation on the strings and the intersection corresponds to bitwise AND.

Application problems

1. Define the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   (a) Express each of the following subsets of U using binary strings:

   i. $\{3, 4, 5\}$

   ii. $\{1, 3, 6, 10\}$

   iii. $\{a \in U \mid a \text{ is prime}\}$.

   (b) Using the same U, find the set represented by the following strings:

   i. 1111001111

   ii. 0101111000

   iii. 1000000001

   (c) Use binary strings to compute the following set operations.

   i. $\{1, 3, 4, 6, 10\} \cap \{2, 3, 6, 9, 10\}$

   ii. $\{2, 4, 6, 8\} \cup \{3, 4, 5\}$

Application solutions

1. (a) i. 0011100000

   ii. 1010010001

   iii. 0110101000 — the primes in U are $2, 3, 5, 7$. (The source PDF prints 1010111000 here, which decodes to $\{1, 3, 5, 6, 7\}$ and is not the set of primes; the string above is the correct one.)

   (b) i. $\{1, 2, 3, 4, 7, 8, 9, 10\}$

   ii. $\{2, 4, 5, 6, 7\}$

   iii. $\{1, 10\}$

   (c) i. 1011010001 AND 0110010011 = 0010010001, so the intersection is $\{3, 6, 10\}$.

   ii. 0101010100 OR 0011100000 = 0111110100, so the union is $\{2, 3, 4, 5, 6, 8\}$.

§22 — More Definitions and Examples of Sets

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Let $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$. List the elements of the following sets.
   (a) $A \cap C$
   (b) $(A \cup C) - B$
   (c) $(A \times B) \cap (A \times C)$
   (d) $\mathcal{P}(B \cap C)$
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\}$
2. Are the following statements true or false?
   (a) $\mathbb{Q} \in \mathbb{R}$.
   (b) $\{1, 2\} \subseteq \mathbb{Z}$.
   (c) $\{-3, 0\} \subseteq \mathcal{P}(\mathbb{Z})$.
   (d) $\{(1, 2), (0, 1)\} \in \mathbb{Z} \times \mathbb{Z}$.
3. Let $X = \mathcal{P}(\emptyset)$ and $Y = \mathcal{P}(\mathcal{P}(\emptyset))$. List the elements of each of the following sets.
   (a) X (b) Y (c) $X \cap Y$ (d) $X \cup Y$
4. Define sets $S = \{3, 5\}$ and $T = \{2, 3, 7\}$. Are the following statements true or false?
   (a) $S \subseteq T$
   (b) $\emptyset \in \mathcal{P}(S)$
   (c) $\emptyset \in T$
   (d) $(3, 3, 3) \in S \times T$

Solutions

1. (a) $A \cap C = \emptyset$.
   (b) $(A \cup C) - B = \{1, 4\}$.
   (c) $(A \times B) \cap (A \times C) = \{(1, 3), (2, 3)\}$.
   (d) $\mathcal{P}(B \cap C) = \{\emptyset, \{3\}\}$.
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\} = \{\emptyset, \{2\}\}$.
2. (a) **False.** ($\mathbb{Q}$ is a *subset* of $\mathbb{R}$, not an element of it.)
   (b) **True.**
   (c) **False.** (The elements of $\mathcal{P}(\mathbb{Z})$ are sets of integers; -3 and 0 are integers, not sets.)
   (d) **False.** (It is a *subset* of $\mathbb{Z} \times \mathbb{Z}$, not an element — the elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs.)
3. (a) $X = \mathcal{P}(\emptyset) = \{\emptyset\}$.
   (b) $Y = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
   (c) $X \cap Y = \{\emptyset\}$.
   (d) $X \cup Y = \{\emptyset, \{\emptyset\}\}$.
4. (a) **False.** ($5 \in S$ but $5 \notin T$.)
   (b) **True.** (The empty set is an element of every power set.)
   (c) **False.** (T's elements are 2, 3 and 7.)
   (d) **False.** (The elements of $S \times T$ are ordered *pairs*, not triples.)

§23 — Properties of Sets

Epp 4th ed. pp. 352–366 · 5th ed. (metric) pp. 391–407. Lecture 18 (week 7).

Problems

1. (a) Use the element method to prove that for all sets A and B

$$A \cup (B - A) = A \cup B.$$

   (b) Use the element method to prove that for all sets X, Y and Z,

$$(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset.$$

   (c) Use set identities to prove that for all sets A, B and C

$$(A - B) - C = A - (B \cup C).$$

2. Prove or disprove the following:

   (a) For all sets A and B, we have $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

   (b) For all sets A and B, we have $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.

   (c) There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

   (d) Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$.

3. Let A, B and C be sets. Prove that

$$A - (B \cup C) = (A - B) - C.$$

Solutions

1. (a) **For all sets A and B, $A \cup (B - A) = A \cup B$.**

   Proof. First we show that $A \cup (B - A) \subseteq A \cup B$.

   Consider an arbitrary element $x \in A \cup (B - A)$. Then we know $x \in A$ or $x \in B - A$. This means $x \in A$, or $x \in B$ and $x \notin A$. If $x \in A$, then $x \in A \cup B$. Similarly if $x \in B - A$, then it must be in B and so $x \in A \cup B$. In either case, we have $x \in A \cup B$, thus $A \cup (B - A) \subseteq A \cup B$.

   Now we show that $A \cup B \subseteq A \cup (B - A)$.

   Let $x \in A \cup B$, then $x \in A$ or $x \in B$ or it is in both A and B. If $x \in A$, then $x \in A \cup (B - A)$. If $x \notin A$ then $x \in B$ since $x \in A \cup B$. So we have that $x \in B$ and $x \notin A$, hence $x \in B - A$ and thus $x \in A \cup (B - A)$. This proves that $A \cup B \subseteq A \cup (B - A)$, and together this proves that $A \cup B = A \cup (B - A)$. $\square$

(b) **For all sets X, Y and Z, $(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset$.**

Proof. Assume that $(X - Z) \cap (Y - Z) \cap (X - Y) \neq \emptyset$.

So let $x \in (X - Z) \cap (Y - Z) \cap (X - Y)$. Then, in particular, $x \in Y - Z$ and $x \in X - Y$. The former implies $x \in Y$, but the latter implies $x \notin Y$. No such x exists. Therefore the set is empty. □

(c) **For all sets A, B and C, $(A - B) - C = A - (B \cup C)$.**

Proof. Using $A - B = A \cap B^c$, $(S - T) = S \cap T^c$, and De Morgan's law, we have

$$(A-B)-C = (A\cap B^c)\cap C^c = A\cap(B^c\cap C^c) = A\cap(B\cup C)^c = A-(B\cup C). \qquad \square$$

2. (a) **For all sets A and B, $\mathcal{P}(A\cup B) = \mathcal{P}(A)\cup\mathcal{P}(B)$. False.** Counterexample: $A = \{1\}$, $B = \{2\}$. Then

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \neq \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}.$$

(b) **For all sets A and B, $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$. True.**

($\Longleftarrow$) If $A = B$ then clearly $\mathcal{P}(A) = \mathcal{P}(B)$.

($\Longrightarrow$) We next show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Suppose (for a contradiction) that $\mathcal{P}(A) = \mathcal{P}(B)$ but $A \neq B$. Then (without loss of generality), there exists an element x in A that is not in B. Therefore, there is an element $\{x\}$ in $\mathcal{P}(A)$ that is not in $\mathcal{P}(B)$. Therefore $\mathcal{P}(A) \neq \mathcal{P}(B)$ — a contradiction. Thus, for all sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$. □

(c) **There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. False.**

No such set exists. The power set of any set must contain the empty set — that is, $\emptyset \in \mathcal{P}(A)$, where A is any set. Also, the power set of any set of size n has cardinality 2^n. The power set above contains 7 elements, and there does not exist any integer n such that $2^n = 7$.

(d) **Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$. True.**

First note that if $A = \emptyset$ then $A \times B = A \times C = \emptyset$ and the statement is true. Also, if $B = \emptyset$ then $A \times B = \emptyset$ and $\emptyset \subseteq A \times C$ for any C, so the statement is true.

Suppose A, B and C are non-empty sets with $B \subseteq C$. Thus if $b \in B$, then $b \in C$. Consider any element $(a, b) \in A \times B$, where $a \in A$ and $b \in B$. Since

$b \in B$, $b \in C$. As such, $a \in A$ and $b \in C$ for all a or b, so $(a, b) \in A \times C$. Therefore $A \times B \subseteq A \times C$. □

3. **For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.**

   Proof Option 1. For any x, we have

   $$x \in A - (B \cup C) \iff x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge (x \notin B) \wedge (x \notin C).$$

   Also, we have

   $$x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff (x \in A \wedge x \notin B) \wedge x \notin C.$$

   The statements on the right-hand side are equivalent. Hence $A - (B \cup C) = (A - B) - C$. □

   Proof Option 2.

   $$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c && \text{by the Set Difference Law} \\ &= A \cap (B^c \cap C^c) && \text{by De Morgan's law} \\ &= (A \cap B^c) \cap C^c && \text{by Associative law} \\ &= (A - B) \cap C^c && \text{by the Set Difference Law} \\ &= (A - B) - C && \text{by the Set Difference Law} \quad \square \end{aligned}$$

§24 — Functions Defined on General Sets

Epp 4th ed. pp. 383–396 · 5th ed. (metric) pp. 425–439. Lecture 18 (week 7).

Problems

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 1$.
   (a) What is the domain, codomain and range of f?
   (b) What is the image of $\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$ under f?
   (c) What is the preimage of $\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}$ under f?
2. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$ be sets. Define $f : X \to Y$ by the arrow diagram

   $$1 \mapsto v, \qquad 3 \mapsto s, \qquad 5 \mapsto v$$

   (the elements t and u of Y receive no arrows).

(a) Write the domain of f and the co-domain of f.

(b) Determine $f(1)$, $f(3)$, and $f(5)$.

(c) Determine the range of f.

(d) Is 3 an inverse image of s? Is 1 an inverse image of u?

(e) What is the inverse image of s? of u? of v?

(f) Represent f as a set of ordered pairs.

3. Let D be the set of all finite subsets of $\mathbb{Z}^+$. Consider the function $T : \mathbb{Z}^+ \to D$ defined by $T(n) := \{d \mid d \in \mathbb{Z}^+ \text{ and } d \text{ divides } n\}$. Find the following:

(a) $T(1)$ (b) $T(15)$ (c) $T(17)$ (d) $T(5)$ (e) $T(18)$ (f) $T(21)$

4. Let S be the set of all strings of a's and b's.

(a) Define the function $f : S \to \mathbb{Z}$ by

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s, & \text{if } s \text{ contains an } a, \\ 0, & \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

(b) Define the function $g : S \to S$ by

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

Solutions

1. (a) The domain is $\mathbb{R}$, the codomain is $\mathbb{R}$, and the range is $[-1, \infty)$.

(b) $f(\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}) = [-1, 3]$.

(c) $f^{-1}(\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} = [-2, -1] \cup [1, 2]$.

2. (a) The domain is $X = \{1, 3, 5\}$ and the codomain is $Y = \{s, t, u, v\}$.

(b) $f(1) = v$, $f(3) = s$, $f(5) = v$.

(c) $\text{range}(f) = \{s, v\}$.

(d) **Yes**, 3 is an inverse image of s. **No**, 1 is not an inverse image of u.

(e) $f^{-1}(s) = \{3\}$, $f^{-1}(u) = \emptyset$, $f^{-1}(v) = \{1, 5\}$.

(f) $f = \{(1, v), (3, s), (5, v)\}$.

3. (a) $T(1) = \{1\}$.

(b) $T(15) = \{1, 3, 5, 15\}$.

(c) $T(17) = \{1, 17\}$.

(d) $T(5) = \{1, 5\}$.

(e) $T(18) = \{1, 2, 3, 6, 9, 18\}$.

(f) $T(21) = \{1, 3, 7, 21\}$.

4. (a) $f(aba) = 0$, $f(bbab) = 2$, $f(b) = 0$, $\text{range}(f) = \mathbb{Z}^{\geq 0}$.

(b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, $\text{range}(g) = S$.

§25 — one-to-one, Onto, and Inverse Functions

Epp 4th ed. pp. 397–416 · 5th ed. (metric) pp. 439–461. Lecture 19 (week 7).

Problems

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \left\lfloor \dfrac{1 - 6n}{3} \right\rfloor$.

(a) Is f one-to-one?

(b) Is f onto?

(c) Is f bijective?

(d) Prove or disprove that for all $m, n \in \mathbb{Z}$, we have $f(mn) = f(m)f(n)$.

2. Define the set $A = \{0, 1, 2, 3, 4\}$ and the functions $f : A \to A$ and $g : A \to A$ by

$$f(a) = (a + 4)^2 \pmod 5, \qquad g(a) = (a^2 + 3a + 1) \pmod 5.$$

Is $f = g$?

3. Consider the function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f((m, n)) = 2^m 3^n$.

(a) Determine $f((3, 1))$.

(b) Determine the pre-image of $\{36\}$.

(c) Prove f is one-to-one.

4. Consider the function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x^2 \rfloor$.

   (a) What is the image $f([-1, 1])$?

   (b) What is the preimage $f^{-1}(\{1\})$?

   (c) Is f one-to-one?

   (d) Is f onto?

   (e) Is f bijective?

Solutions

1. First, we note that, for $n \in \mathbb{Z}$,

$$f(n) = \left\lfloor \frac{1 - 6n}{3} \right\rfloor = \left\lfloor -2n + \frac{1}{3} \right\rfloor = -2n$$

   since $-2n \in \mathbb{Z}$ and $\frac{1}{3} \in [0, 1)$.

   (a) **Yes.** If $f(m) = f(n)$ then $-2m = -2n$, hence $m = n$. Therefore f is one-to-one.

   (b) **No.** Since $f(n) = -2n$ we see that f never maps to any odd integer; for example, there is no integer w with $f(w) = 1$. Therefore f is not onto.

   (c) **No**, f is not a bijection. (It is injective but not surjective.)

   (d) This is **false**; take $m = n = 1$. Then $f(mn) = -2$ but $f(m)f(n) = 4$.

2. **Yes.** First note f and g have the same domain and codomain. This means we just need to show $f(a) = g(a)$ for all $a \in A$. Notice that we have

$$(a + 4)^2 = a^2 + 8a + 16 \equiv a^2 + 3a + 1 \pmod 5,$$

   so $f(a) = g(a)$ for all $a \in A$, and hence $f = g$.

3. (a) $f((3, 1)) = 2^3 3^1 = 24$.

   (b) $36 = 2^2 3^2$, so $f((m, n)) = 36$ if and only if $(m, n) = (2, 2)$. Hence $f^{-1}(\{36\}) = \{(2, 2)\}$.

   (c) If $f((m, n)) = f((m', n'))$, then $2^m 3^n = 2^{m'} 3^{n'}$, so $2^{m-m'} = 3^{n'-n}$. By unique prime factorisation, this forces $m - m' = 0$ and $n' - n = 0$. That is, $m = m'$ and $n = n'$, and hence $(m, n) = (m', n')$. So f is one-to-one.

4. (a) Note that if $x \in [-1, 1]$ then $x^2 \in [0, 1]$. This means we have $\lfloor x^2 \rfloor \in \{0, 1\}$. Both values occur because $\lfloor 0^2 \rfloor = 0$ and $\lfloor 1^2 \rfloor = 1$. Thus $f([-1, 1]) = \{0, 1\}$.

(b) $f^{-1}(\{1\}) = \{x \in \mathbb{R} : 1 \leq x^2 < 2\} = (-\sqrt{2}, -1] \cup [1, \sqrt{2})$.

(c) **No**, f is not one-to-one. For example, $f\left(\frac{1}{2}\right) = 0 = f\left(-\frac{1}{2}\right)$ but $\frac{1}{2} \neq -\frac{1}{2}$.

(d) **No**, f is not onto since $f(x) = \lfloor x^2 \rfloor \geq 0$ for all x. This means, for instance, that -1 is not in the image of f.

(e) **No**, f is not bijective.

§26 — Composition of Functions

Epp 4th ed. pp. 416–427 · 5th ed. (metric) pp. 461–472. Lecture 20 (week 7).

Problems

1. Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^3 - 1$ and $g(x) = x + 5$.

   (a) Determine the functions $(g \circ f)(x)$ and $(f \circ g)(x)$.

   (b) Is $g \circ f$ a bijection?

2. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(x) = 2\lfloor x + 1 \rfloor$.

   (a) What is the range of f?

   (b) Is f one-to-one?

   (c) Is f onto?

   (d) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = 2x - 1$. Determine the composition $(g \circ f)(x)$.

   (e) Calculate $(g \circ f)\left(-\frac{3}{4}\right)$.

   (f) What is the range of $g \circ f$?

3. Let f and g be functions. Prove or disprove the following statements:

   (a) If f and $f \circ g$ are one-to-one, then g is one-to-one.

   (b) If f and $f \circ g$ are onto, then g is onto.

Solutions

1. (a) We have

$$(g \circ f)(x) = g(x^3 - 1) = x^3 + 4$$

and

$$(f \circ g)(x) = f(x + 5) = (x + 5)^3 - 1 = x^3 + 15x^2 + 75x + 124.$$

(b) **No**, $g \circ f$ is not a bijection. The map $x \mapsto x^3 + 4$ is one-to-one on $\mathbb{Z}$, but it is not onto (e.g. 0 is not in its image since $x^3 = -4$ has no integer solution).

2. (a) The range is a subset of the even integers because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. If $2m$ is an even integer then $f(m - 1) = 2\lfloor m - 1 + 1 \rfloor = 2m$, so the range is the set of all even integers.

(b) **No**, f is not one-to-one. For example,

$$f(0) = 2\lfloor 0 + 1 \rfloor = 2\lfloor 1 \rfloor = 2 \times 1 = 2, \quad \text{and}$$
$$f\left(\tfrac{1}{2}\right) = 2\left\lfloor \tfrac{1}{2} + 1 \right\rfloor = 2\left\lfloor \tfrac{3}{2} \right\rfloor = 2 \times 1 = 2,$$

but $0 \neq \frac{1}{2}$.

(c) **No**, f is not onto since $\text{range}(f) \neq \mathbb{Z}$ (e.g. there is no $x \in \mathbb{Q}$ such that $f(x) = 1$ because 1 is odd).

(d) We have

$$(g \circ f)(x) = g(f(x)) = 2(2\lfloor x + 1 \rfloor) - 1 = 4\lfloor x + 1 \rfloor - 1.$$

(e) We have

$$(g \circ f)\left(-\frac{3}{4}\right) = 4 \cdot 0 - 1 = -1.$$

(f) The range is a subset of $\{4n - 1 \mid n \in \mathbb{Z}\}$ because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. This *is* the range because, given an integer $4n - 1$, we have $f(n - 1) = 4\lfloor n - 1 + 1 \rfloor - 1 = 4n - 1$. Note that you can also write the range as $\{n \in \mathbb{Z} \mid n \equiv -1 \pmod 4\}$ which is the same as $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 4\}$.

3. (a) The statement is **true**.

Proof. Suppose that f and $f \circ g$ are one-to-one functions. Suppose for a contradiction that g is not one-to-one. Thus there exist two distinct elements in the domain of g, say x_1 and x_2, for which $g(x_1) = g(x_2)$. Let $g(x_1) = y = g(x_2)$. Thus $f(g(x_1)) = f(y) = f(g(x_2))$, but $x_1 \neq x_2$, which contradicts the fact that $f \circ g$ is one-to-one. Therefore g must be one-to-one. □

(b) The statement is **false**.

Counterexample. Consider the functions $g : \{1\} \to \{2, 3\}$ defined by $g(1) = 2$, and $f : \{2, 3\} \to \{4\}$ defined by $f(2) = 4$ and $f(3) = 4$. Then f is onto, and $f \circ g$ is onto (since $f \circ g : \{1\} \to \{4\}$ and $f(g(1)) = 4$). However, g is not onto. □

§27 — Cardinalities

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 21 (week 8).

Problems

1. Let $A = \{-2, -1, 0, 1\}$ and $B = \{3, 4, 5, 6\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.
2. Prove that $|\{1, 2, 3\}| \leq |\mathbb{Z}|$ by providing an appropriate injective (one-to-one) function.
3. Consider the intervals

$$[6, 12] = \{x \in \mathbb{R} \mid 6 \leq x \leq 12\} \quad \text{and} \quad (6, 12) = \{x \in \mathbb{R} \mid 6 < x < 12\}.$$

   Prove that $|[6, 12]| \leq |(6, 12)|$ by providing an appropriate injective (one-to-one) function.
4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.

Solutions

1. Define the function $f : A \to B$ by

$$f(-2) = 3, \qquad f(-1) = 4, \qquad f(0) = 5, \qquad f(1) = 6.$$

   Then f is bijective, hence $|A| = |B|$.
2. Define the function $g : \{1, 2, 3\} \to \mathbb{Z}$ by $g(1) = 1$, $g(2) = 2$, and $g(3) = 3$. Then g is injective (one-to-one), so $|\{1, 2, 3\}| \leq |\mathbb{Z}|$.

3. Define $h : [6, 12] \to (6, 12)$ by

$$h(x) = \frac{x}{2} + 4.$$

For each $x \in [6, 12]$ we have

$$\begin{aligned} \frac{6}{2} + 4 \leq h(x) &\leq \frac{12}{2} + 4 \\ 7 \leq h(x) &\leq 10. \end{aligned}$$

Thus h is indeed a function from $[6, 12]$ to $(6, 12)$, and h has range $[7, 10] \subseteq (6, 12)$.

Suppose $x, y \in [6, 12]$ and $h(x) = h(y)$. Then $\frac{x}{2} + 4 = \frac{y}{2} + 4$, so $x = y$. Therefore h is injective (one-to-one).

Thus $|[6, 12]| \leq |(6, 12)|$.

4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$.

Consider the function $f : A \to B$ where $f(x) = 2x + 5$. Since $x \geq -1$, $f(x) = 2x + 5 \geq 2(-1) + 5 = 3$, and since $x \leq 1$, $f(x) = 2x + 5 \leq 2(1) + 5 = 7$. Also each value of x gives a unique value of $2x + 5$. Thus f is a function with the correct domain and codomain.

We now prove that f is one-to-one. Suppose that $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Thus $2x_1 + 5 = 2x_2 + 5$, and so $x_1 = x_2$. Thus f is one-to-one.

We now prove that f is onto. Suppose $y \in [3, 7]$. Let $x = \frac{y-5}{2}$. Since $y \leq 7$, we have $x \leq 1$ and since $y \geq 3$, we have $x \geq -1$. So $x \in [-1, 1]$. Furthermore $f(x) = f\left(\frac{y-5}{2}\right) = 2\left(\frac{y-5}{2}\right) + 5 = y - 5 + 5 = y$. Thus f is onto.

Hence f is a bijection and so $|A| = |B|$.

§28 — Countable and Uncountable Sets

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 22 (week 8).

Note that this content will not be assessed in MATH1061.

Problems

1. Determine whether each of the following sets is countable or uncountable.
   (a) $\{1, 2, \ldots, n\}$.
   (b) $\mathbb{Z} \times \mathbb{Z}$.
   (c) $\mathbb{Q} \times \mathbb{Q}$.
   (d) $\mathbb{Z} \times \mathbb{Z} \times \cdots$ (infinitely many copies of $\mathbb{Z}$).
2. (a) Is $|\mathbb{Z}| = |\mathbb{Q}|$?
   (b) Is $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$?
   (c) Is $|\mathbb{R}| = |\mathbb{Q} \times \mathbb{Q}|$?
3. (a) Show that the union of a countable number of countable sets is countable.
   (b) Show that the set of all finite binary strings is countable.
   (c) Use (a) to show that the set of all irrational numbers is uncountable.

Solutions

1. (a) The set is **countable** because the function $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ defined by $f(i) = i$ is injective.
   (b) The set $\mathbb{Z} \times \mathbb{Z}$ is **countable**. Define the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ by

$$f(a,b) = \begin{cases} 2^a 3^b, & a > 0,\ b > 0, \\ 5^{-a} 7^{-b}, & a < 0,\ b < 0, \\ 11^a 13^{-b}, & a > 0,\ b < 0, \\ 17^{-a} 19^b, & a < 0,\ b > 0, \\ 23^b, & a = 0,\ b > 0, \\ 29^a, & a > 0,\ b = 0, \\ 31^{-b}, & a = 0,\ b < 0, \\ 37^{-a}, & a < 0,\ b = 0, \\ 1, & (a,b) = (0,0). \end{cases}$$

   We claim f is injective. Suppose $f(a,b) = f(c,d)$. By unique prime factorisation, the set of primes dividing $f(a,b)$ and the set of primes dividing $f(c,d)$ must be equal. Hence (a,b) and (c,d) lie in the same case. Again, by unique prime factorisation, the corresponding exponents must agree, so $a = c$ and $b = d$. Therefore f is injective.

(c) The set $\mathbb{Q} \times \mathbb{Q}$ is **countable**. First define an injection $e : \mathbb{Z} \to \mathbb{N}$ by

$$e(z) = \begin{cases} 2z, & z \geq 0, \\ -2z - 1, & z < 0. \end{cases}$$

Next define an injection $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$c(m, n) = 2^m 3^n.$$

Write each rational in lowest terms with positive denominator: $x = \frac{p}{q}$, $y = \frac{r}{s}$ with $p, r \in \mathbb{Z}$ and $q, s \in \mathbb{N}$. Define $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$ by

$$F\left(\frac{p}{q}, \frac{r}{s}\right) = 2^{\,c(e(p),\, q)}\, 3^{\,c(e(r),\, s)}.$$

If $F\left(\frac{p}{q}, \frac{r}{s}\right) = F\left(\frac{p'}{q'}, \frac{r'}{s'}\right)$, then by unique prime factorisation we get $c(e(p), q) = c(e(p'), q')$ and $c(e(r), s) = c(e(r'), s')$. Since c is injective, we have $e(p) = e(p')$, $q = q'$, $e(r) = e(r')$, $s = s'$. Moreover, since e is injective, we have $p = p'$ and $r = r'$. Therefore $\frac{p}{q} = \frac{p'}{q'}$ and $\frac{r}{s} = \frac{r'}{s'}$, so F is injective.

(d) The set $\mathbb{Z} \times \mathbb{Z} \times ...$ is **not countable**. We will prove this by giving an injection $\mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$.

For each $x \in \mathbb{R}$, write $x = n + r$ with $n = \lfloor x \rfloor \in \mathbb{Z}$ and $r \in [0, 1)$. Choose the unique decimal expansion of r that does not end with an infinite tail of 9's. Write this decimal expansion as

$$r = 0.d_1 d_2 d_3 \cdots, \qquad d_k \in \{0, 1, \ldots, 9\}.$$

Then define the function $\iota : \mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$ by

$$\iota(x) = (n, d_1, d_2, d_3, \ldots) \in \mathbb{Z} \times \mathbb{Z} \times \cdots.$$

This is injective; if $\iota(x) = \iota(y)$ then the decimals of x and y are equal, so $x = y$.

2. (a) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Q}$ are countable and infinite.

   (b) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are countable and infinite.

   (c) **No.** $\mathbb{Q} \times \mathbb{Q}$ is countable, while $\mathbb{R}$ is uncountable.

3. (a) Let $A_1, A_2, A_3, ...$ be countable. Then for each n we can list A_n as

$$A_n = \{a_{n,1}, a_{n,2}, a_{n,3}, ...\}.$$

Now list the union by going along diagonals:

$$a_{1,1};\ a_{1,2}, a_{2,1};\ a_{1,3}, a_{2,2}, a_{3,1};\ a_{1,4}, a_{2,3}, a_{3,2}, a_{4,1};\ ...$$

Every element of every A_n appears somewhere in this list, so $\bigcup_{n=1}^{\infty} A_n$ can be listed in a sequence. Hence $\bigcup_{n=1}^{\infty} A_n$ is countable.

(b) Let B_n be the set of all binary strings of length n. Each B_n is finite (there are 2^n such strings), hence countable. Every finite binary string has some length, so

$$B = \{\text{all finite binary strings}\} = \bigcup_{n=0}^{\infty} B_n.$$

By (a), a countable union of countable sets is countable, so B is countable.

(c) Suppose, for contradiction, that the set of irrationals $\mathbb{R} \setminus \mathbb{Q}$ were countable. We already know $\mathbb{Q}$ is countable. Then by part (a),

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

would be a union of two countable sets, hence countable. But $\mathbb{R}$ is uncountable. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

Application — Computability of Functions

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 170–177.*

An important application of the topic of countability to computer science is examining the **computability** of functions. In computer science, a function is **computable** if there is a computer program in some programming language that can find the values of the function. If there is no such program, we say the function is **uncomputable**.

Application problems

1. (a) Show the set of all computer programs in any given computer language is countable.

   Hint: a computer program written in a programming language can be thought of as a string of symbols from a finite alphabet.

   (b) Let T be the set of all functions from $\mathbb{Z}^+$ to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.

   Hint: start by finding an injection between the interval $(0, 1)$ *and a subset of* T*.*

   (c) Hence show that there are uncomputable functions.

Application solutions

1. (a) Given a computer language with a finite alphabet A, we let P be the set of all computer programs in the language. If P is finite, then it is countable and we are done, so assume P is infinite.

   Now we use the fact that we can think of each computer program as a series of strings made using the alphabet A. Consider all strings of length m made from alphabet A, and denote this set by A_m. It is easy to show that there are $|A|^m$ distinct strings of this type, and since A is finite, $|A|^m$ is also finite. Now P is a subset of $\bigcup_{i=1}^{\infty} A_m$. Since the union of a countable number of countable sets is also countable (see Question 3(a) from earlier in this section) it follows that $\bigcup_{i=1}^{\infty} A_m$ is countable and hence P is countable.

   (b) We use the hint and start by defining a function from $(0, 1)$ to T as follows. Recall that every real number in the interval $(0, 1)$ can be written in decimal notation as $0.a_1a_2a_3 \ldots a_n \ldots$ where each a_i is an integer from 0 to 9. Also recall that T is the set of all functions from $\mathbb{Z}^+$ to $\{0, 1, \ldots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

   $$f(0.a_1a_2a_3 \ldots a_n \ldots) = g,$$

   where g is the function in T such that $g(n) = a_n$ for all $n \in \mathbb{Z}^+$.

   So for example, if $f(0.457013) = g$ then g is the function where $g(1) = 4$, $g(2) = 5$, $g(3) = 7$, $g(4) = 0$, $g(5) = 1$, $g(6) = 3$ and $g(n) = 0$ for all $n \geq 7$.

   Now we will prove that this function is one-to-one. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in (0, 1)$. Then for these functions to be equal, they map every integer to the same value. For this to happen, every decimal digit of x_1 must be equal to the same decimal digit of x_2 and so we must have $x_1 = x_2$.

   Now denote the set of all outputs of f as S. Hence $S \subseteq T$. Now if we set the codomain of f to be S, which is the range of f, we have made this function surjective and hence a

bijection. This means that the subset $S \subseteq T$ is in bijection with the interval $(0, 1)$. Since the interval $(0, 1)$ is uncountable, we must have that S is also uncountable and since $S \subseteq T$, T must also be uncountable.

(c) Part (a) showed us that the set of all computer programs in a given language is countable. This means that there are a countable number of computable functions. However part (b) showed us that there is an uncountable number of functions in the set T, so we must have that some functions are uncomputable.

§29 — Relations on Sets

Epp 4th ed. pp. 442–449 · 5th ed. (metric) pp. 487–494. Lecture 23 (week 8).

Problems

1. Define a relation P on $\mathbb{Z}$ as follows: for every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \; P \; n \iff m \text{ and } n \text{ have a common prime factor.}$$

   (a) Is $15 \; P \; 25$?

   (b) Is $22 \; P \; 27$?

   (c) Is $0 \; P \; 5$?

   (d) Is $8 \; P \; 8$?

2. Let $X = \{a, b, c\}$. Define a relation S on the power set $\mathcal{P}(X)$ as follows: for all sets A and B in $\mathcal{P}(X)$,

$$A \; S \; B \iff A \text{ has the same number of elements as } B.$$

   (a) Is $\{a, b\} \; S \; \{b, c\}$?

   (b) Is $\{a\} \; S \; \{a, b\}$?

   (c) Is $\{c\} \; S \; \{b\}$?

3. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ be sets. Let R be the 'divides' relation. That is, for every ordered pair (a, b) in $A \times B$, we have $a \; R \; b$ if and only if $a \mid b$. Draw an arrow diagram (i.e. the directed graph) of this relation.

Solutions

1. (a) **Yes**, since $15 = 3 \cdot 5$ and $25 = 5 \cdot 5$ share the prime factor 5.

   (b) **No**, since $22 = 2 \cdot 11$ and $27 = 3^3$ share no common prime factor.

   (c) **Yes**, since 0 is divisible by every prime; in particular $5 \mid 0$ and $5 \mid 5$, so 0 and 5 have a common prime factor.

   (d) **Yes**, since $8 = 2^3$ and 2 is a prime factor of 8 (so they share the prime factor 2).

2. (a) **Yes**, since $|\{a, b\}| = 2 = |\{b, c\}|$.

   (b) **No**, since $|\{a\}| = 1 \neq 2 = |\{a, b\}|$.

   (c) **Yes**, since $|\{c\}| = 1 = |\{b\}|$.

3. We have $A \times B = \{(3,4), (3,5), (3,6), (4,4), (4,5), (4,6), (5,4), (5,5), (5,6)\}$. The pairs (a, b) satisfying $a \mid b$ are

$$\{(3,6),\ (4,4),\ (5,5)\} \subseteq A \times B.$$

   So the directed graph has an arrow from 3 (in A) to 6 (in B), an arrow from 4 to 4, and an arrow from 5 to 5 — and no other arrows.

§30 — Reflexivity, Symmetry, Transitivity

Epp 4th ed. pp. 449–459 · 5th ed. (metric) pp. 495–505. Lecture 23 (week 8).

Problems

1. Let $X = \{1, 2, 3, 4, 5\}$ and consider the subset $R \subseteq X \times X$ given by

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3), (3,4), (4,5), (5,1)\}.$$

   (a) Draw an arrow diagram for the binary relation R.

   (b) Draw an arrow diagram for the binary relation R^{-1}.

   (c) Draw an arrow diagram for the binary relation $R \cup R^{-1}$.

   (d) Is R symmetric? Is R^{-1} symmetric? Is $R \cup R^{-1}$ symmetric?

   (e) Is R transitive? Is R^{-1} transitive? Is $R \cup R^{-1}$ transitive?

2. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

- $(1, 2) \in R$
- $(2, 3) \in R$
- R is reflexive
- R is transitive

What is the minimum number of arrows required in an arrow diagram for a relation R that satisfies these criteria?

Solutions

1. (a) The arrow diagram for R has the five vertices $1, 2, 3, 4, 5$ drawn around a circle, with a **loop at every vertex** (from the pairs $(1, 1), \ldots, (5, 5)$) together with the directed 5-cycle

$$1 \to 2 \to 3 \to 4 \to 5 \to 1.$$

(b) The arrow diagram for R^{-1} is the same picture with every non-loop arrow reversed: a loop at every vertex, together with the directed 5-cycle

$$1 \to 5 \to 4 \to 3 \to 2 \to 1,$$

that is, $R^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$.

(c) The arrow diagram for $R \cup R^{-1}$ has a loop at every vertex and a **double-headed arrow** between each consecutive pair around the cycle — that is, both $(i, i + 1)$ and $(i + 1, i)$ for the cycle $1, 2, 3, 4, 5, 1$.

(d) R is **not** symmetric because $(1, 2) \in R$ but $(2, 1) \notin R$.

R^{-1} is **not** symmetric because $(2, 1) \in R^{-1}$ but $(1, 2) \notin R^{-1}$.

$R \cup R^{-1}$ **is** symmetric. If $(a, b) \in R \cup R^{-1}$ then $(a, b) \in R$ or $(a, b) \in R^{-1}$, which means $(b, a) \in R^{-1}$ or $(b, a) \in R$, and thus, in either case, $(b, a) \in R \cup R^{-1}$.

(e) R is **not** transitive because $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

R^{-1} is **not** transitive because $(3, 2), (2, 1) \in R^{-1}$ but $(3, 1) \notin R^{-1}$.

$R \cup R^{-1}$ is **not** transitive because $(1, 2), (2, 3) \in R \cup R^{-1}$ but $(1, 3) \notin R \cup R^{-1}$.

2. R is reflexive, so $(1,1),(2,2),(3,3) \in R$ — a loop on each point of the arrow diagram. We are also given $(1,2),(2,3) \in R$, and R is transitive, so $(1,3) \in R$. R is *not* required to be symmetric, so no further arrows are forced.

$$R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$$

So the **minimum number of arrows required is 6**.

§31 — Equivalence Relations

Epp 4th ed. pp. 459–478 · 5th ed. (metric) pp. 505–523. Lecture 24 (week 9).

Problems

1. Define the binary relations α, β and γ on $\mathbb{Z}$ as follows:

$$\begin{aligned} x \,\alpha\, y &\iff x + y \text{ is an even integer,} \\ x \,\beta\, y &\iff x \text{ is a multiple of } y, \\ x \,\gamma\, y &\iff 3 \text{ is a factor of } x^2 - y^2. \end{aligned}$$

   (a) Fill in the table with 'Yes'/'No' to indicate the properties satisfied by each relation.

	α	β	γ
Reflexive			
Symmetric			
Transitive			
Equivalence relation			

   (b) For each equivalence relation, state its equivalence classes.

2. Let $A = \{a,b,c,d,e\}$ be a set and ρ be a binary relation defined by

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

   For instance, $(a,b) \in \rho$ means $a \,\rho\, b$.

   (a) Draw the directed graph representing ρ.

   (b) Is ρ reflexive? Is ρ symmetric? Is ρ transitive?

(c) Is ρ an equivalence relation on A? If so, give its equivalence classes.

(d) What is the smallest subset τ of ρ which forms an equivalence relation on A?

(e) Give the equivalence classes for τ.

3. Consider a positive integer n and any set of strings S. Define a relation R_n on S by the condition $s\ R_n\ t$ if and only if $s = t$ or both s and t have at least n characters and the first n characters are the same. Show that R_n is an equivalence relation.

Solutions

1. (a)

	α	β	γ
Reflexive	Yes	Yes	Yes
Symmetric	Yes	No	Yes
Transitive	Yes	Yes	Yes
Equivalence relation	Yes	No	Yes

(b) The equivalence relations are α and γ.

For α, notice $x\ \alpha\ y \iff x + y$ is even $\iff x$ and y have the same parity. This means the equivalence classes are $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

For γ, notice $x\ \gamma\ y \iff 3 \mid (x^2 - y^2) \iff x^2 \equiv y^2 \pmod 3$. But modulo 3 the only possible square residues are

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 1 \pmod 3.$$

Hence $x^2 \equiv 0 \pmod 3$ exactly when $3 \mid x$, and $x^2 \equiv 1 \pmod 3$ exactly when $3 \nmid x$. Therefore $x\ \gamma\ y$ iff either both x and y are multiples of 3, or neither is. So the equivalence classes are $\{n \in \mathbb{Z} : 3 \mid n\}$ and $\{n \in \mathbb{Z} : 3 \nmid n\}$. Note that another way to write the equivalence classes is $\{3n \mid n \in \mathbb{Z}\}$ and $\{3n + 1,\ 3n + 2 \mid n \in \mathbb{Z}\}$.

2. (a) A digraph for ρ (vertex set $A = \{a, b, c, d, e\}$) has a **loop at every vertex**, double-headed arrows between each pair of $\{a, b, d\}$ — that is between a and b, between a and d, and between b and d — and a double-headed arrow between c and e. There are no arrows between $\{a, b, d\}$ and $\{c, e\}$.

(b) ρ is **reflexive**: we have $(x, x) \in \rho$ for all $x \in A$ (loops on all vertices).

ρ is **symmetric**: whenever $(x, y) \in \rho$, we have $(y, x) \in \rho$ (no single-direction arrow between any two distinct vertices).

ρ is **transitive**: within $\{a, b, d\}$ all relations occur, within $\{c, e\}$ all relations occur, and there are no relations between $\{a, b, d\}$ and $\{c, e\}$. That is, whenever (x, y) and (y, z) are in ρ, then (x, z) is also in ρ (and $x = z$ is possible).

(c) **Yes**, ρ is an equivalence relation. Its equivalence classes are

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

(d) An equivalence relation $\tau \subseteq \rho$ must be reflexive, so $(x, x) \in \tau$ for all $x \in A$. But notice if τ is the relation

$$\tau = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$$

then τ is an equivalence relation. Therefore this is the smallest relation which is an equivalence relation.

(e) The equivalence classes for τ are the singletons:

$$[a] = \{a\},\ [b] = \{b\},\ [c] = \{c\},\ [d] = \{d\},\ [e] = \{e\}.$$

3. Let S be any set of strings and fix $n \in \mathbb{Z}^+$.

   R_n **is reflexive:** for any $s \in S$, since $s = s$, by definition $s\ R_n\ s$.

   R_n **is symmetric:** let $s, t \in S$, and assume $s\ R_n\ t$. If $s = t$ then $t\ R_n\ s$; otherwise both s and t must have at least n characters and, since $s\ R_n\ t$, they must have the same first n characters, so $t\ R_n\ s$.

   R_n **is transitive:** let $s, t, u \in S$ and assume $s\ R_n\ t$ and $t\ R_n\ u$. Since $s\ R_n\ t$ we either have $s = t$, or s and t both have at least n characters and have the same first n characters. Similarly, since $t\ R_n\ u$, either $t = u$, or t and u both have at least n characters and have the same first n characters. Thus either $s = t = u$, or s and u both have at least n characters and they both share the first n characters with t (and hence each other). Thus $s\ R_n\ u$ and so R_n is transitive.

   Since R_n is reflexive, symmetric and transitive it is an equivalence relation. □

Application — Identifiers

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 608–618.*

In the C programming language, an **identifier** is the name of a variable, a function or another type of entity.

Each identifier is a nonempty string of characters where each character is a lowercase or uppercase English letter, a digit, or an underscore.

There is no limit on the number of characters used in the identifier; however, for some compilers for some versions of C, there is a limit on the number of characters checked when two names are compared.

For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. We see that two identifiers will be considered the same if and only if they are related under the relation R_n when $n = 31$ (defined in a previous question).

Application problems

1. Using R_{31} on the set of all possible identifiers, determine the equivalence classes of each of the following identifiers:

   (a) `file_1`

   (b) `Number_of_tropical_storms`

   (c) `Number_of_named_tropical_storms`

   (d) `Number_of_named_tropical_storms_in_the_Atlantic_in_2005`

Application solutions

1. Let I be the set of all possible identifiers (strings over letters, digits and underscores).

   (a) Since `file_1` has length $6 < 31$, its equivalence class is just

   $$[\texttt{file_1}]_{R_{31}} = \{\texttt{file_1}\}.$$

   (b) Since `Number_of_tropical_storms` has length $25 < 31$, its equivalence class is

   $$[\texttt{Number_of_tropical_storms}]_{R_{31}} = \{\texttt{Number_of_tropical_storms}\}.$$

(c) The identifier `Number_of_named_tropical_storms` has length exactly 31, so two identifiers are R_{31}-equivalent to it iff they have at least 31 characters and their first 31 characters equal this string. Hence

$$[\texttt{Number_of_named_tropical_storms}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 31 characters of} \\ t \text{ are } \texttt{Number_of_named_tropical_storms} \end{array} \right\}.$$

(d) The identifier `Number_of_named_tropical_storms_in_the_Atlantic_in_2005` begins with the same first 31 characters `Number_of_named_tropical_storms`, so it has the same R_{31}-equivalence class as in (c):

$$[\texttt{Number_of_named_tropical_storms_in_the_Atlantic_in_2005}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 3} \\ t \text{ are } \texttt{Number_of_name} \end{array} \right.$$

§32 — Partial Order Relations

Epp 4th ed. pp. 498–515 · 5th ed. (metric) pp. 546–563. Lecture 25 (week 9).

Problems

1. Let ρ be a relation on $\mathbb{Z}$ defined by $x \rho y$ if and only if $x^3 - 1 < y^3$.

   (a) Prove ρ is a partial order relation.

   (b) Is ρ a total order?

2. Let S be the set of binary strings of length 6. Define the **weight** of a binary string as the number of ones it contains. (For example, weight(110110) = 4.) Define a relation ρ on S by

   $$s \rho t \text{ if and only if } \text{weight}(s) \leq \text{weight}(t).$$

   (a) Prove that ρ is not an equivalence relation.

   (b) Prove that ρ is not a partial order relation.

3. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

   - $(2, 3) \in R$
   - $(3, 2) \in R$
   - $(1, 1) \notin R$

- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) To show that ρ is a partial order, we need to show that ρ is reflexive, antisymmetric and transitive.

   Reflexive: let $x \in \mathbb{Z}$. Then $x^3 - 1 < x^3$ and so $x \;\rho\; x$, so ρ is reflexive.

   Antisymmetric: suppose $x \;\rho\; y$ where $x \neq y$. (We must show that then $y \not\rho\, x$.) Now $x \;\rho\; y$ means that $x^3 - 1 < y^3$. And since $x \neq y$ we must have $x^3 < y^3$ and so $x^3 \leqslant y^3 - 1$. Hence $y^3 - 1 \not< x^3$ and so we do not have $y \;\rho\; x$. Therefore ρ is antisymmetric.

   Transitive: suppose that $x \;\rho\; y$ and $y \;\rho\; z$. Then we know that $x^3 - 1 < y^3$ and $y^3 - 1 < z^3$. So $x^3 - 1 \leqslant y^3 - 1 < z^3$, that is, $x^3 - 1 < z^3$ so that $x \;\rho\; z$, which means that ρ is transitive.

   Hence ρ is a partial order. □

   (b) To check whether ρ is a total order, let x and y be any two distinct integers. Then $x^3 \neq y^3$ and so either $x^3 < y^3$ or else $y^3 < x^3$.

   If $x^3 < y^3$ then $x^3 - 1 < y^3$ and so $x \;\rho\; y$.

   If $y^3 < x^3$ then $y^3 - 1 < x^3$ and so $y \;\rho\; x$.

   So for any integers $x \neq y$, we have either $x \;\rho\; y$ or else $y \;\rho\; x$. So any two integers are comparable under ρ. Hence ρ **is** a total order.

2. (a) It is **not an equivalence relation** because it is not symmetric. For instance, let $s = 000000$ and $t = 111111$. Then $\text{weight}(s) = 0 \leq 6 = \text{weight}(t)$, so $(s, t) \in \rho$, but $(t, s) \notin \rho$.

   (b) It is **not a partial order** because it is not antisymmetric. For instance, let $s = 100000$ and $t = 010000$. Then $\text{weight}(s) = \text{weight}(t) = 1$, so $s \;\rho\; t$ and $t \;\rho\; s$, but $s \neq t$.

3. One relation on $\{1, 2, 3\}$ satisfying all conditions is

$$R = \{(1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3, 2)\}.$$

(It contains $(2,3)$ and $(3,2)$; it is transitive; it is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$; it is not antisymmetric since $2 \neq 3$ and $(2,3),(3,2) \in R$; and $(1,1) \notin R$.)

An arrow diagram for this R has vertices $1,2,3$ with: arrows $1 \to 2$ and $1 \to 3$; loops at 2 and at 3; and a double-headed arrow between 2 and 3. There is no loop at vertex 1.

§33 — Definitions and Examples of Groups

No relevant textbook pages. Lecture 26 (week 9).

Problems

1. Show $\mathbb{Z}_9 - \{0\} = \{1,2,3,\ldots,7,8\}$ is not a group under multiplication modulo 9.
2. Let G be the set of all odd integers. Define the binary operation $\star$ on G by

$$x \star y = x + y - 1.$$

   Show that $(G, \star)$ is an abelian group.
3. Show $\mathbb{Z}_9 - \{0,3,6\} = \{1,2,4,5,7,8\}$ is a group under multiplication modulo 9. Is the group abelian?
4. Define the group $H = \mathbb{Z}_5 - \{0\} = \{1,2,3,4\}$ under multiplication modulo 5. Write the Cayley table for H.
5. Define the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ under component-wise addition modulo 2. That is,

$$(a,b) + (c,d) = (a + c \bmod 2,\ b + d \bmod 2).$$

   Write the Cayley table for G.

Solutions

1. It is not a group under multiplication mod 9 because, for example, it is **not closed** ($3 \cdot 3 = 0 \notin \mathbb{Z}_9 - \{0\}$).

2. **Closure:** if x and y are odd, then $x+y$ is even, so $x+y-1$ is odd. Hence $x \star y \in G$.

   Associativity: for $x, y, z \in G$,

$$(x \star y) \star z = (x+y-1)+z-1 = x+y+z-2 = x+(y+z-1)-1 = x \star (y \star z).$$

   Commutativity: for $x, y \in G$,

$$x \star y = x+y-1 = y+x-1 = y \star x.$$

   Identity: we seek $e \in G$ such that $x \star e = x = e \star x$ for all x. Now the requirement $x \star e = x+e-1 = x$ implies that $e = 1$. Note 1 lies in G. Moreover, commutativity implies that $e \star x = x$ as well. Thus the identity is 1.

   Inverses: given $x \in G$, we want $y \in G$ with $x \star y = 1$. This means $x+y-1 = 1$, so $y = 2-x$. Since x is odd, $2-x$ is odd, hence $2-x \in G$. Thus the inverse of x is $x^{-1} = 2-x$.

   Therefore $(G, \star)$ is an abelian group. $\square$

3. **Closure:** if $a, b \in \{1,2,4,5,7,8\}$, then $3 \nmid a$ and $3 \nmid b$, hence $3 \nmid ab$, so $ab \not\equiv 0, 3, 6 \pmod 9$; thus $\{1,2,4,5,7,8\}$ is closed under multiplication modulo 9.

   Associativity and commutativity: normal multiplication between integers is associative and commutative, so multiplication modulo 9 in the set $\{1,2,4,5,7,8\}$ is also associative and commutative. This means the group **is abelian**.

   Identity: $1 \in G$ is the identity because $1 \cdot x \equiv x \pmod 9$.

   Inverse: every element has an inverse. We explicitly calculate the inverses:

$$\begin{aligned}
1^{-1} &= 1 \quad \text{because } 1 \cdot 1 \equiv 1 \pmod 9,\\
2^{-1} &= 5 \quad \text{because } 2 \cdot 5 = 10 \equiv 1 \pmod 9,\\
4^{-1} &= 7 \quad \text{because } 4 \cdot 7 = 28 \equiv 1 \pmod 9,\\
5^{-1} &= 2 \quad \text{because } 5 \cdot 2 = 10 \equiv 1 \pmod 9,\\
7^{-1} &= 4 \quad \text{because } 7 \cdot 4 = 28 \equiv 1 \pmod 9,\\
8^{-1} &= 8 \quad \text{because } 8 \cdot 8 = 64 \equiv 1 \pmod 9.
\end{aligned}$$

4. For $H = \mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ under multiplication mod 5, the Cayley table is:

$\cdot$	1	2	3	4
1	1	2	3	4

$\cdot$	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition mod 2, the Cayley table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(\mathbf{1},\mathbf{0})$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

§34 — Elementary Properties of Groups

No relevant textbook pages. Lecture 27 (week 10).

Problems

1. Let $H = \{3n \mid n \in \mathbb{Z}\}$ be the set of multiples of 3. Prove H is a subgroup of $(\mathbb{Z}, +)$.
2. Fix elements g and h in a group G where e is the group identity. Prove the following statements:
   (a) If $g^{-1} = h$ then $h^{-1} = g$.
   (b) $(g^{-1})^{-1} = g$.
   (c) $(gh)^{-1} = h^{-1}g^{-1}$.
3. Prove $K = \{(0,0),(0,1),(2,0),(2,1)\}$ is a subgroup of $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ where the group operation is componentwise addition:

$$(a,b) + (c,d) = (a + c \pmod 4,\ b + d \pmod 2).$$

4. Consider the group $(\mathbb{Z}_{11} - \{0\}, \cdot)$. Show that this group is cyclic.
   Hint: express every element of $\mathbb{Z}_{11} - \{0\}$ as a power of 2.

Solutions

1. First we note that $H \subseteq \mathbb{Z}$, and $H \neq \emptyset$.

   Closure: if $x, y \in H$ then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}$. Therefore $x + y = 3a + 3b = 3(a + b) \in H$.

   Identity: the identity of $(\mathbb{Z}, +)$ is 0, and since $0 = 3 \cdot 0$, we have $0 \in H$.

   Inverse: in $\mathbb{Z}$, the inverse of x is $-x$. In H, if $x \in H$ then $x = 3a$ for some $a \in \mathbb{Z}$. This means $-x = -3a = 3 \cdot (-a)$, and so $-x \in H$ also.

   Note that we do not need to check associativity for subgroups, since this property is automatically inherited from the parent group $(\mathbb{Z}, +)$. □

2. (a) Suppose $g^{-1} = h$. Now $gh = gg^{-1} = e$ and $hg = g^{-1}g = e$. Thus $h^{-1} = g$.

   (b) By definition, $gg^{-1} = e = g^{-1}g$, so $(g^{-1})^{-1} = g$.

   (c) Notice we have

   $$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = e$$

   and

   $$(h^{-1}g^{-1})(gh) = h^{-1}g^{-1}gh = e.$$

   This means $(gh)^{-1} = h^{-1}g^{-1}$.

3. We draw the Cayley table of $K = \{(0,0), (0,1), (2,0), (2,1)\}$ under componentwise addition in $\mathbb{Z}_4 \times \mathbb{Z}_2$:

$+$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(2,1)$	$(2,0)$
$(\mathbf{2},\mathbf{0})$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(\mathbf{2},\mathbf{1})$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$

   Notice the operation is closed in K and every element of K has an inverse in K. Therefore K is a subgroup. □

4. Note that 2 is a generator of $(\mathbb{Z}_{11} - \{0\}, \cdot)$, so it is cyclic:

   $$1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ 8 = 2^3,\ 5 = 2^4,\ 10 = 2^5,\ 9 = 2^6,\ 7 = 2^7,\ 3 = 2^8,\ 6 = 2^9.$$

§35 — Group Isomorphisms

No relevant textbook pages. No lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36).

This content is optional and will not be assessed. The source document carries no practice problems or solutions for this section.

§36 — Definitions and Examples of Fields

No relevant textbook pages. Lecture 28 (week 10).

Problems

1. (a) Solve $3x + 4 = 2$ in the field $(\mathbb{Z}_5, +, \cdot)$.
   (b) Solve $8x - 9 = 6$ in the field $(\mathbb{Z}_{11}, +, \cdot)$.
   (c) Solve $4(1 - x) = 10$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.
   (d) Solve $16(x - 6) = 15$ in the field $(\mathbb{Z}_{19}, +, \cdot)$.
2. Prove $\mathbb{Z}_{12}$ with addition modulo 12 and multiplication modulo 12 is not a field.
3. Define addition and multiplication on $\mathbb{Q} \times \mathbb{Q}$ by

$$(a, b) + (c, d) = (a + c,\ b + d)$$

   and

$$(a, b) \cdot (c, d) = (ac + 3bd,\ ad + bc)$$

   for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$. Prove that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field.

Solutions

1. (a)

$$\begin{aligned} 3x + 4 &= 2 \\ \rightarrow 3x &= -2 \end{aligned}$$

Now, since $3 \times 2 = 6 \equiv 1 \pmod 5$, 2 is the multiplicative inverse of 3, and so we multiply both sides by 2 and obtain $x = -4$. That is, $x = 1$.

Check: $3 \cdot 1 + 4 = 7 \equiv 2 \pmod 5$.

(b)

$$\begin{aligned} 8x - 9 &= 6 \\ \rightarrow 8x &= 15 = 4 \end{aligned}$$

Now, since $8 \times 7 = 56 \equiv 1 \pmod{11}$, 7 is the multiplicative inverse of 8, and so we multiply both sides by 7 and obtain $x = 28$. That is, $x = 6$.

Check: $8 \cdot 6 - 9 = 39 \equiv 6 \pmod{11}$.

(c) Since $4 \times 10 = 40 \equiv 1 \pmod{13}$, 10 is the multiplicative inverse of 4, and so we multiply both sides by 10 and obtain $1 - x = 100 = 9$. That is, $x = 1 - 9 = 14 - 9 = 5$.

Check: $4(1 - 5) = -16 \equiv 10 \pmod{13}$.

(d) Since $16 \times 6 = 96 \equiv 1 \pmod{19}$, 6 is the multiplicative inverse of 16, and so we multiply both sides by 6 and obtain $x - 6 = 90 = 14$. That is, $x = 20 = 1$.

Check: $16(1 - 6) = -80 \equiv 15 \pmod{19}$.

2. $\mathbb{Z}_{12}$ is not a field because 2 has no multiplicative inverse modulo 12. Indeed $2 \cdot k \equiv 1 \pmod{12}$ has no solution since $2k$ is always even.

3. We show that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field in three steps.

Step 1 — $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Closure: for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Q} \times \mathbb{Q}$.

Associative: for all $(a, b), (c, d), (e, f) \in \mathbb{Q} \times \mathbb{Q}$ we have $\big((a, b) + (c, d)\big) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) = (a, b) + (c + e, d + f) = (a, b) + \big((c, d) + (e, f)\big)$.

Identity: for all $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0) + (a, b)$.

Inverses: for all $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a,b) + (-a,-b) = (a-a, b-b) = (0,0)$ and $(-a,-b) + (a,b) = (-a+a, -b+b) = (0,0)$. So $(-a,-b)$ is the inverse of (a,b).

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b)$.

Thus $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Step 2 — $((\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\},\ \cdot)$ is an abelian group.

Closure: for all $(a,b),(c,d) \in (\mathbb{Q}\times\mathbb{Q}) - \{(0,0)\}$, we have $(a,b)\cdot(c,d) = (ac+3bd, ad+bc) \in \mathbb{Q} \times \mathbb{Q}$. So we only need to show that $(ac+3bd, ad+bc) \neq (0,0)$. For a contradiction, suppose $(ac+3bd, ad+bc) = (0,0)$. That is, $ac+3bd = 0$ and $ad+bc = 0$. Multiplying the first equation by d and the second by c we obtain $acd + 3bd^2 = 0$ and $acd + bc^2 = 0$, from which it follows that $3bd^2 = bc^2$.

Now, if $b = 0$, then $ac = 0$, $ad = 0$ and $a \neq 0$, and so $c = d = 0$; a contradiction. Thus $b \neq 0$ and we have $3d^2 = c^2$. This is a contradiction because if $d = 0$, then $c \neq 0$ and the equation does not hold, and if $d \neq 0$, then we have $3 = \frac{c^2}{d^2}$, which implies $\sqrt{3} = \frac{c}{d}$ is rational. Thus $(ac+3bd, ad+bc) \neq (0,0)$ and we have closure.

Associative: for all $(a,b),(c,d),(e,f) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have

$$\begin{aligned}(a,b)\cdot\big((c,d)\cdot(e,f)\big) &= (a,b)\cdot(ce+3df,\ cf+de)\\ &= (a(ce+3df)+3b(cf+de),\ a(cf+de)+b(ce+3df))\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf)\end{aligned}$$

and

$$\begin{aligned}\big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac+3bd,\ ad+bc)\cdot(e,f)\\ &= \big((ac+3bd)e+3(ad+bc)f,\ (ac+3bd)f+(ad+bc)e\big)\\ &= (ace+3bde+3adf+3bcf,\ acf+3bdf+ade+bce)\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf).\end{aligned}$$

Identity: for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have $(a,b)\cdot(1,0) = (a,b)$ and $(1,0)\cdot(a,b) = (a,b)$, so $(1,0)$ is a multiplicative identity.

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have

$$(a,b)\cdot(c,d) = (ac+3bd,\ ad+bc) = (ca+3db,\ cb+da) = (c,d)\cdot(a,b).$$

Inverses: we check that for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2-3b^2},\ \frac{-b}{a^2-3b^2}\right).$$

First, note that $a^2-3b^2 \neq 0$, because $a^2-3b^2=0$ implies either $(a,b)=(0,0)$ or $\sqrt{3}=\frac{a}{b}$, both of which are contradictions (the second because $\sqrt{3}$ is not rational). Thus $(a,b)^{-1} \in (\mathbb{Q}\times\mathbb{Q})-\{(0,0)\}$, and notice

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2-3b^2},\frac{-b}{a^2-3b^2}\right) &= \left(a\cdot\frac{a}{a^2-3b^2}+3b\cdot\frac{-b}{a^2-3b^2},\ a\cdot\frac{-b}{a^2-3b^2}+b\cdot\frac{a}{a^2-3b^2}\right)\\ &= \left(\frac{a^2-3b^2}{a^2-3b^2},\ \frac{-ab+ab}{a^2-3b^2}\right)\\ &= (1,0).\end{aligned}$$

So every nonzero element has an inverse. Thus $((\mathbb{Q}\times\mathbb{Q})-\{(0,0)\},\cdot)$ is an abelian group.

Step 3 — the distributive laws. For all $(a,b),(c,d),(e,f)\in\mathbb{Q}\times\mathbb{Q}$ we have

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,\ d+f)\\ &= (a(c+e)+3b(d+f),\ a(d+f)+b(c+e))\\ &= ((ac+3bd)+(ae+3bf),\ (ad+bc)+(af+be))\\ &= (ac+3bd,\ ad+bc)+(ae+3bf,\ af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)\end{aligned}$$

and (since we have already shown that multiplication and addition are commutative)

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f) &= (e,f)\cdot((a,b)+(c,d))\\ &= (e,f)\cdot(a,b)+(e,f)\cdot(c,d) \quad \text{(by the first distributive law)}\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f).\end{aligned}$$

Thus $(\mathbb{Q}\times\mathbb{Q},+,\cdot)$ is a field. □

§37 — Introduction to Counting

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 29 (week 11).

Problems

1. The UQ drama club is auditioning for its annual production of *Romeo and Juliet*. Six people are auditioning for the role of Romeo, and eight other people are auditioning for the role of Juliet. In how many ways can the director cast the lead couple?
2. There are eleven questions on the final exam, but you decide — based on your successful grade for your in-semester exam — that you will only do five of them. How many combinations of questions are there which you could complete?
3. (a) How many permutations of $\{1, 2, \dots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \dots, 15\}$ contain exactly two numbers from $\{1, 2, 3, 4\}$?

Solutions

1. There are 6 choices for Romeo and 8 choices for Juliet, so $6 \cdot 8 = 48$ ways.
2. Since the order in which you do the 5 questions does not matter, there are $\binom{11}{5} = 462$ combinations of questions.
3. (a) There are 8 odd numbers in the set $\{1, \dots, 15\}$. Choose the first entry in 8 ways, then permute the remaining 14 numbers, so $8 \cdot 14!$ permutations.

   (b) We choose exactly 2 numbers from the set $\{1, 2, 3, 4\}$ and exactly 3 numbers from the remaining 11 numbers, so the number of subsets is

$$\binom{4}{2}\binom{11}{3}.$$

Application — Runtime

Not assessable for MATH1061. Taken from S. Epp, Discrete Mathematics with Applications, *5th edition, pages 787–799.*

In many algorithms, the runtime is well approximated by counting how many times the basic instructions are executed.

For programs with nested `for`-loops and no early exits, the total number of executions of the inner loop body equals the number of choices of the outer-loop index multiplied by the number of choices of the inner-loop index.

Concretely, if i runs through M values and, for each fixed i, the variable j runs through N values, then the inner loop body is executed exactly MN times.

Application problems

1. The following algorithms are written in pseudo-code and contain nested loops. For each algorithm, count the total number of iterations of the inner loop that the algorithm will run.

   (a)

```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (b)

```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (c) (Fix integers $a, b, c, d \in \mathbb{Z}^+$ with $a \leq b$ and $c \leq d$.)

```
for i := a to b
    for j := c to d
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

Application solutions

1. (a) $i = 1, \ldots, 30$ gives 30 iterations and $j = 1, \ldots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

   (b) $i = 5, \ldots, 50$ gives $50 - 5 + 1 = 46$ iterations and $j = 10, \ldots, 20$ gives $20 - 10 + 1 = 11$ iterations, so the inner loop runs $46 \cdot 11 = 506$ times.

   (c) $i = a, \ldots, b$ gives $b - a + 1$ iterations and $j = c, \ldots, d$ gives $d - c + 1$ iterations, so the inner loop runs $(b - a + 1)(d - c + 1)$ times.

§38 — Counting Selections

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 30 (week 11).

Problems

1. (a) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY?

   (b) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with R and end with P?

   (c) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with I and end with Y?

   (d) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that have all four Os next to each other?

2. (a) How many distinct arrangements can be made of the letters of the word WOOLLOONGABBA?

   (b) How many distinct arrangements are there of the letters of the word WOOLLOONGABBA such that **exactly one** of the following is true?

   - The two As are not next to each other.
   - The two Bs are not next to each other.
   - The two Ls are not next to each other.

3. (a) How many one-to-one (injective) functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

   (b) How many onto (surjective) functions are there from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$?

Solutions

1. (a) There are 13 letters in INDOOROOPILLY, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!} = 64\,864\,800.$$

   (b) Fix R in the first position and P in the last position. There are 11 letters remaining, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!\,2!} = 415\,800.$$

(c) Fix I in the first position and Y in the last position. There are 11 letters remaining, with four O's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!} = 831\,600.$$

(d) Treat the four O's as one 'letter'. There are 10 'letters' with two I's, two L's, and the remaining 'letters' appearing once each. Therefore the number of distinct arrangements is

$$\frac{10!}{2!\,2!} = 907\,200.$$

2. (a) There are 13 letters in WOOLLOONGABBA, with four O's, two L's, two A's, two B's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!\,2!} = 32\,432\,400.$$

(b) We want exactly one of the pairs AA, BB, LL to be non-adjacent. That is, there are three cases to consider:

- **Case 1:** the two A's are not adjacent but BB and LL are adjacent.
- **Case 2:** the two B's are not adjacent but AA and LL are adjacent.
- **Case 3:** the two L's are not adjacent but AA and BB are adjacent.

Note that the number of ways Case 1 can occur is exactly the same as the number of ways Case 2 can occur (and similarly for Case 3).

To count the number of ways Case 1 can occur, we first count arrangements with BB adjacent and LL adjacent. Treat BB as one 'letter' and LL as one 'letter'. Then there are 11 'letters' (W, O, O, LL, O, O, N, G, A, BB, A) to arrange, with four O's, two A's, and the remaining 'letters' appearing once each. Therefore the number of such arrangements is

$$\frac{11!}{4!\,2!}.$$

In order to determine the number of these for which the two A's are not adjacent, we take this total and subtract those where AA is also adjacent. For this, treat AA, BB, and LL as 'letters'. Then there are 10 'letters' to arrange, with four O's and the remaining 'letters' appearing once each. Therefore the number of arrangements with AA adjacent and BB adjacent and LL adjacent is

$$\frac{10!}{4!}.$$

Hence, the number of ways that Case 1 can occur is

$$\frac{11!}{4!\,2!} - \frac{10!}{4!}.$$

Case 2 and Case 3 have exactly the same number of occurrences as Case 1. Also note that the three cases are mutually exclusive (you cannot have both Case 1 and Case 2 occurring at the same time, for example).

So the number of arrangements of the word WOOLLOONGABBA for which exactly one of the three cases occurs is

$$3\left(\frac{11!}{4!\,2!} - \frac{10!}{4!}\right).$$

3. (a) An injective function $f : \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ is determined by choosing distinct images for a, b, c. The number of choices is

$$5 \cdot 4 \cdot 3 = {}^5P_3 = 60.$$

(b) The number of surjective functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ is the total number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ minus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ which are not surjective. The former number is 3^5. A function which is not surjective must have image of size 1 or 2.

- In the first case, there are 3 such functions (one for each of the three choices for the image).
- In the latter case, first choose which 2 elements of $\{a, b, c\}$ will be in the image. There are $\binom{3}{2}$ such choices. For this fixed two-element image, the number of functions with this image is

$$2^5 - 2,$$

since there are 2^5 total functions from a 5-element set to a 2-element set, and we subtract the 2 constant ones (which fall into the first case, having image of size 1). Thus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ with an image of size 2 is

$$\binom{3}{2}(2^5 - 2) = 3 \cdot 30 = 90.$$

This means there are 93 functions which are not surjective, so the number of surjective functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ is

$$3^5 - 93 = 150.$$

§39 — Introduction to Probability

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 31 (week 11).

Problems

1. To form a committee, five people are to be chosen from a group of ten people.
   (a) How many different committees of five can be chosen?
   (b) Amongst the ten people, we have Alice, Bob, Eve and Oscar. Alice and Bob are extremely talkative during meetings, and so at most one of these two can be chosen. Eve and Oscar are inseparable, and so a committee must either contain both of them or neither of them. With these constraints, how many different five-person committees can be formed?
   (c) What is the probability that none of Alice, Bob, Eve and Oscar are on a committee, given that a random committee of five is chosen subject to the constraints in part (b)?
2. (a) How many positive two-digit integers are multiples of 3?
   (b) What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
   (c) What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

Solutions

1. (a) Number of different committees of five is

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252.$$

   (b) Let A, B be Alice and Bob, and let E, O be Eve and Oscar. There are 6 other people. We split into cases.

   Case 1: the committee contains both E and O. Then we choose 3 more people from the remaining 8 with the restriction that we cannot choose both A and B. There are $\binom{8}{3}$ ways to choose 3 more people from the remaining 8 to be on the committee; of these, there are $\binom{6}{1}$ ways in which both A and B are chosen (such a committee must have E, O, A, B so there is only one more person to choose from the remaining 6 people). Thus the number of committees for this case is

$$\binom{8}{3} - \binom{6}{1} = 56 - 6 = 50.$$

   Case 2: the committee contains neither E nor O. Then we choose 5 people from the remaining 8, again not allowing both A and B. There are $\binom{8}{5}$ ways to choose 5 people from the remaining 8 people to be on the committee; of these, there are $\binom{6}{3}$ ways in which both A and B are chosen. Thus the number of committees for this case is

$$\binom{8}{5} - \binom{6}{3} = 56 - 20 = 36.$$

   Hence the total number is $50 + 36 = 86$.

   (c) To have none of Alice, Bob, Eve, or Oscar on the committee, we must choose all 5 members from the other 6 people, which can be done in $\binom{6}{5} = 6$ ways. Therefore the probability is

$$\frac{6}{86} = 0.069767\ldots$$

2. (a) The positive two-digit multiples of 3 occur as every third number from 12 to 99, so there are

$$\frac{99 - 12}{3} + 1 = 30$$

such numbers.

(b) There are 90 positive two-digit integers (9 choices for the first digit and 10 choices for the second digit). Thus, by part (a), the probability that a randomly selected positive two-digit number is a multiple of 3 is

$$\frac{30}{90} = \frac{1}{3}.$$

(c) The positive two-digit multiples of 4 occur as every fourth number from 12 to 96, so there are

$$\frac{96-12}{4} + 1 = 22$$

such numbers. Hence the probability that a randomly selected positive two-digit number is a multiple of 4 is

$$\frac{22}{90} = \frac{11}{45}.$$

§40 — Binomial Coefficients

Epp 4th ed. pp. 565–591 · 5th ed. (metric) pp. 617–641. Lecture 31 (week 11).

Problems

1. What is the coefficient of x^4 in $(2+3x)^7$?
2. (a) What is the coefficient of x^{12} in $(3-x^3)^6$?
   (b) What is the coefficient of x^8 in $(3-x^3)^6$?
3. What is the coefficient of x^2 in the expansion of $(3-x)^6$?
4. What is the coefficient of x^5 in the expansion of $(2x+1)^{20}$?
5. What is the coefficient of x^5 in the expansion of $\left(3x^2 - \dfrac{2}{x}\right)^7$?

Solutions

1. By the binomial theorem,

$$(2+3x)^7 = \sum_{k=0}^{7} \binom{7}{k} 2^{7-k}(3x)^k.$$

The term x^4 appears only when $k=4$. This term is $\binom{7}{4}2^3(3x)^4$. Therefore the coefficient of x^4 is

$$\binom{7}{4}2^3 3^4 = 35 \times 8 \times 81 = 22\,680.$$

2. By the binomial theorem,

$$(3-x^3)^6 = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-x^3)^k = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-1)^k x^{3k}.$$

(a) The term involving x^{12} is $\binom{6}{4}3^2(-1)^4 x^{3\cdot 4}$, so the coefficient of x^{12} is

$$15 \times 9 \times (-1)^4 = 135.$$

(b) Every power of x that appears is a multiple of 3. Since 8 is not a multiple of 3, there is no x^8 term, so the coefficient of x^8 is $\mathbf{0}$.

3. By the binomial theorem,

$$(3-x)^6 = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-x)^i = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-1)^i x^i.$$

The term x^2 appears only when $i=2$, so the coefficient of x^2 is

$$\binom{6}{2}3^{6-2}(-1)^2 = \binom{6}{2}3^4 = 1215.$$

4. By the binomial theorem,

$$(2x+1)^{20} = \sum_{k=0}^{20} \binom{20}{k} (2x)^{20-k}(1)^k.$$

The term x^5 appears only when $k = 15$, where the term is $\binom{20}{15}(2x)^5$, so the coefficient of x^5 is

$$\binom{20}{5} 2^5 = 496\,128.$$

5. By the binomial theorem,

$$\left(3x^2 - \frac{2}{x}\right)^7 = \sum_{i=0}^{7} \binom{7}{i} (3x^2)^{7-i} \left(-\frac{2}{x}\right)^i = \sum_{i=0}^{7} \binom{7}{i} 3^{7-i}(-2)^i x^{14-3i}.$$

The term x^5 appears only when $14 - 3i = 5$, i.e. $i = 3$. Therefore the coefficient of x^5 is

$$\binom{7}{3} 3^4(-2)^3 = -22\,680.$$

§41 — Inclusion Exclusion

Epp 4th ed. pp. 545–549 · 5th ed. (metric) pp. 595–599. Lecture 32 (week 12).

Problems

1. Out of 100 people surveyed, 40 people like apples, 50 like bananas and 40 like cherries. 15 like apples and bananas, 16 like bananas and cherries, 17 like cherries and apples and 10 people like all three. How many people do not like any of the three fruits?
2. How many integers between 1 and 600 inclusive are coprime with 15? That is, how many integers n satisfy $1 \leq n \leq 600$ and $\gcd(n, 15) = 1$?
3. Seven friends, named Alice, Bob, Charlie, Delia, Edward, Fred and George, stand in a line for a photograph. How many different arrangements are there of the seven friends standing in a line such that Alice is not next to Charlie and Bob is not next to Delia?

Solutions

1. Let A be the set of people who like apples, B the set of people who like bananas, and C the set of people who like cherries. We are given

$$|A| = 40,\ |B| = 50,\ |C| = 40, \quad |A \cap B| = 15,\ |B \cap C| = 16,\ |C \cap A| = 17, \quad |A \cap B \cap C| = 10.$$

   By inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \\ &= 40 + 50 + 40 - 15 - 17 - 16 + 10 \\ &= 92. \end{aligned}$$

   Hence the number of people who do not like any of the three fruits is

$$100 - |A \cup B \cup C| = 100 - 92 = 8.$$

2. Let $U = \{1, 2, \ldots, 600\}$. Define

$$A = \{n \in U : 3 \mid n\}, \qquad B = \{n \in U : 5 \mid n\}.$$

   Then n is not coprime to 15 if and only if $n \in A \cup B$. We have

$$|A| = \frac{600}{3} = 200, \qquad |B| = \frac{600}{5} = 120, \qquad |A \cap B| = \frac{600}{15} = 40.$$

   By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 200 + 120 - 40 = 280.$$

   Therefore the number of n with $\gcd(n, 15) = 1$ is

$$|U| - |A \cup B| = 600 - 280 = 320.$$

3. Let U be the set of all linear arrangements of the 7 friends, so $|U| = 7!$. Define

$$A = \{\text{arrangements in which Alice is next to Charlie}\},$$
$$B = \{\text{arrangements in which Bob is next to Delia}\}.$$

We want to count the number of arrangements in U which are neither in A nor in B. The required number is $|U \setminus (A \cup B)| = |U| - |A \cup B|$.

To count $|A|$, treat {Alice, Charlie} as a single block. There are 6! ways to arrange the 6 "objects", and for each of these there are 2 ways to order Alice and Charlie within their block (either Alice or Charlie to the left). Hence

$$|A| = 2 \cdot 6!.$$

Similarly, $|B| = 2 \cdot 6!$.

To count $|A \cap B|$, treat both pairs {Alice, Charlie} and {Bob, Delia} as two single blocks. There are 5! ways to arrange the 5 objects (two blocks plus the other three people), and for each of these there are $2 \cdot 2$ internal orders of the two blocks. Hence

$$|A \cap B| = 4 \cdot 5!.$$

By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!.$$

Therefore

$$|U \setminus (A \cup B)| = 7! - (2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!) = 2640.$$

§42 — The Pigeonhole Principle

Epp 4th ed. pp. 554–565 · 5th ed. (metric) pp. 604–616. Lecture 33 (week 12).

Problems

1. (a) Explain why, in a group of 50 people, at least five people were born in the same month.

   (b) How many people do you need to ensure that at least seven people were born in the same month?

2. Show that, if we select six distinct integers from the set $\{1, 2, \ldots, 10\}$, two of these must add to give 11.

3. A computer network consists of six computers. Each computer is directly connected to zero or more of the other computers. Show that there are at least two computers in the network that are directly connected to the same number of other computers.

4. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

5. Let $S = \{1, 2, \ldots, 100\}$. What is the minimum number of integers you must pick from S to be sure that at least one pair has a difference which is divisible by 3?

Solutions

1. (a) There are 12 months (pigeonholes) and 50 people (pigeons). If each month had at most 4 birthdays, then there would be at most $12 \cdot 4 = 48$ people. Since $50 > 48$, by the pigeonhole principle some month must contain at least 5 people.

   (b) To guarantee at least 7 people are born in the same month, note that if each month had at most 6 birthdays, then there could be at most $12 \cdot 6 = 72$ people. Therefore with **73** people, by the pigeonhole principle some month has at least 7 people. Moreover, 72 people is not enough (take 6 born in each month), so the minimum is 73.

2. Partition $A = \{1, 2, \ldots, 10\}$ into the 5 pairs

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\},\ \{5, 6\},$$

   each summing to 11. In order for a selection of distinct integers from the set A to **not** have two that add to give 11, at most one integer can be chosen from each of the subsets. Choosing 6 distinct integers from A forces us to select two numbers from the same pair (there are 5 pairs but 6 choices), by the pigeonhole principle. Those two numbers then add to 11.

3. For each computer, let its **degree** be the number of other computers it is directly connected to. With 6 computers, each degree is an integer in $\{0, 1, 2, 3, 4, 5\}$. It is impossible to have both a computer of degree 0 and a computer of degree 5 (if one is connected to everyone, then none has degree 0). Hence the degrees must all lie in one of the two 5-element sets

$$\{0, 1, 2, 3, 4\} \quad \text{or} \quad \{1, 2, 3, 4, 5\}.$$

So, in either case, there are only 5 possible degree values available for 6 computers. By the pigeonhole principle, at least two computers have the same degree, i.e. are connected to the same number of other computers.

4. Let g_i be the total number of games played in the first i days, for $i = 1, 2, \ldots, 30$. Then

$$1 \leq g_1 < g_2 < \cdots < g_{30} \leq 45$$

because at least one game is played each day. Consider also the 30 numbers

$$g_1 + 14,\ g_2 + 14,\ \ldots,\ g_{30} + 14,$$

which satisfy $15 \leq g_1 + 14 < \cdots < g_{30} + 14 \leq 59$. Thus we have 60 integers

$$g_1, \ldots, g_{30},\ g_1 + 14, \ldots, g_{30} + 14$$

all lying in the set $\{1, 2, \ldots, 59\}$ of size 59. By the pigeonhole principle, two of these 60 integers are equal. Since the g_i are strictly increasing, no equality can occur among the g_i themselves, and likewise no equality can occur among the $g_i + 14$ themselves. Therefore we must have

$$g_j = g_i + 14$$

for some $i, j \in \{1, \ldots, 30\}$. Then the number of games played from day $i + 1$ through day j is

$$g_j - g_i = 14,$$

so there is a period of consecutive days during which exactly 14 games are played.

5. First, we note that two integers have a difference that is divisible by 3 if and only if they are congruent modulo 3 (have the same remainder when divided by 3). Now, the set S can be partitioned into three sets based on their congruence class modulo 3. By the pigeonhole principle, if we select **4** numbers from S, at least two of them must belong to the same congruence class. These two will have difference that is divisible by 3. Note that 4 is the minimum number of selections that guarantees this, since it is possible to select 3 numbers where no two of them have difference divisible by 3 (select one from each congruence class).

§43 — Introduction to Graph Theory

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 33 (week 12).

Problems

1. For each of the following, state whether or not there exists a simple graph with the stated number of vertices and degrees. Draw the graph, or explain why one does not exist.
   (a) Five vertices with degrees 3, 3, 2, 2, 2.
   (b) Seven vertices with degrees 4, 2, 3, 1, 1, 1, 1.
   (c) Five vertices with degrees 5, 4, 3, 1, 1.
2. A graph has 10 edges and 6 vertices. Five of the vertices have degree 3. What is the degree of the remaining vertex?
3. Let n be a positive integer and let K_n be the complete graph with n vertices. How many edges does K_n have?
4. A graph has 27 edges and every vertex has degree 2, 3 or 4. If there are 7 vertices that have degree 4 and 4 vertices that have degree 3, then how many vertices of degree 2 are there?

Solutions

1. (a) **Yes**, such a simple graph exists. One drawing has vertices a, b, c, d, e and the six edges

$$ab, \quad ac, \quad ad, \quad bc, \quad be, \quad de,$$

   giving $\deg(a) = 3$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 2$, $\deg(e) = 2$ as required.

   (b) **No** such graph exists. If the degrees are 4, 2, 3, 1, 1, 1, 1, then the sum of degrees is

$$4 + 2 + 3 + 1 + 1 + 1 + 1 = 13,$$

which is odd. Remember (by the Handshake Theorem) that the sum of the degrees in any graph equals twice the number of edges, and so is always even. So such a graph cannot exist.

(c) **No** such graph exists. In a simple graph on 5 vertices, the largest possible degree is 4, but the sequence contains a vertex of degree 5, which is impossible. So there is no such simple graph.

2. Since the graph has 10 edges, the sum of all the degrees is $2 \cdot 10 = 20$. If five vertices have degree 3, the sum of their degrees is $5 \cdot 3 = 15$, so the remaining vertex has degree

$$20 - 15 = 5.$$

3. In K_n, an edge is determined by choosing 2 distinct vertices, so the number of edges is

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

4. Let x be the number of vertices of degree 2. Since the graph has 27 edges, the sum of degrees is $2 \cdot 27 = 54$. Given that there are seven vertices of degree 4 and four vertices of degree 3, and all other vertices have degree 2, we have

$$2x + 4 \cdot 7 + 3 \cdot 4 = 54.$$

This means $x = 7$.

§44 — Walks, Trails and Circuits

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 34 (week 12).

Problems

1. Let G and H be the graphs below.

   G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is drawn with a **loop at** v_2, a **loop at** v_5, and **two parallel edges between** v_1 **and** v_2. Its degree sequence is

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   so G is connected with 10 edges.

   H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is a simple connected graph drawn as the 4-cycle $v_1v_2v_3v_4v_1$ with a single pendant edge v_3v_5, giving degrees

   $$\deg(v_1) = 2, \quad \deg(v_2) = 2, \quad \deg(v_3) = 3, \quad \deg(v_4) = 2, \quad \deg(v_5) = 1.$$

   For each of the following statements, explain why it is true or false.

   (a) G is a simple graph.

   (b) The sum of the degrees of the vertices of G is 18.

   (c) G contains an Euler circuit.

   (d) H contains an Euler trail.

2. Does the following graph contain an Euler circuit? (The graph shown is connected and has exactly two vertices of degree 3.)

3. Let G be a simple, connected, Eulerian graph with eight vertices and let e be the number of edges in G. Prove that $8 \leq e \leq 24$.

Solutions

1. (a) This statement is **false**. The graph G has loops (at v_2 and v_5) and it also has multiple edges between v_1 and v_2, so G is not simple.

   (b) This statement is **false**. A loop contributes 2 to the degree, so we have

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   and thus the sum of the degrees is $4 + 6 + 4 + 2 + 4 = 20 \neq 18$.

   (c) This statement is **true**. The graph G is connected and every vertex has even degree (as computed above), so G contains an Euler circuit.

(d) This statement is **true**. In H, the degrees are

$$\deg(v_1) = 2,\ \deg(v_2) = 2,\ \deg(v_4) = 2,\ \deg(v_3) = 3,\ \deg(v_5) = 1,$$

so exactly two vertices have odd degree (namely v_3 and v_5). Therefore H has an Euler trail (starting at one of v_3, v_5 and ending at the other).

2. **No.** The graph is connected, but has two vertices of degree 3, so not all vertices have even degree. Hence there is no Euler circuit.

3. Since G is connected and Eulerian, every vertex has even degree, and (because G is simple and connected with 8 vertices) each vertex has degree at least 2. Hence

$$2e = \sum_{v} \deg(v) \geq 8 \cdot 2 = 16,$$

so $e \geq 8$. Moreover, in a simple graph on 8 vertices we have $\deg(v) \leq 7$, and because G is Eulerian all degrees are even, so in fact $\deg(v) \leq 6$ for every vertex. Therefore

$$2e = \sum_{v} \deg(v) \leq 8 \cdot 6 = 48,$$

so $e \leq 24$. Hence $8 \leq e \leq 24$. □

§45 — Matrix Representations of Graphs

Epp 4th ed. pp. 661–675 · 5th ed. (metric) pp. 698–712. Lecture 35 (week 13).

Problems

1. Let G be the graph with vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{a, b, c, d, e, f\}$, where the edges are

edge	endpoints
a	$v_1 v_2$
b	$v_2 v_3$
c	$v_2 v_3$ (parallel to b)
d	$v_3 v_4$
e	$v_2 v_4$
f	loop at v_4

(a) Write down an adjacency matrix for G. Make sure you clearly label the rows and columns of your matrix.

(b) Write down an incidence matrix for G. Make sure you clearly label the rows and columns of your matrix.

(c) Does G have an Euler circuit? If yes, write it out as a sequence of vertices and edges. If not, determine the fewest number of edges that would need to be added to G to create a new graph that does have an Euler circuit.

2. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(a) Draw the graph G.

(b) Explain whether or not G has an Euler circuit or an Euler trail.

3. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Explain whether or not G is Eulerian.

Solutions

1. (a) The labelled adjacency matrix for G is

	v_1	v_2	v_3	v_4
$\mathbf{v_1}$	0	1	0	0
$\mathbf{v_2}$	1	0	2	1
$\mathbf{v_3}$	0	2	0	1
$\mathbf{v_4}$	0	1	1	1

(where the entry 1 on the diagonal at v_4 records the single loop at v_4).

(b) The labelled incidence matrix for G is

	a	b	c	d	e	f
$\mathbf{v_1}$	1	0	0	0	0	0
$\mathbf{v_2}$	1	1	1	0	1	0
$\mathbf{v_3}$	0	1	1	1	0	0
$\mathbf{v_4}$	0	0	0	1	1	2

(where the entry 2 in the bottom right indicates the loop that is incident twice with v_4).

(c) The degrees are

$$\deg(v_1) = 1, \quad \deg(v_2) = 4, \quad \deg(v_3) = 3, \quad \deg(v_4) = 4,$$

so G does **not** have an Euler circuit (since v_1 and v_3 have odd degree).

The fewest edges to add to make all degrees even is **1**; for example, adding an edge g between vertices v_1 and v_3 creates a new connected graph in which all of the vertices have even degree.

An example of an Euler circuit in the new graph is

$$v_1,\ a,\ v_2,\ b,\ v_3,\ d,\ v_4,\ f,\ v_4,\ e,\ v_2,\ c,\ v_3,\ g,\ v_1.$$

2. (a) Reading the matrix off (with vertices $v_1, \ldots, v_5$ in matrix order), G has the edges

- v_1v_2 — a single edge,
- v_1v_5 — **three** parallel edges,
- v_2v_3 — **two** parallel edges,
- v_3v_4 — a single edge,
- v_3v_5 — a single edge,
- v_4v_5 — a single edge.

(b) The degrees are

$$\deg(v_1) = 4,\ \deg(v_2) = 3,\ \deg(v_3) = 4,\ \deg(v_4) = 2,\ \deg(v_5) = 5,$$

so there is **no Euler circuit** (since v_2 and v_5 have odd degree), but there **is an Euler trail** (exactly two odd-degree vertices) from v_2 to v_5.

3. Let the vertices be $v_1, v_2, v_3, v_4, v_5, v_6$ in the order of the matrix. Reading the matrix off, G has edges

$$v_1v_2, \quad v_1v_4, \quad v_2v_4, \quad v_3v_5, \quad v_3v_6, \quad v_5v_6,$$

that is, two disjoint triangles: one on $\{v_1, v_2, v_4\}$ and one on $\{v_3, v_5, v_6\}$.

The graph is **not connected** (e.g. there is no walk from vertex v_1 to vertex v_3). Hence G is not Eulerian.

(Errata note: the source document's solution to 1(b) was corrected on 11 August 2026 — the note in brackets had previously copied the note from 1(a). The corrected note is the one given above.)

§46 — Trees

Epp 4th ed. pp. 683–701 · 5th ed. (metric) pp. 720–742. Lecture 36 (week 13).

Problems

1. A tree has 11 vertices, of which exactly four vertices have degree 1 and exactly one vertex has degree 4. Determine the degrees of the remaining six vertices.
2. Let T be a tree with p vertices, where $p \geq 11$. Suppose T has precisely six vertices of degree 1 and precisely four vertices of degree 3. Determine the degree of each of the remaining $p - 10$ vertices of T.
3. Let T be a tree on 12 vertices. Suppose T has exactly three vertices of degree 3 and each of the remaining vertices has degree 1 or 5. Using theorems that were given in lectures, determine the number of vertices of degree 5.
4. Two trees with the same vertex set $\{1, 2, \ldots, n\}$ are **distinct** if their edge sets are not equal. Use mathematical induction to prove that for each integer $n \geq 2$, the number of distinct trees with vertex set $\{1, 2, \ldots, n\}$ is at least $(n-1)!$.

Solutions

1. A tree with 11 vertices has $e = 10$ edges, so by the Handshake Theorem, the sum of degrees is $2e = 20$. We are given that exactly four vertices have degree 1 and exactly one vertex has degree 4. Let $v_1, v_2, \ldots, v_6$ be the remaining vertices whose degrees are to be determined. We have

$$\sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20$$

$$\sum_{i=1}^{6} \deg(v_i) = 12.$$

None of these six vertices $v_1, v_2, \ldots, v_6$ can have degree 1 (since there are exactly four vertices of degree 1, already accounted for). Hence each has degree at least 2. Because six vertices of degree at least 2 have total degree 12, each must have degree exactly 2.

Thus the remaining six vertices all have **degree 2**.

2. T is a tree with p vertices and so must have $p-1$ edges. Now by the Handshake Theorem we know

$$2(p-1) = \sum_{i=1}^{p} \deg(v_i).$$

Using the known degrees we can write this as

$$\begin{aligned} 2(p-1) &= 6 \cdot 1 + 4 \cdot 3 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-1) &= 18 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2p - 2 - 18 &= \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-10) &= \sum_{i=1}^{p-10} \deg(v_i). \end{aligned}$$

Rewriting the final line as

$$\frac{\sum_{i=1}^{p-10} \deg(v_i)}{p-10} = 2, \qquad \text{i.e.} \qquad \frac{\deg(v_1) + \deg(v_2) + \cdots + \deg(v_{p-10})}{p-10} = 2,$$

we see that the average degree of the remaining $p-10$ vertices is 2. However, we know that there are no more vertices of degree 1. Thus each of the remaining $p-10$ vertices must have **degree exactly 2**.

3. Let x be the number of vertices of degree 5 and y the number of vertices of degree 1. Then, because the tree has 12 vertices, we have

$$x + y + 3 = 12.$$

This simplifies to give $x + y = 9$.

Now, since T is a tree on 12 vertices, it must have $e = 11$ edges. By the Handshake Theorem, the sum of degrees is $2e = 22$, so

$$3 \cdot 3 + 5x + 1 \cdot y = 22.$$

This simplifies to give $5x + y = 13$.

Subtracting $x + y = 9$ from $5x + y = 13$ gives $4x = 4$, hence $x = 1$. Therefore there is exactly **one** vertex of degree 5.

4. We prove by induction that the number of distinct trees with vertex set $\{1, 2, \dots, n\}$ is at least $(n-1)!$.

Basis: let $n = 2$. Here $(n-1)! = (2-1)! = 1$. There is exactly one tree on $\{1, 2\}$, namely the single edge $\{1, 2\}$. So the base case is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and there are at least $(k-1)!$ distinct trees on $\{1, 2, \dots, k\}$.

Now consider $n = k + 1$. We aim to show that there are at least $k!$ distinct trees on vertex set $\{1, 2, \dots, k, k+1\}$.

Let T be a tree on vertex set $\{1, 2, \dots, k\}$. For any choice of $m \in \{1, 2, \dots, k\}$, we form a graph T_m on vertex set $\{1, 2, \dots, k, k+1\}$ as follows: start with tree T, add a new vertex $k+1$, and the edge $\{k+1, m\}$.

Note that T_m is connected (since $k+1$ is joined to m, and T was connected). Also, T_m has no circuit because T is a tree and adding a new leaf does not create a circuit. Thus T_m is a tree. Moreover, different choices of m give rise to distinct trees T_m, because their edge sets are different.

By the inductive hypothesis, there are at least $(k-1)!$ choices for the tree T. Since there are k choices for the vertex m, there are at least $k \cdot (k-1)! = k!$ trees T_m on vertex set $\{1, 2, \dots, k+1\}$.

By the principle of mathematical induction, this completes the proof. $\square$

See also

- math1061[176] — assessment weights and the full lecture schedule
- Logic: logical-connectives[177] · logical-equivalence-laws[178] · conditional-statements[179] · valid-argument-forms[180] · determining-argument-validity[181] · quantified-statements[182]
- Number theory and proof: proof-techniques[183] · rational-and-irrational-numbers[184] · divisibility-and-factorisation[185] · modular-arithmetic[186] · gcd-lcm-and-euclidean-algorithm[187]
- Graph theory (§43–§46): graphs[188] · walks-trails-and-circuits[189] · euler-circuits-and-trails[190] · adjacency-matrices[191] · incidence-matrices[192] · trees[193]

Proof Techniques — Direct, Counterexample, Contradiction, Contraposition

The four methods for establishing (or demolishing) a statement of the form $\forall x \in D, P(x) \to Q(x)$, plus the definitions every proof in this course is expected to unfold.

Definitions to prove from

Proofs are written by **demonstrating facts using the definitions** — so these have to be at your fingertips. Each is a biconditional: it can be used in either direction.

Term	Definition
n is **even**	$n = 2k$ for some integer k
n is **odd**	$n = 2k + 1$ for some integer k (equivalently $n = 2k - 1$ for some integer k)

[176] courses/math1061/math1061.pdf
[177] courses/math1061/logical-connectives.pdf
[178] courses/math1061/logical-equivalence-laws.pdf
[179] courses/math1061/conditional-statements.pdf
[180] courses/math1061/valid-argument-forms.pdf
[181] courses/math1061/determining-argument-validity.pdf
[182] courses/math1061/quantified-statements.pdf
[183] courses/math1061/proof-techniques.pdf
[184] courses/math1061/rational-and-irrational-numbers.pdf
[185] courses/math1061/divisibility-and-factorisation.pdf
[186] courses/math1061/modular-arithmetic.pdf
[187] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[188] courses/math1061/graphs.pdf
[189] courses/math1061/walks-trails-and-circuits.pdf
[190] courses/math1061/euler-circuits-and-trails.pdf
[191] courses/math1061/adjacency-matrices.pdf
[192] courses/math1061/incidence-matrices.pdf
[193] courses/math1061/trees.pdf

Term	Definition
n is **prime**	$n \in \mathbb{Z}$, $n > 1$, and $\forall r, s \in \mathbb{Z}^+$, if $n = rs$ then $(r = 1$ and $s = n)$ or $(r = n$ and $s = 1)$
n is **composite**	$n \in \mathbb{Z}$, $n > 1$, and $\exists r, s \in \mathbb{Z}^+$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$
r is **rational**	$\exists a, b \in \mathbb{Z}$ such that $r = \frac{a}{b}$ and $b \neq 0$
$d \mid n$	$d \neq 0$ and $n = dk$ for some integer k

Two facts used constantly, and worth naming explicitly when you lean on them:

- **Fact**: the sum, difference, and product of integers is an integer.
- **Fact**: every integer is either even or odd.

Parity

Almost every early proof in this course turns on whether something is even or odd, so the consequences of those two definitions are worth having ready rather than re-deriving:

	Result
even + even, odd + odd	even
even + odd	odd
even× anything	even
odd × odd	odd
consecutive integers	opposite parity — so two integers **two apart share their parity**

Each row follows from the two definitions by a one-line substitution. Subtraction behaves like addition throughout, since $m - n$ and $m + n$ differ by $2n$.

The "two apart" row is the whole content of the warm-up in 2026-07-27-welcome-and-intro-problems[194], where consecutive $p < q < r$ forces $p + r$ to be even and $r - p$ to be exactly 2, while pr is free to be either.

Prime vs. not-prime. For $n \in \mathbb{Z}^{>1}$, "n is not prime" means "n is composite". For $n \in \mathbb{Z}$ generally, "n is not prime" means "n is composite **or** $n \leq 1$" — the integers split into $\mathbb{Z}^{\leq 1}$, $\mathbb{Z}^{\text{prime}}$, and $\mathbb{Z}^{\text{composite}}$, and 1 and everything below it is in none of the latter two. This is why $n = 1$ is the standard counterexample to "every positive integer is prime or composite".

Warning: don't assume something that seems like an "obvious fact" until you have proven it, or can name the lecture or pre-work video it was proved in.

[194] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

The four methods

All four target $\forall x \in D, P(x) \to Q(x)$. Recall the truth table for $p \to q$ — the only row that makes it false is p true, q false:

p	q	$p \to q$
T	T	T
T	F	F
F	T	T
F	F	T

Every method below is a different way of attacking that one row.

Direct proof (shows the statement is true)

> Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$. $\square$

Why suppose $P(x)$ is true, when $P(x) \to Q(x)$ holds anyway if $P(x)$ is false? Because the only case that could make the statement false is $P(x)$ true and $Q(x)$ false. Ruling that out is the whole job — the $P(x)$-false rows are true for free.

Disproof by counterexample (shows the statement is false)

> Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true. However, $Q(x)$ is false. So x is a counterexample and the statement is false.

A counterexample to $p \to q$ needs p **true** and q **false** — a value where the hypothesis fails proves nothing.

Proof by contradiction (shows the statement is true)

> Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true. That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false. ... Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$. This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. $\square$

The set-up comes straight from quantified-statements[195]: the negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D$ such that $P(x) \wedge \sim Q(x)$.

[195] courses/math1061/quantified-statements.pdf

Proofs of the statement $\forall x \in D,\ P(x) \to Q(x)$

Direct proof:

Let $x \in D$ and suppose $P(x)$.

...

Hence $Q(x)$. □

Shows the statement is true.

Disproof by counterexample:

Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true.

However, $Q(x)$ is false.

So x is a counterexample and the statement is false.

Shows the statement is false.

Proof by contradiction:

Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true.

That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false.

...

Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$.

This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. □

Shows the statement is true.

Proof by contraposition:

We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely that $\forall x \in D, \sim Q(x) \to \sim P(x)$.

Let $x \in D$ and suppose $\sim Q(x)$.

...

Hence, $\sim P(x)$. □

Figure 20: The skeletons of the four methods for a statement of the form x D, P(x) → Q(x). Three of the four establish the statement and one demolishes it, which is what the red verdict lines record.

Useful negations to have ready (see logical-equivalence-laws[196]):

$$\sim (p \vee q) \equiv \sim p \wedge \sim q \qquad \sim (p \wedge q) \equiv \sim p \vee \sim q \qquad \sim (p \to q) \equiv p \wedge \sim q$$

Proof by contraposition (shows the statement is true)

> We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely that $\forall x \in D, \sim Q(x) \to \sim P(x)$. Let $x \in D$ and suppose $\sim Q(x)$. ... Hence, $\sim P(x)$. $\square$

This is valid because $p \to q \equiv \sim q \to \sim p$ (see conditional-statements[197]).

Choosing a method

- **Contradiction is the most versatile**, but it needs more set-up, so a direct proof is often easier when one is available.
- **Contraposition** is the natural choice when $\sim Q(x)$ gives you something concrete to work with and $P(x)$ doesn't — typically when the conclusion is a negative statement ("r is irrational", "n is odd") whose negation is a definition you can expand.
- **Contradiction vs. contraposition**: a contraposition proof is a contradiction proof that never actually needs the assumption $P(x)$ — you derive $\sim P(x)$ from $\sim Q(x)$ alone. If your "contradiction" proof only ever uses the $\sim Q(x)$ half of the assumption, write it as a contraposition instead.
- **Counterexample vs. contradiction**: counterexample is a **disproof**, contradiction is a **proof**. They are not variants of each other.

Worked comparisons on the same statements live in the lecture notes: 2026-08-13-proof-by-contradiction[198] proves $\forall n \in \mathbb{Z}$, if n is odd then $3n+2$ is odd both directly and by contradiction, and 2026-08-13-proof-by-contraposition[199] works through statements where one method gets stuck and another doesn't.

Worked examples

Direct proof

$\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd.

[196] courses/math1061/logical-equivalence-laws.pdf
[197] courses/math1061/conditional-statements.pdf
[198] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[199] courses/math1061/2026-08-13-proof-by-contraposition.pdf

Let $n \in \mathbb{Z}$ and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Now

$$3n + 2 = 3(2k+1) + 2 = 6k + 5 = 2(3k+2) + 1.$$

Since $k \in \mathbb{Z}$, we have $3k + 2 \in \mathbb{Z}$, and hence $3n + 2$ is odd. □

For any integer x, if $x + 6 = 4y$ for some integer y, then $\frac{x}{2}$ is an odd integer.

Let $x \in \mathbb{Z}$ and suppose $x + 6 = 4y$ for some $y \in \mathbb{Z}$. Then $x = 4y - 6 = 2(2y - 3)$, so

$$\frac{x}{2} = \frac{2(2y-3)}{2} = 2y - 3 = 2(y-1) - 1.$$

Since $y \in \mathbb{Z}$ we have $2y - 3 \in \mathbb{Z}$, so $\frac{x}{2} \in \mathbb{Z}$; and $y - 1 \in \mathbb{Z}$, so by definition $\frac{x}{2}$ is odd. □

The sum of any pair of even integers is even.

Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence $m + n = 2k + 2\ell = 2(k + \ell)$, which is even. □

$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

Suppose $n \in \mathbb{Z}^+$ and $n \geq 4$. Factor $2n^2 - 5n + 2 = (2n-1)(n-2)$. Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers greater than 1. Hence the expression is composite. □

Disproof by counterexample

- **For all integers m and n, if $2m + n$ is odd then m and n are both odd.** Counterexample $m = 4, n = 5$: $2(4) + 5 = 13$ is odd, but m is even. (Not $m = 3, n = 5$ — there the conclusion holds; not $m = 3, n = 6$ or $m = 4, n = 6$ — there the hypothesis fails.)
- **$\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n+1$ is composite.** Take $n = 2$: both 2 and 3 are prime.
- **For each integer $n \geq 2$, the product of the first n primes minus 1 is prime.** Take $n = 4$: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, composite.
- **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** Take $x = 1, y = -2$: $4 > 1$ but $-2 \not> 1$.
- **$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** Take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1$. (See modular-arithmetic[200] for the floor function.)

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

Disproof by proving the negation

When the statement to disprove is existential, a single counterexample isn't available — you must prove the universal negation.

$\exists n \in \mathbb{Z}^+$ **such that** $n^2 + 5n + 6$ **is prime.** This is false; the negation is $\forall n \in \mathbb{Z}^+$, $n^2 + 5n + 6$ is composite.

> Let $n \in \mathbb{Z}^+$. Now $n^2 + 5n + 6 = (n + 2)(n + 3)$. Since $n \geq 1$ we have $n + 2 > 1$ and $n + 3 > 1$, so $n^2 + 5n + 6$ is composite. □

(Because $n \geq 1$ forces $n^2 + 5n + 6 \geq 2$, "not prime" here does mean "composite".)

There is an even integer n **such that** $5n - 4$ **is prime.** False; prove $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

> Suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $5n - 4 = 10k - 4 = 2(5k - 2)$, which is even. The only even prime is 2; if $2(5k-2) = 2$ then $k = \frac{3}{5} \notin \mathbb{Z}$. Therefore $5n - 4$ is not prime. □

Proof by contradiction

$\forall m, n \in \mathbb{Z}$**, if** mn **is even, then** m **is even or** n **is even.**

> Suppose $\exists m, n \in \mathbb{Z}$ such that mn is even and both m and n are odd. Since m is odd, $m = 2k + 1$ for some $k \in \mathbb{Z}$; since n is odd, $n = 2\ell + 1$ for some $\ell \in \mathbb{Z}$ — **a new variable**, since m and n need not be equal. Now
>
> $$mn = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$
>
> Since $k, \ell \in \mathbb{Z}$, $2k\ell + k + \ell \in \mathbb{Z}$, so mn is odd. It is impossible for mn to be both even and odd, a contradiction. Therefore the original statement is true. □

$\forall n \in \mathbb{Z}$**, if** $3n^3 - 2$ **is odd, then** n **is odd.**

> Suppose the statement is false: $\exists n \in \mathbb{Z}$ such that $3n^3 - 2$ is odd and n is even. Since n is even, $n = 2a$ for some $a \in \mathbb{Z}$. Then
>
> $$3n^3 - 2 = 3(2a)^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$
>
> Since $a \in \mathbb{Z}$, $12a^3 - 1 \in \mathbb{Z}$, so $3n^3 - 2$ is even — a contradiction. Therefore the original statement is true. □

$\forall m, n \in \mathbb{Z}$**, if** $m + n$ **is even, then** m **and** n **are both even or both odd.**

Suppose the statement is false. Then $\exists m, n \in \mathbb{Z}$ such that $m+n$ is even but exactly one of m, n is even. **Without loss of generality**, assume m is even and n is odd — the other case (m odd, n even) follows because $m+n = n+m$. Thus $m = 2a$ for some $a \in \mathbb{Z}$ and $n = 2b+1$ for some $b \in \mathbb{Z}$. Now $m+n = 2a+2b+1 = 2(a+b)+1$, and $a+b \in \mathbb{Z}$, so $m+n$ is odd. This contradicts the assumption that $m+n$ is even. Therefore the original statement is true. □

For integers a and b, if $6a+3b$ is odd, then b is odd.

Suppose there exist integers a, b with $6a+3b$ odd and b even. Then $b = 2k$ for some $k \in \mathbb{Z}$, so $6a+3b = 6a+6k = 2(3a+3k)$, which is even — contradicting that $6a+3b$ is odd. □

For all positive integers x and y, $x^2 - y^2 \neq 1$.

Suppose $x, y \in \mathbb{Z}^+$ with $x^2 - y^2 = 1$. Factoring, $1 = (x-y)(x+y)$. Since x, y are positive integers we must have $x-y = 1$ and $x+y = 1$, so $2x = 2$ and $x = 1$; then $y = 0$, which is not a positive integer — a contradiction. □

Proof by contraposition

$\forall r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

We prove the contrapositive: $\forall r \in \mathbb{R}$, if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$. Suppose $r \in \mathbb{R}$ with $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Now $r^2 = \frac{a^2}{b^2}$. Since $a, b \in \mathbb{Z}$ we have $a^2, b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $r^2 \in \mathbb{Q}$. □

$\forall m, n \in \mathbb{Z}$, if mn is odd, then m and n are both odd.

We prove the contrapositive: $\forall m, n \in \mathbb{Z}$, if at least one of m, n is even then mn is even. Without loss of generality, assume m is even, so $m = 2k$ for some $k \in \mathbb{Z}$. Now $mn = (2k)n = 2(kn)$, and $kn \in \mathbb{Z}$, so mn is even. □

For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.

Contrapositive: if a is even or b is even, then $(ab)^2$ is even. WLOG suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ and $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even. □

For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.

Contrapositive: if x is even or y is even, then $x^2(y^2-2y)$ is even. Here the two cases need separate treatment.

Case 1: x even. $x = 2k$ for some $k \in \mathbb{Z}$, so $x^2(y^2-2y) = 4k^2(y^2-2y) = 2(2k^2(y^2-2y))$, and $2k^2(y^2-2y) \in \mathbb{Z}$.

Case 2: y even. $y = 2\ell$ for some $\ell \in \mathbb{Z}$, so $x^2(y^2 - 2y) = x^2(4\ell^2 - 4\ell) = 2(x^2(2\ell^2 - 2\ell))$, and $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$.

In both cases $x^2(y^2 - 2y)$ is even. □

For any integer n, n^2 is odd if and only if n is odd. A biconditional needs both directions, and they want different methods:

($\Leftarrow$, direct) Suppose n is odd, so $n = 2k+1$. Then $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd.

($\Rightarrow$, contraposition) The contrapositive is: if n is even then n^2 is even. Suppose $n = 2k$. Then $n^2 = 4k^2 = 2(2k^2)$ is even. □

This lemma — **for all integers n, if n^2 is even then n is even** — is used in the proof that $\sqrt{2}$ is irrational (see rational-and-irrational-numbers[201]).

Common proof errors

The course explicitly tests spotting these. The seven below are the list given with the practice problems' §9 Q3 (see practice-problems[202], where the four proofs you are asked to find the errors in are worked):

- **Arguing from examples** — a single example never establishes a universal statement. ("$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = 1$. Proof: if $x = 10$ take $y = \frac{1}{10}$." Not a proof — and the statement is false, since $x = 0$ has no such y.)
- **Using the same variable to mean two different things** — "let $m = 2k + 1$ and $n = 2k$" only proves the case $m = n + 1$. Use a fresh variable for each quantity.
- **Jumping to the conclusion** — writing down the definition you need to satisfy and then asserting it holds, without exhibiting the witnesses.
- **Assuming what is to be proved** — starting from "$4a + 2b = 2\ell$" and manipulating both sides assumes the conclusion. Derive the conclusion; don't begin with it.
- **Confusion between what is known and what is to be shown.**
- **Use of the word *any* instead of *some*.**
- **Misuse of the word *if*.**

One more, not on that list: **forgetting to state your assumptions**, or forgetting to say where a variable lives ("for some $r, s \in \mathbb{Z}$"). Introduce every existential witness with its domain.

[201] courses/math1061/rational-and-irrational-numbers.pdf
[202] courses/math1061/practice-problems.pdf

See also

- quantified-statements[203] — the negations these proofs are built on
- conditional-statements[204] · logical-equivalence-laws[205]
- 2026-07-27-welcome-and-intro-problems[206] — the parity warm-up, the course's first proof-shaped problem
- proving-set-properties[207] — the element method, and these techniques applied to sets
- rational-and-irrational-numbers[208] · divisibility-and-factorisation[209]
- practice-problems[210] — §9 Direct Proofs and Counterexamples, with full worked solutions
- practice-problems[211] — §10 Proof by Contradiction, with full worked solutions
- practice-problems[212] — §11 Proof by Contraposition, with full worked solutions

Proving Properties of Sets

Three different ways to prove a statement about sets, when to reach for each, and the set identities the third one runs on. See sets-and-set-notation[213] for the definitions being manipulated and proof-techniques[214] for the general proof shapes underneath.

Three methods

Method	Useful for	How it works
Element method	a **variety** of results about sets	argue about an arbitrary element
Laws of logical equivalence	proving two sets are **equal**	rewrite membership as a logical statement and transform it
Set identities	proving two sets are **equal**	rewrite the set expression itself, citing named identities

[203] courses/math1061/quantified-statements.pdf
[204] courses/math1061/conditional-statements.pdf
[205] courses/math1061/logical-equivalence-laws.pdf
[206] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[207] courses/math1061/proving-set-properties.pdf
[208] courses/math1061/rational-and-irrational-numbers.pdf
[209] courses/math1061/divisibility-and-factorisation.pdf
[210] courses/math1061/practice-problems.pdf
[211] courses/math1061/practice-problems.pdf
[212] courses/math1061/practice-problems.pdf
[213] courses/math1061/sets-and-set-notation.pdf
[214] courses/math1061/proof-techniques.pdf

The element method is the general-purpose one — it is the only one of the three whose stated forms reach a containment ($\subseteq$, $\subset$) rather than an equality; the other two are given only for proving that two sets are equal. Those other two are **quicker**, and the choice between them is yours.

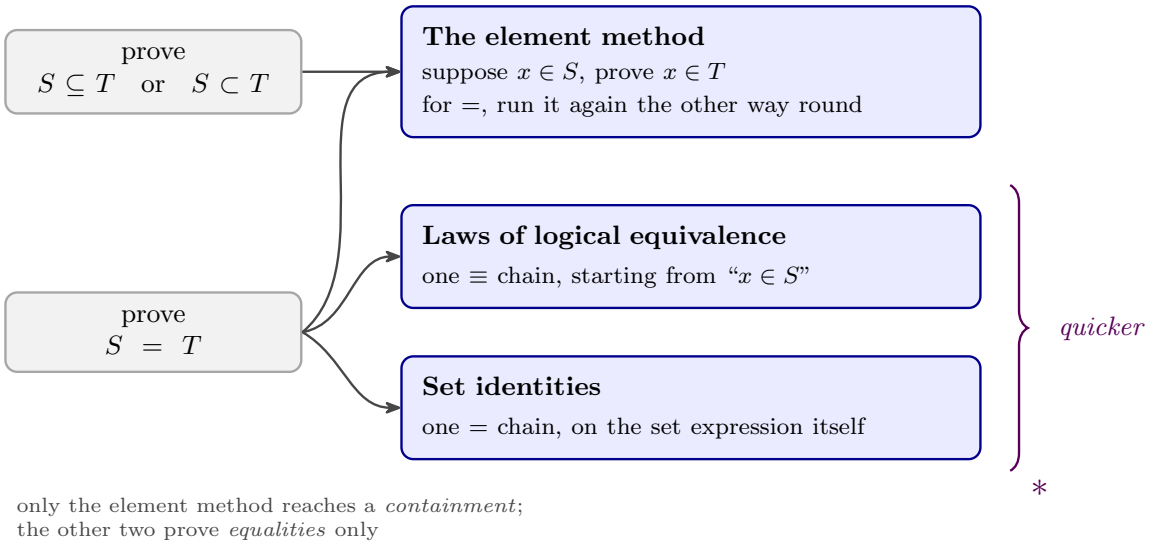


Figure 21: Which method can reach which goal. A containment has only one route open to it; an equality has three, and the two braced as quicker do it in a single chain rather than two separate containment proofs.

The element method

To prove $S \subseteq T$, consider an arbitrary element $x \in S$ and show that $x \in T$.

To prove $S \subset T$, prove $S \subseteq T$ and then prove $\exists\, t \in T$ such that $t \notin S$.

To prove $S = T$, prove $S \subseteq T$ and also prove $T \subseteq S$.

There is a fourth shape worth naming separately, since it is the one that does not mention two sets at all:

To prove that **all elements of a set S have property P**, suppose $x \in S$ and then prove that x has property P.

Worked: a containment that is proper

Let $S = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\}$ and $T = \{x \in \mathbb{Z} \mid x \equiv 5 \pmod 6\}$. Prove $T \subset S$.

Listing a few elements first is a good habit — it tells you which way the containment can possibly go:

$$S = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\} \qquad T = \{\dots, -7, -1, 5, 11, \dots\}$$

T is visibly the sparser set, so $T \subset S$ is the direction to attempt. The proof has the two parts the definition of $\subset$ demands:

Proof.

(i) $T \subseteq S$**.** Suppose $t \in T$. Then $t = 6k + 5$ for some integer k. Thus

$$t = 6k + 5 = 3(2k + 1) + 2$$

and since $2k + 1 \in \mathbb{Z}$, we have $t \equiv 2 \pmod 3$, so $t \in S$. Therefore $T \subseteq S$.

(ii) The containment is proper. $2 \in S$ but $2 \notin T$. Therefore $T \subset S$. ■

Part (i) is a general argument about an arbitrary t; part (ii) is a single exhibited witness. **Getting those two registers the right way round is most of the skill** — a general claim needs a general argument, a "there exists" needs one example.

Worked: complementation reverses containment

Prove that for all sets A and B in some universe U, if $A \subseteq B$ then $B^c \subseteq A^c$.

Proof. Let $x \in B^c$. Then $x \in U - B$ by definition of complement, and thus $x \in U$ and $x \notin B$ by definition of set difference.

Since $A \subseteq B$ we have: every element in A is also an element of B. Taking the contrapositive,

$$x \notin B \implies x \notin A$$

Since $x \in U$ and $x \notin A$, by definition of complement $x \in A^c$. Therefore $B^c \subseteq A^c$. ■

A picture is not a proof

For all sets A, B, C: $(A - B) \cap (B - A) = \emptyset$. **True.**

The diagrams make the claim obvious, and they are still **not a proof**. That is a point worth dwelling on, because Venn diagrams are so persuasive:

- A diagram shows **one** configuration of the sets. The claim is about **all** sets A, B, C — including cases the picture does not draw, such as $A = B$, or either set empty, or one contained in the other.

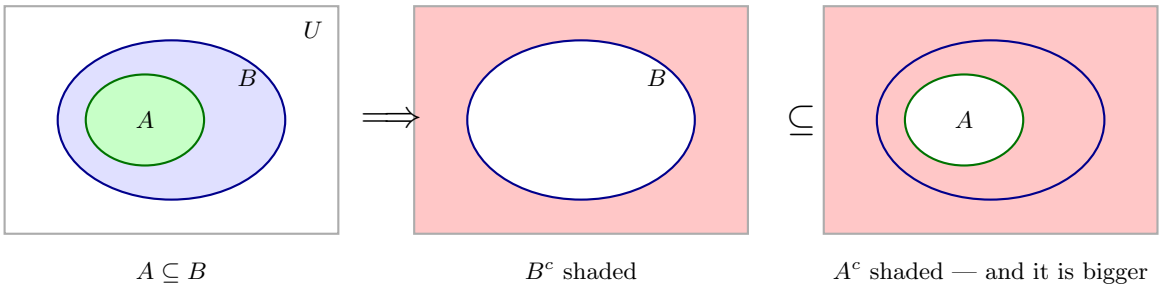


Figure 22: Complementation reverses containment. The smaller set has the larger complement — everything outside B is also outside A, because A was inside B to begin with. The shaded region on the right contains the shaded region on the left.

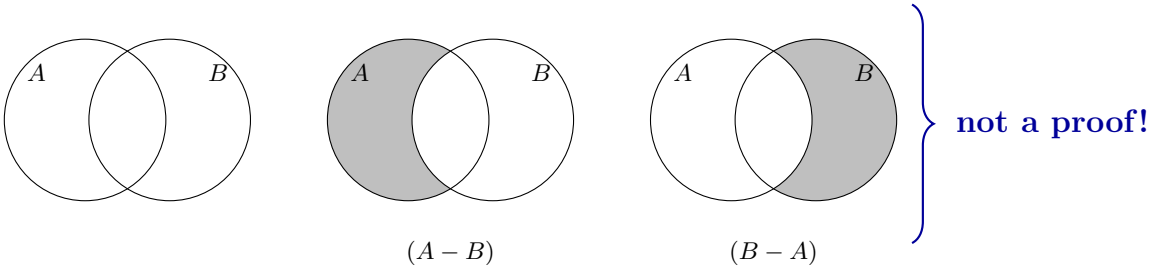


Figure 23: The sets A and B, then A − B shaded, then B − A shaded. The two shaded regions are visibly disjoint, which makes the result believable and is exactly what a proof may not rest on.

- The regions in a Venn diagram are drawn as non-empty; the statement has to hold when they are not.

The proof is short and needs no picture: suppose $x \in (A - B) \cap (B - A)$. Then $x \in A - B$, so $x \in A$ and $x \notin B$; and $x \in B - A$, so $x \in B$ and $x \notin A$. Then $x \in B$ and $x \notin B$, a contradiction. So no such x exists and the intersection is empty. ■

Use diagrams to **find** the answer and to check your intuition. Write the element argument to **justify** it.

The laws of logical equivalence method

The idea: **"$x \in S$" is a logical statement**, so the laws of logical-equivalence-laws[215] apply to it directly. Write out what membership of S means, transform it, and read off membership of T at the end.

Example. Prove that for all sets A and B, $A - (A - B) = A \cap B$.

$$
\begin{aligned}
x \in A - (A - B) &\equiv (x \in A) \wedge (x \notin (A - B)) && \text{by definition of set difference} \\
&\equiv (x \in A) \wedge \sim (x \in (A - B)) && \text{by definition of } \notin \\
&\equiv (x \in A) \wedge \sim ((x \in A) \wedge (x \notin B)) && \text{by definition of set difference} \\
&\equiv (x \in A) \wedge (\sim (x \in A) \vee \sim (x \notin B)) && \text{by De Morgan's law} \\
&\equiv (x \in A) \wedge ((x \notin A) \vee (x \in B)) && \text{by definition of } \in \text{ and } \notin \\
&\equiv ((x \in A) \wedge (x \notin A)) \vee ((x \in A) \wedge (x \in B)) && \text{by the distributive law} \\
&\equiv \mathbf{c} \vee ((x \in A) \wedge (x \in B)) && \text{by the negation law} \\
&\equiv (x \in A) \wedge (x \in B) && \text{by the identity law} \\
&\equiv x \in A \cap B && \text{by the definition of } \cap
\end{aligned}
$$

Two things to copy from the layout. **Every line is justified by name** — the marks are in the justification column as much as the algebra. And only four of the nine steps are logical manipulation at all: De Morgan, distributive, negation and identity. The other five are *definitions* translating set language into logic and back — the three at the top, the last one, and the "$\in$ and $\notin$" line, which sits in the middle of the chain rather than at either end.

Note this method proves the equality **in one pass**, not two. The chain is a string of $\equiv$, so it reads correctly in both directions — which is what saves you the second containment proof the element method would demand.

[215] courses/math1061/logical-equivalence-laws.pdf

Set identities

For all sets A, B and C that are subsets of a universal set U:

	Law	(a)	(b)
1	Commutative	$A \cup B = B \cup A$	$A \cap B = B \cap A$
2	Associative	$(A \cup B) \cup C = A \cup (B \cup C)$	$(A \cap B) \cap C = A \cap (B \cap C)$
3	Distributive	$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$	$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
4	Identity	$A \cup \emptyset = A$	$A \cap U = A$
5	Complement	$A \cup A^c = U$	$A \cap A^c = \emptyset$
6	Double Complement	$(A^c)^c = A$	
7	Idempotent	$A \cup A = A$	$A \cap A = A$
8	Universal Bound	$A \cup U = U$	$A \cap \emptyset = \emptyset$
9	De Morgan's	$(A \cup B)^c = A^c \cap B^c$	$(A \cap B)^c = A^c \cup B^c$
10	Absorption	$A \cup (A \cap B) = A$	$A \cap (A \cup B) = A$
11	Complement of U and $\emptyset$	$U^c = \emptyset$	$\emptyset^c = U$
12	Set Difference	$A - B = A \cap B^c$	

> **Provided in the exam.** These are printed on the *MATH1061/MATH7861 Examination Formula Page* alongside the laws of logical equivalence — see formula-sheet[216]. They do not need memorising; the marks are in picking the right one and naming it.

The correspondence with logical-equivalence-laws[217] is not a coincidence: $\cup$ behaves like $\vee$, $\cap$ like $\wedge$, ^{c} like $\sim$, U like **t** and $\emptyset$ like **c**. Laws 1–11 are the eleven logical equivalences with the symbols swapped, in the same order and under the same names bar the rename of *negation* to *complement* — which is precisely why the previous method works. **Law 12 is the exception**: the formula page's logical equivalences have no entry corresponding to set difference, which is why it has to be cleared out of the way first.

Law 12 is the one to reach for first in almost any problem containing a minus sign: it converts set difference — which none of the other eleven laws mention — into intersection and complement, which all of them do.

[216] courses/math1061/formula-sheet.pdf
[217] courses/math1061/logical-equivalence-laws.pdf

The set identities method

Same result again, this time by transforming the set expression rather than a membership statement.

> **Prove that for all sets A and B, $A - (A - B) = A \cap B$.**

$$\begin{aligned}
A - (A - B) &= A - (A \cap B^c) && \text{by the set difference law (12)} \\
&= A \cap (A \cap B^c)^c && \text{by the set difference law (12)} \\
&= A \cap (A^c \cup (B^c)^c) && \text{by De Morgan's law (9b)} \\
&= A \cap (A^c \cup B) && \text{by the double complement law (6)} \\
&= (A \cap A^c) \cup (A \cap B) && \text{by the distributive law (3b)} \\
&= \emptyset \cup (A \cap B) && \text{by the complement law (5b)} \\
&= A \cap B && \text{by the identity law (4a)}
\end{aligned}$$

Seven lines against the previous method's nine, and no logic notation at all. Two details worth noting:

- **Law 12 is applied twice**, to the inner difference and then the outer one. Clearing *both* minus signs before doing anything else is the move that makes the rest routine.
- The last step cites identity law (4a), $A \cup \emptyset = A$, applied to $\emptyset \cup (A \cap B)$ — the operands are the other way round, so **commutativity (1a) is being used silently**. That is normal practice, but it is worth seeing that the step is really two.

Russell's paradox

When mathematicians wanted to show that all of mathematics could be built on set theory, **Bertrand Russell** discovered a problem.

> Let S be the set of all sets that are not elements of themselves:
>
> $$S = \{A \mid A \text{ is a set and } A \notin A\}$$
>
> Is S an element of itself?
>
> If $S \in S$, then $S \notin S$. If $S \notin S$, then $S \in S$. So both $S \in S$ and $S \notin S$, which is impossible.

The natural objection — *surely a set is never an element of itself?* — is the right instinct but is not available as an answer, because it is exactly the thing the naive theory fails to guarantee. Nothing in "a set is any collection of objects" forbids self-membership, and S is built by a rule

that looks as legitimate as any other. The contradiction is not in S being strange; it is in the assumption that **every describable collection is a set**.

Several ways to define the basic concepts of set theory were found so that Russell's paradox does not arise — modern axiom systems restrict which collections count as sets. For more detail, read pages 419–421 (5th edition) or 378–380 (4th edition) of the textbook. For more set theory generally, the course to take is **MATH3306 Set Theory and Logic**.

See also

- sets-and-set-notation[218] — the definitions and operations being proved about
- logical-equivalence-laws[219] — the laws the second method uses, and the source of the set identities
- proof-techniques[220] — contradiction, contraposition and the general proof shapes
- formula-sheet[221] — what is provided in the exam
- inclusion-exclusion[222] — the identities cited by number to prove the three-set counting rule
- functions-on-general-sets[223] — the next thing built on these definitions
- 2026-09-03-set-properties-and-functions[224] — Lecture 18
- practice-problems[225] — §23 Properties of Sets, with full worked solutions

Recursive Definitions

Defining a sequence, or a set, by saying how to build its members out of members you already have. See sequences-and-summations[226] for the other ways to define a sequence, and strong-induction-and-the-well-ordering-principle[227] for the proof method that recursive definitions almost always call for.

Recursively defined sequences

To define a sequence recursively, two things are needed:

1. **Initial conditions** — the values of some number of initial terms of the sequence.

[218] courses/math1061/sets-and-set-notation.pdf
[219] courses/math1061/logical-equivalence-laws.pdf
[220] courses/math1061/proof-techniques.pdf
[221] courses/math1061/formula-sheet.pdf
[222] courses/math1061/inclusion-exclusion.pdf
[223] courses/math1061/functions-on-general-sets.pdf
[224] courses/math1061/2026-09-03-set-properties-and-functions.pdf
[225] courses/math1061/practice-problems.pdf
[226] courses/math1061/sequences-and-summations.pdf
[227] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

2. **A recurrence relation** — a formula specifying how to calculate the value of a term of the sequence from the values of one or more previous terms.

Neither half is optional, and **the same recurrence relation with different initial conditions can give a completely different sequence**:

Definition	Sequence
$a_1 = 2$ and $a_k = 3a_{k-1}$ for each integer $k \geq 2$	$2, 6, 18, 54, ...$
$b_1 = 7$ and $b_k = 3b_{k-1}$ for each integer $k \geq 2$	$7, 21, 63, 189, ...$

The recurrence is identical; only the seed differs, and the two sequences share no terms.

Checking that a sequence satisfies a recurrence

Given an explicit formula and a candidate recurrence, the check is a one-step calculation: **assume the formula at $k-1$, substitute it into the recurrence, and see whether what comes out is the formula at k.**

For $b_n = 4n + 3$ and the candidate $b_k = 4 + b_{k-1}$:

$$b_k = 4 + b_{k-1} = 4 + \big(4(k-1) + 3\big) = 4k + 3 \quad \checkmark$$

For the candidate $b_k = 4b_{k-1}$, the same substitution gives

$$b_k = 4b_{k-1} = 4\big(4(k-1) + 3\big) = 16k - 16 + 3 = 16k - 13 \quad \times$$

which is not $4k + 3$, so that recurrence is not satisfied.

Reading a recursive definition off an explicit formula

> This section goes explicit → recursive. The reverse trip — recursive → explicit, which is the harder and more useful one — is solving-recurrence-relations[228].

Going the other way — from an explicit formula to a recursive definition — means computing the first few terms, spotting what is done to each term to get the next, then proving the guess.

Factorial. For $n \in \mathbb{Z}^+$, $n! = n(n-1)\cdots(2)(1)$, and $0! = 1$ **by definition**. Worth memorising: the $0! = 1$ convention is what makes formulas involving $n!$ work at $n = 0$ without a special case.

[228] courses/math1061/solving-recurrence-relations.pdf

Example: $a_n = \dfrac{(-1)^n}{n!}$ **for each integer** $n \geq 0$**.**

The first five terms, and the factor taking each to the next:

$$\underbrace{1}_{a_0} \xrightarrow{\times -1} \underbrace{-1}_{a_1} \xrightarrow{\times -\frac{1}{2}} \underbrace{\frac{1}{2}}_{a_2} \xrightarrow{\times -\frac{1}{3}} \underbrace{-\frac{1}{6}}_{a_3} \xrightarrow{\times -\frac{1}{4}} \underbrace{\frac{1}{24}}_{a_4}$$

The multiplier at step n is $-\frac{1}{n}$, suggesting $a_n = -\frac{1}{n} a_{n-1}$. Verifying it against the explicit formula:

Suppose $a_{n-1} = \dfrac{(-1)^{n-1}}{(n-1)!}$. Then

$$a_n = -\frac{1}{n} \cdot a_{n-1} = \frac{(-1)(-1)^{n-1}}{n \cdot (n-1)!} = \frac{(-1)^n}{n!} \quad \checkmark$$

So the recursive definition is

- *initial condition*: $a_0 = 1$
- *recurrence relation*: $a_n = -\dfrac{1}{n} a_{n-1}$ for all $n \geq 1$

Note how the recurrence relation's range starts one past the last initial condition — that is the general rule, and it is what makes the definition cover every term exactly once.

Recursively defined sets

To define a set recursively, **three** things are needed:

1. **Base** — a statement that certain (usually small) objects belong to the set.
2. **Recursion** — rules on how to build new set objects from those objects already known to be in the set.
3. **Restriction** — a statement saying that all objects in the set come from the Base and the Recursion.

The Restriction is the part that is easy to forget and easy to underrate. Without it the Base and Recursion only say what *must* be in the set; the Restriction is what says nothing *else* is, and it is what licenses arguing that a given object is **not** a member.

The set of all binary strings

A **binary string** is a sequence of 0's and 1's. The set B of all binary strings is defined recursively:

- **Base**: the empty string ε is in B.
- **Recursion**: if $s \in B$, then $s0 \in B$ and $s1 \in B$.
- **Restriction**: nothing is in B other than objects defined by the Base and the Recursion.

Every string therefore has a build history from ε, one character at a time — the string 011 is built up as $\varepsilon \to 0 \to 01 \to 011$. Applying the two rules repeatedly generates a binary tree of strings, and a build history is just a path down it from the root:

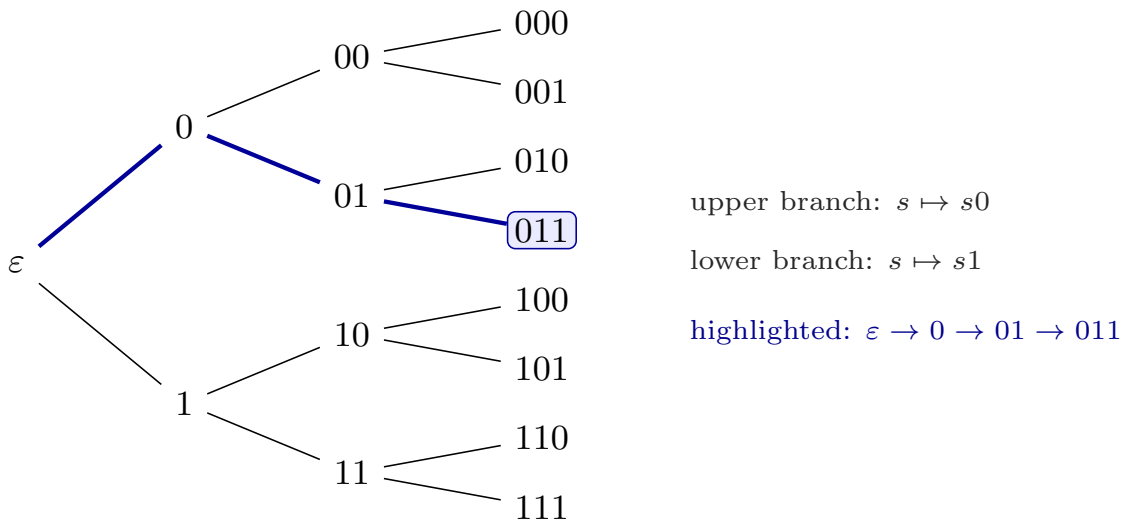


Figure 24: The Recursion applied three times over, drawn the way the lecture drew it: the Base object ε at the root on the left, the two rules fanning rightwards as plain segments with no arrowheads, and each node labelled with the string it is. The upper branch appends a 0 and the lower a 1, so the level a string sits at is its length. **The highlighted path is added here** — the lecture wrote the build history of 011 out as a separate chain rather than marking it on the tree; drawn on the tree it shows what a build history actually is, a route from the Base to the object.

Two things the picture makes plain that the rules alone do not. Every binary string appears **exactly once** in this tree, at depth equal to its length — so for B a build history is unique, and there is no ambiguity about how a given string was made. And the tree only ever grows: neither rule shortens a string, so a property that holds at the root and survives both rules holds everywhere below. That is the shape of argument the Restriction licenses, and it is what the next section turns into a method.

Arguing about membership

For a recursively defined set, the two directions of argument look quite different:

- **To show an object is in the set**, exhibit a build history — a chain from the Base to the object, with each step naming the rule used.
- **To show an object is not in the set**, find a property that the Base has and that every Recursion rule preserves, and observe the object lacks it. This is an induction over the structure of the set, and it works only because of the Restriction.

See also

- solving-recurrence-relations[229] — the other direction: recursive definition to explicit formula, and proving it
- sequences-and-summations[230] · strong-induction-and-the-well-ordering-principle[231] · mathematical-induction[232]
- counting-principles[233] — $n!$ as the number of arrangements of n objects
- 2026-08-31-recursive-definitions[234] — Lecture 15
- practice-problems[235] — §19 Recursive Definitions, with full worked solutions

Sequences and Summations

Standard notation for sequences and summations, and the manipulations — change of variable, splitting off the last term — that every induction proof over a sum relies on. See mathematical-induction[236] for the proofs those manipulations feed into.

Notation

A sequence is an ordered list of terms, written in any of these ways:

$$a_1, a_2, a_3, \ldots \qquad (a_n)_{n\geq 0} \qquad \{a_n\}_{n=1}^{\infty}$$

These are notations for the same *kind* of object, not for the same sequence — note that the middle one starts at $n = 0$ and the other two at $n = 1$. Always read the bound.

[229] courses/math1061/solving-recurrence-relations.pdf
[230] courses/math1061/sequences-and-summations.pdf
[231] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[232] courses/math1061/mathematical-induction.pdf
[233] courses/math1061/counting-principles.pdf
[234] courses/math1061/2026-08-31-recursive-definitions.pdf
[235] courses/math1061/practice-problems.pdf
[236] courses/math1061/mathematical-induction.pdf

The course uses all of these interchangeably and does not privilege one. A recursively defined sequence may be written $\{b_n\}_{n\geq 0}$, and the braces may be dropped entirely for a bare $a_0, a_1, a_2, ...$ Read whichever form is in front of you; do not expect a house standard.

The subscript is the **index**; the bound on the index says where the sequence starts (and, if finite, where it stops). A sum over a range of the index is written

$$\sum_{n=1}^{m} a_n$$

Three ways to define a sequence

By an explicit formula that lets you calculate the value of any particular term directly.

> $a_1, a_2, a_3, ...$ where $a_n = 2^n - 1$, giving $1, 3, 7, 15, 31, ...$

Recursively, by a rule that calculates a term from the value of one or more preceding terms.

> $\{b_n\}_{n\geq 0}$ where $b_0 = 3$ and $b_n = 2 \cdot b_{n-1}$ for $n \geq 1$, giving $3, 6, 12, 24, 48, ...$

The "or more" matters: the Fibonacci numbers are the standard example of a sequence whose rule reaches back **two** terms rather than one. A recursive definition needs both a recurrence relation *and* initial conditions — see recursive-definitions[237] for what each part contributes and how to move between a recursive and an explicit definition.

In words.

> For all positive integers n, the sequence in which the n^{th} term is the sum of the digits of n^2, giving $1, 4, 9, 7, 7, 9, ...$

(Check: $1^2 = 1$, $2^2 = 4$, $3^2 = 9$, $4^2 = 16 \to 7$, $5^2 = 25 \to 7$, $6^2 = 36 \to 9$.)

A sequence cannot be defined by listing its first few terms

Unless you can list *all* of them. Initial terms never pin down a sequence — infinitely many sequences agree on any finite prefix.

What is the next term in the sequence with initial terms $1, 4, 9, 16$?

Definition	Sequence
$a_n = n^2$	$1, 4, 9, 16, 25, 36, ...$
$a_n = n^2 \bmod 20$	$1, 4, 9, 16, 5, 16, 9, ...$

[237] courses/math1061/recursive-definitions.pdf

Both are legitimate, and they disagree from the fifth term on. The Online Encyclopedia of Integer Sequences (https://oeis.org) returns **397** sequences for a search on $1, 4, 9, 16$.

Working with sums

Sums over the same index range add and scale termwise:

$$\sum_{i=m}^{n} a_i \pm \sum_{i=m}^{n} b_i = \sum_{i=m}^{n} (a_i \pm b_i) \qquad\qquad \sum_{i=m}^{n} c\, a_i = c \sum_{i=m}^{n} a_i$$

The second is just factoring out the common c once the sum is written out. The general statement is on the left below and the $c = 2$ case on the right:

$$c\, a_m + c\, a_{m+1} + \cdots + c\, a_n = c\,(a_m + \cdots + a_n) \qquad\qquad 2a_m + 2a_{m+1} + \cdots + 2a_n = 2(a_m + \cdots + a_n)$$

Note the precondition on the first identity: **the two index ranges must match** before the terms can be combined. Making them match is what the change of variable below is for.

Change of variable

Substituting a new index shifts the limits and rewrites the general term. To apply $j = i + 1$ (equivalently $i = j - 1$) to $\displaystyle\sum_{i=0}^{n-1}(2i + 5)$, do three things:

- **lower limit**: $j = 0 + 1 = 1$
- **upper limit**: $j = (n - 1) + 1 = n$
- **general term**: $2i + 5 = 2(j - 1) + 5 = 2j + 3$

$$\sum_{i=0}^{n-1}(2i + 5) = \sum_{j=1}^{n}(2j + 3)$$

The sum is unchanged — only its description moved. Figure 25 lays the two descriptions over the terms they describe, which is what makes that claim checkable rather than a rule to trust.

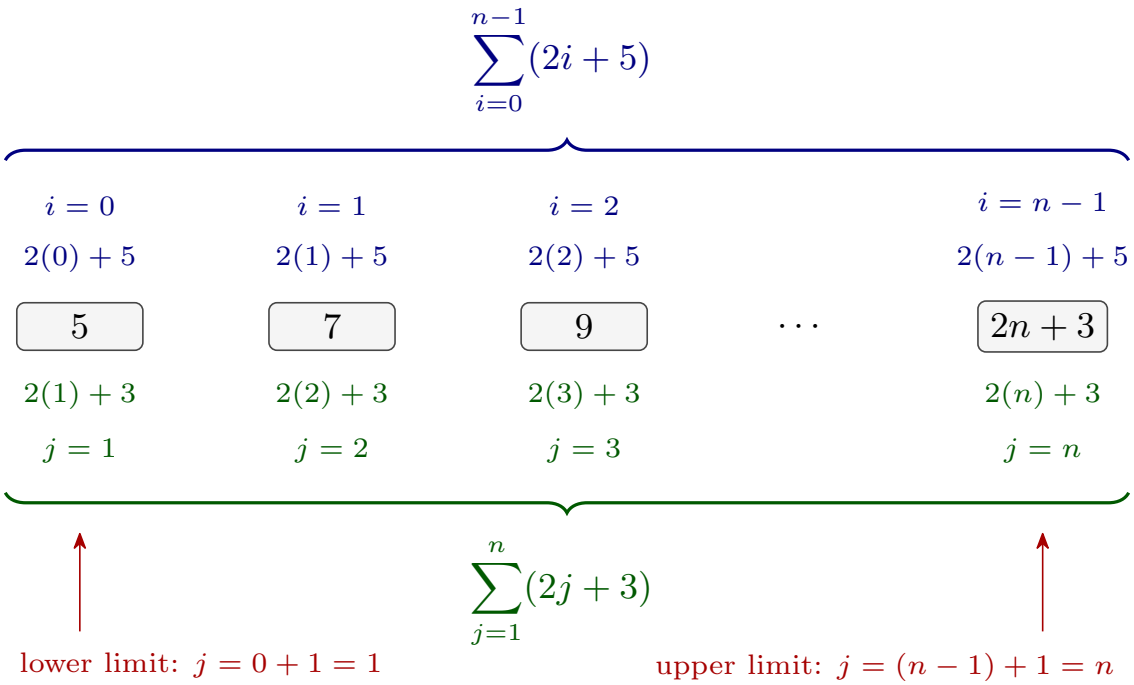


Figure 25: A change of variable relabels, it does not recompute. The boxed row is the list of numbers being added — $5, 7, 9, \ldots, 2n+3$ — and it is identical under both descriptions; only the index written above and below it changes. The three red checks are the three things the substitution has to fix, each attached to the part of the picture it governs.

Splitting off the last term

Writing a sum out and peeling the final term off is the manoeuvre used in almost every induction proof of a summation property, since it is what turns the $P(k+1)$ side into "the $P(k)$ side, plus one more term":

$$\sum_{i=1}^{n+1}(3i+2) = \underbrace{(3\cdot 1+2)+(3\cdot 2+2)+\cdots+(3n+2)}_{i\,=\,1\,\ldots\,n} + \underbrace{(3(n+1)+2)}_{i\,=\,n+1}$$

$$= \sum_{i=1}^{n}(3i+2) \;+\; (3(n+1)+2)$$

The same sum can also be split further back — peeling off the last *two* terms, or shifting the whole index — which is why a single sum has many equal-looking rewrites.

See also

- mathematical-induction[238] — the proof method these manipulations serve
- recursive-definitions[239] · solving-recurrence-relations[240] — arithmetic and geometric sequences, and finding explicit formulas
- 2026-08-24-sequences-and-mathematical-induction[241] — Lecture 13
- practice-problems[242] — §16 Sequences, with full worked solutions

Sets and Set Notation

The language the rest of mathematics is written in: what a set is, the difference between belonging to one and being contained in one, and the operations that build new sets from old. See proving-set-properties[243] for the proof methods that go with these definitions, and functions-on-general-sets[244] for what gets built on top of them.

[238] courses/math1061/mathematical-induction.pdf
[239] courses/math1061/recursive-definitions.pdf
[240] courses/math1061/solving-recurrence-relations.pdf
[241] courses/math1061/2026-08-24-sequences-and-mathematical-induction.pdf
[242] courses/math1061/practice-problems.pdf
[243] courses/math1061/proving-set-properties.pdf
[244] courses/math1061/functions-on-general-sets.pdf

Writing a set down

Two ways, both used constantly:

- **By listing the elements**, inside braces: $\{1, 2, 3\}$, $\{a\}$, $\{\emptyset, \{\emptyset\}\}$. An infinite list gets an ellipsis: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
- **By a defining condition** — *set-builder* notation: $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$, read "the set of integers n such that $n \equiv 2 \bmod 8$".

Both a vertical bar and a colon are used as the "such that" separator, interchangeably. $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and $\{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$ take the bar; $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x + 1\}$ and $f^{-1}(B) = \{x \in X : f(x) \in B\}$ take the colon. Read either as "such that"; nothing turns on which one is written.

Two conventions worth naming, because everything below relies on them: **sets take capital italic letters** (A, B, C, S, T, X, Y), with U reserved for the universal set, and **elements take lower case** (x, y, t, n). And $|A|$ denotes the **cardinality** of A — the number of elements it has (for infinite sets, where "number of elements" needs care, see cardinality[245]).

"Is an element of" versus "is a subset of"

> **Warning.** Take care with the distinction between *is an element of* ($\in$) and *is a subset of* ($\subseteq$).

This is the single most common source of error in the whole topic, and it is worth being blunt about why: the two relate **different kinds of thing**.

	Reads	Left-hand side is	Right-hand side is
$x \in A$	x is an element of A	an **object**	a **set**
$A \subseteq B$	A is a subset of B	a **set**	a **set**

Is $\mathbb{Z} \in \mathbb{Q}$? False. The elements of $\mathbb{Q}$ are rational *numbers*, and $\mathbb{Z}$ is not a number — it is a set of numbers. The true statement in the neighbourhood is $\mathbb{Z} \subseteq \mathbb{Q}$.

The instinct behind the mistake ("but aren't all integers rational?") is right; it is the symbol that is wrong. "All integers are rational" is exactly the claim $\mathbb{Z} \subseteq \mathbb{Q}$.

The same care applies one level down: **a single element is not the same as the set containing that element**, so $2 \neq \{2\}$.

[245] courses/math1061/cardinality.pdf

Worked: true or false?

	Statement		Why
a)	$4 \in \{4\}$	**True**	$\{4\}$ contains 4 as an element
b)	$4 \in \{\{4\}\}$	**False**	$\{\{4\}\}$ does not contain 4 as an element — it contains $\{4\}$ as an element
c)	$\{4\} \in \{2, 3, 4\}$	**False**	$\{2, 3, 4\}$ does not contain $\{4\}$ as an element — it contains 4 as an element

Each false line becomes true if you swap the symbol or the braces, which is the point of the exercise. In (c), $\{4\} \subseteq \{2, 3, 4\}$ **is** true.

The reliable technique: **write out the set's elements and ask whether the left-hand object is literally one of the things in the list.** For $\{\{4\}\}$ that list is a single item, the set $\{4\}$ — and 4 is not on it.

Subsets and proper subsets

> A set S is a **subset** of a set T, written $S \subseteq T$, if every element in S is also in T. Formally, $\forall x$, if $x \in S$ then $x \in T$.
>
> A set S is a **proper subset** of T, written $S \subset T$, if $S \subseteq T$ **and** there is an element in T that is not in S.

So $\subset$ is $\subseteq$ plus "and they are not equal" — exactly parallel to $<$ against $\leq$ for numbers.

	Holds	Fails
$\subseteq$	$\mathbb{Z} \subseteq \mathbb{Q}$, and $\mathbb{Z} \subseteq \mathbb{Z}$	
$\subset$	$\mathbb{Z} \subset \mathbb{Q}$	$\mathbb{Z} \not\subset \mathbb{Z}$

A set is always a subset of itself and never a *proper* subset of itself — that single line is the whole difference between the two symbols.

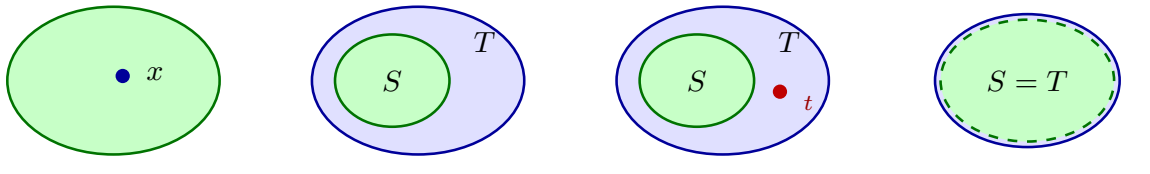


Figure 26: The four situations the symbols distinguish. An element sits inside a set; a subset is a set inside a set; a proper subset leaves something over; and equality is containment holding both ways at once. The contained set is green and the containing set pale blue, with elements as small blue dots; the red dot is the element that keeps the containment proper.

Proving one set is a subset of another

> To prove $S \subseteq T$, consider an **arbitrary** element of S and show it is also in T. That is: **suppose $x \in S$, and prove $x \in T$.**

This is the *element method*, and it is used so heavily that proving-set-properties[246] treats it in full. The word doing the work is "arbitrary" — you may assume nothing about x beyond membership of S, which is what makes the one argument cover every element at once.

Worked. Let $D = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and let E be the set of even integers, i.e. $E = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 2\}$. Prove $D \subseteq E$.

> *Proof.* Let $x \in D$. Then $x \equiv 2 \pmod 8$, so there exists $k \in \mathbb{Z}$ such that
>
> $$x = 8k + 2 = 2(4k + 1) + 0$$
>
> Since $4k + 1 \in \mathbb{Z}$, we have $x \equiv 0 \pmod 2$, and therefore $x \in E$. Thus $D \subseteq E$. ■

Rewriting $8k + 2$ as $2(4k + 1)$ is the entire proof — see modular-arithmetic[247] for the definition being applied.

Is $D \subset E$? Yes. We have $D \subseteq E$, and $4 \in E$ while $4 \notin D$ (since $4 \not\equiv 2 \bmod 8$), so the containment is proper. Note that upgrading $\subseteq$ to $\subset$ needs **one** witness, not a general argument.

[246] courses/math1061/proving-set-properties.pdf
[247] courses/math1061/modular-arithmetic.pdf

When are two sets equal?

For sets S and T, $S = T$ means $\forall x$, $x \in S$ **if and only if** $x \in T$.

Recall that $S \subseteq T$ means $\forall x$, if $x \in S$ then $x \in T$. Since $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p)$, it follows that

$$S = T \quad \text{is logically equivalent to} \quad (S \subseteq T) \wedge (T \subseteq S)$$

So **to prove two sets are equal, do two separate proofs**:

- Suppose $x \in S$, and prove $x \in T$. This shows $S \subseteq T$.
- Suppose $x \in T$, and prove $x \in S$. This shows $T \subseteq S$.

Together these give $S = T$. This is not a convention but a consequence — the double containment argument is just the biconditional law of logical-equivalence-laws[248] read through the definition of $\subseteq$, which is why "prove both directions" is never optional.

The empty set

$\emptyset = \{\ \}$ — the set with no elements.

Why is $\emptyset \subseteq A$ for every set A? Because "$\forall x$, if $x \in \emptyset$ then $x \in A$" is true for every set A. The hypothesis $x \in \emptyset$ is never satisfied, and a conditional with a false hypothesis is true — so the statement holds **vacuously**. See conditional-statements[249] for that truth-table row, which is doing all the work here.

Do not confuse this with $\emptyset \in A$. Some sets do contain the empty set as an element; many do not. $\emptyset \subseteq A$ is a theorem about every set; $\emptyset \in A$ is a claim about one particular set that usually fails.

Why is $A \subseteq A$ for every set A? Because "$\forall x$, if $x \in A$ then $x \in A$" is true for every set A — this one for the opposite reason, that the conclusion simply restates the hypothesis.

[248] courses/math1061/logical-equivalence-laws.pdf
[249] courses/math1061/conditional-statements.pdf

There is only one empty set

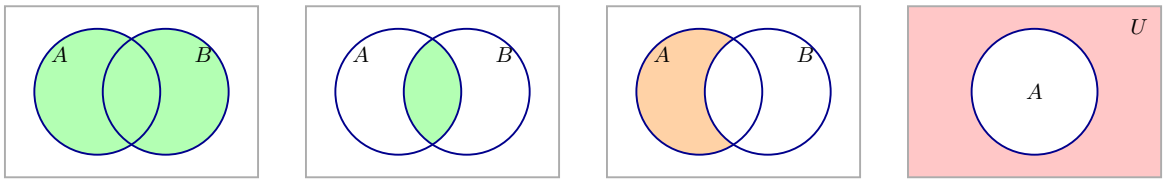
Lemma. There is only one empty set.

Proof (by contradiction). Suppose $\emptyset_1$ and $\emptyset_2$ are distinct sets each having no elements, so $\emptyset_1 \neq \emptyset_2$. Since $\emptyset_1$ has no elements, it is a subset of $\emptyset_2$; that is, $\emptyset_1 \subseteq \emptyset_2$. Also, since $\emptyset_2$ has no elements, $\emptyset_2 \subseteq \emptyset_1$. Thus $\emptyset_1 = \emptyset_2$ by definition of set equality — contradicting the supposition. ■

This is why we say *the* empty set and write a single symbol for it. The proof is a neat demonstration of the double-containment criterion doing real work: both containments come free from vacuous truth, and equality falls out.

Unions and intersections

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\} \qquad A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$



$A \cup B$ $A \cap B$ $A - B$ (also written $A \setminus B$) $A^c = U - A$

Figure 27: The four operations as shaded regions. Union takes everything in either circle, intersection only the overlap, difference removes B from A, and the complement is everything in the universe outside A — which is why a complement is only meaningful once the universe U is fixed. The enclosing rectangle is that universe.

Worked. Let $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 4\}$ and $A_3 = \{3, 4, 5\}$.

$$A_1 \cup A_2 = \{1, 2, 3, 4\} \qquad A_1 \cap A_2 = \{1, 2\} \qquad A_1 \cap A_3 = \{3\} \qquad A_2 \cap A_3 = \{4\}$$

Indexed over all three:

$$\bigcup_{i=1}^{3} A_i = A_1 \cup A_2 \cup A_3 = \{1, 2, 3, 4, 5\} \qquad \bigcap_{i=1}^{3} A_i = (A_1 \cap A_2) \cap A_3 = \{1, 2\} \cap \{3, 4, 5\} = \emptyset$$

Worth noticing: **the three sets intersect pairwise in a non-empty set every time, and yet the triple intersection is empty.** Pairwise overlap does not survive to the whole family, so an indexed intersection has to be computed, not inferred.

Indexed families

$$\bigcup_{i\in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{at least one } i \in I\} \qquad \bigcap_{i\in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{every } i \in I\}$$

These extend to infinite index sets unchanged, which is where they earn their keep.

Worked, over $i = 0, 1, 2, \ldots$:

$$\bigcup_{i=0}^{\infty} \{i, -i\} = \{0\} \cup \{1, -1\} \cup \{2, -2\} \cup \cdots = \{\ldots, -2, -1, 0, 1, 2, \ldots\} = \mathbb{Z}$$

$$\bigcap_{i=0}^{\infty} [-i,\, i] = \{0\}$$

recalling the interval notation $[a, b] = \{x \in \mathbb{R} \mid a \le x \le b\}$.

The intersection is the interesting one. The intervals **grow** as i increases, so the intersection is pinned by the *smallest* of them, the $i = 0$ term $[0, 0] = \{0\}$. Every larger interval contains 0, so nothing is lost, and nothing else survives.

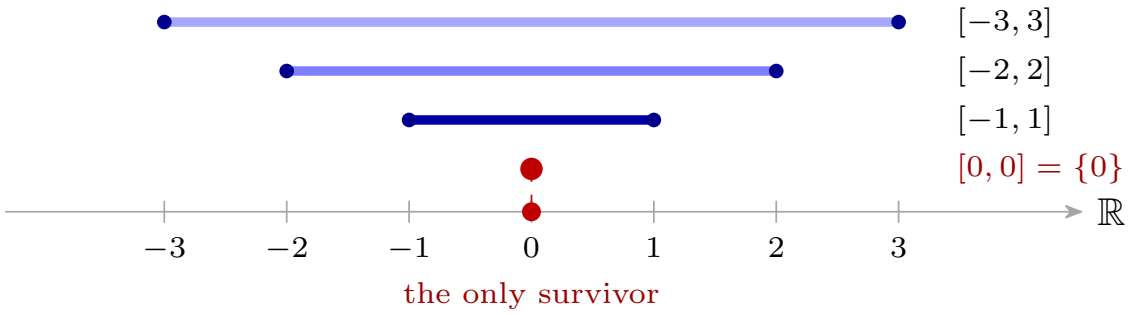


Figure 28: An intersection over an increasing family is decided by its smallest member. Each interval contains the one below it, so the only real number lying in all of them is the single point the innermost interval contains. The intervals sit above the number line, with a filled dot at each closed endpoint.

Set difference and complement

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

Both are drawn in Figure 27 above.

The backslash and the minus sign mean the same thing: $A - B$ can equally be written $A \setminus B$. Different textbooks pick different ones; there is no distinction to learn.

The **complement** A^c is the set difference from the universal set U under discussion: $A^c = U - A$. It is only meaningful once U is fixed, so a complement always sits inside a stated universe.

The power set

$\mathcal{P}(A)$ is the set of **all subsets** of A.

Worked. Let $S = \{1, 2, 3\}$. Then

$$\mathcal{P}(S) = \{\, \emptyset,\ \{1\},\ \{2\},\ \{3\},\ \{1,2\},\ \{1,3\},\ \{2,3\},\ \{1,2,3\} \,\}$$

Note that the elements of $\mathcal{P}(S)$ are **sets**, which resets the $\in$ / $\subseteq$ trap one level up:

Statement		Why
$\{1,2\} \in \mathcal{P}(S)$	**True**	$\{1,2\}$ is one of the eight things listed
$\{1,2\} \subseteq \mathcal{P}(S)$	**False**	that would need 1 and 2 themselves to be elements of $\mathcal{P}(S)$, i.e. to be subsets of S — and they are numbers, not sets
$\{\{1,2\}\} \subseteq \mathcal{P}(S)$	**True**	the one element it has, $\{1,2\}$, is in $\mathcal{P}(S)$

Also worth recording as a standing fact: since $\emptyset \subseteq A$ for every set A, it follows that $\emptyset \in \mathcal{P}(A)$ for every set A. Every power set is non-empty, including $\mathcal{P}(\emptyset)$.

Fact. If T is a **finite** set with n elements, then $|\mathcal{P}(T)| = 2^n$.

The finiteness matters — the count is meaningless otherwise. The 2^n comes from building a subset by making n independent in/out choices. Sorting the same subsets by size instead gives $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ (binomial-coefficients[250]).

[250] courses/math1061/binomial-coefficients.pdf

Worked: is $\{1, 3, -1\} \subset \mathcal{P}(\mathbb{Z})$?

False, and the reasoning is the $\in/\subseteq$ distinction again, run carefully:

- $1, 3, -1 \in \mathbb{Z}$, so $\{1, 3, -1\} \subseteq \mathbb{Z}$.
- Therefore $\{1, 3, -1\} \in \mathcal{P}(\mathbb{Z})$ — it is one of the subsets of $\mathbb{Z}$, hence an *element* of the power set.
- So $\{1, 3, -1\} \not\subset \mathcal{P}(\mathbb{Z})$: for that, its **elements** 1, 3 and -1 would have to be elements of $\mathcal{P}(\mathbb{Z})$, i.e. subsets of $\mathbb{Z}$ — and they are integers, not sets.

The statement is off by exactly one level, which is the characteristic failure mode with power sets.

Worked: power sets of power sets

Building up from the empty set, with the 2^n fact as a running check:

	Value	$\lvert\cdot\rvert$ of the input	Check
$\mathcal{P}(\{a\})$	$\{\emptyset,\ \{a\}\}$	$\lvert\{a\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\emptyset)$	$\{\emptyset\}$	$\lvert\emptyset\rvert = 0$	$2^0 = 1$ ✓
$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$	$\{\emptyset,\ \{\emptyset\}\}$	$\lvert\{\emptyset\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset, \{\emptyset\}\})$	$\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\}\}$	$\lvert\{\emptyset, \{\emptyset\}\}\rvert = 2$	$2^2 = 4$ ✓

$\mathcal{P}(\emptyset) = \{\emptyset\}$ is the line to get right: the empty set has exactly one subset — itself — so its power set has **one** element and is **not** empty. Counting the elements at each stage and checking against 2^n is the cheapest way to catch a dropped or duplicated brace.

Cartesian products

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

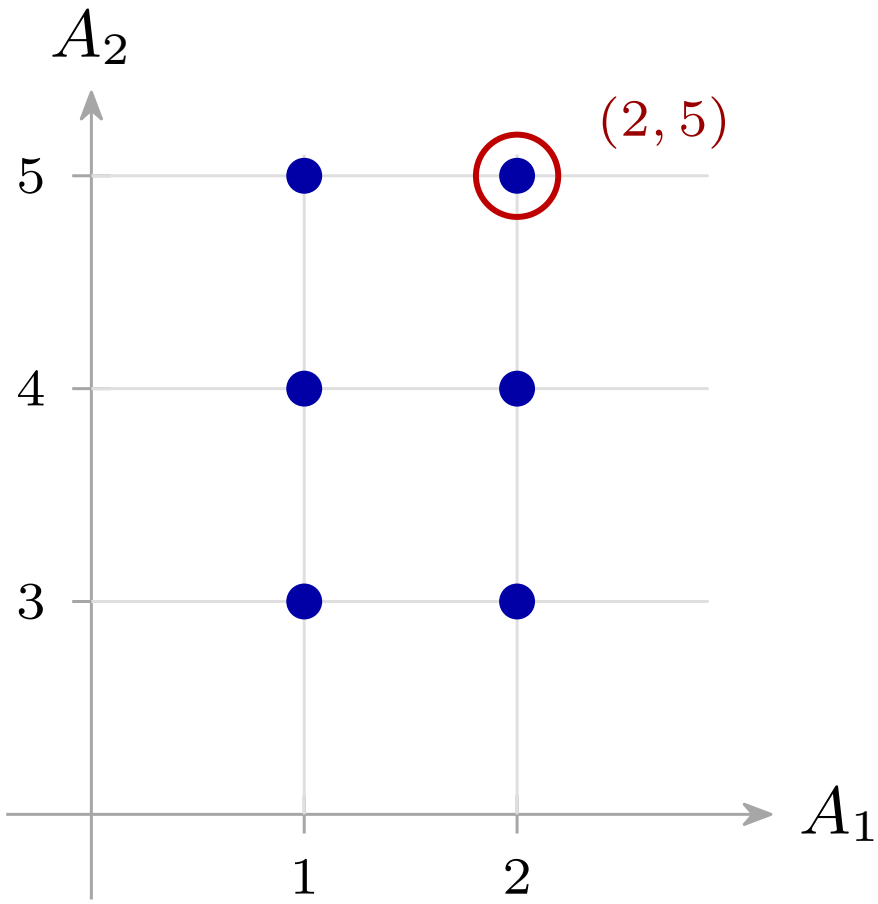
the set of **ordered pairs** with first coordinate from A and second from B.

Worked. $A_1 = \{1, 2\}$, $A_2 = \{3, 4, 5\}$, $A_3 = \{6\}$.

$$A_1 \times A_2 = \{(1, 3), (1, 4), (1, 5), (2, 3), (2, 4), (2, 5)\}$$

$$A_1 \times A_2 \times A_3 = \{(1, 3, 6), (1, 4, 6), (1, 5, 6), (2, 3, 6), (2, 4, 6), (2, 5, 6)\}$$

Worked. Let $S = \{a, b, c\}$ and $T = \{c, d\}$.



$$|A_1 \times A_2| = |A_1| \cdot |A_2| = 2 \times 3 = 6$$

Figure 29: A Cartesian product laid out as a grid: one row per element of the first set, one column per element of the second, one ordered pair at every crossing. The rectangular shape is the counting fact — the number of pairs is the product of the two sizes.

- $(d, c) \notin S \times T$, since $d \notin S$ — the **order matters**, and d is disqualified as a first coordinate.
- $(c, d) \in S \times T$, since $c \in S$ and $d \in T$.
- $S \times T$ contains $3 \times 2 = 6$ elements.

The familiar case is $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$, usually written $\mathbb{R}^2$ — the plane is a Cartesian product, which is where the name comes from.

Two facts:

- If $A = \emptyset$ or $B = \emptyset$ then $A \times B = \emptyset$ — there is no way to choose a coordinate from an empty set.
- For finite sets, $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

  Notation clash to be aware of. (a, b) can mean an **ordered pair**, and (a, b) can also mean an **open interval** — the real numbers x with $a < x < b$. Nothing in the symbols distinguishes them; only the context does.

Partitions

A finite or infinite collection of **non-empty** sets $\{A_1, A_2, A_3, \dots\}$ is a **partition** of a set A if and only if

$$A = A_1 \cup A_2 \cup A_3 \cup \cdots \qquad \text{and} \qquad A_i \cap A_j = \emptyset \text{ for each } i, j \geq 1,\ i \neq j$$

Three conditions, all of which are checkable and all of which get tested: the pieces are **non-empty**, they **cover** A, and they are **pairwise disjoint**.

Examples over $\mathbb{Z}$:

- $\{E, O\}$, where E is the even integers and O the odd integers, is a partition of $\mathbb{Z}$.
- $\{\{0\},\ \mathbb{Z}^+,\ \mathbb{Z}^-\}$ is another partition of $\mathbb{Z}$ — a set can be partitioned in many ways.

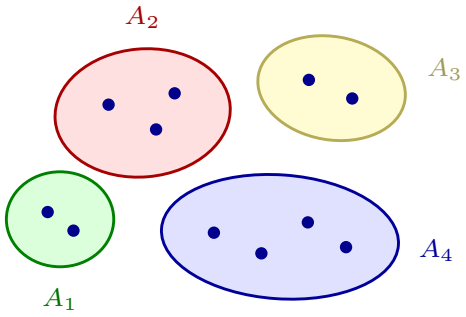
Worked: a collection that fails

Let $S = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\}$, let $T = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4\}$, and let $R = S \cup T$. **Is $\{S, T\}$ a partition of R?**

No. The covering condition holds by construction — $R = S \cup T$ is how R was defined. But disjointness fails:

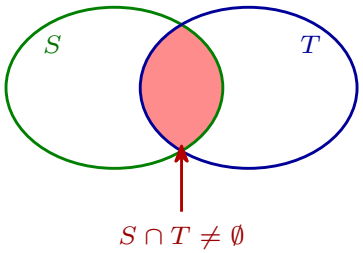
$$10 = 3(3) + 1 \ \Rightarrow\ 10 \equiv 1 \pmod 3 \ \Rightarrow\ 10 \in S$$

$$10 = 4(2) + 2 \ \Rightarrow\ 10 \equiv 2 \pmod 4 \ \Rightarrow\ 10 \in T$$



a partition of A

$A = A_1 \cup A_2 \cup A_3 \cup A_4$, pairwise disjoint



not a partition of R

$R = S \cup T$, but the pieces overlap

Figure 30: A partition cuts a set into non-empty pieces that cover it with no overlap — every element lands in exactly one piece. Failing any one of the three conditions is enough to disqualify a collection. On the left is a partition: separate closed curves, one per piece, each holding its elements as dots. On the right, two pieces share an element, so the collection is not a partition.

so $10 \in S \cap T$ and $S \cap T \neq \emptyset$. Therefore $\{S, T\}$ is **not** a partition of R.

A single witness settles it — disjointness is a universal claim, so one counterexample is a complete disproof.

Worked: two partitions of $\mathbb{Z} \times \mathbb{Z}$

Any rule that sorts every pair into exactly one bucket works. Two independent ways:

By the sign of the first coordinate.

$$P = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \geq 0\} \qquad N = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a < 0\}$$

$\{N, P\}$ is a partition of $\mathbb{Z} \times \mathbb{Z}$ — every integer a is either ≥ 0 or < 0, never both.

By the parity of the second coordinate.

$$E = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 0 \pmod 2\} \qquad O = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid b \equiv 1 \pmod 2\}$$

$\{E, O\}$ is another partition of $\mathbb{Z} \times \mathbb{Z}$.

The recipe generalises: **take any property that every element either has or lacks, and the two resulting sets partition the whole** — provided neither comes out empty. That connection is made exact by equivalence relations: every partition is the set of classes of one, and the other way round (equivalence-classes-and-partitions[251]).

[251] courses/math1061/equivalence-classes-and-partitions.pdf

See also

- proving-set-properties[252] — the element method, the set identities, and proofs about these operations
- functions-on-general-sets[253] — functions defined as subsets of a Cartesian product
- equivalence-classes-and-partitions[254] — partitions as the classes of an equivalence relation
- modular-arithmetic[255] — the congruence sets used throughout the worked examples
- counting-principles[256] · counting-selections[257] — $|A \times B| = |A| \times |B|$ as the multiplication rule, and $\binom{n}{r}$, the number of r-element subsets of an n-element set
- inclusion-exclusion[258] · probability[259] — the size of a union of sets that overlap, with De Morgan's law for "neither", and events as subsets of a sample space
- pigeonhole-principle[260] — a partition as the set of pigeonholes
- conditional-statements[261] · logical-equivalence-laws[262] — vacuous truth, and the biconditional behind set equality
- 2026-09-03-set-theory-definitions[263] — Lecture 17
- practice-problems[264] — §21 Set Theory Definitions, with full worked solutions
- practice-problems[265] — §22 More Definitions and Examples of Sets

Solving Recurrence Relations

recursive-definitions[266] builds a sequence out of its own earlier terms. This note goes the other way: given a recursive definition, find an **explicit formula** for the n^{th} term, and prove the formula is right. See mathematical-induction[267] and strong-induction-and-the-well-ordering-principle[268] for the proof machinery the second method leans on.

[252] courses/math1061/proving-set-properties.pdf
[253] courses/math1061/functions-on-general-sets.pdf
[254] courses/math1061/equivalence-classes-and-partitions.pdf
[255] courses/math1061/modular-arithmetic.pdf
[256] courses/math1061/counting-principles.pdf
[257] courses/math1061/counting-selections.pdf
[258] courses/math1061/inclusion-exclusion.pdf
[259] courses/math1061/probability.pdf
[260] courses/math1061/pigeonhole-principle.pdf
[261] courses/math1061/conditional-statements.pdf
[262] courses/math1061/logical-equivalence-laws.pdf
[263] courses/math1061/2026-09-03-set-theory-definitions.pdf
[264] courses/math1061/practice-problems.pdf
[265] courses/math1061/practice-problems.pdf
[266] courses/math1061/recursive-definitions.pdf
[267] courses/math1061/mathematical-induction.pdf
[268] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

Two ways of writing the same sequence

Every sequence here can be described twice over, and the two descriptions are worth naming precisely because the whole topic is moving between them:

	Shape	What it lets you do
Recurrence relation	$a_k = \dots a_{k-1} \dots$	get the next term from the ones before it
Explicit formula	$a_n = \dots n \dots$	get *any* term without computing the others

The subscript is the tell. A rule written in k that mentions a_{k-1} is a recurrence relation; a rule written in n that mentions only n is an explicit formula.

Arithmetic and geometric sequences

The two standard families, in both forms — for a sequence $a_0, a_1, a_2, \dots$:

	Recurrence relation	Explicit formula
Arithmetic	$a_k = a_{k-1} + d$ for integers $k \geq 1$	$a_n = a_0 + dn$ for integers $n \geq 0$
Geometric	$a_k = r \cdot a_{k-1}$ for integers $k \geq 1$	$a_n = a_0 \cdot r^{\,n}$ for integers $n \geq 0$

d is the **common difference** and r the **common ratio**. Both explicit formulas are the recurrence applied n times from a_0, which is why the index of the seed and the exponent agree: a_n is n steps away from a_0.

Worked the other way, from terms to a formula: $2, 6, 18, 54, \dots$ multiplies by 3 each step, so $r = 3$; the seed is $a_0 = 2$; hence $a_n = 2 \cdot 3^{\,n}$.

Telling them apart

Deciding which family a run of terms belongs to is a matter of computing the gaps both ways, not of eyeballing.

Do $\frac{5}{8}, \frac{5}{2}, 10$ sit in an arithmetic sequence, a geometric one, both, or neither?

Put everything over the same denominator — $\frac{5}{8}, \frac{20}{8}, \frac{80}{8}$ — and both tests become easy:

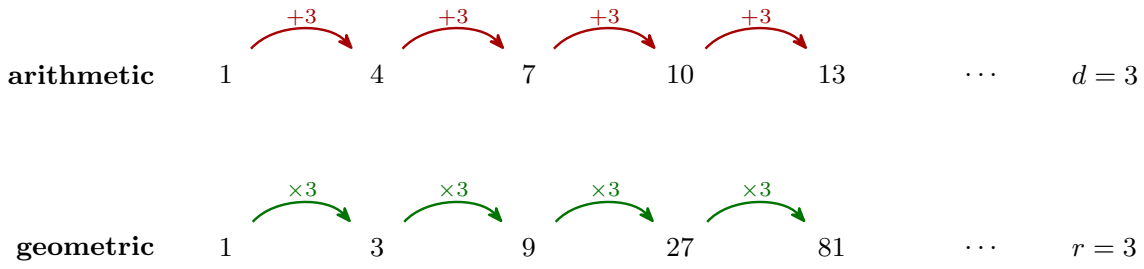


Figure 31: The two families as operations between consecutive terms. Arithmetic adds the same d at every step; geometric multiplies by the same r. Reading a sequence means testing the gaps: constant differences means arithmetic, constant ratios means geometric.

Test	First gap	Second gap	Verdict
Differences	$\frac{20}{8} - \frac{5}{8} = \frac{15}{8}$	$\frac{80}{8} - \frac{20}{8} = \frac{60}{8}$	not equal — **not arithmetic**
Ratios	$\frac{5}{2} \div \frac{5}{8} = 4$	$10 \div \frac{5}{2} = 4$	equal — **geometric**, $r = 4$

So the answer is *geometric only*. The common trap is "both": a sequence that passes the ratio test has no obligation to pass the difference test, and here it plainly fails it.

Do $2, 2, 2$? This one is **both**. The differences are all 0, so it is arithmetic with $d = 0$; the ratios are all 1, so it is geometric with $r = 1$. It is **a constant sequence** $a_n = c$, which is what you get from $d = 0$ on one side and $r = 1$ on the other. The constant sequences are the *whole* of the overlap and not merely examples of it: $a_0 + dn$ and $a_0 r^n$ can agree for every n only if $d = 0$, and then both are constant.

> One convention worth knowing: many texts require $a_0 \neq 0$ and $r \neq 0$ for a geometric sequence, which excludes the all-zeros sequence $0, 0, 0, \ldots$ — every r satisfies $0 = r \cdot 0$, so the common ratio would not be determined. $2, 2, 2$ is unaffected.

From a recursive definition to an explicit formula

The workflow is always the same three steps:

1. **Calculate** the first few terms from the recursive definition.
2. **Guess** an explicit formula that fits them.
3. **Prove** the guess is correct.

Step 3 is not optional, and it is the whole difficulty: any finite run of terms is consistent with infinitely many formulas (see sequences-and-summations[269] on why listing terms never defines a sequence). Two methods are available.

	Method 1	Method 2
What you show	the formula gives the right initial conditions, *and* satisfies the recurrence relation	the formula holds for every n, by (strong) mathematical induction
In a word	quicker	rigorous

Why Method 1 is a proof and not just a check

Method 1 can look like it is only testing a couple of cases, so it is worth seeing why it settles the matter. A recursive definition **determines its sequence uniquely**: the initial conditions fix the first terms, and the recurrence relation then forces every later one. So if your formula reproduces the initial conditions and obeys the same recurrence, it generates the same sequence term by term — there is nowhere for the two to diverge. That is the entire content of Method 1, and it is why the two checks it makes are exactly the two halves of the definition.

Method 2 makes that argument explicitly rather than appealing to it, which is why it is the more rigorous of the two and the one to use when a question says "prove by induction".

The Method 1 template

Given a guess $a_n = f(n)$:

- **Initial conditions.** Substitute the seed index into f and check it returns the stated value. One check per initial condition.
- **Recurrence relation.** Write down both sides separately, substituting the guess wherever an earlier term appears, and show they agree:

$$\text{LHS} = a_k = f(k) \qquad \text{RHS} = (\text{the recurrence, with } f(k-1),\ f(k-2),\ \ldots \text{ substituted})$$

Set the two sides out under the labels **LHS** and **RHS** and meet in the middle. That keeps you from the circularity of starting with what you are trying to prove.

[269] courses/math1061/sequences-and-summations.pdf

The Method 2 template

Take $P(n)$ to be the predicate $a_n = f(n)$ and run an induction. Which induction depends on the recurrence:

The recurrence reaches back	Use	Basis step needs
one term (a_{k-1})	ordinary induction (MI)	one base case
two or more terms ($a_{k-1}, a_{k-2}, \ldots$)	strong induction (SMI)	one base case per initial condition

The rule is not arbitrary: to get $P(k+1)$ from a recurrence mentioning a_{k-1}, you need $P(k-1)$ as well as $P(k)$, and only the strong hypothesis hands you both.

Worked examples

A recurrence reaching back one term

> $c_1 = 1$ and $c_k = c_{k-1} + 2^k$ for each integer $k \geq 2$. Is this the sequence $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$?

Method 1.

Initial condition ($n = 1$): $c_1 = 2^{1+1} - 3 = 4 - 3 = 1$

Recurrence relation:

$$\text{LHS} = c_k = 2^{k+1} - 3$$

$$\text{RHS} = c_{k-1} + 2^k = (2^{(k-1)+1} - 3) + 2^k = 2^k + 2^k - 3 = 2(2^k) - 3 = 2^{k+1} - 3$$

LHS = RHS, so the formula satisfies the recurrence. **The statement is true.**

Method 2. Let $P(n)$ be the predicate $c_n = 2^{n+1} - 3$.

Basis step. $c_1 = 1$ by the recursive definition, and $2^{1+1} - 3 = 4 - 3 = 1$, so $P(1)$ is true.

Inductive hypothesis. Suppose $P(k)$ is true for some integer $k \geq 1$, i.e. $c_k = 2^{k+1} - 3$. Then

$$c_{k+1} = c_k + 2^{k+1} = (2^{k+1} - 3) + 2^{k+1} = 2(2^{k+1}) - 3 = 2^{k+2} - 3$$

so $P(k+1)$ is true. Hence by mathematical induction $c_n = 2^{n+1} - 3$ for each integer $n \geq 1$. ■

Note the shape of the inductive step: substitute the recurrence, then the hypothesis, then collect. The two 2^{k+1} terms combining into 2^{k+2} is the only real move.

A recurrence reaching back two terms

$b_0 = 0$, $b_1 = 1$ and $b_k = \frac{1}{2}(b_{k-1} + b_{k-2} + 1) + 3(k-1)$ for each integer $k \geq 2$.

Calculating terms. Each one uses the two before it:

$$b_2 = \tfrac{1}{2}(1 + 0 + 1) + 3(1) = 1 + 3 = 4$$
$$b_3 = \tfrac{1}{2}(4 + 1 + 1) + 3(2) = 3 + 6 = 9$$
$$b_4 = \tfrac{1}{2}(9 + 4 + 1) + 3(3) = 7 + 9 = 16$$

giving $0, 1, 4, 9, 16, \ldots$ — **guess $b_n = n^2$ for all integers $n \geq 0$.**

Method 1.

Initial conditions: $b_0 = 0^2 = 0$ and $b_1 = 1^2 = 1$ — two conditions, two checks.

Recurrence relation:

$$\text{LHS} = b_k = k^2$$

$$\begin{aligned}
\text{RHS} &= \tfrac{1}{2}((k-1)^2 + (k-2)^2 + 1) + 3(k-1) \\
&= \tfrac{1}{2}(k^2 - 2k + 1 + k^2 - 4k + 4 + 1) + 3k - 3 \\
&= \tfrac{1}{2}(2k^2 - 6k + 6) + 3k - 3 \\
&= (k^2 - 3k + 3) + 3k - 3 \\
&= k^2
\end{aligned}$$

LHS = RHS, so the explicit formula satisfies the recurrence relation.

Method 2, by strong induction — two terms back, so SMI and two base cases.

Basis step. $b_0 = 0$ and $0^2 = 0$, so $P(0)$ holds; $b_1 = 1$ and $1^2 = 1$, so $P(1)$ holds.

Inductive hypothesis. Suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are each true. Then

$$\begin{aligned}
b_{k+1} &= \tfrac{1}{2}(b_k + b_{k-1} + 1) + 3((k+1) - 1) \\
&= \tfrac{1}{2}(k^2 + (k-1)^2 + 1) + 3k \\
&= \tfrac{1}{2}(k^2 + k^2 - 2k + 1 + 1) + 3k \\
&= \tfrac{1}{2}(2k^2 - 2k + 2) + 3k \\
&= k^2 - k + 1 + 3k \\
&= k^2 + 2k + 1 = (k+1)^2
\end{aligned}$$

so $P(k+1)$ is true, and by SMI $b_n = n^2$ for each integer $n \geq 0$. ■

The hypothesis is used **twice** here — once for b_k and once for b_{k-1} — which is precisely what ordinary induction could not have supplied.

The same sequence, a different recursive definition

Find a *different* recursive definition of $\{b_n\}_{n\geq 0}$.

Once the explicit formula is known this is easy, and it makes the point that **a sequence does not have one recursive definition**. Look for a one-term recurrence $b_n = b_{n-1} + p$ and solve for the step p:

$$n^2 = (n-1)^2 + p \implies p = n^2 - (n-1)^2 = 2n - 1$$

so $b_0 = 0$ and $b_n = b_{n-1} + (2n-1)$ for all integers $n \geq 1$ defines the same sequence — the familiar fact that the squares are the running totals of the odd numbers. Note it needs only **one** initial condition where the original needed two.

A recurrence that is not a polynomial

$d_0 = 1$ and $d_k = \dfrac{d_{k-1}}{1 + d_{k-1}}$ for each integer $k \geq 1$.

Calculating terms. The useful move is multiplying by a disguised 1 to clear the fraction inside the fraction:

$$d_1 = \frac{1}{1+1} = \frac{1}{2}$$

$$d_2 = \frac{\frac{1}{2}}{1+\frac{1}{2}} \cdot \frac{2}{2} = \frac{1}{2+1} = \frac{1}{3} \qquad d_3 = \frac{\frac{1}{3}}{1+\frac{1}{3}} \cdot \frac{3}{3} = \frac{1}{3+1} = \frac{1}{4}$$

giving $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$ — **guess** $d_n = \dfrac{1}{n+1}$ **for all integers** $n \geq 0$**.**

That $\times\frac{k}{k}$ trick is worth keeping: multiplying numerator and denominator by the denominator of the inner fraction turns a compound fraction into a simple one in one step, with no common-denominator bookkeeping.

Method 1.

Initial condition ($d_0 = 1$): $d_0 = \dfrac{1}{0+1} = 1$

Recurrence relation:

$$\text{LHS} = d_k = \frac{1}{k+1} \qquad \text{RHS} = \frac{d_{k-1}}{1+d_{k-1}} = \frac{\frac{1}{k}}{1+\frac{1}{k}} \cdot \frac{k}{k} = \frac{1}{k+1}$$

LHS = RHS.

Method 2, by ordinary induction — the recurrence reaches back one term, so MI and one base case.

Basis step. $d_0 = 1$ from the definition and $\frac{1}{0+1} = 1$, so $P(0)$ is true.

Inductive hypothesis. Suppose $P(k)$ is true for some integer $k \geq 0$. Then

$$d_{k+1} = \frac{d_k}{1+d_k} = \frac{1/(k+1)}{1+1/(k+1)} = \frac{1/(k+1)}{(k+2)/(k+1)} = \frac{1}{k+1} \cdot \frac{k+1}{k+2} = \frac{1}{k+2}$$

which is $\frac{1}{(k+1)+1}$, so $P(k+1)$ is true. By MI, $d_n = \dfrac{1}{n+1}$ for each integer $n \geq 0$. ■

The Tower of Hanoi

> Given a tower of 8 discs of decreasing size on one of three pegs, transfer the whole tower to another peg, subject to two rules: **move only one disc at a time**, and **never move a larger disc onto a smaller one**. Is there a solution, and if so what is the fewest number of moves?

This is the standard example of a recurrence that comes out of an argument rather than out of a formula. For $n \geq 1$ let m_n be the **minimum number of moves** needed to transfer a tower of n discs from one peg to another.

Small cases first: $m_1 = 1$ — move the single disc. $m_2 = 3$ — small disc to the spare peg, large disc to the target, small disc back on top.

The general case is the recursive insight:

Reading the picture off as arithmetic gives, for example, $m_4 = m_3 + 1 + m_3$, and in general

$$m_1 = 1 \qquad \text{and} \qquad m_k = 2m_{k-1} + 1 \ \text{ for all integers } k \geq 2$$

The explicit formula. The textbook (p. 310 in the 4th edition, p. 346 in the 5th) guesses $m_n = 2^n - 1$ for all integers $n \geq 1$. By Method 1:

Initial condition ($m_1 = 1$): $m_1 = 2^1 - 1 = 2 - 1 = 1$

Recurrence relation:

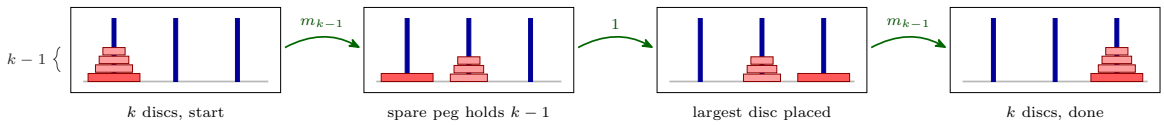


Figure 32: Why the recurrence doubles and adds one. Each box is one position of the three pegs, with discs as bars, the widest at the bottom, and the moves run left to right. To move k discs you must at some point move the largest, and it can only go onto an empty peg — so the other $k-1$ discs have to be parked on the spare peg first, then brought back on top afterwards. Two sub-transfers of $k-1$ discs, plus the single move of the largest. The $k-1$ smaller discs are drawn as a stack of three for legibility; nothing in the argument depends on how many there are.

$$\text{LHS} = m_k = 2^k - 1$$

$$\text{RHS} = 2m_{k-1} + 1 = 2(2^{k-1} - 1) + 1 = 2 \cdot 2^{k-1} - 2 + 1 = 2^k - 1$$

LHS = RHS, so the guess is correct. The textbook proves the same result by mathematical induction — either method is acceptable.

So the eight-disc tower takes $2^8 - 1 = 255$ moves, and the answer to "is there a solution?" is yes, constructively, because the recursion *is* the algorithm.

See also

- recursive-definitions[270] — the other direction, and recursively defined sets
- sequences-and-summations[271] — sequence notation, and why initial terms never define a sequence
- mathematical-induction[272] · strong-induction-and-the-well-ordering-principle[273] — Method 2's machinery
- 2026-08-31-solving-recurrence-relations[274] — Lecture 16
- practice-problems[275] — §20 Solving Recurrence Relations, with full worked solutions

[270] courses/math1061/recursive-definitions.pdf
[271] courses/math1061/sequences-and-summations.pdf
[272] courses/math1061/mathematical-induction.pdf
[273] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[274] courses/math1061/2026-08-31-solving-recurrence-relations.pdf
[275] courses/math1061/practice-problems.pdf

Strong Induction and the Well-Ordering Principle

Strong mathematical induction, the well-ordering principle for the integers, and the sense in which these two and ordinary induction are all the same tool. See mathematical-induction[276] for ordinary induction and the four-step proof template both methods share.

Strong mathematical induction

Let $P(n)$ be a predicate written in terms of some integer n. The difference from ordinary induction is entirely in what the inductive step is allowed to assume: **every** earlier case, not just the immediately preceding one — and, to pay for that, a basis step that establishes several cases rather than one.

	Ordinary induction (MI)	Strong induction (SMI)
Basis step	$P(2)$	$P(2) \wedge P(3) \wedge P(4)$
Inductive step	$\forall k \in \mathbb{Z}$ with $k \geq 2$, if $P(k)$ then $P(k+1)$	$\forall k \in \mathbb{Z}$ with $k \geq 4$, if $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ then $P(k+1)$
Conclusion	$P(n)$ for each integer $n \geq 2$	$P(n)$ for each integer $n \geq 2$

Both reach the same conclusion by the same kind of chain. For MI, $P(5)$ follows from $P(2)$ by three applications of the implication; for SMI with the basis above, $P(6)$ follows in two.

How many base cases?

As many as the inductive step reaches back for. This is the whole reason the basis step of an SMI proof is not a single case, and the answer to "why two values and not three?"

Count *how far back* the recurrence reaches, not how many terms it uses — those differ. $a_n = a_{n-1} - a_{n-3}$ uses only two earlier terms, but the deepest is three positions back, so all three of $P(0), P(1), P(2)$ must be established or the step could reach for an unproven case.

If the basis step establishes fewer cases than the inductive step consumes, the chain has a hole in it: the first few applications of the inductive step would reach for a case nobody ever proved.

[276] courses/math1061/mathematical-induction.pdf

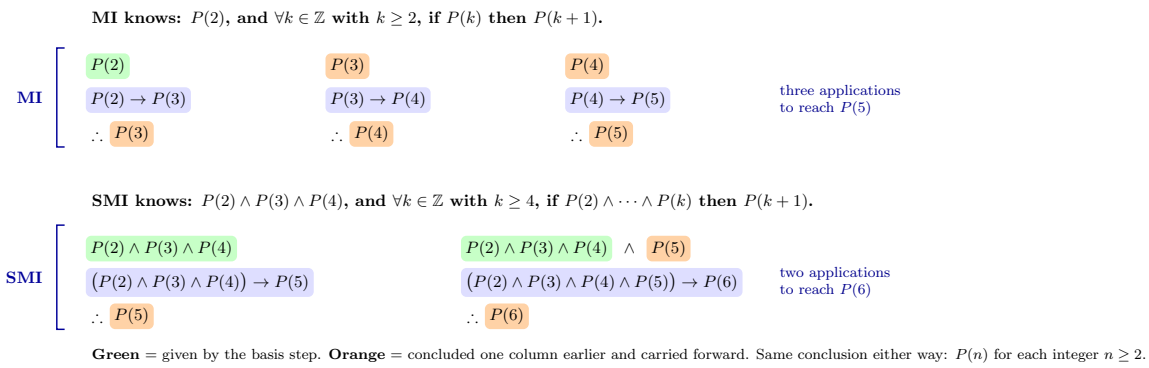


Figure 33: Mathematical induction and strong mathematical induction as chains of inferences. Each column is an argument — premises stacked, conclusion prefixed by $\therefore$, no rule line. MI climbs one rung at a time from a single base case; SMI starts from three base cases and each step may lean on everything established so far, which is why it lands on P(6) in two moves rather than four. Colour tracks one expression as it moves: green is what the basis step supplies, orange is a statement concluded one column earlier and carried forward. There are no arrows between columns — the repeated colour alone shows where a statement moves.

Worked example — a two-term recurrence

Suppose $b_1, b_2, b_3, \ldots$ is defined by $b_1 = 4$, $b_2 = 12$, and $b_n = b_{n-2} + b_{n-1}$ for each integer $n \geq 3$. Prove that $4 \mid b_n$ for each integer $n \geq 1$.

Proof. Let $P(n)$ be the predicate $4 \mid b_n$.

Basis step. We know that $b_1 = 4$ and $b_2 = 12$. Since $4 \mid 4$ and $4 \mid 12$, $P(1)$ is true and $P(2)$ is true.

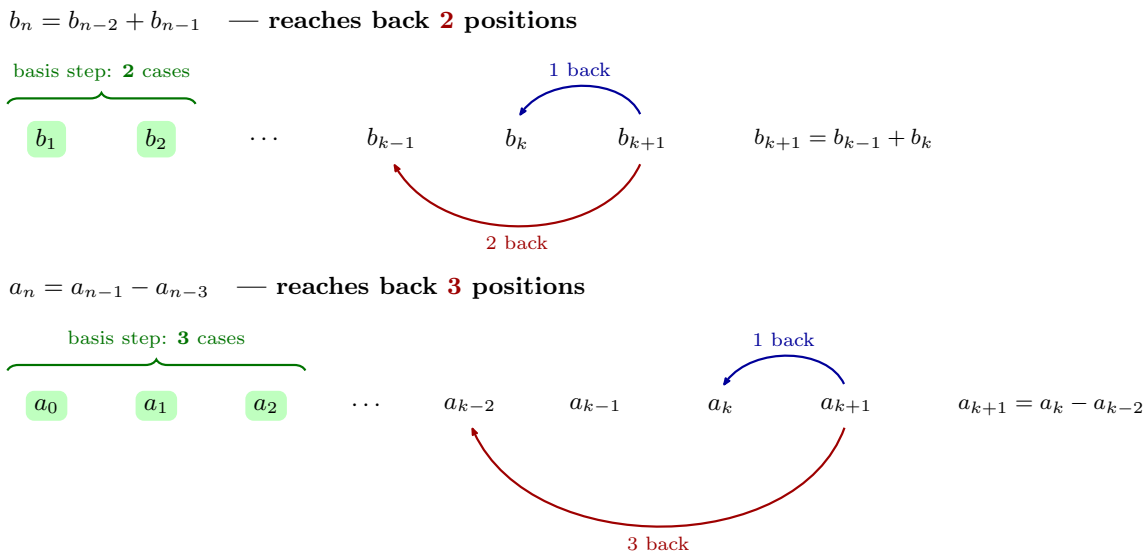
Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(1), P(2), \ldots, P(k)$ are true. Since $P(k)$ is true, $b_k = 4x$ for some $x \in \mathbb{Z}$. Since $P(k-1)$ is true, $b_{k-1} = 4y$ for some $y \in \mathbb{Z}$.

Inductive step. Consider $n = k + 1$:

$$\begin{aligned} b_{k+1} = b_{k-1} + b_k &= 4y + 4x \qquad \text{(by the inductive hypothesis)} \\ &= 4(y + x) \end{aligned}$$

Thus $4 \mid b_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 1$, $4 \mid b_n$. $\square$



The longest arrow sets the count, not the number of arrows: both recurrences use exactly two earlier terms, but the second reaches three positions back, so it needs three base cases.

Figure 34: How many base cases a strong induction needs, on the two sequences worked below: b_n = b_{n-2} + b_{n-1} and a_n = a_{n-1} − a_{n-3}. Both use exactly two earlier terms, so counting terms gives the wrong answer; what settles it is the longest arrow. Reaching two positions back means the basis step must cover two cases; reaching three means three. The terms sit in a row, and each short curved arrow is labelled with what it does.

Note where strong induction actually earns its keep: the step uses $P(k)$ **and** $P(k-1)$. Ordinary induction only hands you $P(k)$, which is not enough to say anything about b_{k-1}.

Worked example — every integer $n > 1$ is a product of primes

Theorem. Every integer $n > 1$ can be written as a product of primes.

> *Proof.* Let $P(n)$ be the predicate *n can be written as a product of primes*, for $n \geq 2$.
>
> **Basis step.** $n = 2$ is prime and thus is a product of primes, so $P(2)$ is true.
>
> **Inductive step.** Suppose that for some integer $k \geq 2$, every integer $2, 3, \ldots, k$ can be written as a product of primes — that is, $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$. We now need to prove that $k+1$ is a product of primes. Since $k+1 > 1$, either $k+1$ is prime or $k+1$ is composite.
>
> - *Case 1: $k+1$ is prime.* Then $k+1$ is a product of primes.
> - *Case 2: $k+1$ is composite.* Then $k+1 = rs$ for some positive integers $r \neq 1$ and $s \neq 1$. This implies $1 < r < k+1$ and $1 < s < k+1$. So by the inductive hypothesis — specifically $P(r)$ and $P(s)$ — both r and s are products of primes. Let $r = p_1 p_2 \ldots p_a$ and $s = q_1 q_2 \ldots q_b$ where the p_i and q_j are primes; thus $k+1 = rs = p_1 p_2 \ldots p_a q_1 q_2 \ldots q_b$ is a product of primes.
>
> In either case, $k+1$ is a product of primes.
>
> Therefore, by SMI, every integer $n > 1$ can be written as a product of primes. □

Why strong induction and not ordinary induction? Because r and s can be *any* integers from 2 to k — the factorisation gives no control over which — so the proof needs the inductive hypothesis available at all of those values, not just at k.

The well-ordering principle for the integers

> Let S be a **non-empty** set of integers, each of which is **greater than some fixed integer**. Then S has a **least element**.

Four pieces of terminology, all load-bearing:

- **non-empty** — the empty set has no least element, trivially.
- **of integers** — not of rationals or reals. This clause is not decoration: the positive rationals are non-empty *and* bounded below by 0, and still have no least element, because between any candidate and 0 there is always another one (halve it). See 2026-08-27-strong-induction-and-well-ordering[277].

[277] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf

- **greater than some fixed integer** — S must be bounded below. Without this the principle fails: $\mathbb{Z}^-$ is a non-empty set of integers with no least element.
- **a least element** — an element *of* S that is $\leq$ every element of S. It lives inside the set, not outside it.

Example — integers congruent to $1 \bmod 4$

True or false? The set of all integers congruent to $1 \bmod 4$ **has a least element.**

False. The set is $\{\dots, -7, -3, 1, 5, 9, \dots\}$.

> Suppose this set did have a least element, call it x. Then, since $x \equiv 1 \pmod 4$, we have $x - 4 \equiv 1 \pmod 4$, so $x - 4$ is also in the set. But $x - 4$ is smaller than x — a contradiction. $\square$

The set is non-empty, but it fails the "bounded below" condition, so the well-ordering principle simply does not apply to it.

MI, SMI and the WOP are equivalent

Anything provable by one is provable by the other two. Two of the translations:

SMI $\to$ MI: reword the statement. A strong-induction proof of $P(n)$ becomes an ordinary-induction proof of the *accumulated* predicate

$$Q(n) \;\equiv\; P(0) \wedge P(1) \wedge \cdots \wedge P(n)$$

Assuming $Q(k)$ in ordinary induction gives you exactly what assuming $P(0), \dots, P(k)$ gave you in strong induction. (Epp, Q27 p. 279.)

MI $\to$ WOP: argue by contradiction. Suppose the set of integers $\geq a$ for which $P(n)$ is *false* is non-empty. It is bounded below by a, so by the WOP it has a least element; derive a contradiction from that least element. (Epp, Q31 p. 279.)

The same theorem, three ways

Suppose $a_0, a_1, a_2, \dots$ **is defined by** $a_0 = 6$**,** $a_1 = 9$**,** $a_2 = 12$ **and** $a_n = a_{n-1} - a_{n-3}$ **for each integer** $n \geq 3$**. Prove that for all integers** $n \geq 0$**,** $3 \mid a_n$**.**

By SMI.

Let $P(n)$ be the predicate $3 \mid a_n$.

Basis step. $a_0 = 6$, $a_1 = 9$ and $a_2 = 12$. Since $3 \mid 6$, $3 \mid 9$ and $3 \mid 12$, $P(0)$, $P(1)$ and $P(2)$ are true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(0), P(1), \ldots, P(k)$ are true. Since $P(k-2)$ is true, $a_{k-2} = 3y$ for some $y \in \mathbb{Z}$; since $P(k)$ is true, $a_k = 3x$ for some $x \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 0$, $3 \mid a_n$. $\square$

By MI, on the reworded predicate.

Let $Q(n)$ be the predicate $3 \mid a_j$ *for all integers* j *where* $0 \leq j \leq n$ — that is, $Q(n) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$.

Basis step. Consider $n = 2$. Since $3 \mid a_0$, $3 \mid a_1$ and $3 \mid a_2$, $Q(2)$ is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $Q(k)$ is true. Since $Q(k)$ is true and $k \geq 2$, $a_k = 3x$ and $a_{k-2} = 3y$ for some $x, y \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$. Since $Q(k)$ already gives $3 \mid a_i$ for every $0 \leq i \leq k$, adding $3 \mid a_{k+1}$ gives $Q(k+1)$.

(That last step is the point of rewording the predicate: $Q(k+1)$ is a conjunction over *all* indices up to $k+1$, so it needs $Q(k)$ **and** the new case — $3 \mid a_{k+1}$ alone would not establish it.)

Therefore, by PMI, for each integer $n \geq 0$, $3 \mid a_n$. $\square$

The two proofs have the *same* algebraic core: the line $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$ is identical in each. All the reworded predicate does is let a single assumption, $Q(k)$, carry the several earlier facts the algebra needs.

Two details of the MI proof are easy to get wrong:

- **The basis is $n = 2$, not $n = 0$.** $Q(2)$ already asserts $3 \mid a_0$, $3 \mid a_1$ *and* $3 \mid a_2$, so verifying $Q(2)$ discharges all three of the SMI proof's base cases in one statement. Three base cases have not disappeared; they have been packed into one predicate.
- **The step concludes $Q(k+1)$, not $P(k+1)$.** An ordinary induction on Q has to deliver $Q(k+1)$, and $3 \mid a_{k+1}$ on its own does not — it needs $Q(k)$ alongside it.

The conjunction in Q starts at $P(0)$, not $P(1)$. The predicate is $3 \mid a_j$ *for all integers* j *where* $0 \leq j \leq n$, so $Q(2) \equiv P(0) \wedge P(1) \wedge P(2)$ — which is also what the basis step checks.

By the WOP, by contradiction.

Suppose the statement is false, so there exists an integer $n \geq 0$ such that 3 does not divide a_n. Let

$$A = \{\, n \in \mathbb{Z}^{\geq 0} \;:\; 3 \nmid a_n \,\}$$

By the WOP and our assumption, A has a least element — the smallest n for which $3 \nmid a_n$. Call it k. Thus $3 \nmid a_k$, but $3 \mid a_i$ for all $0 \leq i \leq k-1$.

Note that $k \geq 3$, since a_0, a_1 and a_2 are all divisible by 3.

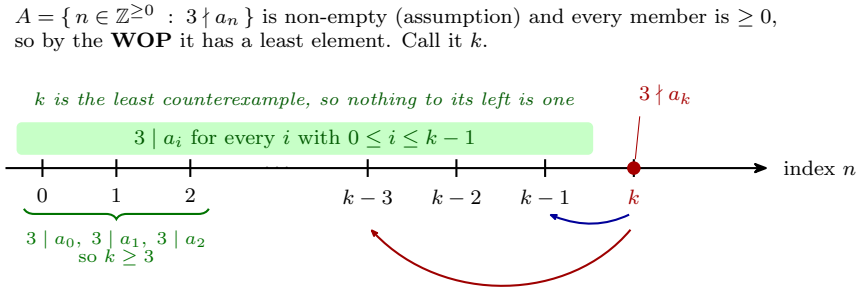
Thus $a_{k-1} = 3x$ and $a_{k-3} = 3y$ for some $x, y \in \mathbb{Z}$, so

$$a_k = a_{k-1} - a_{k-3} = 3x - 3y = 3(x - y)$$

Thus $3 \mid a_k$, which is a contradiction.

Therefore, for each integer $n \geq 0$, $3 \mid a_n$. □

Reading the WOP proof next to the SMI one: "let k be the least counterexample" plays the role of the inductive hypothesis (everything below k works), and "$3 \mid a_k$, contradiction" plays the role of the inductive step. Drawn on the index line, the whole proof is one picture:



Both arrows land inside the green stretch (this is what $k \geq 3$ buys), so $a_{k-1} = 3x$ and $a_{k-3} = 3y$ for some $x, y \in \mathbb{Z}$:

$$a_k = a_{k-1} - a_{k-3} = 3x - 3y = 3(x - y) \quad \text{— so } 3 \mid a_k \text{ after all. Contradiction.}$$

Figure 35: The well-ordering proof of 3 | a_n as a picture of its own least counterexample. Everything to the left of k is green not because it was proved, but because k was chosen least — that single step is the only place the WOP is used, and it is exactly what the strong inductive hypothesis supplies in the SMI proof. The least element here is the smallest number that gives a contradiction. k 3 is what guarantees both arrows land inside the green stretch, since a_{k-3} has to be a term of the sequence at all.

Note which term the WOP proof reaches for. The SMI proof used a_k and a_{k-2} to build a_{k+1}; the WOP proof is standing at k rather than at $k+1$, so the same recurrence reads $a_k = a_{k-1} - a_{k-3}$ and it reaches for a_{k-1} and a_{k-3}. Same recurrence, index shifted by one — and that shift is why the "$k \geq 3$" line has to be there.

Spotting a WOP proof

A proof is using the well-ordering principle whenever it says **"choose the smallest such n"** about a set it has just argued is non-empty. That phrase is not free — it is the WOP being invoked, and it needs the set to be non-empty and bounded below.

For instance, the primes theorem above can be rewritten as a contradiction proof: suppose some integer $n > 1$ is not a product of primes; by the WOP, choose the smallest such n; then n is prime (done) or $n = rs$ with $1 < r, s < n$, and both r and s *are* products of primes precisely because n was chosen smallest — contradicting the choice of n. Structurally it is the SMI proof with the induction turned inside out.

See also

- mathematical-induction[278] · proof-techniques[279] · sequences-and-summations[280]
- recursive-definitions[281] · solving-recurrence-relations[282] — where a two-term recurrence forces the strong hypothesis
- trees[283] — strong induction on the number of vertices: a tree with n vertices has $n-1$ edges
- 2026-08-27-strong-induction-and-well-ordering[284] — Lecture 14
- practice-problems[285] — §18, with full worked solutions

[278] courses/math1061/mathematical-induction.pdf
[279] courses/math1061/proof-techniques.pdf
[280] courses/math1061/sequences-and-summations.pdf
[281] courses/math1061/recursive-definitions.pdf
[282] courses/math1061/solving-recurrence-relations.pdf
[283] courses/math1061/trees.pdf
[284] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf
[285] courses/math1061/practice-problems.pdf