MATH1061 — Week 3 Notes

Table of contents

Lecture 7 — Direct Proof, Counterexample 2
- Learning goals . . . 2
- Student questions and comments . . . 2
- Proof or disproof of $\forall x \in D, P(x) \to Q(x)$ . . . 3
- Q1 from the pre-class questions . . . 3
- Example proof . . . 4
- Activity 1 . . . 4
- Activity 2 — prove or disprove . . . 4
- Activity 4 — disprove by proving the negation . . . 5
- See also . . . 5

Lecture 8 — Proof by Contradiction 5
- Learning goals . . . 5
- Recall . . . 6
- Student questions and comments . . . 6
- The three methods so far . . . 7
- Q1 from the pre-class questions . . . 7
- Q2 from the pre-class questions . . . 8
- Activity 1 — the same statement, both ways . . . 8
- Activity 2 — where contradiction earns its keep . . . 9
- Activity 3 . . . 9
- Activity 4 — completing a started proof . . . 9
- See also . . . 10

Lecture 9 — Proof by Contraposition, Rational Numbers 10
- Learning goals . . . 10
- Student questions and comments . . . 11
- The four methods . . . 11
- The last lemma from Video 12, by contraposition . . . 11
- Activity 1 . . . 12

Activity 2 12
Activity 3 13
Activity 4 — $\sqrt{2}$ is irrational 13
See also 14

Reference material **14**
Conditional & Biconditional Statements 14
Logical Equivalence & Laws 16
Practice Problems — Applied Class Source 17
Proof Techniques — Direct, Counterexample, Contradiction, Contraposition 140
Quantified Statements 147
Rational & Irrational Numbers 152

Lecture 7 — Direct Proof, Counterexample

Pre-work: Video 009 (Direct Proofs and Counterexamples). First lecture of the number theory and methods of proof topic — see proof-techniques[1] for the reference definitions, proof templates and the catalogue of common proof errors.

Learning goals

- How to write a direct proof.
- How to disprove a statement by exhibiting a counterexample.

Student questions and comments

What precise definitions should we know for proofs and disproofs? Know the definitions of even, odd, prime, composite, rational, divides — each is an "if and only if", usable in both directions. They're tabulated in proof-techniques[2].

How much detail to give in a proof? Demonstrate facts **using the definitions**.

Two facts used throughout, worth naming when you rely on them:

- **Fact**: the sum, difference, and product of integers is an integer.
- **Fact**: every integer is either even or odd — $\mathbb{Z}$ splits into $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

Note on "not prime": for $n \in \mathbb{Z}^{>1}$, "n not prime" means "n composite". For $n \in \mathbb{Z}$ generally, "n not prime" means "composite or $n \leq 1$" — the primes and composites together only cover $\mathbb{Z}^{\geq 2}$.

[1] courses/math1061/proof-techniques.pdf
[2] courses/math1061/proof-techniques.pdf

Proof or disproof of $\forall x \in D, P(x) \to Q(x)$

Recall the truth table — the only row that makes $p \to q$ false is p true, q false:

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

Direct proof (shows the statement is true):

> Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$. $\square$

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.

Student comment: why do you suppose that $P(x)$ is true, when $P(x) \to Q(x)$ would still be true if $P(x)$ is false? We just need to rule out the case that $P(x)$ is true and $Q(x)$ is false — so we suppose $P(x)$ is true and prove that in this case $Q(x)$ must also be true. The other rows of the table are true for free.

Q1 from the pre-class questions

Which values for m and n give a counterexample disproving: *for all integers m and n, if $2m+n$ is odd, then m and n are both odd*?

a. $m = 3, n = 5$	m, n both odd — conclusion holds	not a counterexample
b. $m = 3, n = 6$	$2(3) + 6 = 12$ even — hypothesis fails	not a counterexample
c. $m = 4, n = 5$	$2(4) + 5 = 13$ odd, and m is even	**counterexample**
d. $m = 4, n = 6$	$2(4) + 6 = 14$ even — hypothesis fails	not a counterexample

For a counterexample to $p \to q$ we require p **true** and q **false**.

Example proof

$\forall n \in \mathbb{Z}$, if n is odd then $3n+2$ is odd.

Proof. Let $n \in \mathbb{Z}$ and suppose n is odd. $\leftarrow$ *hypothesis* Since n is odd, $n = 2k+1$ 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 $3k+2 \in \mathbb{Z}$. Hence $3n+2$ is odd. $\leftarrow$ *conclusion* $\square$

Note the shape: state the hypothesis, unfold the definition, do the algebra so the target definition is visible, confirm the witness is an integer, then state the conclusion.

Activity 1

For any integer x, if $x+6 = 4y$ for some integer y, then $\frac{x}{2}$ is an odd integer.

Proof. Let $x \in \mathbb{Z}$ and suppose $x+6 = 4y$ for some $y \in \mathbb{Z}$. Now $x = 4y-6$, so $x = 2(2y-3)$. Hence $\frac{x}{2} = \frac{2(2y-3)}{2} = 2y-3 = 2(y-1)-1$. Thus, because $y \in \mathbb{Z}$, 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. $\square$

Both halves are needed: that $\frac{x}{2}$ is an *integer*, and that it has the *odd* form. ($2(y-1)-1$ uses the $n = 2k-1$ form of odd; $2(y-2)+1$ works just as well.)

Activity 2 — prove or disprove

(a) There are distinct integers m and n such that $\frac{1}{m} + \frac{1}{n}$ is an integer.

True. Take $m = 1$ and $n = -1$. Then $\frac{1}{m} + \frac{1}{n} = 1 + (-1) = 0 \in \mathbb{Z}$.

(b) $\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n+1$ is composite.

False. Take $n = 2$: then $n = 2$ and $n+1 = 3$, which are both prime.

(c) For each integer $n \geq 2$, the product of the first n prime numbers minus 1 is prime.

False. (Hint: try $n = 2, 3, 4, \ldots$) Take $n = 4$: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, which is composite.

Note that $n = 2$ and $n = 3$ both work, which is exactly why "arguing from examples" is on the list of common proof errors in proof-techniques[3].

[3] courses/math1061/proof-techniques.pdf

Activity 4 — disprove by proving the negation

Show that $\exists n \in \mathbb{Z}^+$ such that $n^2 + 5n + 6$ is prime is false, by proving the negation.

The statement is existential, so a single counterexample won't do — the negation is universal and must be proved outright:

> Negation: $\forall n \in \mathbb{Z}^+$, $n^2 + 5n + 6$ is composite.
>
> *Proof of the negation.* Let $n \in \mathbb{Z}^+$. Now $n^2 + 5n + 6 = (n+2)(n+3)$. Since $n \geq 1$ we have $n + 2 > 1$ and $n + 3 > 1$. Thus $n^2 + 5n + 6$ is composite. $\square$

Because $n \geq 1$ forces $n^2 + 5n + 6 \geq 2$, "not prime" here really does mean "composite".

See also

- proof-techniques[4] · quantified-statements[5]
- 2026-08-13-proof-by-contradiction[6] — Lecture 8
- practice-problems[7] — §9 Direct Proofs and Counterexamples, with full worked solutions

Lecture 8 — Proof by Contradiction

Pre-work: Video 010 (Proof by Contradiction). Adds a third method to the direct proof and counterexample of 2026-08-10-direct-proof-and-counterexample[8] — see proof-techniques[9] for all four side by side.

Learning goals

- How to write a proof by contradiction.

[4] courses/math1061/proof-techniques.pdf
[5] courses/math1061/quantified-statements.pdf
[6] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[7] courses/math1061/practice-problems.pdf
[8] courses/math1061/2026-08-10-direct-proof-and-counterexample.pdf
[9] courses/math1061/proof-techniques.pdf

Recall

The negations this method depends on (see logical-equivalence-laws[10] and quantified-statements[11]):

$$\sim (p \vee q) \equiv \sim p \wedge \sim q$$
$$\sim (p \wedge q) \equiv \sim p \vee \sim q$$
$$\sim (p \rightarrow q) \equiv p \wedge \sim q$$
$$\sim (\exists x \in D \text{ such that } P(x)) \equiv \forall x \in D, \sim P(x)$$
$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ such that } \sim P(x)$$

Plus the definitions of even, odd, prime, composite, rational and divides, tabulated in proof-techniques[12].

Fact: the sum, difference and product of integers is an integer.

Warning: don't assume something that seems like an "obvious fact" until you have proven it, or can say which lecture or pre-work video it was proved in.

Student questions and comments

Can proof by contradiction be used for every proof? / Does this type of proof only work for universal statements, or does it just work best for them? / What situations are best for proof by contradiction vs the direct proof?

Proof by contradiction is the **most versatile** method, but it requires more set-up, so sometimes a direct proof is easier.

What is the difference between proof by counterexample and proof by contradiction? Counterexample is a **disproof**; contradiction is a **proof**. They do opposite jobs.

[10] courses/math1061/logical-equivalence-laws.pdf
[11] courses/math1061/quantified-statements.pdf
[12] courses/math1061/proof-techniques.pdf

Method	Shape	Shows

The three methods so far

Method	Shape	Shows
Direct proof	Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$.	statement is **true**
Disproof by counterexample	Let $x = \cdots$. Then $x \in D$, $P(x)$ true, $Q(x)$ false.	statement is **false**
Proof by contradiction	Suppose $\exists x \in D$ such that $P(x)$ true, $Q(x)$ false. ... Hence something obviously wrong.	statement is **true**

For a proof by contradiction we begin by **assuming that the statement is false** — equivalently, that the negation of the statement is true. The negation of $\forall x \in D, P(x) \to Q(x)$ is

$$\exists x \in D \text{ such that } P(x) \wedge \sim Q(x)$$

and we derive from it something that cannot hold — $P(x)$ false, or $Q(x)$ true, or $1 = 0$.

Q1 from the pre-class questions

Claim: $\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd. An appropriate way to start a proof by contradiction is:

> *Proof:* Suppose that n is an odd integer and that $3n + 2$ is even.

which means **exactly the same thing** as

> Suppose $\exists n \in \mathbb{Z}$ such that n is odd but $3n + 2$ is even.

Q2 from the pre-class questions

Claim: for all integers m and n, if mn is even, then m is even or n is even. Consider the first sentence of a proof:

> *Proof:* Suppose that m and n are integers, mn is even and both m and n are odd.

This is the start of a proof of what type?

(a) A direct proof. (b) A disproof by counterexample. **(c) A proof by contradiction.**

It assumes the hypothesis *and* the negation of the conclusion ("m even or n even" negates to "m odd and n odd" by De Morgan).

Activity 1 — the same statement, both ways

$\forall n \in \mathbb{Z}$, if n is odd then $3n + 2$ is odd.

Direct proof

Let $n \in \mathbb{Z}$ and suppose n is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$ (by definition). Now

$$3n + 2 = 3(2k + 1) + 2 = 6k + 5 = 2(3k + 2) + 1.$$

Since $k \in \mathbb{Z}$, we know $3k + 2 \in \mathbb{Z}$, and hence $3n + 2$ is odd (by definition). $\square$

Proof by contradiction

Suppose $\exists n \in \mathbb{Z}$ such that n is odd and $3n + 2$ is **even**. Then (since n is odd), $n = 2k + 1$ 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 know $3k + 2 \in \mathbb{Z}$, hence $3n + 2$ is **odd** — contradicting the assumption that it is even. Therefore the original statement is true. $\square$

The body of the two proofs is identical; contradiction just wraps it in an extra assumption and an extra closing line. That's the "more set-up" cost — and here the direct proof is the better choice.

Activity 2 — where contradiction earns its keep

$\forall m, n \in \mathbb{Z}$, if mn is even, then m is even or n is even.

Direct proof — suppose $m, n \in \mathbb{Z}$ and mn is even. We can write $mn = 2k$ for some $k \in \mathbb{Z}$ … and now there's no way forward: knowing $mn = 2k$ tells you nothing about m and n individually.

Proof by contradiction

> 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 $\ell \in \mathbb{Z}$ — **use a new variable**; 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. □

Reusing k for both m and n is one of the standard proof errors listed in proof-techniques[13].

Activity 3

Prove by contradiction: $\forall n \in \mathbb{Z}$, if $3n^3 - 2$ is odd, then n is odd.

> *Proof.* Suppose the statement is false. That means $\exists n \in \mathbb{Z}$ such that $3n^3 - 2$ is odd and n is even. Since n is even, $n = 2a$ for some $a \in \mathbb{Z}$. Now
>
> $$3n^3 - 2 = 3(2a)^3 - 2 = 3 \cdot 8a^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$
>
> 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. □

Activity 4 — completing a started proof

$\forall m, n \in \mathbb{Z}$, if $m + n$ is even, then m and n are both even or m and n are both odd.

> *Proof.* Suppose the statement is false. Thus $\exists m, n \in \mathbb{Z}$ such that $m + n$ is even but exactly one of m, n is even (and the other is odd).
>
> **Without loss of generality**, assume m is even and n is odd. (The two cases are (1) m even, n odd and (2) m odd, n even; since $m + n = n + m$, the second is the first with the names swapped, so proving one proves both.)

[13] courses/math1061/proof-techniques.pdf

Thus $m = 2a$ for some $a \in \mathbb{Z}$, and $n = 2b + 1$ for some $b \in \mathbb{Z}$. Now

$$m + n = 2a + (2b + 1) = 2(a + b) + 1.$$

We know $a + b \in \mathbb{Z}$ because $a, b \in \mathbb{Z}$, so $m + n$ is odd. This contradicts the assumption that $m + n$ is even. Therefore the original statement is true. $\square$

"Without loss of generality" is only legitimate when the omitted case really is the stated one relabelled — say why, as above.

See also

- proof-techniques[14] · quantified-statements[15] · logical-equivalence-laws[16]
- 2026-08-13-proof-by-contraposition[17] — Lecture 9
- practice-problems[18] — §10 Proof by Contradiction, with full worked solutions

Lecture 9 — Proof by Contraposition, Rational Numbers

Pre-work: Video 011 (Proof by Contraposition), Video 012 (Rational Numbers). Completes the set of four methods — see proof-techniques[19] for the full comparison, and rational-and-irrational-numbers[20] for the $\mathbb{Q}$ / $\overline{\mathbb{Q}}$ definitions and closure results.

Learning goals

1. Understand the definitions of rational and irrational numbers.
2. Gain fluency in proof techniques (direct proof, proof by contradiction and proof by contraposition).

Recall: $r \in \mathbb{Q} \iff r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$; and $r \in \overline{\mathbb{Q}} \iff r \notin \mathbb{Q}$, where $\overline{\mathbb{Q}} = \mathbb{R} \setminus \mathbb{Q}$. So $\frac{3}{4} \in \mathbb{Q}$, while $\sqrt{2} \in \overline{\mathbb{Q}}$ and $\pi \in \overline{\mathbb{Q}}$.

[14] courses/math1061/proof-techniques.pdf
[15] courses/math1061/quantified-statements.pdf
[16] courses/math1061/logical-equivalence-laws.pdf
[17] courses/math1061/2026-08-13-proof-by-contraposition.pdf
[18] courses/math1061/practice-problems.pdf
[19] courses/math1061/proof-techniques.pdf
[20] courses/math1061/rational-and-irrational-numbers.pdf

Student questions and comments

What is the relationship between proof by contradiction and proof by contraposition?

How do we decide if we should use a direct proof, proof by contradiction or proof by contraposition?

Both are answered by working the activities below — each one is annotated with which methods work and which get stuck.

The four methods

Method	Shape	Shows
Direct proof	Let $x \in D$ and suppose $P(x)$. ... Hence $Q(x)$.	true
Disproof by counterexample	Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true. However $Q(x)$ is false.	false
Proof by contradiction	Suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false. ... Hence something obviously wrong.	true
Proof by contraposition	We prove $\forall x \in D, \sim Q(x) \to \sim P(x)$. Let $x \in D$ and suppose $\sim Q(x)$. ... Hence $\sim P(x)$.	true

Contraposition is valid because $p \to q \equiv \sim q \to \sim p$ (see conditional-statements[21]).

The last lemma from Video 12, by contraposition

Lemma: the sum of any rational number and any irrational number is irrational.

Symbolically, either of:

$$\forall r, s \in \mathbb{R},\ \text{if } r \in \mathbb{Q} \text{ and } s \in \overline{\mathbb{Q}} \text{ then } r + s \in \overline{\mathbb{Q}}$$

$$\forall r \in \mathbb{Q} \text{ and } \forall s \in \mathbb{R},\ \text{if } s \in \overline{\mathbb{Q}} \text{ then } r + s \in \overline{\mathbb{Q}}$$

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

- **Direct proof**: suppose $r \in \mathbb{Q}$ and $s \in \overline{\mathbb{Q}}$. Now we are stuck — $s \in \overline{\mathbb{Q}}$ gives nothing to substitute.
- **Proof by contradiction**: suppose $\exists r \in \mathbb{Q}$ and $s \in \mathbb{R}$ such that $s \in \overline{\mathbb{Q}}$ and $r + s \in \mathbb{Q}$. (Done in the video.)
- **Proof by contraposition**:

  The contrapositive is: $\forall r \in \mathbb{Q}$ and $\forall s \in \mathbb{R}$, if $r + s \in \mathbb{Q}$ then $s \in \mathbb{Q}$.

  Suppose $r \in \mathbb{Q}$, $s \in \mathbb{R}$ and $r + s \in \mathbb{Q}$. Since $r \in \mathbb{Q}$, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Since $r + s \in \mathbb{Q}$, $r + s = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$. Now

  $$s = (r + s) - r = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$

  Since $a, b, c, d \in \mathbb{Z}$ we know $bc - ad \in \mathbb{Z}$ and $bd \in \mathbb{Z}$. Also $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Thus $s \in \mathbb{Q}$. $\square$

The move that unlocks it is writing $s = (r + s) - r$ — expressing the unknown in terms of the two things you were handed.

Activity 1

Prove that $\forall r \in \mathbb{R}$, if r^2 is irrational, then r is irrational.

What type of proof will work? ~~Direct proof~~ · contradiction · contraposition

> *Proof.* We prove the contrapositive: $\forall r \in \mathbb{R}$, if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$. Suppose $r \in \mathbb{R}$ where $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some integers a, b with $b \neq 0$. Now $r^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$. Since $a, b \in \mathbb{Z}$ we have $a^2, b^2 \in \mathbb{Z}$; also $b^2 \neq 0$ since $b \neq 0$. So $r^2 \in \mathbb{Q}$. $\square$

Activity 2

Prove that $\forall r \in \mathbb{Q}, (2r^2 - 3r + 1) \in \mathbb{Q}$.

What type of proof will work? direct proof (**best**) · contradiction · ~~contraposition~~ (stuck)

> *Proof.* Let $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Now
>
> $$2r^2 - 3r + 1 = 2\left(\frac{a}{b}\right)^2 - 3\left(\frac{a}{b}\right) + 1 = \frac{2a^2}{b^2} - \frac{3ab}{b^2} + \frac{b^2}{b^2} = \frac{2a^2 - 3ab + b^2}{b^2}.$$
>
> Since $a, b \in \mathbb{Z}$ we have $2a^2 - 3ab + b^2 \in \mathbb{Z}$ and $b^2 \in \mathbb{Z}$. Also $b^2 \neq 0$ since $b \neq 0$. So $2r^2 - 3r + 1 \in \mathbb{Q}$. $\square$

Contraposition stalls here because the negation of "$2r^2 - 3r + 1 \in \mathbb{Q}$" — that it's irrational — gives nothing to substitute. The direction of the useful information decides the method.

Activity 3

Prove by contraposition: $\forall m, n \in \mathbb{Z}$**, if** mn **is odd, then** m **and** n **are both odd.**

What type of proof will work? direct proof (not as easy) · contradiction · contraposition

> *Proof.* 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 $mn = (2k)n = 2(kn)$. Since $k, n \in \mathbb{Z}$, $kn \in \mathbb{Z}$, so mn is even. □

Note that "m and n are both odd" negates to "m is even **or** n is even" by De Morgan — hence "at least one of".

Activity 4 — $\sqrt{2}$ is irrational

What type of proof will work? ~~Direct proof~~ · **contradiction** · ~~contraposition~~

Two ingredients:

- **Fact**: every rational number can be written as a fraction in lowest terms (numerator and denominator have no common factors).
- **Lemma (Video 11)**: for all integers n, if n^2 is even then n is even.

> *Proof.* Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and we assume $\frac{a}{b}$ is in **lowest terms**.
>
> Now $(\sqrt{2})^2 = \left(\frac{a}{b}\right)^2$, so $2 = \frac{a^2}{b^2}$ and hence $a^2 = 2b^2$; thus a^2 is even. By the lemma, a **is even**, so $a = 2\ell$ for some $\ell \in \mathbb{Z}$.
>
> Then $2b^2 = a^2 = (2\ell)^2 = 4\ell^2$, so $b^2 = 2\ell^2$ and b^2 is even. By the lemma again, b **is even**.
>
> This contradicts the assumption that $\frac{a}{b}$ is in lowest terms — a and b share the factor 2.
>
> Therefore $\sqrt{2} \in \overline{\mathbb{Q}}$. □

The "in lowest terms" assumption is what the contradiction lands on; without it the argument has nothing to contradict.

See also

- proof-techniques[22] · rational-and-irrational-numbers[23] · conditional-statements[24]
- 2026-08-13-proof-by-contradiction[25] — Lecture 8
- 2026-08-17-divisibility[26] — Lecture 10
- practice-problems[27] — §11 Proof by Contraposition, with full worked solutions
- practice-problems[28] — §12 Rational Numbers, with full worked solutions

Reference material

Conditional & Biconditional Statements

Conditional ($\to$)

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

By definition, $p \to q \equiv \sim p \lor q$ — this lets any law of logical equivalence (see logical-equivalence-laws[29]) be applied to conditionals.

$p \to q$ 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: $p \to q \not\equiv q \to p$.

Contrapositive, converse, inverse

[22] courses/math1061/proof-techniques.pdf
[23] courses/math1061/rational-and-irrational-numbers.pdf
[24] courses/math1061/conditional-statements.pdf
[25] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[26] courses/math1061/2026-08-17-divisibility.pdf
[27] courses/math1061/practice-problems.pdf
[28] courses/math1061/practice-problems.pdf
[29] courses/math1061/logical-equivalence-laws.pdf

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

Necessary and sufficient conditions

- p is a **necessary condition** for q "if $\sim p$ then $\sim q$" "if q then p" "q only if p".
- p is a **sufficient condition** for q "if p then q" "q if p".

Examples:

- Non-negative is **necessary but not sufficient** for being a perfect square (-9 isn't a square; 7 is non-negative but not a square).
- Divisible by 4 is **sufficient but not necessary** for being even (8: divisible by 4 even; 10: even but not divisible by 4).

Biconditional ($\leftrightarrow$)

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

"a iff b" "a only if b, and a if b" "b is necessary and sufficient for a".

Order of operations

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

Parenthesise explicitly rather than relying on left-to-right tie-breaking.

See also

- logical-connectives[30]
- logical-equivalence-laws[31]
- practice-problems[32] — §3 Conditional Statements, with full worked solutions

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.

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 — the marks are in choosing and applying them, and in naming the one you used at each step. The same page also carries the valid-argument-forms[33] and the set identities.

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	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
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 $\mathbf{t}/\mathbf{c}$	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

[30] courses/math1061/logical-connectives.pdf
[31] courses/math1061/logical-equivalence-laws.pdf
[32] courses/math1061/practice-problems.pdf
[33] courses/math1061/valid-argument-forms.pdf

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".

See also

- logical-connectives[34]
- conditional-statements[35]
- practice-problems[36] — §2 Logical Equivalence, with full worked solutions

Practice Problems — Applied Class Source

This is the single problem set used in **every** Applied Class for the whole semester — there is no separate 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[37]). Each week's class applies the *previous* week's lecture content, so the sections in play are roughly one week behind the lecture column below.

How each section is laid out

1. Relevant textbook pages for Epp 4th edition and 5th (metric) edition
2. **Practice problems**
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: 11 August 2026** — on page 195, the solution to 1(b) was corrected (the note in brackets had previously copied the note from 1(a)); that correction is already applied in §45 below. If something looks wrong, post on the Ed Discussion board.

[34] courses/math1061/logical-connectives.pdf
[35] courses/math1061/conditional-statements.pdf
[36] courses/math1061/practice-problems.pdf
[37] courses/math1061/math1061.pdf

Section index

Every section is reproduced in full below. 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[38]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[39]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[40]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[41]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[42]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[43]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[44]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[45]
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[46]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[47]

[38] courses/math1061/logical-connectives.pdf
[39] courses/math1061/logical-equivalence-laws.pdf
[40] courses/math1061/conditional-statements.pdf
[41] courses/math1061/valid-argument-forms.pdf
[42] courses/math1061/determining-argument-validity.pdf
[43] courses/math1061/quantified-statements.pdf
[44] courses/math1061/quantified-statements.pdf
[45] courses/math1061/quantified-statements.pdf
[46] courses/math1061/proof-techniques.pdf
[47] courses/math1061/proof-techniques.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[48]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[49]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[50]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[51]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[52]
16	Sequences	L13 (wk 5)	227–244	258–275	
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	
23	Properties of Sets	L18 (wk 7)	352–366	391–407	

[48] courses/math1061/proof-techniques.pdf
[49] courses/math1061/rational-and-irrational-numbers.pdf
[50] courses/math1061/divisibility-and-factorisation.pdf
[51] courses/math1061/modular-arithmetic.pdf
[52] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	
25	one-to-one, Onto, and Inverse Functions	L19 (wk 7)	397–416	439–461	
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	

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
39	Introduction to Probability	L31 (wk 11)	516–553	564–604	
40	Binomial Coefficients	L31 (wk 11)	565–591	617–641	
41	Inclusion Exclusion	L32 (wk 12)	545–549	595–599	
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
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[53].

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?

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

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.

   (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[54].

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

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

(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

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

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[55].

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.

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

(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.

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	$q \vee r$	$p \rightarrow (q \vee r)$	$\sim q$	$p \wedge \sim q$	$(p \wedge \sim q) \rightarrow r$
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	$(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$
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 $(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$:

p	q	r	$p \rightarrow$	$(q \vee r)$	$\leftrightarrow$	$(p \wedge \sim q)$	$\rightarrow r$
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[56].

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.

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

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

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 ($p \rightarrow q$) 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	$(p \wedge q) \to \sim r$	$p \vee \sim q$	$\sim q \to p$	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[57].

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.

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

(a)

$$p \to q \quad q \to p \quad \therefore p \vee q$$

(b)

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

(c)

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

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

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

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

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

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. $n \to k$
3. $\sim k \vee i$
4. $\sim m \to i$
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.	$n \to k$	specification
3.	$\sim k \vee i$	specification
4.	$\sim m \to i$	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.	$(m \to n) \land (n \to m)$	from 1 by definition of $\leftrightarrow$
9.	$m \to n$	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. $r \to a$
2. $a \to s$
3. $s \to r$
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[58].

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

Problems

1. Rewrite each of the following in the form "$\forall$__, __." 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 "$\exists$__ 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) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

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[59].

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.

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 $x \not\geq 2$.

    (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 $xy \notin \mathbb{Z}$.

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

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[60].

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:
   (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.

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

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[61]*.*

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*

   (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.

[61] courses/math1061/proof-techniques.pdf

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	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$((p \vee q) \wedge (\sim p \vee r)) \to (q \vee r)$
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. $r \to u \equiv \sim r \vee u$ (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. $r \to u$
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[62].

Problems

1. Prove the following statement using a proof by contradiction:

$$\text{For integers } a \text{ and } b, \text{ if } 6a+3b \text{ is odd, then } b \text{ is odd.}$$

2. Use a proof by contradiction to prove the following statement:

$$\text{For all positive integers } x \text{ and } y,\ x^2 - y^2 \neq 1.$$

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. □

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. □

[62] courses/math1061/proof-techniques.pdf

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[63].

Problems

1. Use proof by contraposition to prove the following statement:

$$\text{For all integers } a \text{ and } b,\ \text{if } (ab)^2 \text{ is odd then } a \text{ is odd and } b \text{ is odd.}$$

2. Prove the following statement:

$$\text{For any integer } n,\ n^2 \text{ is odd if and only if } n \text{ is odd.}$$

   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:

$$\text{For all integers } x \text{ and } y,\ \text{if } x^2(y^2 - 2y) \text{ is odd then } x \text{ and } y \text{ are odd.}$$

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.

[63] courses/math1061/proof-techniques.pdf

(⇐) 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.

(⇒) 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

$$x^2(y^2-2y) = x^2\big((2\ell)^2 - 2(2\ell)\big) = 2\big(x^2(2\ell^2-2\ell)\big).$$

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[64].

[64] courses/math1061/rational-and-irrational-numbers.pdf

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:

   $$\text{For a real number } r, \text{ if } 2r^2 - 3r \text{ is irrational, then } r \text{ is irrational.}$$

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

   $$\text{For every rational number } r, \text{ if } r \neq 0, \text{ then } r\sqrt{2} \text{ is an irrational number.}$$

   (a) Write down the negation of the statement.

   (b) Use a proof by contradiction to prove the statement.

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. $\square$

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[65]*.*

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.

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

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 $m^2 \mid nq$. $\square$

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 $4 \mid \big[(k+2)^2 - (m-3)^2\big]$. $\square$

   (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. $\square$

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. $\square$

§14 — Modular Arithmetic

Epp 4th ed. pp. 482–485 · 5th ed. (metric) pp. 528–531. Lecture 11 (week 4). Notes: modular-arithmetic[66].

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 $58 \bmod 11$.

   (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 $r^2 \bmod 5$:

   $$0^2 \equiv 0, \quad 1^2 \equiv 1, \quad 2^2 \equiv 4, \quad 3^2 \equiv 9 \equiv 4, \quad 4^2 \equiv 16 \equiv 1 \pmod 5.$$

   Thus $y^2 \equiv 0, 1, \text{ or } 4 \pmod 5$, and never 2 or 3. $\square$

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

2. (a) Since $58 = 11 \cdot 5 + 3$ with $0 \le 3 < 11$, we have

$$58 \operatorname{div} 11 = 5 \quad \text{and} \quad 58 \bmod 11 = 3.$$

(b) We want $-95 = 11q + r$ with $0 \le r < 11$. 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, $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$.** 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. $\square$

§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[67].

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 $\operatorname{lcm}(116, 88)$.

[67] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

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. $\square$

(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 $n \geq 2$. $\square$

(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 $n \geq 7$, $3^n < n!$. $\square$

(d) **For each integer $n \geq 1$, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$.**

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 $n \geq 1$. $\square$

(e) **For each integer $n \geq 0$, $1 + 4n \leq 5^n$.**

Proof. Let $P(n)$ be the predicate $1+4n \le 5^n$.

Basis: when $n=0$ we have $1+4\cdot 0 \le 5^0$, so $P(0)$ is true.

(The inductive step is to show that for all integers $k \ge 0$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose $k \ge 0$ is an integer and $P(k)$ is true; that is, $1+4k \le 5^k$.

Now consider $n = k+1$. Starting with the left-hand side of $P(k+1)$, we have

$$\begin{aligned} 1+4(k+1) &= 1+4k+4 \\ &\le 5^k + 4 && \text{by the inductive hypothesis} \\ &\le 5^k + 4\cdot 5^k && \text{since } k \ge 0 \text{ so } 5^k \ge 1 \\ &= 5(5^k) \\ &= 5^{k+1} \end{aligned}$$

so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $1+4n \le 5^n$ for every integer $n \ge 0$. ☐

§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

   $$\text{For every integer } n \ge 2, \text{ there exist integers } a, b \ge 0 \text{ such that } n = 2a+3b.$$

   (a) Prove the statement using the well-ordering principle.

   (b) Prove the statement using strong mathematical induction.

2. The Lucas sequence $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. 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 $n \ge 0$.

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 $n \geq 2$. □

   (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. □

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 $m = 0, 1, \dots, k$.

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 $n \geq 0$. $\square$

§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 $U = \{a_1, a_2, \dots, a_n\}$, 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 $A \times B \subseteq A \times C$. $\square$

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 $A - (B \cup C) = (A - B) - C$. $\square$

   Proof Option 2.

   $$\begin{aligned} A - (B \cup C) &= A \cap (B \cup C)^c && \text{by the Set Difference Law} \\ &= A \cap (B^c \cap C^c) && \text{by De Morgan's law} \\ &= (A \cap B^c) \cap C^c && \text{by Associative law} \\ &= (A - B) \cap C^c && \text{by the Set Difference Law} \\ &= (A - B) - C && \text{by the Set Difference Law} \qquad \square \end{aligned}$$

§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) $f(aba) = 0$, $f(bbab) = 2$, $f(b) = 0$, range$(f) = \mathbb{Z}^{\geq 0}$.

   (b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, 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 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 $\mathbb{Z} \times \mathbb{Z} \times \ldots$ 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 $A_1, A_2, A_3, \ldots$ be countable. Then for each n we can list A_n as

$$A_n = \{a_{n,1}, a_{n,2}, a_{n,3}, \ldots\}.$$

Now list the union by going along diagonals:

$$a_{1,1};\ a_{1,2}, a_{2,1};\ a_{1,3}, a_{2,2}, a_{3,1};\ a_{1,4}, a_{2,3}, a_{3,2}, a_{4,1};\ \ldots$$

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 $0.a_1a_2a_3 \dots a_n \dots$ 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 $\{0, 1, \dots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

   $$f(0.a_1a_2a_3 \dots a_n \dots) = g,$$

   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:

- $(2,3) \in R$
- $(3,2) \in R$
- $(1,1) \notin R$
- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) 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. 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.

§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. $\square$

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

$$s \, \rho \, t \text{ if and only if } \operatorname{weight}(s) \leq \operatorname{weight}(t).$$

   (a) Prove that ρ is not an equivalence relation.

   (b) Prove that ρ is not a partial order relation.

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. $\square$

   (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 $s \neq t$.

§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
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 $(\mathbb{Z}, +)$. $\square$
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. $\square$

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

$$
\begin{aligned}
(a,b)\cdot((c,d)\cdot(e,f)) &= (a,b)\cdot(ce+3df,\ cf+de)\\
&= \big(a(ce+3df)+3b(cf+de),\ a(cf+de)+b(ce+3df)\big)\\
&= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf)
\end{aligned}
$$

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 $\{1, 2, \ldots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \ldots, 15\}$ 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) $i = 1, \dots, 30$ gives 30 iterations and $j = 1, \dots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

   (b) $i = 5, \dots, 50$ gives $50 - 5 + 1 = 46$ iterations and $j = 10, \dots, 20$ gives $20 - 10 + 1 = 11$ iterations, so the inner loop runs $46 \cdot 11 = 506$ times.

   (c) $i = a, \dots, b$ gives $b - a + 1$ iterations and $j = c, \dots, d$ 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 $\binom{6}{4}3^2(-1)^4x^{3\cdot 4}$, 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 $U = \{1, 2, \dots, 600\}$. 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 $\{1, 2, \dots, 10\}$, 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 $S = \{1, 2, \dots, 100\}$. 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 $A = \{1, 2, \dots, 10\}$ 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 $i = 1, 2, \dots, 30$. Then

$$1 \le g_1 < g_2 < \cdots < g_{30} \le 45$$

because at least one game is played each day. Consider also the 30 numbers

$$g_1 + 14,\ g_2 + 14,\ \dots,\ g_{30} + 14,$$

which satisfy $15 \le g_1 + 14 < \cdots < g_{30} + 14 \le 59$. Thus we have 60 integers

$$g_1, \dots, g_{30},\ g_1 + 14, \dots, g_{30} + 14$$

all lying in the set $\{1, 2, \dots, 59\}$ 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_1v_2
b	v_2v_3
c	v_2v_3 (parallel to b)
d	v_3v_4
e	v_2v_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

$$\begin{aligned} \sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20 \\ \sum_{i=1}^{6} \deg(v_i) = 12. \end{aligned}$$

   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. □

See also

- math1061[68] — assessment weights and the full lecture schedule
- Logic: logical-connectives[69] · logical-equivalence-laws[70] · conditional-statements[71] · valid-argument-forms[72] · determining-argument-validity[73] · quantified-statements[74]
- Number theory and proof: proof-techniques[75] · rational-and-irrational-numbers[76] · divisibility-and-factorisation[77] · modular-arithmetic[78] · gcd-lcm-and-euclidean-algorithm[79]

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)

[68] courses/math1061/math1061.pdf
[69] courses/math1061/logical-connectives.pdf
[70] courses/math1061/logical-equivalence-laws.pdf
[71] courses/math1061/conditional-statements.pdf
[72] courses/math1061/valid-argument-forms.pdf
[73] courses/math1061/determining-argument-validity.pdf
[74] courses/math1061/quantified-statements.pdf
[75] courses/math1061/proof-techniques.pdf
[76] courses/math1061/rational-and-irrational-numbers.pdf
[77] courses/math1061/divisibility-and-factorisation.pdf
[78] courses/math1061/modular-arithmetic.pdf
[79] courses/math1061/gcd-lcm-and-euclidean-algorithm.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.

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.

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 obviously wrong — $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$. This is a contradiction, and we conclude the original statement is true. $\square$

The set-up comes straight from quantified-statements[80]: the negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D$ such that $P(x) \wedge \sim Q(x)$.

Useful negations to have ready (see logical-equivalence-laws[81]):

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

Proof by contraposition (shows the statement is true)

> We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely $\forall x \in D, \sim Q(x) \to \sim P(x)$. 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[82]).

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.

[80] courses/math1061/quantified-statements.pdf
[81] courses/math1061/logical-equivalence-laws.pdf
[82] courses/math1061/conditional-statements.pdf

- **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[83] 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[84] 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.

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. $\square$

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. $\square$

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. $\square$

$\forall n \in \mathbb{Z}^+$, 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. $\square$

[83] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[84] courses/math1061/2026-08-13-proof-by-contraposition.pdf

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[85] for the floor function.)

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. □

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

$\forall n \in \mathbb{Z}$, 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. $\square$

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. $\square$

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. $\square$

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[86]).

Common proof errors

The course explicitly tests spotting these:

- **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.
- **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.
- **Jumping to the conclusion** — writing down the definition you need to satisfy and then asserting it holds, without exhibiting the witnesses.
- **Forgetting to state assumptions**, or forgetting to say where a variable lives ("for some $r, s \in \mathbb{Z}$").

[86] courses/math1061/rational-and-irrational-numbers.pdf

- **Confusion between what is known and what is to be shown.**
- **Use of the word *any* instead of *some***, and **misuse of the word *if***.

See also

- quantified-statements[87] — the negations these proofs are built on
- conditional-statements[88] · logical-equivalence-laws[89]
- rational-and-irrational-numbers[90] · divisibility-and-factorisation[91]
- practice-problems[92] — §9 Direct Proofs and Counterexamples, with full worked solutions
- practice-problems[93] — §10 Proof by Contradiction, with full worked solutions
- practice-problems[94] — §11 Proof by Contraposition, with full worked solutions

Quantified Statements

Where logical-connectives[95] and conditional-statements[96] deal with whole statements, **predicates** let us talk about statements whose truth depends on a variable, and **quantifiers** turn those predicates back into statements that are definitely true or false.

Predicates

A **predicate** is a sentence with a finite number of variables that becomes a statement when particular values are assigned to those variables.

- Predicates: $x > 0$, "x divides y".
- Not predicates: "Is it raining?" (a question), "She is happy." (no objective truth value).

A predicate is written $P(x)$, and the set of values x may take is its **domain** D.

Common domains

[87] courses/math1061/quantified-statements.pdf
[88] courses/math1061/conditional-statements.pdf
[89] courses/math1061/logical-equivalence-laws.pdf
[90] courses/math1061/rational-and-irrational-numbers.pdf
[91] courses/math1061/divisibility-and-factorisation.pdf
[92] courses/math1061/practice-problems.pdf
[93] courses/math1061/practice-problems.pdf
[94] courses/math1061/practice-problems.pdf
[95] courses/math1061/logical-connectives.pdf
[96] courses/math1061/conditional-statements.pdf

Symbol	Set
$\mathbb{R}$	real numbers
$\mathbb{Q}$	rational numbers
$\overline{\mathbb{Q}}$	irrational numbers ($\mathbb{R} \setminus \mathbb{Q}$)
$\mathbb{Z}$	integers, $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$\mathbb{N}$	natural numbers
$\mathbb{Z}^+$	positive integers, $\{1, 2, 3, \dots\}$
$\mathbb{Z}^{\text{nonneg}} = \mathbb{Z}^{\geq 0}$	$\{0, 1, 2, 3, \dots\}$
$\mathbb{Z}^{\text{even}}$	$\{\dots, -4, -2, 0, 2, 4, \dots\}$

Nesting: $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$, with $\overline{\mathbb{Q}}$ sitting alongside $\mathbb{Q}$ inside $\mathbb{R}$.

Take care with $\mathbb{N}$ — different sources define it as $\{0, 1, 2, \dots\}$ *or* $\{1, 2, 3, \dots\}$. Prefer the unambiguous $\mathbb{Z}^+$ or $\mathbb{Z}^{\geq 0}$ in your own writing.

$\in$ means "belongs to" / "is an element of"; $\notin$ means "is not an element of". Note that $\{\mathbb{Z}\} \neq \mathbb{Z}$ — writing $x \in \{\mathbb{Z}\}$ says x *is* the set $\mathbb{Z}$, not that x is an integer.

The two quantifiers

Symbol	Reads	Associated English words
$\forall$	"for all"	all, every, any, each, none, no
$\exists$	"there exists"	there is, some, at least one, not all

- **Universal**: $\forall x \in D, P(x)$ — "for all x in D, $P(x)$".
- **Existential**: $\exists x \in D$ such that $P(x)$ — "there exists an x in D such that $P(x)$". "such that" is commonly abbreviated **s.t.**

Note the punctuation convention: $\forall$ takes a comma, $\exists$ takes "such that".

Translating English to symbols

English	Symbolic
Every rational number is a real number.	$\forall x \in \mathbb{Q}, x \in \mathbb{R}$
No integer is an irrational number.	$\forall x \in \mathbb{Z}, x \notin \overline{\mathbb{Q}}$
Some real numbers are rational.	$\exists x \in \mathbb{R}$ s.t. $x \in \mathbb{Q}$
Not all rational numbers are integers.	$\exists x \in \mathbb{Q}$ s.t. $x \notin \mathbb{Z}$
All prime numbers are odd.	$\forall x \in P, x$ is odd

English	Symbolic
If an integer is divisible by 2 then it is divisible by 4.	$\forall x \in \mathbb{Z}$, if $2 \mid x$ then $4 \mid x$

Two things to watch:

- **"No …" is universal, not existential** — "no integer is irrational" becomes $\forall$, with the predicate negated.
- **Sometimes the quantifier is implicit.** "If an integer is a square, then it is nonnegative" carries a hidden $\forall$: $\forall n \in \mathbb{Z}$, if n is a square then $n \geq 0$.

Determining truth

- $\forall x \in D, P(x)$ is shown **false** by one counterexample.
- $\exists x \in D$ s.t. $P(x)$ is shown **true** by one example.

The asymmetry matters: a single value can settle a universal statement only in the negative, and an existential statement only in the positive.

$\exists y \in \mathbb{Z}$ s.t. $y^2 - y = 0$ is **true** — choose $y = 0$ or $y = 1$. That some other choice ($y = 2$) fails is irrelevant; $\exists$ only asks for one witness. The corresponding universal statement $\forall y \in \mathbb{Z}, y^2 - y = 0$ is false, and $y = 2$ is exactly the counterexample that shows it.

$\forall x \in \mathbb{Z}$, if 6 is divisible by x then $x = 2$ is **false** — take $x = 3$: it's an integer, 6 is divisible by 3, but $3 \neq 2$. (The corrected true statement is $\forall x \in \mathbb{Z}$, if 6 is divisible by x then $x = \pm 1, \pm 2, \pm 3$ or ± 6.)

Negation

Negating a quantified statement **flips the quantifier and negates the predicate**:

$$\sim (\forall x \in D, P(x)) \equiv \exists x \in D \text{ s.t. } \sim P(x)$$

$$\sim (\exists x \in D \text{ s.t. } P(x)) \equiv \forall x \in D, \sim P(x)$$

If the negation of a statement is true, the original is false — so proving the negation is a legitimate way to disprove a statement (see proof-techniques[97]).

[97] courses/math1061/proof-techniques.pdf

When the predicate is itself conditional, negate it with $\sim (p \to q) \equiv p \wedge \sim q$ (see logical-equivalence-laws[98]). So the negation of

$$\forall x \in \mathbb{Z}, \text{ if } x^2 > 3 \text{ then } x > 3$$

is $\exists x \in \mathbb{Z}$ s.t. $x^2 > 3$ **and** $x \leq 3$ — *not* "if … then …" with an $\exists$ in front, and not the converse.

A negation is not just "the opposite-sounding statement"

For $S = \{1, 3, 5, 7\}$, $\{1, 2, 3, 4\}$, $\{2, 4, 6, 8\}$:

S	$\forall x \in S, x$ is odd	$\forall x \in S, x$ is not odd	$\exists x \in S$ s.t. x is not odd
$\{1, 3, 5, 7\}$	T	F	F
$\{1, 2, 3, 4\}$	F	F	T
$\{2, 4, 6, 8\}$	F	T	T

The first and *third* columns are exact negations of each other (they disagree in every row). The middle column — "all are not odd" — is **not** the negation: for $S = \{1, 2, 3, 4\}$ both it and the original are false.

Worked negations

Statement	Negation	Which is true
$\exists y \in \mathbb{R}$ s.t. $y^2 < 0$	$\forall y \in \mathbb{R}, y^2 \geq 0$	negation
All dogs are white.	Some dog is not white.	negation
$\forall x \in \mathbb{Z}^+, x$ is prime or x is composite	$\exists x \in \mathbb{Z}^+$ s.t. x is neither prime nor composite	negation ($x = 1$)
$\forall x \in \mathbb{R}$, if $x > 2$ then $x^2 > 4$	$\exists x \in \mathbb{R}$ s.t. $x > 2$ and $x^2 \leq 4$	original
$\forall x \in \mathbb{R}$, if $x^2 > 9$ then $x \geq 2$	$\exists x \in \mathbb{R}$ s.t. $x^2 > 9$ and $x < 2$	negation ($x = -4$)

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

Multiple quantifiers

Order matters. Read the statement left to right as a game:

- $\forall x \in X, \exists y \in Y$ s.t. $P(x, y)$ — "someone gives me an x; can I *always* then find a y?" The choice of y may depend on x.
- $\exists x \in X$ s.t. $\forall y \in Y, P(x, y)$ — "is there a *single* x that works for *every* y?" The x must be chosen before seeing y.

Both of these happen to be true for $xy \geq y$ over $\mathbb{Z}$, but for different reasons:

1. $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $xy \geq y$ — given x, choose $y = x$ (since $x^2 \geq x$ for every integer), or more simply $y = 0$.
2. $\exists x \in \mathbb{Z}$ s.t. $\forall y \in \mathbb{Z}, xy \geq y$ — take $x = 1$, since $y \geq y$ always.

Where order really bites: $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $y = 2x$ is **true** (given x, take $y = 2x$), but $\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $x = 2y$ is **false** — take $x = 3$, and $y = \frac{3}{2} \notin \mathbb{Z}$.

Writing two of the same quantifier

$\exists x \in D$ and $\exists y \in E \ldots$ is the clearest form; $\exists x \in D$ and $y \in E \ldots$ is common shorthand, and $\exists x, y \in D \ldots$ is shorthand when both range over the same domain.

Negating multiple quantifiers

Flip **every** quantifier in order, and negate the predicate at the end:

$$\sim (\forall x \in X, \exists y \in Y \text{ s.t. } P(x, y)) \equiv \exists x \in X \text{ s.t. } \forall y \in Y, \sim P(x, y)$$

Worked examples:

Statement	Negation	Which is true
$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $x + y = 0$	$\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, x + y \neq 0$	original (take $y = -x$)
$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = 1$	$\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, xy \neq 1$	negation ($x = 0$)
$\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R}, xy = 0$	$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy \neq 0$	original (take $x = 0$)
$\exists x \in \mathbb{Z}^+$ s.t. $\forall y \in \mathbb{Z}^+, x \geq y$	$\forall x \in \mathbb{Z}^+, \exists y \in \mathbb{Z}^+$ s.t. $x < y$	negation (take $y = x + 1$)
$\forall x, y \in \mathbb{Z}, \exists z \in \mathbb{Z}$ s.t. $z = x - y$	$\exists x, y \in \mathbb{Z}$ s.t. $\forall z \in \mathbb{Z}, z \neq x - y$	original
$\forall r, s \in \mathbb{R}$, if $rs \in \mathbb{Q}$ then $r \in \mathbb{Q}$ and $s \in \mathbb{Q}$	$\exists r, s \in \mathbb{R}$ s.t. $rs \in \mathbb{Q}$ and ($r \notin \mathbb{Q}$ or $s \notin \mathbb{Q}$)	negation ($r = s = \sqrt{2}$)

A negation trap: the negation of "$\forall x \in \mathbb{Z}, \exists y \in \mathbb{Z}$ s.t. $x + y$ is odd" is "**there exists** an integer x such that **for every** integer y, $x + y$ is even". (The original is true: if x is odd take $y = 0$, if x is even take $y = 1$.)

See also

- logical-connectives[99] · logical-equivalence-laws[100] · conditional-statements[101]
- proof-techniques[102] — proving and disproving quantified statements
- practice-problems[103] — §6 Quantified Statements, with full worked solutions
- practice-problems[104] — §7 Negation of Quantified Statements, with full worked solutions
- practice-problems[105] — §8 Statements with Multiple Quantifiers, with full worked solutions

Rational & Irrational Numbers

The definitions and closure results that make $\mathbb{Q}$ a workable object in proofs, plus the classic irrationality argument.

Definitions

$$r \in \mathbb{Q} \iff \exists a, b \in \mathbb{Z} \text{ such that } r = \frac{a}{b} \text{ and } b \neq 0$$

$$r \in \overline{\mathbb{Q}} \iff r \notin \mathbb{Q}$$

$\overline{\mathbb{Q}} = \mathbb{R} \setminus \mathbb{Q}$ is the set of **irrational** numbers. Examples: $\frac{3}{4} \in \mathbb{Q}$; $\sqrt{2} \in \overline{\mathbb{Q}}$; $\pi \in \overline{\mathbb{Q}}$.

Note the definition is existential: to show r is rational you must **exhibit** integers a and b with $b \neq 0$. Nearly every proof below ends by checking three things — the numerator is an integer, the denominator is an integer, and the denominator is non-zero.

Fact: every rational number can be written as a fraction in **lowest terms** (numerator and denominator have no common factors).

[99] courses/math1061/logical-connectives.pdf
[100] courses/math1061/logical-equivalence-laws.pdf
[101] courses/math1061/conditional-statements.pdf
[102] courses/math1061/proof-techniques.pdf
[103] courses/math1061/practice-problems.pdf
[104] courses/math1061/practice-problems.pdf
[105] courses/math1061/practice-problems.pdf

Why irrationality statements want contradiction or contraposition

"r is irrational" is a *negative* statement — $r \notin \mathbb{Q}$ — so a direct proof has nothing to unfold. Assuming the negation instead ($r \in \mathbb{Q}$) hands you $r = \frac{a}{b}$ to work with. See proof-techniques[106] for the general shape.

Concretely, for **the sum of any rational number and any irrational number is irrational**:

- Symbolically: $\forall r, s \in \mathbb{R}$, if $r \in \mathbb{Q}$ and $s \in \overline{\mathbb{Q}}$ then $r + s \in \overline{\mathbb{Q}}$ — or equivalently $\forall r \in \mathbb{Q}$ and $\forall s \in \mathbb{R}$, if $s \in \overline{\mathbb{Q}}$ then $r + s \in \overline{\mathbb{Q}}$.
- **Direct proof**: suppose $r \in \mathbb{Q}$ and $s \in \overline{\mathbb{Q}}$ — and now you're stuck, because $s \in \overline{\mathbb{Q}}$ gives you nothing to substitute.
- **Contradiction**: suppose $\exists r \in \mathbb{Q}, s \in \mathbb{R}$ with $s \in \overline{\mathbb{Q}}$ and $r + s \in \mathbb{Q}$.
- **Contraposition**: prove $\forall r \in \mathbb{Q}$ and $\forall s \in \mathbb{R}$, if $r + s \in \mathbb{Q}$ then $s \in \mathbb{Q}$.

  Proof by contraposition. Suppose $r \in \mathbb{Q}$, $s \in \mathbb{R}$ and $r + s \in \mathbb{Q}$. Since $r \in \mathbb{Q}$, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Since $r + s \in \mathbb{Q}$, $r + s = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ with $d \neq 0$. Now
  $$s = (r + s) - r = \frac{c}{d} - \frac{a}{b} = \frac{bc - ad}{bd}.$$
  Since $a, b, c, d \in \mathbb{Z}$ we know $bc - ad \in \mathbb{Z}$ and $bd \in \mathbb{Z}$; and $bd \neq 0$ since $b \neq 0$ and $d \neq 0$. Thus $s \in \mathbb{Q}$. $\square$

The trick that makes it work is writing the thing you want in terms of the things you have: $s = (r + s) - r$.

Closure results

$\forall r \in \mathbb{Q}, (2r^2 - 3r + 1) \in \mathbb{Q}$ — direct proof is best here; contraposition gets stuck.

> Let $r \in \mathbb{Q}$, so $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Then
> $$2r^2 - 3r + 1 = \frac{2a^2}{b^2} - \frac{3ab}{b^2} + \frac{b^2}{b^2} = \frac{2a^2 - 3ab + b^2}{b^2}.$$
> Since $a, b \in \mathbb{Z}$ we have $2a^2 - 3ab + b^2 \in \mathbb{Z}$ and $b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $2r^2 - 3r + 1 \in \mathbb{Q}$. $\square$

$\forall r \in \mathbb{R}$, if r^2 is irrational then r is irrational. Proved by contraposition in proof-techniques[107] — the contrapositive is "if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$".

For real m, n: if m is irrational and n is rational, then $m - n$ is irrational.

[106] courses/math1061/proof-techniques.pdf
[107] courses/math1061/proof-techniques.pdf

Proof by contradiction. Suppose m is irrational, n is rational, but $m-n$ is rational. Then $n = \frac{a}{b}$ and $m-n = \frac{c}{d}$ for integers a, b, c, d with $b, d \neq 0$. Since $m = (m-n)+n$,

$$m = \frac{c}{d} + \frac{a}{b} = \frac{bc+ad}{bd},$$

with $bc+ad \in \mathbb{Z}$, $bd \in \mathbb{Z}$ and $bd \neq 0$. So m is rational, contradicting the assumption. □

For a real number r: if $2r^2 - 3r$ is irrational, then r is irrational.

Proof by contraposition. The contrapositive is: if $r \in \mathbb{Q}$ then $2r^2 - 3r \in \mathbb{Q}$. Let $r = \frac{a}{b}$ with $a, b \in \mathbb{Z}$, $b \neq 0$. Then $2r^2 - 3r = \frac{2a^2-3ab}{b^2}$, with integer numerator and non-zero integer denominator. □

For all real r, s and n: if r is irrational, s is rational and n is a positive integer, then $n(r-s)$ is irrational.

Proof by contradiction. Suppose otherwise: $r \in \overline{\mathbb{Q}}$, $s \in \mathbb{Q}$, $n \in \mathbb{Z}^+$, but $n(r-s) \in \mathbb{Q}$. Write $s = \frac{a}{b}$ and $n(r-s) = \frac{c}{d}$ with $b, d \neq 0$. Since $n \neq 0$,

$$r = s + \frac{c}{d} \cdot \frac{1}{n} = \frac{a}{b} + \frac{c}{dn} = \frac{adn+bc}{bdn}.$$

Here $adn + bc \in \mathbb{Z}$, $bdn \in \mathbb{Z}$, and $bdn \neq 0$ since b, d, n are all non-zero. So $r \in \mathbb{Q}$ — a contradiction. □

For every rational r, if $r \neq 0$ then $r\sqrt{2}$ is irrational. Negation: $\exists r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

Proof by contradiction. Suppose the negation holds. Since $r \in \mathbb{Q}$, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and $a \neq 0$ because $r \neq 0$. Since $r\sqrt{2} \in \mathbb{Q}$, $r\sqrt{2} = \frac{c}{d}$ for integers c, d with $d \neq 0$. Then

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad},$$

where $bc \in \mathbb{Z}$, $ad \in \mathbb{Z}$ and $ad \neq 0$ (since $a \neq 0$ and $d \neq 0$). So $\sqrt{2} \in \mathbb{Q}$ — contradicting the theorem below. □

$\sqrt{2}$ is irrational

The set-up needs two ingredients: the lowest-terms fact above, and the lemma **for all integers n, if n^2 is even then n is even** (proved by contraposition — see proof-techniques[108]).

[108]courses/math1061/proof-techniques.pdf

Proof by contradiction. Suppose $\sqrt{2}$ is rational. Then $\sqrt{2} = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and we may assume $\frac{a}{b}$ is in lowest terms.

Squaring, $2 = \frac{a^2}{b^2}$, so $a^2 = 2b^2$ and thus a^2 is even. By the lemma, a is even, so $a = 2\ell$ for some $\ell \in \mathbb{Z}$.

Substituting: $2b^2 = a^2 = (2\ell)^2 = 4\ell^2$, so $b^2 = 2\ell^2$ and b^2 is even. By the lemma again, b is even.

But now a and b are both even, so they share the common factor 2 — contradicting the assumption that $\frac{a}{b}$ is in lowest terms. Therefore $\sqrt{2} \in \overline{\mathbb{Q}}$. $\square$

Neither a direct proof nor a contraposition proof gets off the ground here: the statement isn't a conditional with a usable hypothesis, so contradiction is the only one of the three that has anywhere to start.

See also

- proof-techniques[109] — direct / counterexample / contradiction / contraposition
- quantified-statements[110]
- divisibility-and-factorisation[111]
- practice-problems[112] — §12 Rational Numbers, with full worked solutions

[109] courses/math1061/proof-techniques.pdf
[110] courses/math1061/quantified-statements.pdf
[111] courses/math1061/divisibility-and-factorisation.pdf
[112] courses/math1061/practice-problems.pdf