MATH1061 — Week 13 Notes

Table of contents

Lecture 34 — Walks, Trails and Circuits **1**

Goals . . . 1
The bridges of Königsberg . . . 2
Recap: graphs, degree and the Handshake Theorem . . . 3
Two vertices of the same degree . . . 3
Worked: counting with the Handshake Theorem . . . 3
Complete graphs . . . 4
Walks, trails and circuits . . . 5
Worked: walks, trails and circuits in K_4 . . . 5
Euler circuits and Euler trails . . . 6
Worked: which graphs have an Euler circuit or trail . . . 8
Worked: an Euler trail from a to e . . . 9
Deciding: the flowchart . . . 11
See also . . . 13

Lecture 35 — Matrix Representations of Graphs **13**

Goals . . . 14
The running example . . . 14
Worked: edges between pairs of vertices . . . 15
The adjacency matrix . . . 16
Worked: write down the adjacency matrix . . . 16
Worked: draw the graph of an adjacency matrix . . . 17
Worked: which is an adjacency matrix . . . 19
Worked: how many times is a vertex incident with an edge . . . 20
The incidence matrix . . . 20
Which way round . . . 21
Worked: write down the incidence matrix . . . 21
Worked: draw the graph of an incidence matrix . . . 23
Worked: which is an incidence matrix . . . 23

Worked: Eulerian from the incidence matrix . . . 25
See also . . . 26

Lecture 36 — Trees **27**
Goals . . . 27
Trivial and non-trivial circuits . . . 27
Trees . . . 28
The 11 trees with 7 vertices . . . 28
Deleting an edge from a tree . . . 32
A tree with n vertices has $n-1$ edges . . . 33
Worked: degree 3 or degree 1 . . . 36
Worked: how many vertices . . . 37
Worked: two vertices of degree 1 . . . 38
Worked: degrees $n-2$ and $n-3$ . . . 39
See also . . . 40

Reference material **40**
Adjacency Matrices . . . 40
Euler Circuits and Trails . . . 47
Graphs . . . 57
Incidence Matrices . . . 66
The Pigeonhole Principle . . . 72
Practice Problems — the Semester-wide Set . . . 80
Proof Techniques — Direct, Counterexample, Contradiction, Contraposition . . . 205
Strong Induction and the Well-Ordering Principle . . . 214
Trees . . . 222
Walks, Trails and Circuits . . . 228

Lecture 34 — Walks, Trails and Circuits

A recap of the graph theory so far (degree, the Handshake Theorem, the pigeonhole argument for equal degrees, complete graphs), then getting around a graph: walks, trails, circuits and connected graphs, and the theorem that says exactly when a graph has an Euler circuit, a circuit using every edge once, or an Euler trail. Pre-work: Video 044 (Walks, Trails and Circuits). Walks, trails, circuits and connectedness are in walks-trails-and-circuits[1]. Euler circuits and trails, the theorem with its proof, how to find one, and the decision flowchart are in euler-circuits-and-trails[2]. The basic definitions are in [graphs].

[1] courses/math1061/walks-trails-and-circuits.pdf
[2] courses/math1061/euler-circuits-and-trails.pdf

Goals

1. Understand the basic terminology and definitions of graph theory.
2. Understand the conditions required for a graph to have an Euler circuit or trail.

Two questions to keep in mind:

- **What is the difference between an Euler circuit and an Euler trail?** Both use every edge of the graph exactly once. An Euler circuit finishes at the vertex it started from; an Euler trail from u to v starts at u and finishes at a different vertex v. For a connected graph the odd-degree vertices decide which one there is: none gives an Euler circuit, exactly two gives an Euler trail from one to the other, and more gives neither (the theorem).
- **How do I actually find an Euler circuit?** First decide whether there is one, from the degrees and connectedness (the flowchart). Then build it by splicing: walk along unused edges until stuck, and while edges are left, take a vertex on the route that still has unused edges, walk a circuit from it, and insert that circuit into the route. It is done in full for an Euler trail on ten vertices, and the method, with why it always works, is in euler-circuits-and-trails[3].

The bridges of Königsberg

The city of Königsberg had four land masses, the north bank A, the island B, the south bank C and the eastern part D, joined by seven bridges. Is there a walk around the city that crosses every bridge exactly once? As a graph, each land mass is a vertex and each bridge an edge. A and B are joined by two bridges, and so are B and C, so the graph has multiple edges.

The degrees are $\deg A = 3$, $\deg B = 5$, $\deg C = 3$, $\deg D = 3$, adding to $14 = 2 \cdot 7$. A walk that crosses every bridge once and comes back is an **Euler circuit**, and one that finishes on a different land mass from where it started is an **Euler trail**. By the theorem below the first needs every degree even, and the second needs exactly two odd degrees. Here all four are odd, so neither exists. The problem is set up in 2026-07-27-welcome-and-intro-problems[4], where the land masses are lettered differently.

Recap: graphs, degree and the Handshake Theorem

All in [graphs]: a graph is a non-empty set of vertices and a possibly empty set of edges, each edge having one or two endpoints (graphs[5]). A **loop** has one endpoint, **multiple edges** (parallel edges) share their endpoints, and a graph is **simple** if it has neither (graphs[6]). The

[3] courses/math1061/euler-circuits-and-trails.pdf
[4] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[5] courses/math1061/graphs.pdf
[6] courses/math1061/graphs.pdf

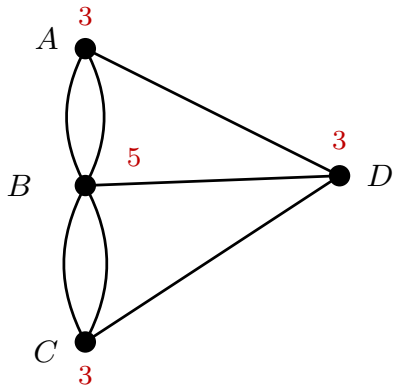


Figure 1: The bridges of Königsberg as a graph: land masses A, B, C, D as vertices and the seven bridges as edges. Every vertex has odd degree, 3, 5, 3 and 3. An Euler circuit needs every degree even and an Euler trail needs exactly two odd degrees, so there is neither: no walk crosses every bridge exactly once.

degree of a vertex is the number of edge ends at it, so a loop adds 2: a vertex with two ordinary edges and a loop has degree 4 (graphs[7]). The **Handshake Theorem**: for a graph with vertices $v_1, \dots, v_n$ and e edges,

$$\sum_{i=1}^{n} \deg(v_i) = 2e,$$

since every edge has two ends (graphs[8]).

Two vertices of the same degree

> **Theorem.** Any simple graph with at least two vertices has two vertices of the same degree.

Proof idea. With n vertices, a vertex of a simple graph has degree between 0 and $n-1$. Degrees 0 and $n-1$ cannot both occur: a vertex of degree $n-1$ is adjacent to every other vertex, so none has degree 0. So the degrees all lie in $\{1, 2, \dots, n-1\}$ or all lie in $\{0, 1, \dots, n-2\}$, at most $n-1$ values for n vertices, and by the pigeonhole principle two vertices share a degree.

For $n = 6$: if some vertex has degree 5, the degrees are among $1, 2, 3, 4, 5$; otherwise they are among $0, 1, 2, 3, 4$. Five values either way, for six vertices. The full proof, with a figure, is in pigeonhole-principle[9].

[7] courses/math1061/graphs.pdf
[8] courses/math1061/graphs.pdf
[9] courses/math1061/pigeonhole-principle.pdf

Worked: counting with the Handshake Theorem

(a) A graph has 5 vertices with degree sequence 3, 3, 2, 2, 2. How many edges does the graph have?

(b) A graph has 6 vertices and 10 edges. If five of its vertices have degree 3, what is the degree of its other vertex?

(a) 6 edges. Let e be the number of edges. By the Handshake Theorem,

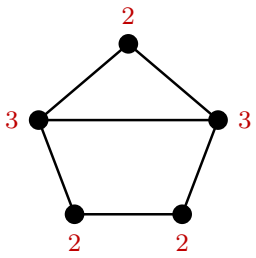
$$3 + 3 + 2 + 2 + 2 = 2e, \qquad 12 = 2e, \qquad e = 6.$$

The degree sequence fixes the number of edges, but not the graph. A pentagon with one chord has these degrees and is simple. So does a graph made of three parallel edges between two vertices, two parallel edges between two more, and a loop at the fifth vertex, which is not simple. Both have 6 edges.

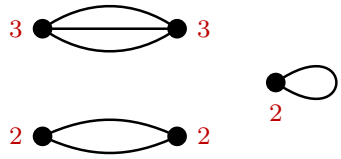
(b) Degree 5. Let x be the degree of the other vertex. By the Handshake Theorem,

$$3 + 3 + 3 + 3 + 3 + x = 2 \cdot 10, \qquad 15 + x = 20, \qquad x = 5.$$

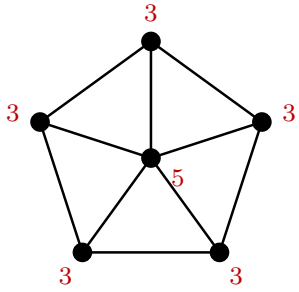
Such a graph exists: join one vertex to all five others, and join those five in a ring. Each ring vertex has its two ring neighbours and the centre, degree 3, and the centre has degree 5. That is $5 + 5 = 10$ edges.



(a) simple, 6 edges



(a) not simple, 6 edges



(b) 10 edges

Figure 2: Graphs for the two counting questions, each vertex labelled with its degree. Left: a pentagon with one chord, a simple graph with degrees 3, 3, 2, 2, 2 and 6 edges. Middle: three parallel edges, two parallel edges and a loop, a non-simple graph with the same degrees and also 6 edges. The degree sequence fixes the number of edges, not the graph. Right: one vertex joined to the five vertices of a ring, 10 edges, with the centre of degree 5 and the other five of degree 3.

Complete graphs

In a simple graph there are no loops, and each pair of vertices is joined by at most one edge. There are $\binom{n}{2}$ pairs of vertices, so a simple graph with n vertices has **at most** $\binom{n}{2}$ **edges**.

> The simple graph with n vertices and $\binom{n}{2}$ edges is called the **complete graph of order** n and is denoted K_n.

It joins every pair of vertices, so every vertex has degree $n-1$. More on these in graphs[10].

n	1	2	3	4	5	6	7
edges of K_n, $\binom{n}{2}$	0	1	3	6	10	15	21
degree of each vertex	0	1	2	3	4	5	6

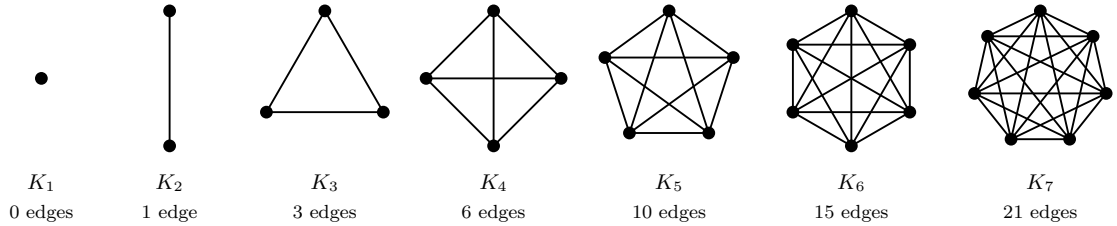


Figure 3: The complete graphs K_1 to K_7. Each joins every pair of its n vertices once, so it has $\binom{n}{2}$ edges and every vertex has degree $n-1$. Lines cross where there is no vertex; only the dots are vertices.

Walks, trails and circuits

The definitions, in full with examples in walks-trails-and-circuits[11]:

> A **walk** is a sequence $v_0\, e_1\, v_1\, e_2\, v_2 \cdots e_n\, v_n$ where each v_i is a vertex and each e_i is an edge with endpoints v_{i-1} and v_i.
> A **trail** is a walk where $e_1, e_2, \ldots, e_n$ are pairwise distinct.
> A **circuit** is a trail $v_0\, e_1\, v_1 \cdots e_n\, v_n$ where $v_0 = v_n$.
> A graph is **connected** if and only if there is a walk from any given vertex to any other given vertex.

A trail has **no repeated edges**, but it may repeat vertices. The route below is a trail that passes through one vertex twice.

[10] courses/math1061/graphs.pdf
[11] courses/math1061/walks-trails-and-circuits.pdf

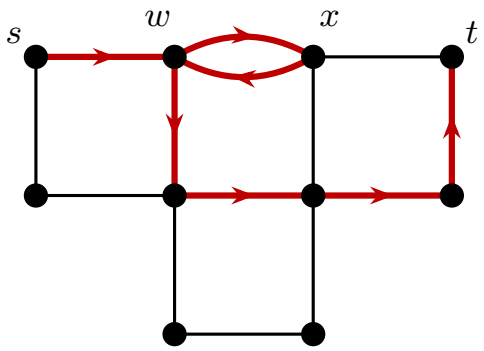


Figure 4: A trail on a graph with two parallel edges at the top. The route, in red, starts at s, goes from w to x along one of the parallel edges and back to w along the other, then goes down and right to finish at t. It passes through w twice but uses no edge twice, since the two parallel edges are different edges, so it is a trail. It ends at $t \neq s$, so it is not a circuit. It uses 7 of the 14 edges, so it is not an Euler trail either.

Worked: walks, trails and circuits in K_4

Determine whether the complete graph K_4 contains the following:
(a) A walk that is not a trail.
(b) A trail that is not a circuit.
(c) An Euler circuit.

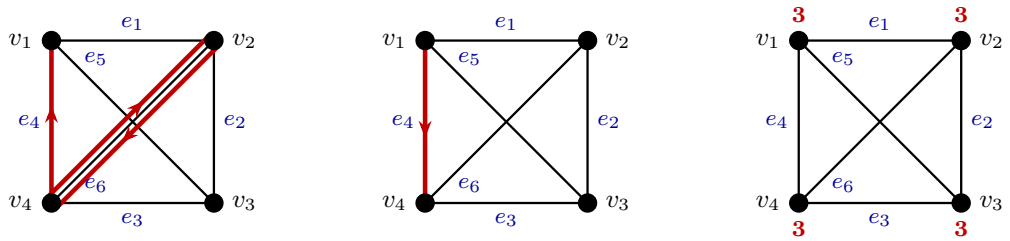
Label K_4 with vertices v_1, v_2, v_3, v_4 and edges $e_1 = v_1v_2$, $e_2 = v_2v_3$, $e_3 = v_3v_4$, $e_4 = v_1v_4$, $e_5 = v_1v_3$, $e_6 = v_2v_4$.

(a) Yes. $v_4\, e_6\, v_2\, e_6\, v_4\, e_4\, v_1$. Each edge joins the vertices on either side of it, so it is a walk. It uses e_6 twice, so it is not a trail.

(b) Yes. $v_1\, e_4\, v_4$. A single edge is a trail, since no edge is repeated, and it ends at $v_4 \neq v_1$, so it is not a circuit.

(c) No. K_4 is connected, but every vertex has degree 3, which is odd, so by the theorem there is no Euler circuit. In fact there is no Euler trail either: that needs exactly two vertices of odd degree, and K_4 has four.

Other answers work for (a) and (b). Any route that goes out and back along one edge answers (a), and any trail that ends somewhere other than its start answers (b), for example $v_1\, e_1\, v_2\, e_2\, v_3\, e_5\, v_1\, e_4\, v_4$, which repeats v_1 but no edge.



(a) walk, not a trail (b) trail, not a circuit (c) all degrees odd: none

Figure 5: The three parts on K_4. (a) The walk $v_4, e_6, v_2, e_6, v_4, e_4, v_1$: the doubled red line is e_6 used twice, so it is a walk but not a trail. (b) The trail v_1, e_4, v_4: one edge, no repeats, and it ends at a different vertex from where it started. (c) Every vertex of K_4 has degree 3, odd, so there is no Euler circuit, and with four odd vertices no Euler trail either.

Euler circuits and Euler trails

> An **Euler circuit** is a circuit that contains every edge of the graph.
> An **Euler trail from vertex u to vertex v** is a trail that starts at u and ends at v and contains every edge of the graph.

A graph with an Euler circuit is called **Eulerian**.

> **Theorem.** Let G be a connected graph. Then G has an Euler circuit if and only if every vertex of G has even degree. Let $u, v \in V(G)$ be distinct vertices of G. Then G has an Euler trail from u to v if and only if u and v have odd degree and all other vertices of G have even degree.

Why the degrees. Each time a route passes through a vertex it arrives along one edge and leaves along another, using two edge ends there. If the route uses every edge exactly once, it uses every edge end at a vertex, so the degree is twice the number of passes, which is even. The exceptions are the start and the end: a trail from u to $v \neq u$ leaves u once without having arrived and arrives at v once without leaving, so those two have odd degree. For a circuit the start and end are the same vertex and pair up. The other direction, that the right degrees **guarantee** an Euler circuit or trail when the graph is connected, is proved by building one, in euler-circuits-and-trails[12].

This course uses the standard definitions above. The textbook defines an Euler circuit as a circuit that contains every vertex **and** every edge. For connected graphs the two agree. In a connected graph with at least one edge every vertex is the endpoint of some edge, so a route

[12] courses/math1061/euler-circuits-and-trails.pdf

using every edge passes through every vertex. A connected graph with no edges is a single vertex, and the trivial circuit there contains it. They differ when there are isolated vertices.

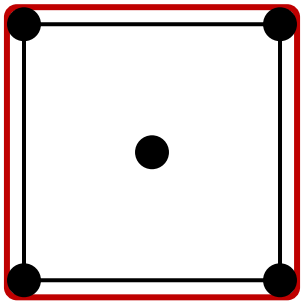


Figure 6: A square and an isolated vertex in the middle. Going once round the square, in red, is a circuit that contains every edge, so by this course's definition the graph has an Euler circuit. By the textbook's definition, which also asks for every vertex, it does not, since no circuit reaches the middle vertex.

More on the two definitions, with the proof that they agree for connected graphs, is in euler-circuits-and-trails[13].

Worked: which graphs have an Euler circuit or trail

> For each of the following graphs, determine whether the graph has an Euler circuit. For those that do not contain an Euler circuit, determine whether the graph has an Euler trail.

Graph	Degrees	Connected?	Odd vertices	Verdict
G_1	2, 4, 4, 2 (top), 2, 4, 4, 2 (middle), 2, 2 (bottom)	yes	none	**Euler circuit**
G_2	3, 2, 2, 2, 3	yes	two	**no Euler circuit; Euler trail**
G_3	5, 3, 3, 5, 4, 4	yes	four	**neither**
G_4	2, 2, 2, 4, 4	yes	none	**Euler circuit**
G_5	2 for all eight	**no**	none	**neither**

[13] courses/math1061/euler-circuits-and-trails.pdf

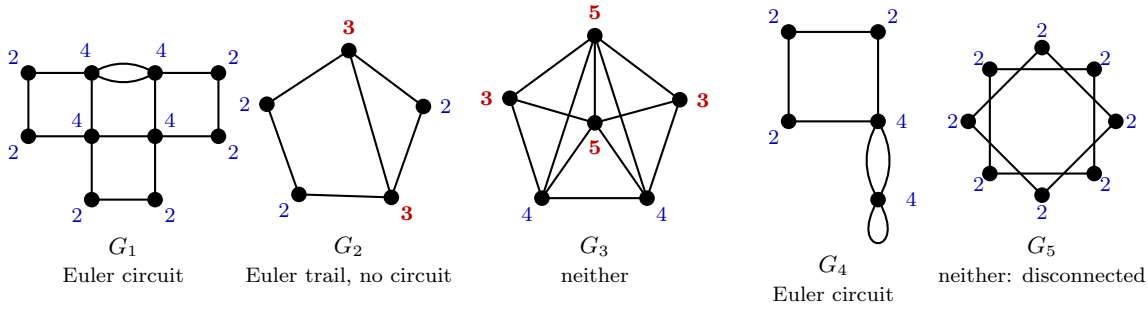


Figure 7: The five graphs, each vertex labelled with its degree, odd degrees in red. G_1 has two parallel edges at the top, and in G_4 the bottom vertex has two parallel edges and a loop, which adds 2. G_1 and G_4 are connected with every degree even, so they have Euler circuits. G_2 has exactly two odd vertices, so it has an Euler trail between them. G_3 has four odd vertices, so it has neither. In G_5 every degree is even, but the graph is two separate squares, since the crossings are not vertices, so it has neither.

- G_1. 14 edges, degrees adding to 28. Every degree is even and the graph is connected, so it has an Euler circuit. The two parallel edges at the top each count once at each end, which is why those two vertices have degree 4.
- G_2. A pentagon with a chord. The two ends of the chord have degree 3 and the rest degree 2. Exactly two odd vertices, so there is no Euler circuit, but there is an Euler trail from one end of the chord to the other: start at the top vertex, go all the way round the pentagon back to the top, then take the chord down.
- G_3. 12 edges. The top vertex and the centre each have degree 5, the left and right vertices degree 3, and the bottom two degree 4. Four odd vertices: no Euler circuit and no Euler trail.
- G_4. 7 edges: the square, the two parallel edges and the loop. The loop adds 2, so the bottom vertex has degree $2 + 2 = 4$, and the square's bottom-right corner has degree 4 too. All even and connected, so there is an Euler circuit: round the square, down one parallel edge, round the loop, back up the other.
- G_5. Every degree is 2, so the degrees alone would suggest an Euler circuit. But the lines cross at points that are not vertices, and the graph is **two separate squares**, an upright one and a tilted one. It is not connected, and a single route cannot use edges in both pieces, so there is no Euler circuit and no Euler trail. The theorem only applies to connected graphs.

Worked: an Euler trail from a to e

Use the theorem to show that the graph below has an Euler trail from a to e, and find one.

The graph has 21 edges: ab, ah, ai, bc, bd, bh, cd, cf, ci, de, df, ef, fg, fi, fj, gh, gi, gj, hi, ij, je. The graph is simple, so a route can be written as a list of vertices.

Vertex	a	b	c	d	e	f	g	h	i	j
Degree	**3**	4	4	4	**3**	6	4	4	6	4

The degrees add to $42 = 2 \cdot 21$. Vertices a and e have odd degree, all other vertices have even degree, and the graph is connected, so by the theorem it has an Euler trail from a to e.

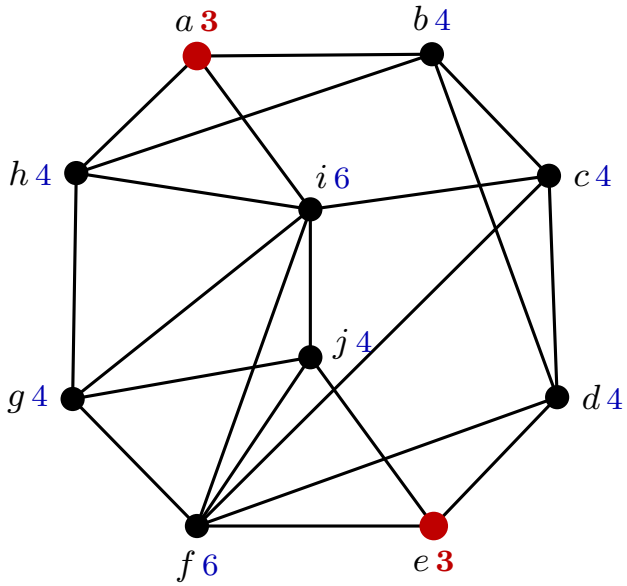


Figure 8: The graph on a to j, each vertex labelled with its degree. Only a and e, in red, have odd degree, and the graph is connected, so there is an Euler trail from a to e and no Euler circuit. Lines cross at several points that are not vertices.

Finding one by splicing. Start at a, one of the two odd vertices, and walk along unused edges until stuck:

$$a,\ b,\ c,\ d,\ e,\ f,\ j,\ e.$$

At e all three edges are now used, so this is stuck, at e as it must be. It uses 7 of the 21 edges. The 14 unused edges give every vertex even degree, and j is on the route and still has unused edges (ji and jg). Walk from j along unused edges until stuck, which brings it back to j:

$$j,\ i,\ c,\ f,\ i,\ a,\ h,\ i,\ g,\ h,\ b,\ d,\ f,\ g,\ j.$$

That uses the other 14 edges. Insert it into the first route at j:

$$a,\ b,\ c,\ d,\ e,\ f,\ \underbrace{j,\ i,\ c,\ f,\ i,\ a,\ h,\ i,\ g,\ h,\ b,\ d,\ f,\ g,\ j}_{\text{inserted}},\ e.$$

This is an Euler trail from a to e: 21 edges, each of the 21 exactly once, starting at a and ending at e. It passes through f and i three times each, using all six edges at each.

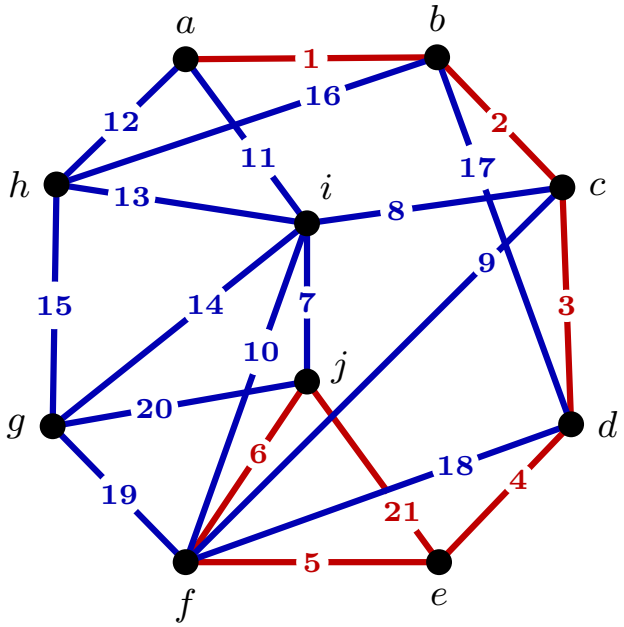


Figure 9: The Euler trail from a to e, with each edge numbered in the order the trail uses it. Red: the first walk from a, which gets stuck at e after 7 edges. Blue: the circuit from j through the 14 unused edges, inserted into the first walk at j, between edges 6 and 21. Following the numbers 1 to 21 gives $a, b, c, d, e, f, j, i, c, f, i, a, h, i, g, h, b, d, f, g, j, e$.

The trail is not unique. Walking differently until stuck, or inserting at a different vertex, gives other Euler trails from a to e, and reversing any of them gives an Euler trail from e to a.

Deciding: the flowchart

How to tell whether a graph has an Euler circuit, connected or not:

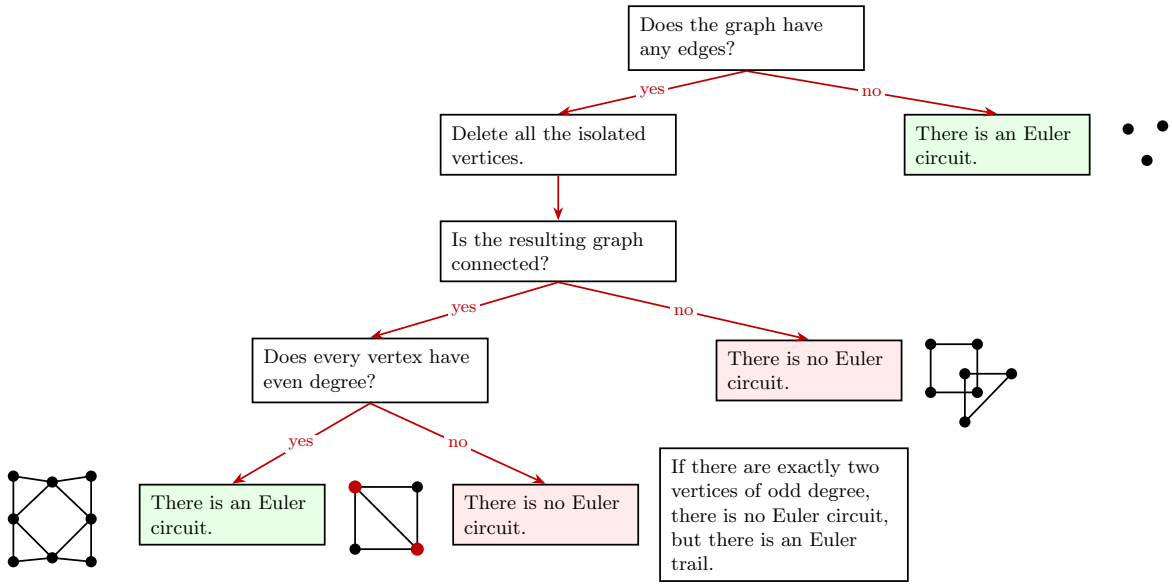


Figure 10: Deciding whether a graph has an Euler circuit, with an example graph at each outcome. No edges: the trivial circuit counts, as for three isolated vertices. Otherwise delete the isolated vertices and check that what is left is connected. A square and a triangle that only cross in the drawing are two pieces, so there is no Euler circuit even though every degree is even. Then check the degrees: the eight-vertex graph has degrees 2 and 4 and has an Euler circuit, while the square with one diagonal has two vertices of degree 3, so it has no Euler circuit but does have an Euler trail.

Each step, in words:

1. **No edges at all.** Then there is an Euler circuit: the trivial circuit, a single vertex, contains every edge, since there are none.
2. **Delete the isolated vertices.** A route never needs to visit a vertex with no edges, and this course's definition only asks for every edge.
3. **Not connected.** Two edges in different pieces cannot be on one route, so there is no Euler circuit, and no Euler trail either.
4. **Connected.** The theorem decides: every degree even gives an Euler circuit. Otherwise there is no Euler circuit, and if there are exactly two vertices of odd degree, there is an Euler trail from one to the other.

A version that also sorts out the Euler trail case completely, with why each step is right, is in euler-circuits-and-trails[14].

See also

- walks-trails-and-circuits[15] — walks, trails, circuits, trivial circuits, circuit-free and connected graphs
- euler-circuits-and-trails[16] — the theorem with a full proof, how to find an Euler circuit or trail, the flowchart, and the textbook's definition
- [graphs] — degree, the Handshake Theorem and complete graphs
- pigeonhole-principle[17] — two vertices of equal degree in a simple graph
- 2026-07-27-welcome-and-intro-problems[18] — the bridges of Königsberg, first posed
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[19] — Lecture 33
- 2026-10-27-matrix-representations-of-graphs[20] — Lecture 35
- practice-problems[21] — §44, with full worked solutions

Lecture 35 — Matrix Representations of Graphs

Two ways to write a graph down as a table of numbers. The **adjacency matrix** has a row and a column for each vertex and records how many edges join each pair of vertices. The **incidence matrix** has a row for each vertex and a column for each edge and records how many times each vertex is incident with each edge. Both go in both directions: a graph gives a matrix,

[14] courses/math1061/euler-circuits-and-trails.pdf
[15] courses/math1061/walks-trails-and-circuits.pdf
[16] courses/math1061/euler-circuits-and-trails.pdf
[17] courses/math1061/pigeonhole-principle.pdf
[18] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[19] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[20] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[21] courses/math1061/practice-problems.pdf

and a matrix of the right kind gives a graph. Pre-work: Video 045 (Matrix Representations of Graphs). The definitions, how loops are counted, reading a graph off a matrix and which matrices qualify are in adjacency-matrices[22] and incidence-matrices[23]. Graphs, degree and the Handshake Theorem are in [graphs].

Goals

1. Learn how to represent a graph by an adjacency matrix.
2. Learn how to represent a graph by an incidence matrix.
3. Learn how to draw a graph from its adjacency matrix.
4. Learn how to draw a graph from its incidence matrix.

Two questions to keep in mind:

- **In an incidence matrix, which are the rows and which are the columns: the vertices or the edges?** The vertices are the rows and the edges are the columns, as in the definition. There is a way to remember it in which way round.
- **Is it OK to swap them?** The swapped matrix holds the same information, but it is not the incidence matrix as this course defines it. Also in which way round.

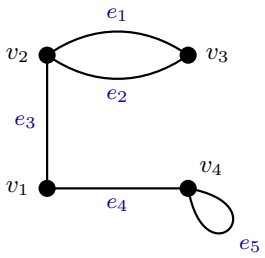
The running example

One graph is used all the way through. It has vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{e_1, e_2, e_3, e_4, e_5\}$, with

Edge	Endpoints
e_1	$\{v_2, v_3\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_1, v_2\}$
e_4	$\{v_1, v_4\}$
e_5	$\{v_4\}$

So e_1 and e_2 are parallel edges, and e_5 is a loop at v_4. The degrees are $\deg(v_1) = 2$, $\deg(v_2) = 3$, $\deg(v_3) = 2$ and $\deg(v_4) = 3$, the loop adding 2 to $\deg(v_4)$. They add to $10 = 2 \cdot 5$.

[22] courses/math1061/adjacency-matrices.pdf
[23] courses/math1061/incidence-matrices.pdf



$A =$

	v_1	v_2	v_3	v_4
v_1	0	1	0	1
v_2	1	0	**2**	0
v_3	0	**2**	0	0
v_4	1	0	0	**1**

$N =$

	e_1	e_2	e_3	e_4	e_5
v_1	0	0	1	1	0
v_2	1	1	1	0	0
v_3	1	1	0	0	0
v_4	0	0	0	1	**2**

Figure 11: The running example and its two matrices. The adjacency matrix A has a row and a column for each vertex, and each entry counts the edges joining that pair of vertices: the 2 is the pair of parallel edges between v2 and v3, and the 1 on the diagonal is the single loop at v4. The incidence matrix N has a row for each vertex and a column for each edge, and each entry counts how many times that vertex is incident with that edge: the 2 is the loop, which meets v4 at both of its ends.

Worked: edges between pairs of vertices

For the running example, how many edges have the following as endpoints?
(a) $\{v_1, v_2\}$
(b) $\{v_1, v_3\}$
(c) $\{v_1, v_4\}$
(d) $\{v_2, v_3\}$
(e) $\{v_4\}$

	Endpoints	Edges	Number
(a)	$\{v_1, v_2\}$	e_3	1
(b)	$\{v_1, v_3\}$	none	0
(c)	$\{v_1, v_4\}$	e_4	1
(d)	$\{v_2, v_3\}$	e_1, e_2	2
(e)	$\{v_4\}$	e_5	1

For (e), the set of endpoints $\{v_4\}$ has one element, so the edges with that set of endpoints are the loops at v_4. There is one, e_5.

These five numbers are entries of the adjacency matrix. Answers (a), (b) and (c), with a 0 for "no loop at v_1", are the first row, 0 1 0 1. Answer (d) is the entry in row v_2, column v_3, and answer (e) is the diagonal entry in row v_4, column v_4.

The adjacency matrix

> The **adjacency matrix** of a graph with vertices $v_1, v_2, \ldots, v_n$ is the $n \times n$ matrix $A = [a_{ij}]$ where each entry a_{ij} is the number of edges with endpoints $\{v_i, v_j\}$.

When $i = j$ the set $\{v_i, v_i\}$ is just $\{v_i\}$, so a diagonal entry a_{ii} is the **number of loops** at v_i. A loop is one edge, so it counts **1** on the diagonal. In the running example $a_{44} = 1$ for the single loop e_5.

Three things follow straight from the definition:

- $\{v_i, v_j\} = \{v_j, v_i\}$, so $a_{ij} = a_{ji}$: **the matrix is symmetric**.
- Every entry counts edges, so every entry is a **non-negative integer**.
- A loop adds 2 to a degree but only 1 to the matrix. So $\deg(v_i)$ **is the row sum plus the diagonal entry**. In the running example row v_4 adds to $1 + 0 + 0 + 1 = 2$, and $\deg(v_4) = 2 + a_{44} = 3$.

More on all three, and the proofs, in adjacency-matrices[24].

Worked: write down the adjacency matrix

> Write down the adjacency matrix for the graph below.

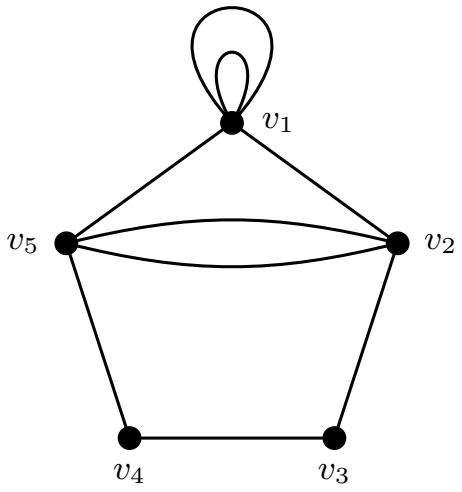


Figure 12: The graph for the first question: five vertices around a pentagon, two loops at v1, and two parallel edges between v5 and v2. It has 9 edges in all.

[24] courses/math1061/adjacency-matrices.pdf

Answer.

$$A = \begin{array}{c|ccccc} & v_1 & v_2 & v_3 & v_4 & v_5 \\ \hline v_1 & 2 & 1 & 0 & 0 & 1 \\ v_2 & 1 & 0 & 1 & 0 & 2 \\ v_3 & 0 & 1 & 0 & 1 & 0 \\ v_4 & 0 & 0 & 1 & 0 & 1 \\ v_5 & 1 & 2 & 0 & 1 & 0 \end{array}$$

Go through the pairs once each, then copy across the diagonal, since the matrix is symmetric.

- **Diagonal.** Two loops at v_1, so $a_{11} = 2$. No other vertex has a loop.
- **Row v_1.** One edge to v_2, one to v_5, none to v_3 or v_4.
- **Row v_2.** One edge to v_3 and two parallel edges to v_5, so $a_{25} = 2$.
- **Rows v_3 and v_4.** One edge v_3v_4 and one edge v_4v_5.

Two checks.

- **Edge count.** Each edge is counted once in the upper triangle with the diagonal: $(2+1+0+0+1)+(0+1+0+2)+(0+1+0)+(0+1)+0 = 4+3+1+1+0 = 9$, the 9 edges of the graph.
- **Degrees.** Row sum plus diagonal entry: $\deg(v_1) = 4+2 = 6$, the two loops giving 4 of it, and $\deg(v_2) = 4$, $\deg(v_3) = 2$, $\deg(v_4) = 2$, $\deg(v_5) = 4$. They add to $18 = 2 \cdot 9$, as the graphs[25] says they must.

Worked: draw the graph of an adjacency matrix

Draw the graph with this adjacency matrix.

	v_1	v_2	v_3	v_4	v_5
v_1	2	1	0	3	1
v_2	1	0	0	0	2
v_3	0	0	0	1	0
v_4	3	0	1	0	1
v_5	1	2	0	1	0

First check that it can be an adjacency matrix: it is square, symmetric and its entries are non-negative integers. Then read **only the diagonal and the entries above it**. Each entry below the diagonal repeats one above it, and reading both would draw every edge twice.

[25] courses/math1061/graphs.pdf

Entry	Value	Edges
a_{11}	2	two loops at v_1
a_{12}	1	one edge v_1v_2
a_{14}	3	three parallel edges v_1v_4
a_{15}	1	one edge v_1v_5
a_{25}	2	two parallel edges v_2v_5
a_{34}	1	one edge v_3v_4
a_{45}	1	one edge v_4v_5

Every other entry on or above the diagonal is 0. That is $2+1+3+1+2+1+1 = 11$ edges.

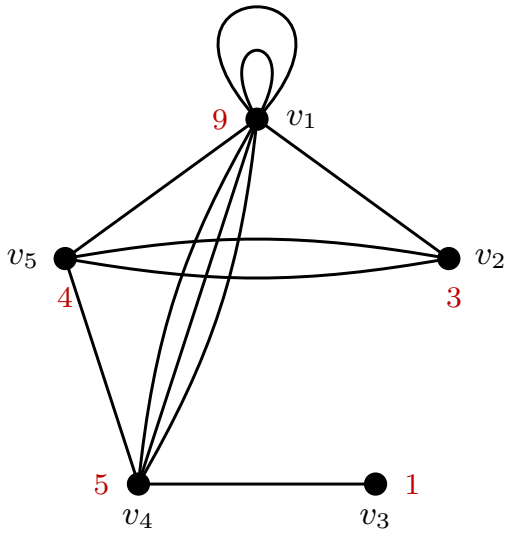


Figure 13: The graph drawn from the matrix: two loops at v1, three parallel edges between v1 and v4, two between v2 and v5, and single edges v1v2, v1v5, v3v4 and v4v5. The three v1v4 edges cross the two v2v5 edges, but crossings are not vertices. The degrees, in red, are each row sum plus the diagonal entry, so v1 has degree $7 + 2 = 9$. They add to 22, twice the 11 edges.

The degrees are $\deg(v_1) = 7 + 2 = 9$, $\deg(v_2) = 3$, $\deg(v_3) = 1$, $\deg(v_4) = 5$ and $\deg(v_5) = 4$, a total of $22 = 2 \cdot 11$. Where the vertices go on the page is free. The matrix fixes only which vertices are joined, and how many times.

Worked: which is an adjacency matrix

Which of the following is an adjacency matrix for a graph?

A. $\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$

B. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

C. $\begin{bmatrix} 73 \end{bmatrix}$

D. $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

Answer: C.

A matrix is an adjacency matrix of some graph exactly when it is **square**, **symmetric** and has **non-negative integer** entries (adjacency-matrices[26]).

- **A** is square and symmetric, but -1 cannot be a number of edges.
- **B** is 2×3. An adjacency matrix has one row and one column for each vertex, so it is always square.
- **C** is 1×1, trivially symmetric, and 73 is a non-negative integer. It is the graph with **one vertex and 73 loops**. That vertex has degree $73 + 73 = 146$, and the graph has 73 edges.
- **D** is square with non-negative integer entries, but not symmetric: $a_{24} = 2$ and $a_{42} = 1$. The number of edges between v_2 and v_4 cannot be both 2 and 1. Every other pair matches across the diagonal; this one pair is enough.

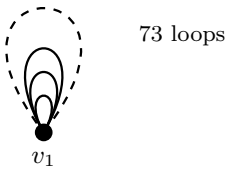


Figure 14: The graph of the 1 by 1 matrix [73]: a single vertex with 73 loops, three of them drawn and the dashed one standing for the rest. Its one diagonal entry counts the loops, 73, and its degree is twice that, 146.

[26] courses/math1061/adjacency-matrices.pdf

Worked: how many times is a vertex incident with an edge

For the running example:
(a) How many times is v_1 incident with e_1?
(b) How many times is v_1 incident with e_4?
(c) How many times is v_2 incident with e_2?
(d) How many times is v_4 incident with e_5?

(a) 0. The endpoints of e_1 are v_2 and v_3, so e_1 does not meet v_1.

(b) 1. e_4 joins v_1 and v_4. One of its ends is at v_1.

(c) 1. e_2 joins v_2 and v_3. One of its ends is at v_2.

(d) 2. e_5 is a loop at v_4. Both of its ends are at v_4, so it meets v_4 twice. This is the same count that makes a loop add 2 to a degree (graphs[27]).

The incidence matrix

The **incidence matrix** of a graph with vertices $v_1, v_2, \dots, v_n$ and edges $e_1, e_2, \dots, e_m$ is the $n \times m$ matrix $N = [n_{ij}]$ where each entry n_{ij} is the number of times vertex v_i is incident with edge e_j.

The answers above are four of its entries: $n_{11} = 0$, $n_{14} = 1$, $n_{22} = 1$ and $n_{45} = 2$. The whole matrix for the running example is in the figure.

- **A column is an edge.** It has a 1 at each of the edge's two endpoints, or a single 2 at the vertex of a loop. Either way **every column adds to 2**: every edge has two ends.
- **A row is a vertex.** It adds up the ends of edges at that vertex, so **the row sum is the degree**, loops included. In the running example the rows add to $2, 3, 2, 3$.
- **Parallel edges are identical columns.** The columns of e_1 and e_2 are both $(0, 1, 1, 0)$.

Adding up all the entries by columns gives $2m$, and by rows gives the sum of the degrees. That is the graphs[28] again. More in incidence-matrices[29].

[27] courses/math1061/graphs.pdf
[28] courses/math1061/graphs.pdf
[29] courses/math1061/incidence-matrices.pdf

Which way round

Rows are vertices, columns are edges. One way to remember it: the entry n_{ij} answers "how many times is **vertex** v_i incident with **edge** e_j", and the index that comes first, i, is the row, so the vertex comes first. Another: the adjacency matrix has a row for each vertex, and so does the incidence matrix. Both matrices have n rows, one per vertex; they differ only in their columns, vertices for A and edges for N.

Swapping them gives the transpose N^{T}, the $m \times n$ matrix with a row for each edge. It holds exactly the same information. The graph can be rebuilt from it just as well, with every *row* adding to 2 and every *column* adding to a degree. But it is not the incidence matrix as this course defines it. When asked for the incidence matrix, put the vertices down the side and the edges across the top, and label both.

The question does not arise for the adjacency matrix, because it is symmetric: swapping rows and columns gives the same matrix. What does matter for both is the **order** of the vertices, and for N the order of the edges. A different order permutes the rows or columns and gives a different matrix for the same graph, which is why the rows and columns should always be labelled.

Worked: write down the incidence matrix

Write down the incidence matrix for the graph below.

Answer.

$$N = \begin{array}{c|cccc} & e_1 & e_2 & e_3 & e_4 \\ \hline v_1 & 2 & 0 & 0 & 0 \\ v_2 & 0 & 1 & 1 & 0 \\ v_3 & 0 & 0 & 0 & 0 \\ v_4 & 0 & 0 & 0 & 1 \\ v_5 & 0 & 1 & 1 & 1 \end{array}$$

Fill it one column, one edge, at a time.

- e_1 is a loop at v_1: a 2 in row v_1 and 0 elsewhere.
- e_2 and e_3 both join v_5 and v_2: a 1 in rows v_2 and v_5. Being parallel, they give the same column.
- e_4 joins v_5 and v_4: a 1 in rows v_4 and v_5.

Checks. Every column adds to 2. The row sums are the degrees, $2, 2, 0, 1, 3$, adding to $8 = 2 \cdot 4$. The row of v_3 is all zeros, because v_3 is isolated: a vertex still gets its row even when no edge meets it.

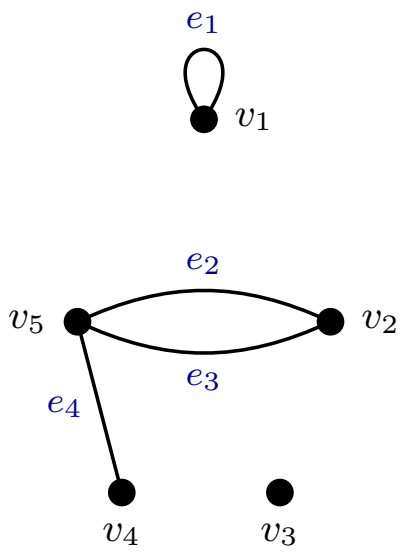


Figure 15: The graph for the incidence-matrix question: a loop e1 at v1, two parallel edges e2 and e3 between v5 and v2, an edge e4 from v5 to v4, and an isolated vertex v3. The loop gives v1 the entry 2 in column e1, and v3, which meets no edge, gives a row of zeros.

Worked: draw the graph of an incidence matrix

Draw the graph with this incidence matrix.

	e_1	e_2	e_3	e_4
v_1	2	1	0	0
v_2	0	1	0	0
v_3	0	0	2	0
v_4	0	0	0	1
v_5	0	0	0	1

Every column adds to 2, so it is an incidence matrix. Read it one column at a time. A column with two 1s is an edge between those two vertices, and a column with a single 2 is a loop.

Column	Entries	Edge
e_1	2 at v_1	loop at v_1
e_2	1 at v_1, 1 at v_2	v_1v_2
e_3	2 at v_3	loop at v_3
e_4	1 at v_4, 1 at v_5	v_4v_5

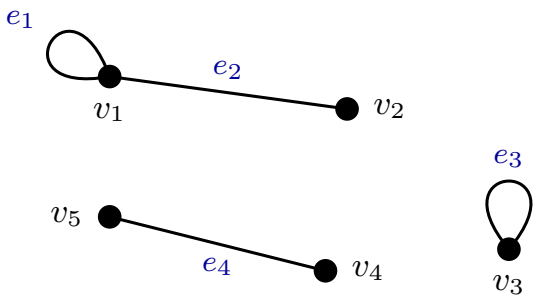


Figure 16: The graph drawn from the incidence matrix: each column is one edge. Columns e1 and e3 each have a single 2, so they are loops, at v1 and at v3. Columns e2 and e4 each have two 1s, so they join v1 to v2 and v4 to v5. The graph falls into three pieces. The row sums 3, 1, 2, 1, 1 are the degrees, and add to 8, twice the 4 edges.

Worked: which is an incidence matrix

Which of the following is an incidence matrix for a graph?

A. $\begin{bmatrix} 1 & 0 \\ 0 & 3 \end{bmatrix}$

B. $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$

C. $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$

D. $\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 2 & 2 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$

Answer: B.

A matrix is an incidence matrix of some graph exactly when its entries are non-negative integers and **every column adds to 2**, so that each column is either two 1s or a single 2 (incidence-matrices[30]). Check the columns.

	Column sums	Verdict
A	1, 3	no: the first column is an edge with one end, and no vertex can meet an edge 3 times
B	2, 2, 2	**yes**
C	1, 1	no: each column is an edge with only one end
D	2, 4, 2, 4	no: columns 2 and 4 would be edges with four ends

B has two rows and three columns, so two vertices and three edges, and each column $(1, 1)$ is an edge joining the two vertices. It is **two vertices joined by three parallel edges**.

In **C** a column with a single 1 is not a loop: a loop meets its vertex twice and is a single 2. In **D** the first and third columns are fine on their own, an edge v_2v_4 and a loop at v_2, but one bad column is enough to rule a matrix out. A square shape, or symmetry, has nothing to do with it: B is not square, and C is square and symmetric.

[30] courses/math1061/incidence-matrices.pdf

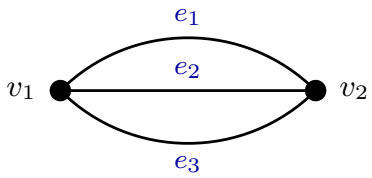


Figure 17: The graph of matrix B: two vertices and three edges. Each column of B is (1, 1), a 1 at each vertex, so each edge joins v1 and v2. The three columns are identical, which is exactly what three parallel edges look like in an incidence matrix.

Worked: Eulerian from the incidence matrix

For each of the following incidence matrices, determine whether the associated graph G is Eulerian. Explain why or why not.

(a) $N =$

	e_1	e_2	e_3	e_4	e_5	e_6
v_1	1	1	0	0	0	0
v_2	1	0	1	1	0	1
v_3	0	1	1	0	1	1
v_4	0	0	0	1	1	0

(b) $N =$

	a	b	c	d
u	1	0	1	0
v	0	1	0	1
w	0	1	0	1
x	1	0	1	0

A graph is **Eulerian** if it has an Euler circuit, a circuit that contains every edge (euler-circuits-and-trails[31]). The test is the theorem (euler-circuits-and-trails[32]):

> A **connected** graph has an Euler circuit if and only if every vertex has even degree.

The incidence matrix gives both halves of the test. The degrees are the row sums, and the columns say which vertices each edge joins, which settles whether the graph is connected.

(a) Yes, G is Eulerian.

The row sums give the degrees:

$$\deg(v_1) = 2, \quad \deg(v_2) = 4, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2.$$

All four are even. Reading the columns, the edges are $e_1 = v_1v_2$, $e_2 = v_1v_3$, $e_3 = v_2v_3$, $e_4 = v_2v_4$, $e_5 = v_3v_4$ and $e_6 = v_2v_3$, so e_3 and e_6 are parallel. G is connected: v_2 is joined to each of v_1, v_3 and v_4. A connected graph with every degree even has an Euler circuit, for example

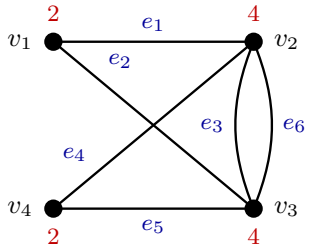
[31] courses/math1061/euler-circuits-and-trails.pdf
[32] courses/math1061/euler-circuits-and-trails.pdf

$$v_1\ e_1\ v_2\ e_3\ v_3\ e_6\ v_2\ e_4\ v_4\ e_5\ v_3\ e_2\ v_1.$$

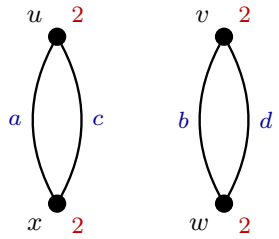
It uses $e_1, e_3, e_6, e_4, e_5, e_2$, each of the six edges exactly once, each edge joins the vertices on either side of it in the list, and it ends where it started.

(b) No, G is not Eulerian.

Every row adds to 2, so every vertex has even degree. But the columns show the edges are $a = ux$, $b = vw$, $c = ux$ and $d = vw$. No edge joins u or x to v or w, so G is **not connected**: it is two separate pieces, u and x joined by a and c, and v and w joined by b and d. A circuit is a walk, and a walk only moves along edges, so it never leaves the piece it starts in. No circuit can contain both a and b, so there is no Euler circuit. Even degrees are not enough on their own: the theorem needs the graph to be connected.



(a) connected, all even: Eulerian



(b) two pieces: not Eulerian

Figure 18: The two graphs read off the incidence matrices, degrees in red. Left, (a): every degree is even and the graph is connected, so it has an Euler circuit; the diagonals e2 and e4 cross without meeting. Right, (b): every degree is 2, but the graph is two separate pieces, and a circuit cannot get from one piece to the other, so no circuit uses every edge.

See also

- adjacency-matrices[33] — the definition, loops on the diagonal, reading a graph off, and which matrices are adjacency matrices
- incidence-matrices[34] — the definition, column sums and row sums, reading a graph off, which matrices qualify, and how the two matrices compare
- [graphs] — loops, parallel edges, degree and the Handshake Theorem
- euler-circuits-and-trails[35] — Euler circuits and trails and the even-degree theorem

[33] courses/math1061/adjacency-matrices.pdf
[34] courses/math1061/incidence-matrices.pdf
[35] courses/math1061/euler-circuits-and-trails.pdf

- walks-trails-and-circuits[36] — walks, circuits and connected graphs
- 2026-10-26-walks-trails-and-circuits[37] — Lecture 34
- 2026-10-29-trees[38] — Lecture 36
- practice-problems[39] — §45, with full worked solutions

Lecture 36 — Trees

Trees: connected graphs with no non-trivial circuits. The topics are trivial and non-trivial circuits, circuit-free graphs, the definition of a tree, what happens when an edge is deleted from a tree, and the main theorem: a graph with n vertices is a tree if and only if it is simple, connected and has $n-1$ edges. That theorem together with the Handshake Theorem answers most counting questions about trees, as in the four worked questions. Pre-work: Video 046 (Trees). The definitions, the theorem, vertices of degree 1 and the counting method are collected in [trees]. Walks, trails, circuits and connectedness are in walks-trails-and-circuits[40], and degree and the Handshake Theorem in [graphs].

Trees are the last topic of the course. For exam revision there is a high-level summary of the course topics, and review sessions for the final exam run the following week.

Goals

1. Understand the definition and properties of trees.
2. Gain fluency in graph theory proofs.

Trivial and non-trivial circuits

A circuit is a trail $v_0 e_1 v_1 e_2 \cdots e_n v_n$ with $v_0 = v_n$: a walk that ends where it starts and never uses an edge twice (walks-trails-and-circuits[41]). Nothing in that definition stops $n = 0$, so a single vertex on its own is a circuit.

> A **trivial circuit** is a circuit consisting of a single vertex and no edges.
> A **non-trivial circuit** is a circuit that has edges.
> A graph is **circuit-free** if there are no non-trivial circuits.

[36] courses/math1061/walks-trails-and-circuits.pdf
[37] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[38] courses/math1061/2026-10-29-trees.pdf
[39] courses/math1061/practice-problems.pdf
[40] courses/math1061/walks-trails-and-circuits.pdf
[41] courses/math1061/walks-trails-and-circuits.pdf

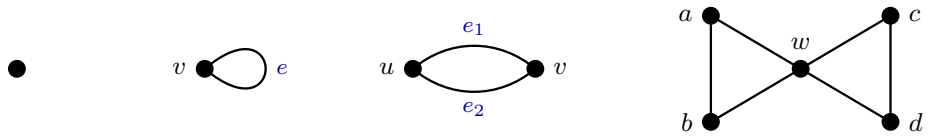
Every vertex is a trivial circuit, so every graph has circuits. That is why circuit-free asks only about the circuits that have edges.

The smallest non-trivial circuits:

- **A loop.** A loop e at v gives the circuit $v\,e\,v$, with one edge.
- **Two multiple edges.** If e_1 and e_2 both join u and v, then $u\,e_1\,v\,e_2\,u$ is a circuit: it ends where it starts, and its two edges are different.

So **a circuit-free graph has no loops and no multiple edges: it is simple.**

A circuit can pass through a vertex more than once. Only its edges cannot repeat.



trivial circuit
no edges

a loop
$v\,e\,v$

two multiple edges
$u\,e_1\,v\,e_2\,u$

$w\,a\,b\,w\,c\,d\,w$
w twice, no edge twice

Figure 19: Left: a single vertex is a trivial circuit, a circuit with no edges. The other three are non-trivial circuits. A loop at v is the circuit v, e, v. Two edges joining u and v make the circuit u, e_1, v, e_2, u, which is why a circuit-free graph has no multiple edges. The circuit on the right, w, a, b, w, c, d, w, visits w twice but uses each of its six edges once, so it is still a circuit.

Trees

Definition. A graph is a **tree** if and only if it is connected and circuit-free.

A single vertex is a tree: it is connected, and with no edges it has no non-trivial circuit. So is a single edge, and so is one vertex joined to three others. A triangle is connected but is a circuit, so it is not a tree. Two edges with no vertex in common are circuit-free but not connected, so that is not a tree either. And by the last section, every tree is simple.

The 11 trees with 7 vertices

There are 11 essentially different trees with 7 vertices. **Essentially different** means different in shape, not just in the names of the vertices or in how the tree is drawn. Two graphs are **isomorphic** when one can be turned into the other by renaming its vertices: there is a way to match the vertices of one with the vertices of the other so that two vertices are joined in the first exactly when the matching vertices are joined in the second. Isomorphic graphs are the

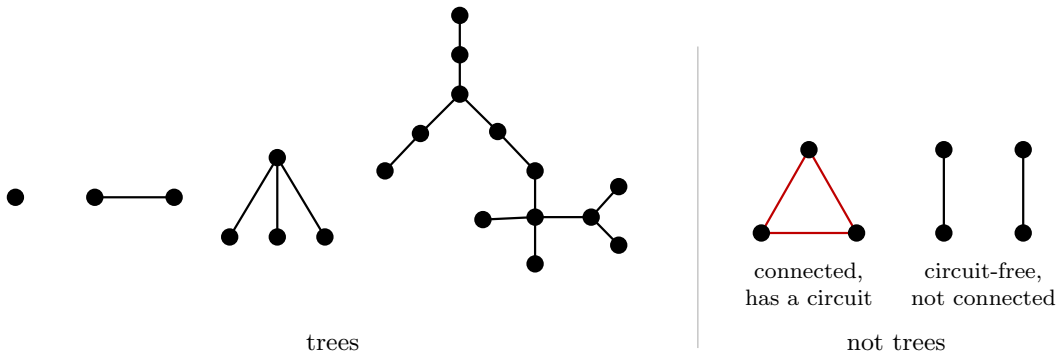


Figure 20: Left: four trees, a single vertex, a single edge, one vertex joined to three others, and a larger tree with 13 vertices. Each is connected, and none has a circuit with edges. Right: two graphs that are not trees. The triangle is connected but is itself a non-trivial circuit, in red. The two separate edges have no circuit, but there is no walk from one edge to the other, so the graph is not connected.

same graph with different labels, and count once. If the 7 vertices are named and two trees count as different whenever their edge sets differ, there are far more of them: $7^5 = 16807$.

Two words for telling trees apart. The **distance** between two vertices is the fewest edges on a walk from one to the other. The **diameter** of a tree is the largest distance between two of its vertices. Renaming vertices changes neither the degrees nor the distances, so **isomorphic trees have the same degree sequence and the same diameter.** Two trees that differ in either one are essentially different.

Tree	Shape	Degree sequence	Diameter	Told apart from the others with the same sequence and diameter by
1	7 vertices in a line	$2, 2, 2, 2, 2, 1, 1$	6	
2	6 in a line, one more on the second	$3, 2, 2, 2, 1, 1, 1$	5	the degree-3 vertex has **two** neighbours of degree 1
3	6 in a line, one more on the third	$3, 2, 2, 2, 1, 1, 1$	5	the degree-3 vertex has **one** neighbour of degree 1

Tree	Shape	Degree sequence	Diameter	Told apart from the others with the same sequence and diameter by
4	5 in a line, a line of two hanging from the middle	$3,2,2,2,1,1,1$	4	
5	5 in a line, two more on the middle	$4,2,2,1,1,1,1$	4	the degree-4 vertex has **two** neighbours of degree 1
6	5 in a line, two more on the second	$4,2,2,1,1,1,1$	4	the degree-4 vertex has **three** neighbours of degree 1
7	5 in a line, one more on the second and one on the fourth	$3,3,2,1,1,1,1$	4	the two degree-3 vertices are **not** joined
8	5 in a line, one more on the second and one on the third	$3,3,2,1,1,1,1$	4	the two degree-3 vertices **are** joined
9	two joined vertices, with 2 and 3 more	$4,3,1,1,1,1,1$	3	
10	two joined vertices, with 1 and 4 more	$5,2,1,1,1,1,1$	3	
11	one vertex joined to the other 6	$6,1,1,1,1,1,1$	2	

Renaming vertices keeps degrees and keeps which vertices are joined, so it also keeps facts like "the degree-3 vertex has two neighbours of degree 1". So in each tied pair the two trees are different, and all 11 are essentially different. Trees 2, 3 and 4 share a degree sequence too, but tree 4 has diameter 4.

Why there are no others. Take two vertices at the largest distance d in a tree, and a walk of d edges between them. A shortest walk never repeats a vertex (cutting out the part between two visits would make it shorter), so this walk is a line of $d+1$ different vertices, $v_0, v_1, \ldots, v_d$.

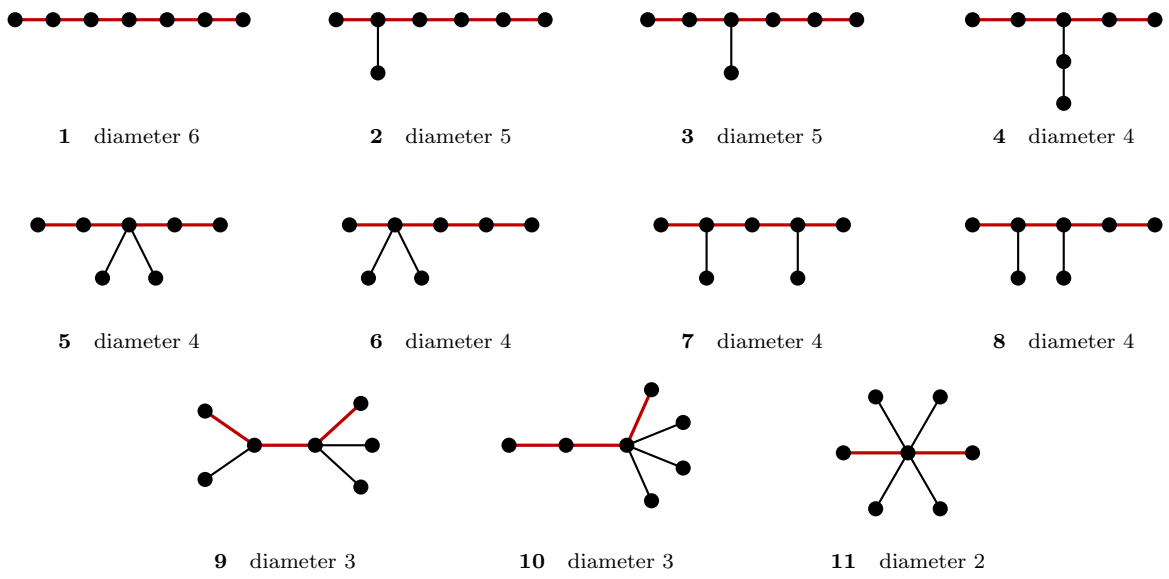


Figure 21: All 11 trees with 7 vertices, numbered as in the table below and grouped by diameter. In each tree the red edges are one longest line in it, and its number of edges is the diameter: 6 for tree 1, 5 for trees 2 and 3, 4 for trees 4 to 8, 3 for trees 9 and 10, and 2 for the star, tree 11. No two of the 11 are the same tree redrawn. Where two share a degree sequence and a diameter, they differ in how the vertices of degree 3 or more sit, as the table explains.

Every other vertex hangs off this line, and nothing can hang so far out that two vertices end up more than d apart. A tree with 7 vertices has diameter between 2 and 6: at most 6, since a line of $d+1$ different vertices needs $d+1 \leq 7$, and at least 2, since diameter 1 would make every two vertices joined, and a tree with 3 or more vertices would then contain a triangle. Going through the diameters:

- $d = 6$**.** All 7 vertices are on the line: tree 1.
- $d = 5$**.** One vertex is left, joined to v_1, v_2, v_3 or v_4. Joining it to an end would make a longer line. v_1 and v_4 give the same tree by reading the line backwards, and so do v_2 and v_3: trees 2 and 3.
- $d = 4$**.** Two vertices are left, x and y. If both are joined to the line, they hang off v_1, v_2 or v_3, giving the pairs $\{v_2, v_2\}$, $\{v_1, v_1\}$, $\{v_1, v_3\}$ and $\{v_1, v_2\}$, up to reading backwards: trees 5, 6, 7 and 8. Otherwise y hangs off x and x off the line, and x must be on the middle vertex v_2, since on v_1 the vertex y would be 5 from v_4: tree 4.
- $d = 3$**.** Three vertices are left, and each must be joined to v_1 or v_2 directly: not to an end, which would make a longer line, and not to another hanging vertex, since a vertex two steps out from v_1 is 4 from v_3, and two steps out from v_2 is 4 from v_0. Splitting 3 as $0+3$ or $1+2$ (up to reading backwards) gives trees 10 and 9.
- $d = 2$**.** Every vertex is within 2 of every other: one vertex joined to all six others, tree 11.

That is $1+2+5+2+1 = 11$.

This count, and the next fact, are for interest only and are not assessed. Call a tree **homeomorphically irreducible** if no vertex has degree 2. There are exactly 10 such trees with 10 vertices. With 7 vertices there are two, trees 9 and 11, the only rows of the table with no 2 in the degree sequence.

Deleting an edge from a tree

Deleting an edge removes that edge and nothing else. Every vertex stays, including the edge's endpoints.

> If any edge is deleted from a tree then the result is a disconnected graph. This disconnected graph consists of two trees.

The proof uses one fact about walks.

Shortcut fact. If there is a walk from x to y, there is one that visits no vertex twice: take a shortest walk from x to y. If it visited some vertex twice, cutting out the part between the two visits would leave a shorter walk from x to y. A walk that visits no vertex twice also uses no edge twice, because the second time it crossed an edge it would arrive at a vertex it had already visited. So it is a trail.

Proof. Let T be a tree and let e be an edge of T with endpoints u and v. A loop is a non-trivial circuit, so e is not a loop and $u \neq v$. Write $T - e$ for T with e deleted.

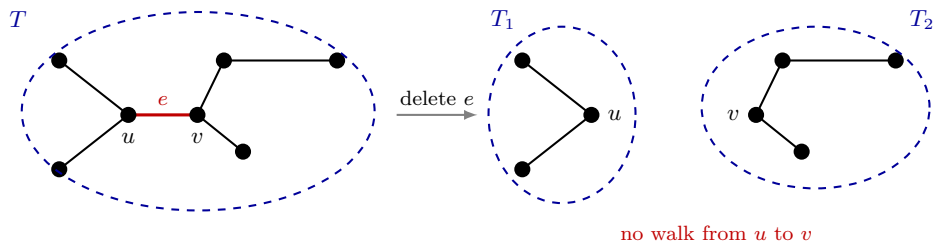


Figure 22: Deleting the edge e, in red, from the tree T with 7 vertices and 6 edges. What is left is two trees: T_1, which is u and the 2 vertices joined to it, and T_2, which is v and the 3 vertices it can still reach. There is no walk from u to v any more, since a shortest such walk together with e would make a non-trivial circuit in T. The edge counts add up: $2 + 3 + 1 = 6$.

1. **There is no walk from u to v in $T - e$.** Suppose there were. By the shortcut fact there is one that visits no vertex twice, $u = w_0\, f_1\, w_1\, f_2 \cdots f_k\, w_k = v$, with $k \geq 1$ since $u \neq v$. Its edges $f_1, \ldots, f_k$ are all different, and none of them is e. Then $u\, f_1\, w_1 \cdots f_k\, v\, e\, u$ ends where it starts and uses no edge twice: a non-trivial circuit in T. That contradicts T being circuit-free. So $T - e$ is disconnected.
2. **Every vertex can reach u or v in $T - e$.** Let x be a vertex. T is connected, so by the shortcut fact there is a walk from x to u in T that visits no vertex twice. If it does not use e, it is a walk in $T - e$. If it does, then since u is an endpoint of e and the walk meets u only at the very end, e is its last edge, crossed from v to u. Leaving off that last step gives a walk from x to v that does not use e.
3. **Two trees.** Let T_1 be the vertices that can reach u in $T - e$, and T_2 those that can reach v, each with the edges of $T - e$ between them. By 2 every vertex is in T_1 or T_2. By 1 no vertex is in both, since a vertex in both would give a walk from u to v. An edge of $T - e$ joins two vertices that can reach each other, so both its endpoints are in the same part. So $T - e$ is exactly T_1 and T_2, with no edge between them. Any two vertices of T_1 can each reach u, so they can reach each other, and every vertex on the way can reach u too, so the walk stays in T_1. So T_1 is connected, and likewise T_2. A non-trivial circuit in T_1 or T_2 would be one in T, so both are circuit-free. So T_1 and T_2 are trees. □

Two things to take into the next section: T_1 contains u and T_2 contains v, so each has at least one vertex; and every edge of T except e is in exactly one of T_1 and T_2.

A tree with n vertices has $n - 1$ edges

> **Theorem.** A graph G with n vertices is a tree if and only if it is simple, connected and has $n - 1$ edges.

There are two directions to prove.

(⇒) Every tree is simple, connected and has $n-1$ edges

A tree is connected by definition, and it is simple because it is circuit-free (above). What is left is the edge count, by strong induction on n.

Let $P(n)$ be: every tree with n vertices has $n-1$ edges.

Basis, $n=1$. A tree with one vertex has no edges: an edge would have to be a loop at that vertex, and a loop is a non-trivial circuit. $0 = 1-1$, so $P(1)$ holds.

Inductive hypothesis. Let $k \geq 1$ be an integer, and suppose that every tree with p vertices, for every p with $1 \leq p \leq k$, has $p-1$ edges.

Inductive step. Let T be a tree with $k+1$ vertices. Since $k+1 \geq 2$, T has two different vertices, and as T is connected there is a walk between them. That walk uses an edge, so T has an edge e. Delete it. By the previous section this leaves two trees, T_1 with p vertices and T_2 with q vertices, where $p, q \geq 1$ and $p+q = k+1$. So $p \leq k$ and $q \leq k$, and by the inductive hypothesis T_1 has $p-1$ edges and T_2 has $q-1$. Every edge of T is e or is in exactly one of T_1, T_2, so T has

$$(p-1)+(q-1)+1 = p+q-1 = (k+1)-1 = k$$

edges. So $P(k+1)$ holds, and by strong induction $P(n)$ holds for every integer $n \geq 1$. □

The induction has to be strong because p and q can be any sizes from 1 to k, not just k (strong-induction-and-the-well-ordering-principle[42]).

(⇐) A simple connected graph with $n-1$ edges is a tree

This direction is by contradiction, and it needs one more fact.

Lemma. If G is connected and e is an edge of a non-trivial circuit in G, then $G-e$ is still connected.

Proof. Write the circuit as $v_0\, e_1\, v_1 \cdots e_m\, v_m$ with $v_0 = v_m$, and say $e = e_i$, with endpoints v_{i-1} and v_i. The edges of a circuit are all different, so e appears in it only once. Going the other way round the circuit,

$$R: \quad v_i\, e_{i+1}\, v_{i+1} \cdots e_m\, v_m = v_0\, e_1\, v_1 \cdots e_{i-1}\, v_{i-1}$$

is a walk from v_i to v_{i-1} that uses every edge of the circuit except e. Now let x and y be any two vertices. G is connected, so there is a walk from x to y in G. Each time it crosses e it steps

[42] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

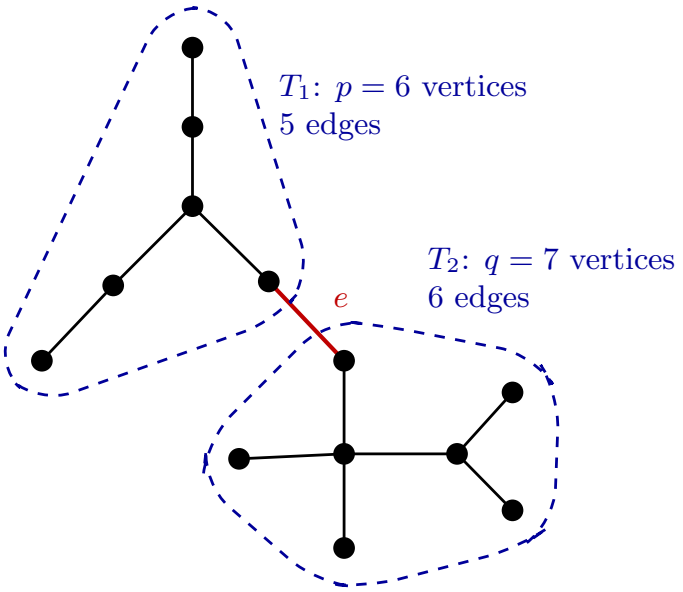


Figure 23: The inductive step on a tree with 13 vertices. Deleting the red edge e leaves two trees: T_1 with $p = 6$ vertices and T_2 with $q = 7$. Both are smaller than the whole tree, so the inductive hypothesis gives them $p-1 = 5$ and $q-1 = 6$ edges. Putting e back gives $5+6+1 = 12 = 13-1$ edges, which is $(p-1)+(q-1)+1 = p+q-1$.

from v_{i-1} to v_i or from v_i to v_{i-1}; replace that step by R backwards or by R. The result is a walk from x to y that does not use e. So $G - e$ is connected. □

(If e is a loop then $v_{i-1} = v_i$ and R is a walk from that vertex back to itself; the same replacement works.)

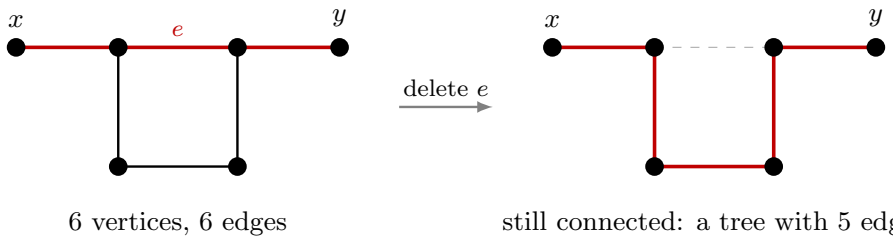


Figure 24: Deleting an edge of a circuit keeps a graph connected. Left: a connected graph whose four middle vertices form a circuit, and the walk from x to y through the edge e. Right: e is deleted, and the walk goes round the rest of the circuit instead, in red. The left graph has 6 vertices and 6 edges, one more than a tree with 6 vertices. The right graph is connected with no circuit, a tree with $6 - 1 = 5$ edges.

Proof of (⇐). Let G be a simple connected graph with n vertices and $n-1$ edges, and suppose, for a contradiction, that G is not a tree. G is connected, so it is not circuit-free: it has a non-trivial circuit. Delete one edge of that circuit. By the lemma the graph is still connected, and it still has all n vertices. If it still has a non-trivial circuit, delete an edge of that one, and keep going. Each deletion removes an edge and keeps the graph connected, and G has only finitely many edges, so this stops, at a graph H with no non-trivial circuit. H is connected and circuit-free, so it is a tree with n vertices. At least one edge was deleted, so H has at most $n-2$ edges. But by (⇒), a tree with n vertices has exactly $n-1$ edges. This is a contradiction, so G is a tree. □

Two remarks on the proof.

- The word *simple* is never used in (⇐). A connected graph with n vertices and $n-1$ edges is already a tree, and so it turns out to be simple.
- Neither direction uses anything about vertices of degree 1. So the next worked question, which proves a fact about them from this theorem, is not going round in a circle.

Worked: degree 3 or degree 1

Every vertex of a tree with 15 edges has either degree 3 or degree 1. How many vertices of the tree have degree 3?

Answer: 7.

A tree with 15 edges has $15+1=16$ vertices, by the theorem. Let x be the number of vertices of degree 3. Then $16-x$ vertices have degree 1.

By the Handshake Theorem (graphs[43]) the degrees add to $2 \cdot 15 = 30$. The degree sum is $3+3+\cdots+3$, x times, plus $1+1+\cdots+1$, $16-x$ times:

$$3x + (16-x) = 30, \qquad 2x = 14, \qquad x = 7.$$

So 7 vertices have degree 3 and 9 have degree 1. Check: $7 \cdot 3 + 9 \cdot 1 = 30 = 2 \cdot 15$.

The count shows what any such tree must have. One such tree:

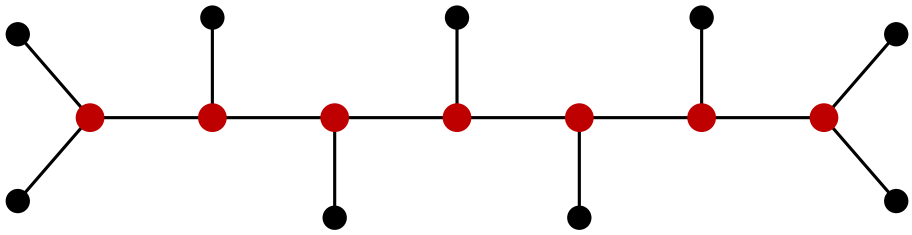


Figure 25: A tree with 15 edges in which every vertex has degree 3 or 1. The 7 vertices of degree 3, in red, lie in a line. The two at the ends each have two more vertices of degree 1 joined to them, and the five in between have one each, so there are $2+5+2=9$ vertices of degree 1. That is 16 vertices and $6+9=15$ edges, and the degrees add to $7 \cdot 3 + 9 \cdot 1 = 30$.

Worked: how many vertices

> A tree has two vertices of degree 4, one vertex of degree 2, and all the other vertices have degree 1. How many vertices does the tree have?

Answer: 9.

Three vertices have degree 4 or 2. Let x be the number of vertices of degree 1, and n the total number of vertices, so

$$n = x + 3.$$

By the theorem the tree has $n-1 = (x+3)-1 = x+2$ edges. By the Handshake Theorem the degrees add to $2(x+2)$:

[43] courses/math1061/graphs.pdf

$$2 \cdot 4 + 1 \cdot 2 + x = 2(x + 2), \qquad 10 + x = 2x + 4, \qquad x = 6.$$

So $n = x + 3 = 9$. Check: the degrees add to $4 + 4 + 2 + 6 \cdot 1 = 16 = 2 \cdot 8$, and $8 = 9 - 1$ edges.

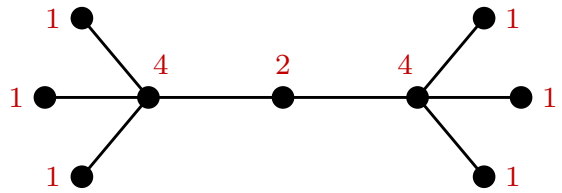


Figure 26: A tree with two vertices of degree 4, one of degree 2 and the rest of degree 1. The vertex of degree 2 sits between the two of degree 4, and each of those has three more vertices of degree 1 joined to it. That is $3 + 6 = 9$ vertices and 8 edges, and the degrees add to $4 + 4 + 2 + 6 = 16 = 2 \cdot 8$.

Both questions use the same two facts: a tree with n vertices has $n - 1$ edges, and the degrees add to twice the number of edges. Naming the unknown count and writing both facts down gives an equation to solve. The method is in trees[44].

Worked: two vertices of degree 1

Prove that every tree with at least two vertices has at least two vertices of degree 1.

Proof (by contradiction). Suppose there is a tree T with $n \geq 2$ vertices that has at most one vertex of degree 1.

By the theorem T has $n - 1$ edges, so by the Handshake Theorem

$$\sum_{v \in V(T)} \deg(v) = 2(n - 1) = 2n - 2.$$

Since T is a tree it is connected, and since it has at least 2 vertices, every vertex has a walk to some other vertex, so no vertex has degree 0. There are two cases.

- **No vertex of degree 1.** Then every vertex has degree at least 2, and $\sum \deg(v) \geq 2n$.
- **Exactly one vertex of degree 1.** All the others have degree at least 2, and $\sum \deg(v) \geq 1 + 2(n - 1) = 2n - 1$.

[44] courses/math1061/trees.pdf

In either case $\sum \deg(v) \geq 2n-1$. But the sum is $2n-2$, so $2n-2 \geq 2n-1$, that is $-2 \geq -1$, which is false. So every tree with at least two vertices has at least two vertices of degree 1. $\square$

Both conditions matter. A line of vertices has exactly two vertices of degree 1, its ends, so "two" cannot be improved. And the tree with one vertex has no vertex of degree 1 at all: its only vertex has degree 0. More on vertices of degree 1, including a second proof, is in trees[45].

Worked: degrees $n-2$ and $n-3$

> Prove that if there exists a tree with n vertices that has a vertex of degree $n-2$ and another vertex of degree $n-3$, then $n \leq 5$.

Read it as: if any tree with n vertices has these two degrees, then $n \leq 5$. The two vertices have different degrees, so they are automatically two different vertices.

Proof (by contradiction). Let T be a tree with $n \geq 6$ vertices that has a vertex v_1 of degree $n-2$ and a vertex v_2 of degree $n-3$.

By the theorem T has $n-1$ edges, so by the Handshake Theorem

$$\sum \deg(v) = 2(n-1) = 2n-2.$$

Since T is connected and has at least 2 vertices, no vertex has degree 0, so every vertex has degree at least 1. Apart from v_1 and v_2 there are $n-2$ vertices, and $n-2 \geq 4$ since $n \geq 6$. They contribute at least 1 each, so at least 4 in all:

$$\sum \deg(v) \geq (n-3) + (n-2) + 4 = 2n-5+4 = 2n-1.$$

So $2n-2 \geq 2n-1$, which is false. So $n \leq 5$. $\square$

The same count without contradiction: if such a tree exists then $n-3 \geq 0$, so $n \geq 3$ and every degree is at least 1. Then

$$2n-2 = \sum \deg(v) \geq (n-2) + (n-3) + (n-2) = 3n-7,$$

which gives $n \leq 5$.

The bound is reached. With $n=5$, a vertex of degree 3 and a vertex of degree 2: join v_1 to v_2 and to two more vertices, and v_2 to a fifth. With $n=4$, a vertex of degree 2 and another of degree 1: four vertices in a line. With $n=3$ the second vertex would need degree 0, which no tree with at least two vertices has, and with $n \leq 2$ the degree $n-3$ is negative. So the trees with this property have exactly 4 or 5 vertices.

[45] courses/math1061/trees.pdf



Figure 27: Trees with a vertex of degree $n-2$ and another of degree $n-3$, the two in red. Left, $n = 5$: degrees 3 and 2, and the other three vertices have degree 1. The degrees add to $3+2+1+1+1 = 8 = 2 \cdot 4$. Right, $n = 4$: four vertices in a line, with degrees 2 and 1 marked. With $n = 6$ the two red vertices alone would need degrees $4+3 = 7$, the four others at least 4 more, and 11 is more than the $2 \cdot 5 = 10$ a tree with 6 vertices allows.

See also

- [trees] — trees, the $n-1$ theorem, vertices of degree 1, and the counting method
- walks-trails-and-circuits[46] — walks, trails, circuits and connected graphs
- graphs[47] — the degrees add to twice the number of edges
- strong-induction-and-the-well-ordering-principle[48] — the induction used for ($\Rightarrow$)
- proof-techniques[49] — the method used for ($\Leftarrow$) and Worked questions 3 and 4
- 2026-10-27-matrix-representations-of-graphs[50] — Lecture 35
- practice-problems[51] — §46, with full worked solutions

Reference material

Adjacency Matrices

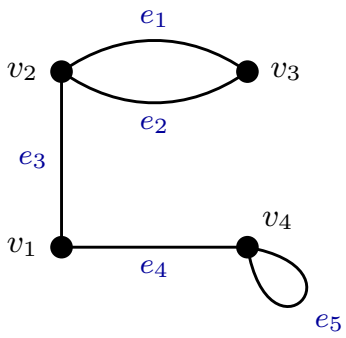
An adjacency matrix writes a graph down as a square table of numbers: a row and a column for each vertex, and in each place the number of edges joining that pair of vertices. It records everything about the graph except the names of the edges, so the graph can be redrawn from it, and the degrees, and with them whether the graph has an Euler circuit, can be read straight off it. The one trap is the loop, which counts 1 in the matrix but 2 in the degree. The other matrix of a graph, with a row for each vertex and a column for each edge, is in incidence-matrices[52]. Graphs, loops, degree and the Handshake Theorem are in [graphs]. First

[46] courses/math1061/walks-trails-and-circuits.pdf
[47] courses/math1061/graphs.pdf
[48] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[49] courses/math1061/proof-techniques.pdf
[50] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[51] courses/math1061/practice-problems.pdf
[52] courses/math1061/incidence-matrices.pdf

met in 2026-10-27-matrix-representations-of-graphs[53].

Definition

The **adjacency matrix** of a graph with vertices $v_1, v_2, \ldots, v_n$ is the $n \times n$ matrix $A = [a_{ij}]$ where each entry a_{ij} is the number of edges with endpoints $\{v_i, v_j\}$.



$A =$

	v_1	v_2	v_3	v_4
v_1	0	1	0	1
v_2	1	0	**2**	0
v_3	0	**2**	0	0
v_4	1	0	0	**1**

Figure 28: A graph and its adjacency matrix. Each entry counts the edges joining the vertex of its row to the vertex of its column: the 2 in row v2, column v3 is the two parallel edges e1 and e2, and the 0 in row v1, column v3 says v1 and v3 are not adjacent. The diagonal counts loops, so the single loop e5 gives a 1 in row v4, column v4. Every entry appears again reflected in the diagonal, because the edges between v2 and v3 are the edges between v3 and v2.

What the definition gives straight away:

- A **is square**, $n \times n$, with one row and one column for each vertex.
- **Every entry is a non-negative integer**, since it counts edges.
- A **is symmetric**: $a_{ij} = a_{ji}$ for all i, j. The set $\{v_i, v_j\}$ is the same set as $\{v_j, v_i\}$, so the two entries count the same edges. Everything below the diagonal repeats something above it.
- **Off the diagonal**, $a_{ij} \geq 1$ exactly when v_i and v_j are adjacent, and $a_{ij} \geq 2$ exactly when they are joined by parallel edges.
- **On the diagonal**, a_{ii} is the number of loops at v_i. See loops.
- **An isolated vertex has a row and a column of zeros.** It still gets its row, because the matrix has one for every vertex.

[53] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf

Simple graphs. A graph is simple when it has no loops and no parallel edges (graphs[54]). In the matrix that is: **every entry is 0 or 1, and the diagonal is all 0**. The complete graph K_4, for example, has a 1 in every place off the diagonal:

	v_1	v_2	v_3	v_4
v_1	0	1	1	1
v_2	1	0	1	1
v_3	1	1	0	1
v_4	1	1	1	0

The matrix depends on the order of the vertices. Listing the same vertices in a different order rearranges the rows and the columns in the same way. With the vertices of the graph above in the order v_2, v_3, v_1, v_4, the matrix is

	v_2	v_3	v_1	v_4
v_2	0	2	1	0
v_3	2	0	0	0
v_1	1	0	0	1
v_4	0	0	1	1

a different matrix for the same graph. So a graph has *an* adjacency matrix for each order of its vertices, and the rows and columns should always be labelled.

The matrix does not name the edges. It says there are two edges between v_2 and v_3, but not which is e_1. A graph rebuilt from its adjacency matrix is the same graph up to the names of the edges.

Loops

A loop at v_i is **one edge** whose set of endpoints is $\{v_i\} = \{v_i, v_i\}$, so it adds **1** to the diagonal entry a_{ii}. In the graph above the one loop e_5 gives $a_{44} = 1$. Two loops at a vertex give a 2 on the diagonal, and the 1×1 matrix [73] is a single vertex with 73 loops.

A loop adds 2 to the degree of its vertex (graphs[55]) but only 1 to the matrix. So when there are loops, **the row sum is not the degree**.

> **Degree from the adjacency matrix.** For each vertex v_i,
>
> $$\deg(v_i) = (a_{i1} + a_{i2} + \cdots + a_{in}) + a_{ii},$$
>
> the sum of row i plus the diagonal entry of row i.

[54] courses/math1061/graphs.pdf
[55] courses/math1061/graphs.pdf

Proof. Every edge with v_i as an endpoint is counted exactly once in row i: an edge joining v_i to a different vertex v_j in a_{ij}, and a loop at v_i in a_{ii}. An edge joining v_i to a different vertex has one end at v_i and adds 1 to $\deg(v_i)$, the same as it adds to the row. A loop has both of its ends at v_i and adds 2 to $\deg(v_i)$, one more than it adds to the row. So the degree is the row sum plus one for each loop at v_i, and there are a_{ii} loops at v_i. □

In the graph above:

Vertex	Row sum	Diagonal entry	Degree
v_1	$0+1+0+1=2$	0	2
v_2	$1+0+2+0=3$	0	3
v_3	$0+2+0+0=2$	0	2
v_4	$1+0+0+1=2$	1	3

v_4 meets e_4 once and the loop e_5 twice, so its degree is 3, not the row sum 2. For a graph **without loops** the diagonal is all 0 and the degree is just the row sum.

Counting the edges. Each edge is counted exactly once on or above the diagonal: an edge joining v_i and v_j with $i < j$ in a_{ij}, and a loop on the diagonal. So

$$\text{number of edges} = \sum_{i \le j} a_{ij},$$

the sum of the diagonal and everything above it. Above, that is $(0+1+0+1)+(0+2+0)+(0+0)+1=5$. Adding up **every** entry counts each non-loop edge twice, once on each side of the diagonal, and each loop once, so adding the diagonal on top gives $2e$. That is the degree formula summed over all the vertices, and it is the Handshake Theorem (graphs[56]): above, $9+1=10=2\cdot 5$.

Reading a graph off a matrix

Given an adjacency matrix, the graph is drawn from the **diagonal and the entries above it**:

1. Check it is an adjacency matrix: square, symmetric, non-negative integer entries (below).
2. Draw a dot for each row and label it $v_1, \ldots, v_n$ in order.
3. For each $i < j$, draw a_{ij} edges between v_i and v_j.
4. For each i, draw a_{ii} loops at v_i.
5. Ignore everything below the diagonal. It repeats what is above, and reading it too would draw every edge twice.

[56] courses/math1061/graphs.pdf

Then check: the number of edges drawn is the sum on and above the diagonal, and each degree in the drawing is its row sum plus its diagonal entry.

For example, take

$$M = \begin{array}{c|cccc} & v_1 & v_2 & v_3 & v_4 \\ \hline v_1 & 1 & 1 & 0 & 0 \\ v_2 & 1 & 0 & 2 & 1 \\ v_3 & 0 & 2 & 0 & 1 \\ v_4 & 0 & 1 & 1 & 0 \end{array}$$

It is square, symmetric and has non-negative integer entries. On and above the diagonal: $a_{11} = 1$ is a loop at v_1; $a_{12} = 1$ is an edge v_1v_2; $a_{23} = 2$ is two parallel edges v_2v_3; $a_{24} = 1$ and $a_{34} = 1$ are edges v_2v_4 and v_3v_4. Every other entry there is 0. That is 6 edges.

$$M = \begin{array}{c|cccc} & v_1 & v_2 & v_3 & v_4 \\ \hline v_1 & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{0} \\ v_2 & 1 & \mathbf{0} & \mathbf{2} & \mathbf{1} \\ v_3 & 0 & 2 & \mathbf{0} & \mathbf{1} \\ v_4 & 0 & 1 & 1 & \mathbf{0} \end{array}$$

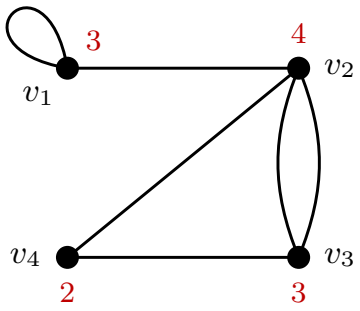


Figure 29: Reading a graph off an adjacency matrix. Only the diagonal and the entries above it, in blue, are used: each entry above the diagonal is a number of edges between two vertices, and each diagonal entry is a number of loops. The grey entries below the diagonal repeat the blue ones and are skipped. The blue entries add to 6, the number of edges. The degrees, in red, are row sum plus diagonal entry: v1 has row sum 2 and one loop, so degree 3.

The degrees are $\deg(v_1) = 2 + 1 = 3$, $\deg(v_2) = 4$, $\deg(v_3) = 3$ and $\deg(v_4) = 2$, adding to $12 = 2 \cdot 6$. A larger example, with two loops and three parallel edges, is worked in 2026-10-27-matrix-representations-of-graphs[57].

[57] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf

Which matrices are adjacency matrices

> A matrix is the adjacency matrix of some graph if and only if it is **square** (with at least one row), **symmetric**, and every entry is a **non-negative integer** $0, 1, 2, ...$

Proof. ($\Rightarrow$) Shown under the definition: an adjacency matrix has a row and a column for each vertex, a graph has at least one vertex, every entry counts edges, and $\{v_i, v_j\} = \{v_j, v_i\}$.

($\Leftarrow$) Let $M = [m_{ij}]$ be an $n \times n$ symmetric matrix with $n \geq 1$ and non-negative integer entries. Build a graph with vertices $v_1, \ldots, v_n$: for each $i < j$ put m_{ij} edges between v_i and v_j, and for each i put m_{ii} loops at v_i. These are whole numbers of edges, at least 0, so this is a graph. The number of edges with endpoints $\{v_i, v_j\}$ is then m_{ij} when $i < j$, it is m_{ii} when $i = j$, and when $i > j$ it is m_{ji}, which equals m_{ij} because M is symmetric. So M is this graph's adjacency matrix. $\square$

So there are three things to check, and a matrix fails if any one of them fails:

Matrix	Square	Symmetric	Entries in $0, 1, 2, ...$	Adjacency matrix?
$\begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}$	yes	yes	yes	yes: two parallel edges and a loop at v_2
$\begin{bmatrix} 0 & 1 & 1 \end{bmatrix}$	no	—	yes	no: one row, three columns
$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$	yes	no	yes	no
$\begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}$	yes	yes	no	no: half an edge
$\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$	yes	yes	yes	yes: two isolated vertices, no edges

Nothing else is needed. The diagonal can hold any non-negative integer, and so can any entry off it. Four more are worked in 2026-10-27-matrix-representations-of-graphs[58].

Degrees and Euler circuits

The matrix holds everything needed to decide whether a graph has an Euler circuit (euler-circuits-and-trails[59]): a connected graph has one exactly when every vertex has even degree.

[58] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[59] courses/math1061/euler-circuits-and-trails.pdf

- **The degrees** are row sum plus diagonal entry, as above.
- **Connectedness** can be read off too. The graph is not connected exactly when the vertices split into two non-empty groups with a 0 in every entry between a vertex of one group and a vertex of the other: then no edge crosses between the groups.

For M above the degrees are $3, 4, 3, 2$. The graph is connected, since v_2 is joined to every other vertex. Two vertices, v_1 and v_3, have odd degree, so there is no Euler circuit, but there is an Euler trail from v_1 to v_3. For the graph in the definition the odd vertices are v_2 and v_4, so it too has an Euler trail and no Euler circuit.

A degree must be computed with the diagonal added in before its parity is judged. A vertex with row sum 2 and one loop has degree 3, which is odd.

Common mistakes

- **Writing 2 on the diagonal for a loop.** The adjacency matrix counts edges, and a loop is one edge, so it counts 1. The 2 for a loop belongs in the incidence matrix[60], which counts how many times a vertex meets an edge.
- **Taking the row sum as the degree when there are loops.** Add the diagonal entry: $\deg(v_i)$ is the row sum plus a_{ii}.
- **Reading the whole matrix when drawing.** Every entry off the diagonal appears twice. Read the diagonal and above only, or every edge comes out doubled.
- **Counting edges by adding all the entries.** That counts each non-loop edge twice. Add the diagonal and the entries above it.
- **Expecting a zero diagonal and only 0s and 1s.** That is true for simple graphs only. Loops put numbers on the diagonal, and parallel edges put numbers bigger than 1 off it.
- **Leaving off the labels.** The matrix depends on the order of the vertices, so label the rows and columns.
- **Accepting a matrix that is not symmetric.** a_{ij} and a_{ji} count the same edges and must be equal.

See also

- incidence-matrices[61] — the other matrix of a graph, with a column for each edge, and how the two compare
- [graphs] — loops, parallel edges, simple graphs, degree and the Handshake Theorem
- euler-circuits-and-trails[62] — the even-degree test for an Euler circuit
- walks-trails-and-circuits[63] — connected graphs

[60] courses/math1061/incidence-matrices.pdf
[61] courses/math1061/incidence-matrices.pdf
[62] courses/math1061/euler-circuits-and-trails.pdf
[63] courses/math1061/walks-trails-and-circuits.pdf

- 2026-10-27-matrix-representations-of-graphs[64] — Lecture 35
- practice-problems[65] — §45, with full worked solutions

Euler Circuits and Trails

An Euler circuit goes along every edge of a graph exactly once and comes back to where it started. An Euler trail does the same but finishes somewhere else. Whether a graph has one is decided by two things only: whether it is connected once its isolated vertices are set aside, and how many of its vertices have odd degree. None gives an Euler circuit, exactly two gives an Euler trail from one of them to the other, and any other number gives neither. This note has the definitions, the theorem with a full proof, how to actually find a circuit or trail, a flowchart for deciding, and how this course's definition differs from the textbook's. It builds on walks, trails, circuits and connectedness in walks-trails-and-circuits[66], and on degree in graphs[67]. First met in 2026-10-26-walks-trails-and-circuits[68].

Euler circuits

> An **Euler circuit** is a circuit that contains every edge of the graph.

A circuit never uses an edge twice (walks-trails-and-circuits[69]), so an Euler circuit uses **every edge exactly once** and ends where it started. It may pass through a vertex many times. A graph that has an Euler circuit is called **Eulerian**.

A graph with no edges has an Euler circuit: the trivial circuit at any vertex contains every edge, since there are none.

Euler trails

> An **Euler trail from vertex u to vertex v** is a trail that starts at u and ends at v and contains every edge of the graph.

The difference from an Euler circuit is only where it finishes. Both use every edge exactly once. An Euler circuit ends at the vertex it started from. An Euler trail from u to v ends at v, and the case that matters is $u \neq v$, an open route. (An Euler circuit is a trail from a vertex to itself, but the theorem below is about $u \neq v$.)

[64] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[65] courses/math1061/practice-problems.pdf
[66] courses/math1061/walks-trails-and-circuits.pdf
[67] courses/math1061/graphs.pdf
[68] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[69] courses/math1061/walks-trails-and-circuits.pdf

For a connected graph the two cannot both happen with $u \neq v$: the theorem says an Euler circuit needs every degree even, and an Euler trail from u to $v \neq u$ needs u and v odd.

The theorem

> **Theorem.** Let G be a connected graph. Then G has an Euler circuit if and only if every vertex of G has even degree.
>
> Let $u, v \in V(G)$ be distinct vertices of G. Then G has an Euler trail from u to v if and only if u and v have odd degree and all other vertices of G have even degree.

Every graph has an even number of vertices of odd degree (graphs[70]), so for a connected graph there are three cases: no odd vertices gives an Euler circuit, exactly two gives an Euler trail between them, and four or more gives neither.

Counting edge ends along a trail

Both directions of the proof rest on one count. Take a trail $T = v_0\, e_1\, v_1 \cdots e_n\, v_n$ and a vertex w. The edge e_i has its two ends at v_{i-1} and v_i (both at the same vertex if it is a loop). So the number of edge ends at w that T uses is

$$\underbrace{\#\{\, i : v_{i-1} = w \,\}}_{\text{times } T \text{ leaves } w} + \underbrace{\#\{\, i : v_i = w \,\}}_{\text{times } T \text{ arrives at } w}.$$

These ends are all different, because the edges of a trail are all different. Reading along the sequence, each arrival at w is followed by a departure, except an arrival at the very end, and each departure is preceded by an arrival, except a departure at the very start. So:

- **If w is not the first or last vertex**, T arrives at w exactly as often as it leaves: every pass through w uses **two** ends, one in and one out, and the number used is even.
- **If T is a circuit** ($v_0 = v_n$), the departure at the start and the arrival at the end pair up at v_0, and every vertex has an even number of ends used.
- **If** $v_0 \neq v_n$, T leaves v_0 once more than it arrives, and arrives at v_n once more than it leaves. At those two vertices the number of ends used is **odd**.

A loop at w is an arrival at w and a departure from w at once, and uses two ends at w, so it never changes these parities.

[70] courses/math1061/graphs.pdf

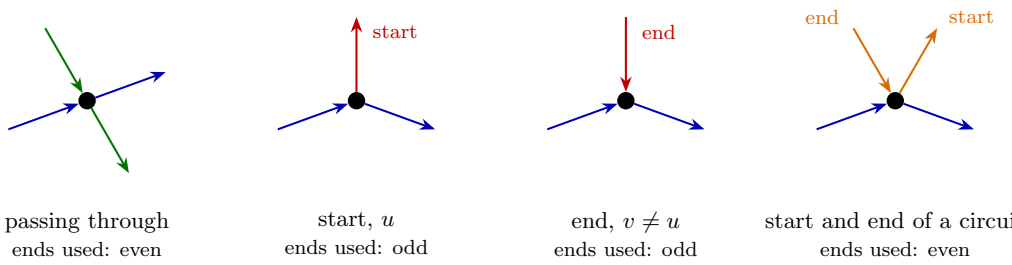


Figure 30: Edge ends used by a trail at one vertex. Arrows show the direction of travel. Left: a vertex in the middle of the trail. Each time the trail passes through, it arrives along one edge and leaves along another, so the ends pair up, blue with blue and green with green, and an even number is used. Second: the start of a trail that ends elsewhere has one departure with no arrival to pair with, in red, so an odd number is used. Third: the end of such a trail has one arrival left over. Right: at the start of a circuit, the first departure pairs with the final arrival, so every end pairs up again.

Proof: every edge used forces the degrees

Proof that an Euler circuit or trail forces the degrees. Suppose T is an Euler circuit of G. It uses every edge exactly once, so it uses every edge end in G exactly once, and the number of ends it uses at a vertex w is all of them, $\deg(w)$. By the count above that number is even. So every vertex has even degree.

Suppose instead T is an Euler trail from u to v with $u \neq v$. Again the ends used at w number $\deg(w)$. By the count, that is odd for $w = u$ and $w = v$, and even for every other vertex. □

This direction does not use connectedness.

Proof: even degrees give an Euler circuit

The construction rests on one fact about walking until stuck.

Lemma (stuck only at the start). Let H be a graph in which every vertex has even degree, and w a vertex with $\deg(w) \geq 1$. Start at w and build a trail one edge at a time: from the current vertex, go along any edge at it that has not been used yet, and stop when there is none. Then this stops, and it stops at w, so it produces a non-trivial circuit through w.

Proof. Each step uses a new edge and there are finitely many, so it stops. Suppose it is at a vertex $x \neq w$, having arrived there. The trail so far starts at w and ends at $x \neq w$, so by the count it has used an odd number of the ends at x. Since $\deg(x)$ is even, some end at x is unused, and the edge it belongs to is unused, because an edge is used all at once. So the trail can go on, and it does not stop at x. It therefore stops at w. It started along an edge, since $\deg(w) \geq 1$, so the circuit has at least one edge. □

Removing a circuit keeps every degree even. If C is a circuit and its edges are deleted (keeping all the vertices), each vertex loses the ends of it that C used, an even number by the count. Even minus even is even.

Proof of the theorem, circuits. Let G be connected with every vertex of even degree. Every vertex is a trivial circuit, so G has circuits. A circuit uses each edge at most once, so it has at most $|E(G)|$ edges, and there is a circuit $C = v_0\, e_1\, v_1 \cdots e_n\, v_n$ with **as many edges as possible**. Suppose, for a contradiction, that some edge of G is not in C.

Let H be G with the edges of C deleted. H has every vertex of even degree and at least one edge.

Some vertex of C has an edge in H. Take an edge of H and an endpoint x of it. If x is on C, done. If not, G is connected, so there is a walk in G from x to v_0. The walk starts off C and ends on C, so there is a first vertex y on it that lies on C, and the vertex z just before y is not on C. The edge f of the walk joining z and y is not an edge of C, since every edge of C has both endpoints on C. So f is in H, and its endpoint y is on C. Call this vertex w.

Splice. w has degree at least 1 in H, so the lemma, applied in H, gives a non-trivial circuit $C' = w\, f_1\, u_1 \cdots f_m\, w$ using only edges of H. w is on C, say $w = v_k$. Replace that one occurrence of v_k in C by the whole of C':

$$v_0\, e_1\, v_1 \cdots e_k\, \underbrace{v_k\, f_1\, u_1 \cdots f_m\, v_k}_{C'}\, e_{k+1} \cdots e_n\, v_n.$$

This is a walk, since C' leaves from v_k and returns to v_k. Its edges are those of C and those of C', which are all different, since the edges of C' are in H and H has none of the edges of C. So it is a trail, and it starts and ends at $v_0 = v_n$, so it is a circuit. It has $n + m > n$ edges, contradicting the choice of C.

So C contains every edge of G, and it is an Euler circuit. □

If G has no edges, C is a trivial circuit and nothing is missing. Connectedness is used in exactly one place: to get from an unused edge back to the circuit.

Proof: two odd vertices give an Euler trail

Proof of the theorem, trails. Let G be connected, with $u \neq v$ of odd degree and every other vertex of even degree. Make a new graph G' by adding one new edge f with endpoints u and v. If u and v are already adjacent, f is a parallel edge, and that is fine. In G', u and v each gain one end, so every vertex of G' has even degree, and G' is still connected. By the circuit case, G' has an Euler circuit C.

C uses f once, either as $\cdots u\, f\, v \cdots$ or as $\cdots v\, f\, u \cdots$. Read backwards if necessary (walks-trails-and-circuits[71]) so that it is $\cdots v\, f\, u \cdots$. Then start the circuit at that u, so that f is the last

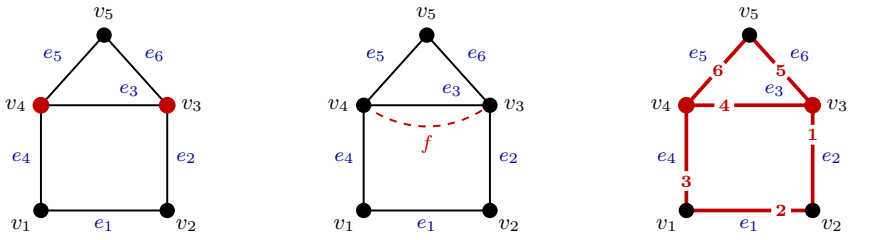
[71] courses/math1061/walks-trails-and-circuits.pdf

edge:

$$C = u \cdots v\, f\, u.$$

Delete the final $f\,u$. What is left is a trail, since its edges are some of the distinct edges of C. It starts at u, ends at v, uses every edge of G' except f exactly once, and so uses every edge of G exactly once. It is an Euler trail from u to v. □

Together with the first direction, that proves the theorem.



G: $\deg v_3 = \deg v_4 = 3$ | G': add f, all degrees even | Euler trail from v_3 to v_4

Figure 31: The trail case from the circuit case. Left: the house graph, connected, with v_3 and v_4 of odd degree, in red, and the others even. Middle: adding a new edge f joining v_3 and v_4, dashed, makes every degree even, so there is an Euler circuit, for example $v_3, e_2, v_2, e_1, v_1, e_4, v_4, e_3, v_3, e_6, v_5, e_5, v_4, f, v_3$, which ends with f. Here f is a second edge between two vertices that were already adjacent. Right: drop the final f. What is left, $v_3, e_2, v_2, e_1, v_1, e_4, v_4, e_3, v_3, e_6, v_5, e_5, v_4$, is an Euler trail from v_3 to v_4, in red with its edges numbered in order.

This course's definition and the textbook's

This course uses the standard definitions above: an Euler circuit contains every **edge**. The textbook defines an Euler circuit as a circuit that contains **every vertex and every edge** of the graph, and an Euler trail likewise.

They differ only when there are vertices that no edge touches. A triangle together with one isolated vertex has an Euler circuit by this course's definition (go once round the triangle), and none by the textbook's, because no circuit can reach the isolated vertex.

For a connected graph the two definitions agree. A circuit or trail that contains every vertex and every edge certainly contains every edge. Conversely, let G be connected and let T contain every edge.

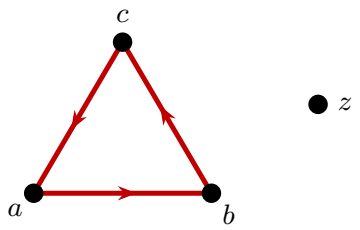


Figure 32: A triangle and an isolated vertex z. Going once round the triangle, in red, uses every edge, so by this course's definition it is an Euler circuit. By the textbook's definition it is not, since it misses z, and no circuit can visit z. The graph is disconnected, so the theorem does not apply to it as it stands. Deleting z leaves a connected graph with all degrees even.

- If G has at least one edge, then every vertex is the endpoint of some edge. With a single vertex, every edge is a loop at it. With two or more vertices, take any vertex x and another vertex y: there is a walk from x to y, and its first edge has x as an endpoint. T uses that edge, so T passes through x.
- If G has no edges, being connected means it has one vertex. The only walk in G is that single vertex, so T is the trivial circuit there, and it contains the vertex.

So T contains every vertex too. The theorem assumes G is connected, so it says the same thing under either definition. The definitions only part ways for disconnected graphs whose edges all lie in one piece, with isolated vertices as the rest, such as the triangle and isolated vertex, and that case is what the first two steps of the flowchart deal with.

How to find one

The theorem says whether an Euler circuit or trail exists. To write one down, I use the splicing method that the proof is built on (it is usually called Hierholzer's algorithm):

1. **Check first.** Delete isolated vertices, check the rest is connected, and count the vertices of odd degree. None: look for a circuit, starting anywhere. Two, u and v: look for a trail, **starting at** u.
2. **Walk until stuck.** From the start, keep going along edges not used yet, choosing freely, until there are none at the current vertex. For a circuit this always stops back at the start (the lemma). For a trail from u it always stops at v: by the count, at any other vertex the trail has used an odd number of ends of an even-degree vertex, or, at u, an even number of ends of an odd-degree vertex, and either way an end is left.
3. **If edges are left, splice.** The unused edges give every vertex even degree, since what was walked used an even number of ends at each vertex except u and v, and an odd number at those two. Pick a vertex already on the route that still has an unused edge.

Walk from it along unused edges until stuck. That is back at the same vertex. Insert this circuit into the route at that vertex.

4. **Repeat** step 3 until every edge is used.

When walking, it helps to tick off each edge on the drawing as it is used, and to write the route as a list of vertices (with edge names where there are multiple edges).

Another method avoids splicing by choosing carefully as you go (Fleury's algorithm): walk from the start, and at each step **don't burn your bridges**, that is, never use an edge whose removal would cut the unused edges into two separate pieces, unless it is the only edge left at the vertex. It gives the circuit or trail in one pass, but checking every step for a bridge is slow by hand, so I splice.

Worked: an Euler circuit by splicing

> Find an Euler circuit of the graph below: six vertices, each joined to every other vertex except one, the vertex "opposite" it. The non-adjacent pairs are v_1, v_6; v_2, v_4; v_3, v_5.

There are 12 edges, $v_1v_2, v_1v_3, v_1v_4, v_1v_5, v_2v_3, v_2v_5, v_2v_6, v_3v_4, v_3v_6, v_4v_5, v_4v_6, v_5v_6$. The graph is connected and every vertex has degree 4, so there is an Euler circuit. The graph is simple, so a route can be written as a list of vertices.

Walk until stuck. From v_1:

$$v_1\, v_2\, v_3\, v_1\, v_4\, v_5\, v_1.$$

At v_1 all four edges are now used, so this is stuck, back at the start, with 6 edges. Left over: $v_2v_5, v_2v_6, v_3v_4, v_3v_6, v_4v_6, v_5v_6$.

First splice. v_2 is on the route and still has the unused edges v_2v_5 and v_2v_6. Walk from v_2 along unused edges: $v_2\, v_5\, v_6\, v_2$, stuck at v_2. Insert it where the route passes v_2:

$$v_1\ \underbrace{v_2\, v_5\, v_6\, v_2}_{\text{inserted}}\ v_3\, v_1\, v_4\, v_5\, v_1.$$

Left over: v_3v_4, v_3v_6, v_4v_6.

Second splice. v_3 is on the route and still has unused edges. Walk from it: $v_3\, v_4\, v_6\, v_3$. Insert it where the route passes v_3:

$$v_1\, v_2\, v_5\, v_6\, v_2\ \underbrace{v_3\, v_4\, v_6\, v_3}_{\text{inserted}}\ v_1\, v_4\, v_5\, v_1.$$

That uses all 12 edges, each once, and returns to v_1: an Euler circuit.

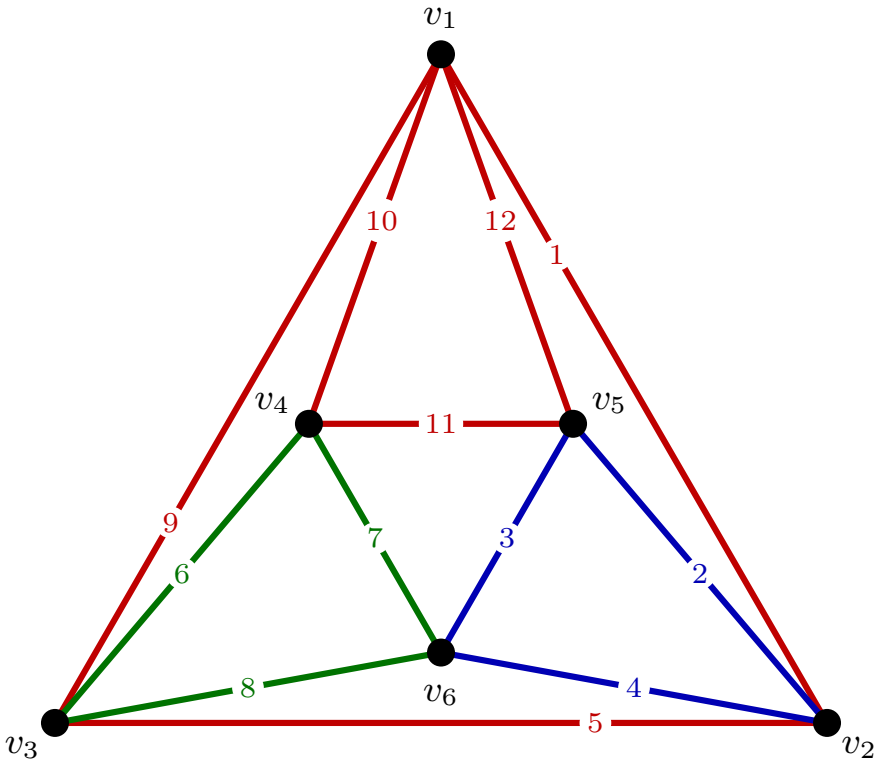


Figure 33: Finding an Euler circuit by splicing. Red: the first circuit, $v_1, v_2, v_3, v_1, v_4, v_5, v_1$, walked from v_1 until stuck. Blue: the circuit v_2, v_5, v_6, v_2 through v_2, built from unused edges and spliced in at v_2. Green: the circuit v_3, v_4, v_6, v_3 through v_3, spliced in at v_3. The small numbers give the order of the edges in the final circuit, $v_1, v_2, v_5, v_6, v_2, v_3, v_4, v_6, v_3, v_1, v_4, v_5, v_1$.

Deciding: the flowchart

For any graph, connected or not:

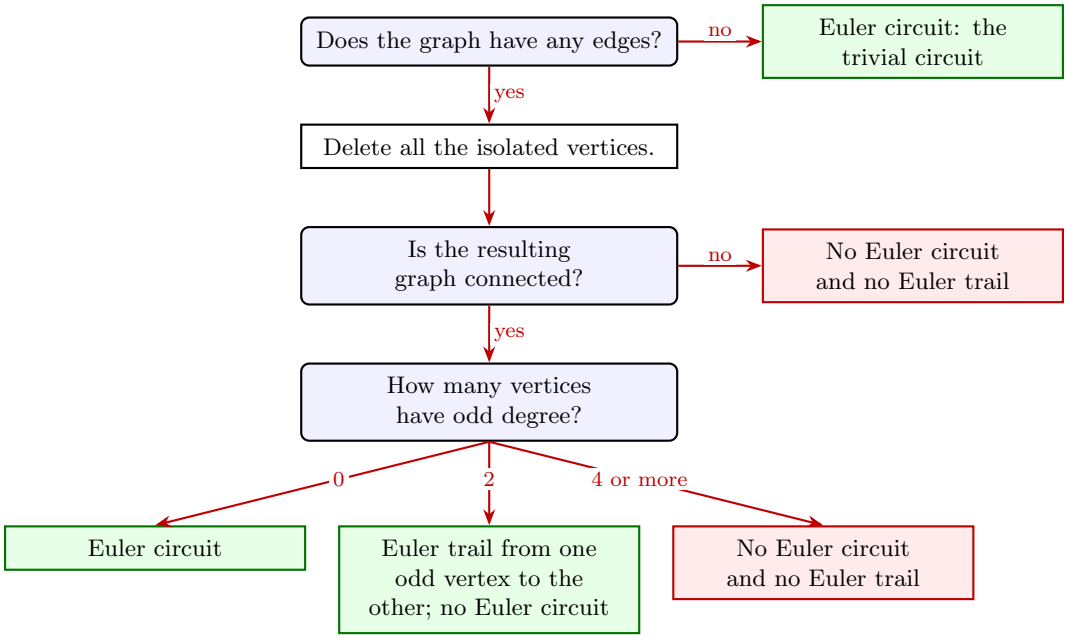


Figure 34: Deciding whether a graph has an Euler circuit or an Euler trail. A graph with no edges has one, the trivial circuit. Otherwise isolated vertices are deleted, since no edge touches them, and what is left must be connected, or some two edges cannot be on one route. Then the number of vertices of odd degree decides, and it is always even: none gives an Euler circuit, exactly two gives an Euler trail from one to the other, and four or more gives neither.

Why each step is right:

- **No edges.** The trivial circuit at any vertex contains every edge, so there is an Euler circuit. This uses this course's definition: by the textbook's, a graph with two or more vertices and no edges would have none.
- **Deleting isolated vertices** changes no edge, so it does not change which routes use every edge. A route that uses every edge never needs to visit an isolated vertex.
- **Not connected, after deleting isolated vertices.** Then there are vertices x and y with no walk between them, and each has an edge, since nothing isolated is left. A circuit or trail containing both edges would contain a walk from x to y. So there is neither.
- **Connected.** Now the theorem applies. The number of odd-degree vertices is even (graphs[72]), so 0, 2, or 4 or more covers everything.

[72] courses/math1061/graphs.pdf

The bridges of Königsberg

The problem that started graph theory: the city of Königsberg had four land masses joined by seven bridges, and the question was whether there is a walk around the city crossing every bridge exactly once, ideally returning to the start. As a graph, the land masses are the vertices and the bridges the edges. The island has degree 5 and each of the other three land masses has degree 3 (2026-10-26-walks-trails-and-circuits[73] has the graph).

All four vertices have odd degree. The graph is connected, so by the theorem there is **no Euler circuit**, since that needs every degree even, and **no Euler trail** either, since that needs exactly two odd vertices. No walk crosses every bridge exactly once, whether or not it returns. The problem is set up in 2026-07-27-welcome-and-intro-problems[74].

Common mistakes

- **Forgetting connectedness.** Even degrees are not enough. Two separate circuits, such as two triangles, have every degree even and no Euler circuit. Check that the graph is connected, after deleting isolated vertices, before using the degrees.
- **Letting isolated vertices decide.** An isolated vertex makes the graph disconnected but does not stop an Euler circuit, by this course's definition. Delete them first. (By the textbook's definition they do stop one, which is why the definitions are compared above.)
- **Counting a loop as 1.** A loop adds 2 to the degree (graphs[75]), so loops never change whether a degree is odd or even.
- **Exactly two odd vertices gives a trail, not a circuit.** The trail must start at one odd vertex and end at the other. Starting at an even vertex will not work.
- **Zero odd vertices gives a circuit, and the trail part of the theorem does not apply.** An Euler circuit is also a trail from a vertex to itself, but the trail statement in the theorem is about $u \neq v$. With every degree even there is no Euler trail from u to a **different** v, since that would need u and v odd.
- **Getting stuck and concluding there is none.** Walking until stuck can leave edges unused even when an Euler circuit exists. That is not a failure: splice in the rest (how to find one). Only the degrees and connectedness decide existence.

See also

- walks-trails-and-circuits[76] — walks, trails, circuits and connected graphs
- [graphs] — degree, loops and the Handshake Theorem

[73] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[74] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[75] courses/math1061/graphs.pdf
[76] courses/math1061/walks-trails-and-circuits.pdf

- 2026-10-26-walks-trails-and-circuits[77] — Lecture 34, with worked questions on the theorem and an Euler trail on ten vertices
- 2026-07-27-welcome-and-intro-problems[78] — the bridges of Königsberg
- [trees] — connected graphs with no non-trivial circuits
- practice-problems[79] — §44, with full worked solutions

Graphs

A graph is a set of points, the vertices, with some of them joined by lines, the edges. Almost all of graph theory is built on the few definitions here: what a graph is, loops and multiple edges, simple graphs, and the degree of a vertex. Then the first theorem, the Handshake Theorem, which says the degrees always add up to twice the number of edges, and what follows from it: every graph has an even number of vertices of odd degree, and many lists of numbers cannot be the degrees of any graph. The pigeonhole argument that two vertices of a simple graph share a degree is in pigeonhole-principle[80]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[81]. What comes after builds on these: getting around a graph (walks-trails-and-circuits[82]), using every edge exactly once (euler-circuits-and-trails[83]), writing a graph as a matrix (adjacency-matrices[84], incidence-matrices[85]), and the connected graphs with no circuits ([trees]).

What a graph is

> A **graph** G is a non-empty set of **vertices** $V(G)$ and a (possibly empty) set of **edges** $E(G)$, where each edge is associated with a set consisting of either one or two vertices.

The vertices an edge is associated with are its **endpoints**. An edge with two endpoints joins them, and an edge with one endpoint joins that vertex to itself.

- A graph must have **at least one vertex**, but it may have **no edges at all**.
- An edge is an object in its own right, not just a pair of vertices. Two different edges can have the same endpoints, and that is why edges are given their own names, $e_1, e_2, \ldots$.

[77] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[78] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[79] courses/math1061/practice-problems.pdf
[80] courses/math1061/pigeonhole-principle.pdf
[81] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[82] courses/math1061/walks-trails-and-circuits.pdf
[83] courses/math1061/euler-circuits-and-trails.pdf
[84] courses/math1061/adjacency-matrices.pdf
[85] courses/math1061/incidence-matrices.pdf

Two standard words: two vertices joined by an edge are **adjacent**, and an edge is **incident** with each of its endpoints. A vertex with no edges at all is **isolated**.

Drawing a graph. Each vertex is a dot and each edge a line between the dots of its endpoints, or a small loop from a dot back to itself. The graph is only the vertices, the edges and which edges have which endpoints. Where the dots go, and whether the lines are straight or curved, carry no information, so the same graph can be drawn in many ways. Two lines that cross in a drawing do not meet at a vertex; only dots are vertices.

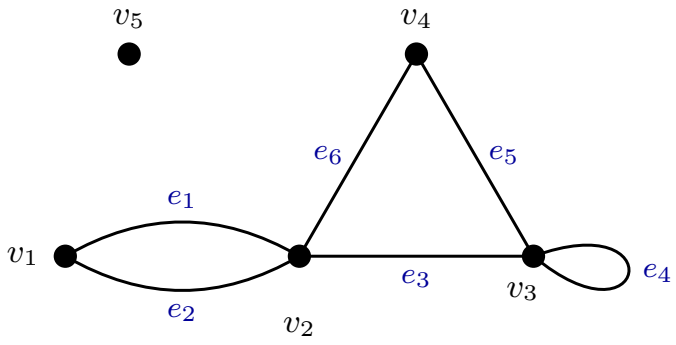


Figure 35: A graph with vertices v_1 to v_5 and edges e_1 to e_6. The edges e_1 and e_2 have the same endpoints, v_1 and v_2, so they are multiple edges. The edge e_4 has the single endpoint v_3, so it is a loop. v_5 is an isolated vertex: no edge has it as an endpoint, but it is still part of the graph. The edge e_6 joins v_2 and v_4, so those two vertices are adjacent and e_6 is incident with each of them; v_1 and v_3 are not adjacent, since no edge joins them. The graph is not simple, because of the loop and because of the multiple edges.

Edge	Endpoints
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_2\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_3\}$
e_5	$\{v_3, v_4\}$
e_6	$\{v_2, v_4\}$

The table is the graph. The drawing is one picture of it.

Loops and multiple edges

- A **loop** is an edge with only one endpoint. It joins a vertex to itself. Above, e_4 is a loop at v_3.
- **Multiple edges** (also called **parallel edges**) are two or more edges with the same set of endpoints. Above, e_1 and e_2 both join v_1 and v_2.

Both come up naturally when a graph models something. In the bridges of Königsberg, two land masses are joined by two bridges, which gives multiple edges (2026-07-27-welcome-and-intro-problems[86]).

Simple graphs

> A graph is **simple** if it has no loops and no multiple edges.

In a simple graph every edge has two different endpoints, and two vertices are joined by at most one edge. So an edge can be named by its endpoints, and a simple graph is just a set of vertices with some pairs of them joined.

A simple graph with n vertices has every degree at most $n-1$. A vertex can be joined to each of the other $n-1$ vertices at most once, and not to itself. This bound is one of the two quick tests for degree sequences.

Degree

> The **degree** of a vertex v, written $\deg(v)$, is the number of edge ends incident with it.

Count the ends of edges at the vertex, not the edges.

- An ordinary edge has one end at each of its two endpoints, so it adds 1 to the degree of each.
- **A loop has both of its ends at the same vertex, so it adds 2** to the degree of that vertex.
- An isolated vertex has degree 0.

In the graph above:

Vertex	Edge ends at it	Degree
v_1	e_1, e_2	2
v_2	e_1, e_2, e_3, e_6	4

[86] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

Vertex	Edge ends at it	Degree
v_3	e_3, e_4 twice, e_5	4
v_4	e_5, e_6	2
v_5	none	0

The degrees add to $2 + 4 + 4 + 2 + 0 = 12$, and there are 6 edges.

Why a loop counts 2: degree counts the ways out of a vertex along an edge. A loop can be set off along in either direction, so it gives two ways out. Counting it as 2 is also what makes the Handshake Theorem hold for every graph.

The Handshake Theorem

> **The Handshake Theorem.** The sum of the degrees of a graph is twice the number of edges. If G is a graph with $V(G) = \{v_1, v_2, \dots, v_n\}$ and $|E(G)| = e$, then
>
> $$\sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2e.$$

Proof. Count the edge ends in the graph two ways. Every edge has exactly two ends: an edge with two endpoints has one at each, and a loop has both at its one endpoint. So there are $2e$ ends in all. Every end is at exactly one vertex, and $\deg(v_i)$ is the number of ends at v_i. So adding the degrees over all the vertices counts each end exactly once, and the sum is $2e$. □

The name comes from people shaking hands at a party. Each handshake involves two hands, so the total number of hands shaken, added up person by person, is twice the number of handshakes.

Using it. The theorem links the degrees to the number of edges, so either can be found from the other.

- **Number of edges from the degrees.** A graph with degrees $4, 4, 3, 3, 2, 2$ has $\frac{18}{2} = 9$ edges.
- **No graph with an odd degree sum.** There is no graph with 7 vertices each of degree 3: the degrees would add to 21, and 21 is not $2e$ for any whole number e. More generally, if every vertex has degree 3 then $3n = 2e$, so the number of vertices n must be even.
- **Edges of a complete graph**, below.

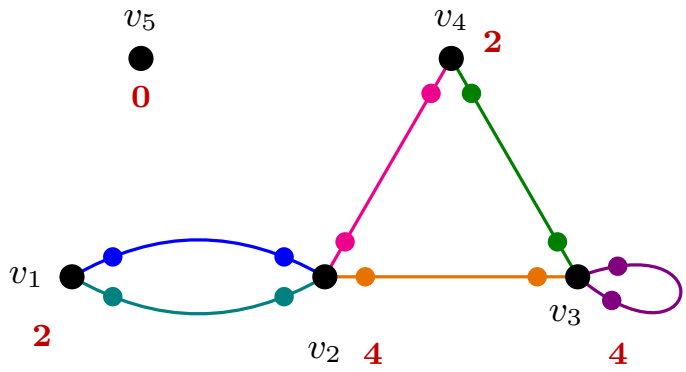


Figure 36: The proof of the Handshake Theorem, on the graph above. Every edge is drawn in its own colour, with a dot of that colour at each of its two ends. The loop e_4 has both of its dots at v_3. The degree of a vertex is the number of dots at it, so adding up the degrees counts every dot once. Each edge has exactly two dots, so the 6 edges give 12 dots, and the degrees add to 12.

Odd-degree vertices come in pairs

Corollary. Every graph has an even number of vertices of odd degree.

Proof. Split the sum of the degrees into the vertices of even degree and the vertices of odd degree:

$$\underbrace{\sum_{\deg(v) \text{ even}} \deg(v)}_{\text{even}} + \sum_{\deg(v) \text{ odd}} \deg(v) = 2e.$$

The first sum is a sum of even numbers, so it is even. The right side is even. So the second sum, being the difference of two even numbers, is even. It is a sum of odd numbers, and a sum of odd numbers is even exactly when there is an even number of terms: odd numbers pair up into even sums, and one left over makes the total odd. So the number of vertices of odd degree is even. □

The corollary says nothing about the vertices of **even** degree. Their number can be odd or even: one vertex joined to four others has one vertex of even degree, and a path of four vertices has two. That is worked as a multiple-choice question in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[87].

[87] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

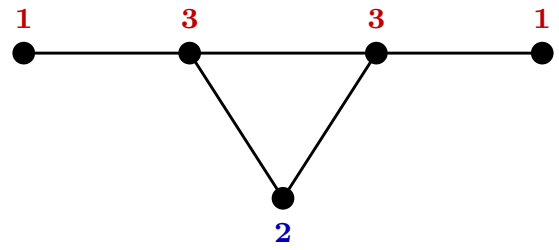


Figure 37: The corollary on a graph with degrees 3, 3, 2, 1, 1, odd degrees in red and even in blue. The degree sum is $2e = 10$, even. Its even part, 2, is even, so its odd part, $3+3+1+1$, must be even as well. A sum of odd numbers is even only when the odd numbers pair off, each pair adding to an even number. Here the four odd degrees make two pairs. A fifth vertex of odd degree would be left without a partner and make the total odd, which no graph allows.

In practice the corollary is the quickest check on a list of degrees: **count the odd entries**. If there is an odd number of them, no graph has those degrees.

Degree sequences

> The list of the degrees of the vertices in a graph is called the **degree sequence** of the graph.

It is usually written largest first. The graph above has degree sequence $4, 4, 2, 2, 0$. Only the list of numbers matters, not which vertex has which.

The usual question runs the other way: given a list, is there a graph, often a **simple** graph, with exactly those degrees? Two checks rule a list out:

1. **The sum must be even**, by the Handshake Theorem. Equivalently, the number of odd entries must be even. This holds for every graph.
2. **For a simple graph with n vertices, no entry can be more than $n-1$.** A list of n numbers with an entry of n or more has no simple graph.

These checks are necessary, not sufficient. A list can pass both and still have no simple graph. Take $3, 3, 3, 1$. The sum is 10, which is even, and no entry is more than $n-1 = 3$. But with 4 vertices, a vertex of degree 3 in a simple graph is joined to all three others. There are

three such vertices, and each of them is joined to the fourth vertex, which therefore has degree 3, not 1. So no simple graph has degree sequence $3, 3, 3, 1$.

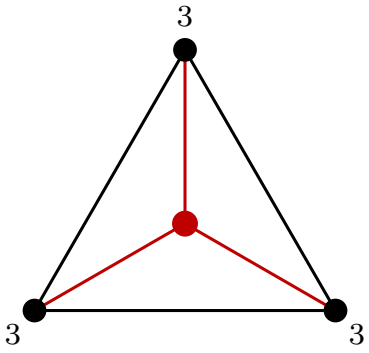


Figure 38: Why no simple graph has degree sequence 3, 3, 3, 1. In a simple graph on 4 vertices, a vertex of degree 3 is joined to every other vertex. The three vertices that need degree 3, black, must each be joined to the fourth vertex, red, which is then forced to have degree 3 as well. The list passes both quick checks, an even sum and no degree above 3, and still has no simple graph.

So, after the two checks, a list that passes either gets a drawing or an argument like this one. Small cases can be settled by hand, building the graph from the vertex of largest degree down. A complete test for when a list is the degree sequence of a simple graph does exist (the Havel–Hakimi and Erdős–Gallai theorems), but it is beyond this course.

Without the word "simple", the answer is easy. If loops are allowed, **every list with an even sum is the degree sequence of some graph**. The odd entries come in an even number, so pair them up and join each pair by an edge. Now every vertex still needs an even number of edge ends, and a loop supplies 2, so add loops until each vertex has its degree. For example, $3, 2, 1$ has no simple graph, since degree 3 is impossible with only 3 vertices, but a graph with multiple edges has those degrees (2026-10-22-pigeonhole-principle-introduction-to-graph-theory[88]).

Worked: which lists are degree sequences

For each list, is there a simple graph with those degrees?

[88] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

List	Sum	Largest vs $n-1$	Simple graph?
$2,2,2,2$	8	$2 \le 3$	yes: a square
$3,2,1$	6	$3 > 2$	no: too large
$4,3,2,2,2,2,1,1$	17	$4 \le 7$	no: odd sum (three odd entries)
$1,1,1,1$	4	$1 \le 3$	yes: two edges with no common vertex
$5,5,5,5,5,5$	30	$5 \le 5$	yes: the complete graph K_6
$3,3,3,1$	10	$3 \le 3$	no: passes both checks, fails as shown
$4,4,3,3,2,2$	18	$4 \le 5$	yes: 9 edges

The first five are drawn in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[89]. For the last, name the vertices a, b, c, d, e, f with the degrees in that order, and take the edges $ac, ad, ae, af, bc, bd, be, bf, cd$. Then a and b are each joined to c, d, e, f; c and d to a, b and each other; and e and f to a and b.

Complete graphs

The **complete graph** K_n is the simple graph with n vertices in which every pair of different vertices is joined by an edge. It is the standard name for this graph. Every vertex is joined to the other $n-1$, so every degree is $n-1$, the most a simple graph allows. K_6 is the graph with degree sequence $5,5,5,5,5,5$.

How many edges? By the Handshake Theorem,

$$n(n-1) = 2e, \qquad \text{so} \qquad e = \frac{n(n-1)}{2}.$$

Or count directly: an edge of K_n is a choice of 2 of the n vertices, so there are $\binom{n}{2} = \frac{n(n-1)}{2}$ edges (counting-selections[90]). The two counts agree. K_6 has $\frac{6\cdot 5}{2} = 15$ edges.

$\binom{n}{2}$ is the most edges a simple graph on n vertices can have. Each edge of a simple graph is a different pair of vertices, and there are only $\binom{n}{2}$ pairs. K_n uses every pair, so it is the only simple graph on n vertices that reaches the bound.

[89] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[90] courses/math1061/counting-selections.pdf

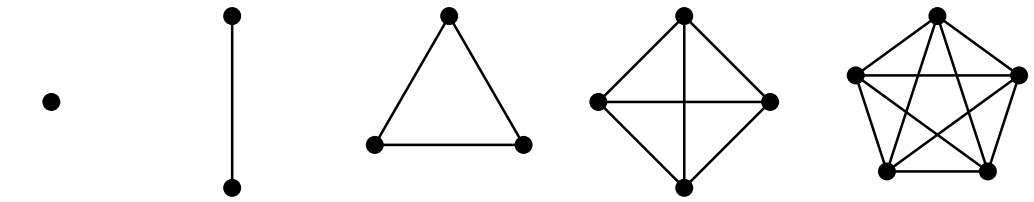


Figure 39: The complete graphs K_1 to K_5, each with every pair of vertices joined. Each vertex of K_n has degree $n-1$, so the degrees add to $n(n-1)$ and there are $\frac{n(n-1)}{2}$ edges: 0, 1, 3, 6 and 10. In K_4 and K_5 some lines cross where there is no vertex. Only the dots are vertices.

Common mistakes

- **Counting a loop once.** A loop adds 2 to the degree of its vertex. Counting it as 1 makes the degree sum odd and breaks the Handshake Theorem.
- **Treating a crossing as a vertex.** Lines that cross in a drawing are not joined. A vertex is a dot.
- **Taking an even sum as enough.** The Handshake Theorem rules a list out when its sum is odd, but an even sum does not make a simple graph exist: $3, 2, 1$ and $3, 3, 3, 1$ both have even sums and no simple graph.
- **Forgetting the word "simple".** Without it, loops and multiple edges are allowed, and any list with an even sum has a graph. With it, every degree is at most $n-1$.
- **Mixing up the corollary.** The number of vertices of **odd** degree is always even. The number of vertices of even degree can be anything.
- **Reading the drawing as the graph.** Where the dots are and how the lines bend do not matter. The graph is the vertices, the edges and their endpoints.

See also

- pigeonhole-principle[91] — every simple graph with at least two vertices has two vertices of equal degree
- counting-selections[92] — $\binom{n}{2}$, the number of edges of K_n
- 2026-07-27-welcome-and-intro-problems[93] — the bridges of Königsberg as a graph
- walks-trails-and-circuits[94] — walks, trails, circuits and connected graphs

[91] courses/math1061/pigeonhole-principle.pdf
[92] courses/math1061/counting-selections.pdf
[93] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[94] courses/math1061/walks-trails-and-circuits.pdf

- euler-circuits-and-trails[95] — when a graph can be traced using every edge exactly once
- adjacency-matrices[96] · incidence-matrices[97] — a graph written as a matrix
- [trees] — connected graphs with no circuits
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[98] — Lecture 33
- 2026-10-26-walks-trails-and-circuits[99] — Lecture 34, which recaps these definitions
- practice-problems[100] — §43, with full worked solutions

Incidence Matrices

An incidence matrix writes a graph down by vertices against edges: a row for each vertex, a column for each edge, and in each place the number of times that vertex is incident with that edge. Each column is one edge, so the matrix is in effect the table of endpoints written as numbers. It has a simple shape that makes it easy to check: every column adds to 2, because every edge has two ends, and every row adds to the degree of its vertex. Putting those together proves the Handshake Theorem again. The other matrix of a graph, vertices against vertices, is in adjacency-matrices[101]. Graphs, loops, degree and the Handshake Theorem are in [graphs]. First met in 2026-10-27-matrix-representations-of-graphs[102].

Definition

> The **incidence matrix** of a graph with vertices $v_1, v_2, \dots, v_n$ and edges $e_1, e_2, \dots, e_m$ is the $n \times m$ matrix $N = [n_{ij}]$ where each entry n_{ij} is the number of times vertex v_i is incident with edge e_j.

Rows are vertices and columns are edges. The entry n_{ij} is about vertex v_i and edge e_j, in that order, and the first index is the row. The matrix is $n \times m$: as many rows as vertices, as many columns as edges. Swapping the roles gives the transpose N^{T}, which holds the same information but is not the incidence matrix as this course defines it, so write the vertices down the side and the edges across the top, and label both. Like the adjacency matrix, N depends on the order chosen for the vertices and for the edges.

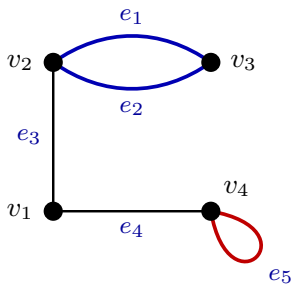
An edge has two ends. For a vertex v_i and an edge e_j there are three cases:

- e_j does not have v_i as an endpoint: $n_{ij} = 0$.
- e_j joins v_i to a different vertex: one end is at v_i, so $n_{ij} = 1$.

[95] courses/math1061/euler-circuits-and-trails.pdf
[96] courses/math1061/adjacency-matrices.pdf
[97] courses/math1061/incidence-matrices.pdf
[98] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[99] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[100] courses/math1061/practice-problems.pdf
[101] courses/math1061/adjacency-matrices.pdf
[102] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf

- e_j is a loop at v_i: both ends are at v_i, so $n_{ij} = 2$.

So **every entry is 0, 1 or 2**, and **a 2 means a loop**.



$N =$

	e_1	e_2	e_3	e_4	e_5	sum
v_1	0	0	1	1	0	2
v_2	1	1	1	0	0	3
v_3	1	1	0	0	0	2
v_4	0	0	0	1	**2**	3
sum	2	2	2	2	2	

Figure 40: A graph and its incidence matrix, one row for each vertex and one column for each edge. Each column is an edge: e3 has a 1 at each of its endpoints v1 and v2, and the loop e5, in red, has a single 2 at v4, because it meets v4 at both of its ends. The parallel edges e1 and e2, in blue, have the same endpoints and so identical columns. Every column adds to 2, and each row adds to the degree of its vertex: 2, 3, 2, 3.

Columns are edges

The column of e_j lists how many times each vertex meets e_j. So:

- **Every column adds to 2.** An edge has exactly two ends, and each end is at one vertex. A column is either **two 1s** (an edge with two different endpoints, the rows of the 1s) or **a single 2** (a loop, at the row of the 2), and 0 everywhere else.
- **Parallel edges have identical columns.** Two edges with the same endpoints meet every vertex the same number of times. In the figure, e_1 and e_2 are both $(0, 1, 1, 0)$.
- **A column is never all zeros**, since every edge has at least one endpoint.

Rows are vertices

The row of v_i lists how many times v_i meets each edge.

- **The row sum is the degree.** Adding the row counts the ends of edges at v_i, a loop's two ends included, which is $\deg(v_i)$ (graphs[103]). Unlike the adjacency matrix, no correction for loops is needed: the loop's 2 is already in the row.
- **An isolated vertex has a row of zeros.** It still gets its row.

[103] courses/math1061/graphs.pdf

The Handshake Theorem again

Add up every entry of N in two ways.

- **Column by column:** each of the m columns adds to 2, so the total is $2m$.
- **Row by row:** row i adds to $\deg(v_i)$, so the total is $\deg(v_1) + \cdots + \deg(v_n)$.

The two totals are the same number, so

$$\sum_{i=1}^{n} \deg(v_i) = 2m,$$

which is the Handshake Theorem (graphs[104]). It is the same proof as counting edge ends, with the ends laid out in a table: each entry counts ends of one edge at one vertex. In the figure, the row sums $2+3+2+3$ and the column sums $2+2+2+2+2$ both come to 10.

Loops

A loop at v_i is incident with v_i **twice**, once at each of its ends, so its column has a **2** in row v_i and 0 everywhere else. In the figure the loop e_5 is the column $(0, 0, 0, 2)$.

This is what keeps the column sums at 2 and makes the row sums the degrees: the 2 is the loop's contribution to $\deg(v_i)$.

The adjacency matrix counts a loop differently. It counts edges, and a loop is one edge, so it puts a **1** on the diagonal (adjacency-matrices[105]). The same loop is a 1 in A and a 2 in N. A column with a single 1 and nothing else is not a loop. It is not an edge at all, since it has only one end.

Reading a graph off a matrix

Read an incidence matrix **one column at a time**:

1. Draw a dot for each row and label it $v_1, \ldots, v_n$.
2. For each column e_j: if it has 1s in rows i and k, draw an edge e_j joining v_i and v_k; if it has a 2 in row i, draw a loop e_j at v_i.
3. Check: every column added to 2, and each vertex's degree in the drawing is its row sum.

[104] courses/math1061/graphs.pdf
[105] courses/math1061/adjacency-matrices.pdf

For example,

$$N = \begin{array}{c|ccccc} & e_1 & e_2 & e_3 & e_4 & e_5 \\ \hline v_1 & 1 & 0 & 0 & 2 & 0 \\ v_2 & 1 & 1 & 1 & 0 & 0 \\ v_3 & 0 & 1 & 1 & 0 & 1 \\ v_4 & 0 & 0 & 0 & 0 & 1 \end{array}$$

has every column adding to 2. Column by column: e_1 joins v_1 and v_2; e_2 and e_3 both join v_2 and v_3, identical columns, so they are parallel; e_4 is a loop at v_1; e_5 joins v_3 and v_4.

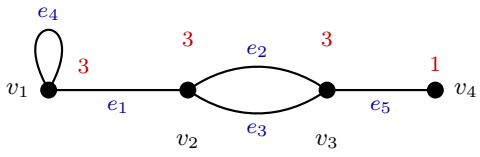


Figure 41: The graph read off the incidence matrix, one column at a time. Columns e2 and e3 are identical, so those two edges are parallel, and column e4 is a single 2 in row v1, so it is a loop at v1. The degrees, in red, are the row sums of the matrix, 3, 3, 3, 1, and they add to 10, twice the 5 edges.

Unlike an adjacency matrix, an incidence matrix names every edge, so the graph comes back with its edge names as well.

Which matrices are incidence matrices

> A matrix with at least one row is the incidence matrix of some graph if and only if every entry is a non-negative integer and **every column adds to 2**. Equivalently, every column is either two 1s and the rest 0, or a single 2 and the rest 0.

The two forms agree: non-negative integers adding to 2 are either $1 + 1$ or 2, with zeros elsewhere.

Proof. ($\Rightarrow$) Shown above: each column is an edge, and an edge is two 1s at its two endpoints or a single 2 at the vertex of a loop.

($\Leftarrow$) Let M be an $n \times m$ matrix, $n \geq 1$, whose columns each have one of the two forms. Build a graph with vertices $v_1, \ldots, v_n$ and, for each column j, an edge e_j: if column j has 1s in rows i and k, let e_j join v_i and v_k; if it has a 2 in row i, let e_j be a loop at v_i. Then v_i is incident with e_j once if v_i is one of two endpoints, twice if e_j is a loop at v_i, and not at all otherwise, which is the entry m_{ij} in every case. So M is this graph's incidence matrix. □

Only the columns are tested. The rows can be anything, a row of zeros included (an isolated vertex), and the matrix does not have to be square or symmetric. A graph with no edges has no columns at all, and then there is nothing to check.

Matrix	Column sums	Incidence matrix?
$\begin{bmatrix}1 & 2\\ 1 & 0\end{bmatrix}$	2, 2	yes: an edge v_1v_2 and a loop at v_1
$\begin{bmatrix}1 & 1\\ 1 & 0\\ 0 & 0\end{bmatrix}$	2, 1	no: the second edge has only one end
$\begin{bmatrix}1\\ 1\\ 1\end{bmatrix}$	3	no: an edge with three ends
$\begin{bmatrix}0\\ 2\\ 0\end{bmatrix}$	2	yes: three vertices, a loop at v_2, and v_1, v_3 isolated

Four more are worked in 2026-10-27-matrix-representations-of-graphs[106].

Adjacency and incidence compared

The graph in the figure has both matrices:

$$A = \begin{array}{c|cccc} & v_1 & v_2 & v_3 & v_4 \\ \hline v_1 & 0 & 1 & 0 & 1 \\ v_2 & 1 & 0 & 2 & 0 \\ v_3 & 0 & 2 & 0 & 0 \\ v_4 & 1 & 0 & 0 & 1 \end{array} \qquad N = \begin{array}{c|ccccc} & e_1 & e_2 & e_3 & e_4 & e_5 \\ \hline v_1 & 0 & 0 & 1 & 1 & 0 \\ v_2 & 1 & 1 & 1 & 0 & 0 \\ v_3 & 1 & 1 & 0 & 0 & 0 \\ v_4 & 0 & 0 & 0 & 1 & 2 \end{array}$$

	Adjacency matrix A	Incidence matrix N
Size	$n \times n$	$n \times m$
Rows	vertices	vertices
Columns	vertices	edges
Entry	number of edges with endpoints $\{v_i, v_j\}$	number of times v_i is incident with e_j
Entries can be	any non-negative integer	0, 1 or 2
A loop at v_i	1 on the diagonal, at a_{ii}	2 in its column, at row v_i

[106] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf

	Adjacency matrix A	Incidence matrix N
Parallel edges	one entry bigger than 1	identical columns
Shape	square and symmetric	any; each column adds to 2
$\deg(v_i)$	row sum plus a_{ii}	row sum
Number of edges	sum on and above the diagonal	number of columns
Edge names	not recorded	one column per named edge

From N to A. Off the diagonal, a_{ij} is the number of columns with a 1 in both row i and row j. On the diagonal, a_{ii} is the number of columns with a 2 in row i. In N above, two columns (e_1 and e_2) have 1s in rows v_2 and v_3, so $a_{23} = 2$, and one column (e_5) has a 2 in row v_4, so $a_{44} = 1$.

From A to N, the edges first have to be named, since A only says how many edges join each pair. Any naming gives an incidence matrix of the same graph, with its columns in a different order.

A is the more compact when there are many edges. N is the one to use when the edges themselves matter, as in listing an Euler circuit edge by edge, which is done from an incidence matrix in 2026-10-27-matrix-representations-of-graphs[107].

Common mistakes

- **Swapping rows and columns.** In this course the vertices are the rows and the edges are the columns. The transpose has the same information but is not the incidence matrix as defined here.
- **Writing 1 for a loop.** A loop meets its vertex twice, so it is a 2. A column with a single 1 has only one end and is not an edge.
- **Adding a loop correction to the row sum.** That is for the adjacency matrix. In N the row sum already is the degree.
- **Checking the rows, or symmetry, instead of the columns.** Whether a matrix is an incidence matrix is decided by its columns alone: each must add to 2.
- **Leaving out an isolated vertex.** Every vertex has a row, even if it is all zeros.
- **Leaving off the labels.** The matrix depends on the order of the vertices and of the edges.

See also

- adjacency-matrices[108] — the vertex-by-vertex matrix, where a loop counts 1

[107] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[108] courses/math1061/adjacency-matrices.pdf

- [graphs] — loops, parallel edges, degree and the Handshake Theorem
- euler-circuits-and-trails[109] — the even-degree test for an Euler circuit
- 2026-10-27-matrix-representations-of-graphs[110] — Lecture 35
- practice-problems[111] — §45, with full worked solutions

The Pigeonhole Principle

If more objects are put into boxes than there are boxes, some box gets two. That is the pigeonhole principle, and it proves that something **must exist** (two chosen numbers that are consecutive, two subsets with the same sum, two vertices with the same degree) without finding it. This note states the principle, gives its form for functions and its generalised form, explains how to choose the pigeons and the holes, and works through the standard arguments. Counting the pigeons and the holes uses counting-principles[112] and counting-selections[113]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[114].

The principle

> **The pigeonhole principle.** If n pigeons fly into m pigeonholes and $n > m$, then at least one pigeonhole contains two or more pigeons.

Proof. Suppose every hole contains at most one pigeon. Then the m holes contain at most m pigeons in total. But there are $n > m$ pigeons, a contradiction. So some hole contains at least two. □

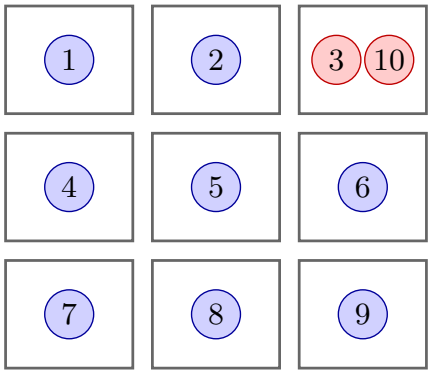
Three things about it:

- **It says some hole has two, not which hole.** A pigeonhole proof is an existence proof.
- **It needs $n > m$ strictly.** Nine pigeons in nine holes can sit one per hole.
- **It says nothing when $n \leq m$.** Then two pigeons might share a hole or might not, and the principle gives no information either way.

As a statement about functions

Putting each pigeon in a hole is a function from the set of pigeons to the set of holes, and "two pigeons in one hole" says two inputs have the same output. So:

[109] courses/math1061/euler-circuits-and-trails.pdf
[110] courses/math1061/2026-10-27-matrix-representations-of-graphs.pdf
[111] courses/math1061/practice-problems.pdf
[112] courses/math1061/counting-principles.pdf
[113] courses/math1061/counting-selections.pdf
[114] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf



10 pigeons, 9 holes: some hole holds 2

Figure 42: Ten pigeons, numbered, in nine holes. However the ten are placed, the nine holes cannot each hold at most one, since that accounts for only nine pigeons. Here pigeons 3 and 10 share the top-right hole. A different placement would make a different pair share a hole, but some hole always holds two.

> **Pigeonhole principle, function form.** If X and Y are finite sets with $|X| > |Y|$, then no function $f : X \to Y$ is one-to-one: there are $x_1 \neq x_2$ in X with $f(x_1) = f(x_2)$.

This is the first of the facts about finite sets in cardinality[115], and "one-to-one" is defined in one-to-one-and-onto-functions[116]. Read this way, a pigeonhole proof has three parts: say what X is (the pigeons), say what Y is (the holes), and say what f does (which hole each pigeon goes to). Then count both sets.

The generalised principle

Sometimes two in a hole is not enough, and the argument needs three, or more. The same proof gives the standard generalisation:

> **Generalised pigeonhole principle.** If n pigeons fly into m pigeonholes and $n > k \cdot m$, then at least one pigeonhole contains $k + 1$ or more pigeons.

Proof. If every hole contained at most k pigeons, there would be at most $k \cdot m$ pigeons, and there are more. □

With $k = 1$ it is the ordinary principle. An equivalent way to say it: **some hole contains at least $\lceil n/m \rceil$ pigeons**, the average rounded up. If $n > k \cdot m$ then $n/m > k$, so $\lceil n/m \rceil \geq k+1$.

[115] courses/math1061/cardinality.pdf
[116] courses/math1061/one-to-one-and-onto-functions.pdf

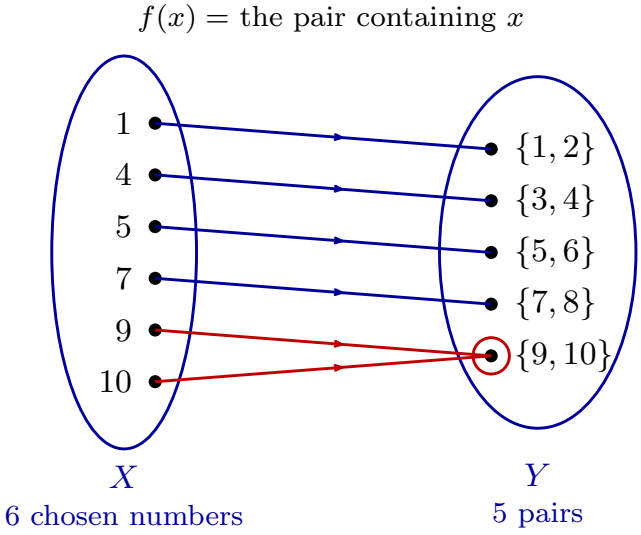
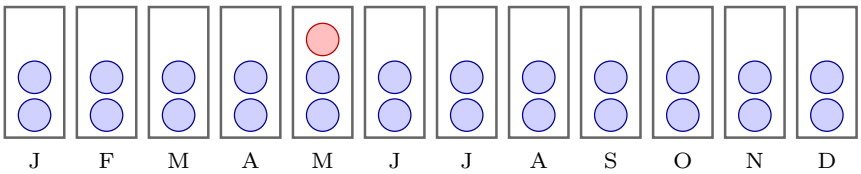


Figure 43: The function form on a small case: six numbers chosen from 1 to 10. X is the set of chosen numbers, the pigeons. Y is the set of five pairs of neighbours $1, 2, 3, 4, \ldots, 9, 10$, the holes. f sends each chosen number to the pair it lies in. Since $|X| = 6 > 5 = |Y|$, f cannot be one-to-one, so two chosen numbers, here 9 and 10, go to the same pair, and two numbers in one pair are consecutive. A different choice of six moves the collision to a different pair but cannot avoid one.

Example: birth months. Among any 25 people, at least 3 were born in the same month. The people are the pigeons and the 12 months are the holes. $25 > 2 \cdot 12$, so some month has at least $\lceil 25/12 \rceil = 3$ of them. 24 people are not enough: two born in each month have no three in the same month.



$24 = 2 \cdot 12$ people fit two to a month; the 25th makes a month with 3

Figure 44: The generalised principle with 25 people and 12 months. Up to 24 people can be spread so that no month has more than 2, two in every month. That fills every month to its limit, so the 25th person, in red, must make some month's count 3. In general, more than $k \cdot m$ pigeons in m holes force some hole to hold $k + 1$.

Choosing the pigeons and the holes

The principle is easy. The work is in choosing what the pigeons and the holes are.

- **The pigeons** are usually the objects the problem chooses: the numbers selected, the subsets, the people, the vertices.
- **The holes** must cover everything. Every pigeon has to land in some hole, and in exactly one. When the pigeons are elements of a set, the holes are a partition of that set (sets-and-set-notation[117]).
- **Two pigeons in one hole must give exactly what is wanted.** This is what decides the holes. To force two consecutive numbers, make the holes pairs of consecutive numbers. To force a sum of 101, make the holes pairs that sum to 101. To force a common remainder, make the holes the remainders.
- **Count both.** The argument works only if there are more pigeons than holes. If the first choice of holes gives too many, look for a way to merge them, as in equal degrees, or a better bound, as in subset sums.

Many problems ask for the **largest** (or smallest) number with some property. The answer always has two halves:

1. **An example.** Show that the number can be reached, by writing down a selection of that size.
2. **A pigeonhole argument.** Show that one more forces the property to fail.

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

The pigeonhole half on its own proves only a bound. Without the example, the true answer might be smaller.

Worked: no two consecutive

> What is the largest number of integers that can be chosen from $\{1, 2, \dots, 100\}$ with no two consecutive?

50. The odd numbers $1, 3, \dots, 99$ are 50 numbers with no two consecutive. For the bound, the holes are the 50 pairs $\{1, 2\}, \{3, 4\}, \dots, \{99, 100\}$. Each pair is two consecutive numbers, so a good selection takes at most one from each pair. Choosing 51 or more puts two in some pair, and they are consecutive.

In general, from $\{1, 2, \dots, 2m\}$ the largest selection with no two consecutive has m numbers. The holes are pairs of neighbours, $\{2i - 1, 2i\}$.

The full question, with the wrong options, is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[118].

Worked: a pair with a given sum

> Prove that if 51 numbers are chosen from $\{1, 2, \dots, 100\}$, then two of them sum to 101.

The holes are the 50 pairs $P_i = \{i, 101 - i\}$ for $i = 1, \dots, 50$:

$$\{1, 100\},\ \{2, 99\},\ \dots,\ \{50, 51\}.$$

Each number from 1 to 100 is in exactly one of them. 51 chosen numbers in 50 pairs put two in one pair P_i, and $i + (101 - i) = 101$.

The same holes answer any question of this shape. From $\{1, 2, \dots, 2m\}$, any $m + 1$ numbers include two that sum to $2m + 1$, using the pairs $\{i, 2m + 1 - i\}$. And m numbers are not enough: $1, 2, \dots, m$ have no two summing to more than $2m - 1$.

The drawing of these pairs is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[119].

[118] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[119] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Worked: no three consecutive

> What is the largest number of integers that can be chosen from $\{1, 2, \dots, 60\}$ with no three consecutive?

40.

- **Example.** Choose everything except the multiples of 3, the numbers congruent to 1 or 2 mod 3. Any three consecutive integers include a multiple of 3, so no three chosen numbers are consecutive. That is $60 \cdot \frac{2}{3} = 40$ numbers.
- **Bound.** The holes are the 20 blocks $\{1, 2, 3\}, \{4, 5, 6\}, \dots, \{58, 59, 60\}$. A block with all three chosen is three consecutive numbers. With 41 numbers in 20 blocks, $41 > 2 \cdot 20$, so by the generalised principle some block holds $\lceil 41/20 \rceil = 3$ chosen numbers.

This is the generalised principle with $k = 2$: the property needs three in one hole, not two.

Worked: two subsets with the same sum

> Show that if A is any 6-element subset of $\{1, 2, \dots, 12\}$, then A has distinct subsets X and Y with the same sum.

- **Pigeons: the subsets of A.** There are $2^6 = 64$ of them, including $\emptyset$ and A (sets-and-set-notation[120], binomial-coefficients[121]).
- **Holes: the possible sums.** Every element is positive, so a subset's sum is between 0 (for $\emptyset$) and the sum of all of A. Six different integers from 1 to 12 add up to at most $7 + 8 + 9 + 10 + 11 + 12 = 57$. So there are at most 58 possible sums, $0, 1, \dots, 57$.
- **Conclusion.** $64 > 58$, so two different subsets have the same sum.

The pigeons here are not the elements of A but its subsets, which are far more numerous than the possible sums: the number of subsets doubles with each extra element, while the largest possible sum grows by at most 12. That gap is what makes the argument work. The bound on the sum has to be the tight one. Using the sum of all of $\{1, \dots, 12\}$, 78, as the bound gives 79 holes for 64 pigeons, and the argument fails.

Leaving out $\emptyset$ works too: 63 non-empty subsets and 57 possible sums, $1, \dots, 57$. Either way, count the pigeons and the holes over the same collection.

The figure for $A = \{2, 4, 6, 8, 10, 12\}$ is in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[122].

[120] courses/math1061/sets-and-set-notation.pdf
[121] courses/math1061/binomial-coefficients.pdf
[122] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

Worked: two with the same remainder

> Show that among any $n+1$ integers there are two whose difference is divisible by n.

The holes are the n possible remainders on division by n, $0, 1, \dots, n-1$. Each integer has exactly one, by the quotient-remainder theorem (modular-arithmetic[123]). $n+1$ integers and n remainders put two integers a and b in one hole. They have the same remainder r, so $a = nq_1 + r$ and $b = nq_2 + r$, and $a - b = n(q_1 - q_2)$ is divisible by n.

n integers are not enough: $0, 1, \dots, n-1$ have all their differences between $-(n-1)$ and $n-1$, and none of those but 0 is divisible by n.

For example, among any 4 integers, two differ by a multiple of 3. From $\{1, 2, \dots, 100\}$ that means 4 picks guarantee such a pair, while the 3 picks $1, 2, 3$ do not.

Worked: two vertices of equal degree

> Show that in any simple graph with at least two vertices, two vertices have the same degree.

Graphs, simple graphs and degree are in [graphs]. Said with people: in any group of two or more people, two of them have the same number of friends within the group, if friendship goes both ways.

Let the graph have $n \geq 2$ vertices. In a simple graph a vertex is joined to at most each of the other $n-1$ vertices once, so every degree is one of the n values $0, 1, \dots, n-1$. That is n pigeons and n holes, which is not enough. The extra step is that **0 and $n-1$ cannot both occur**. A vertex of degree $n-1$ is joined to every other vertex, so no vertex has degree 0. So the degrees all lie in $\{0, 1, \dots, n-2\}$ or all lie in $\{1, 2, \dots, n-1\}$. Either way there are only $n-1$ holes for n vertices, and two vertices share a degree.

This is the problem about five friends in 2026-07-27-welcome-and-intro-problems[124].

Common mistakes

- **Using it with too few pigeons.** If the number of pigeons is not more than the number of holes, the principle proves nothing. It does not make the statement false either: every 5-element subset of $\{1, \dots, 12\}$ also has two subsets with equal sums, but with 32 subsets and up to 51 possible sums the pigeonhole argument cannot show it.
- **Holes that overlap.** Pairs like $\{1, 2\}, \{2, 3\}, \{3, 4\}, \dots$ share numbers, so a pigeon is in two holes and the count no longer works. The holes must split the set: every pigeon in exactly one hole.

[123] courses/math1061/modular-arithmetic.pdf
[124] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

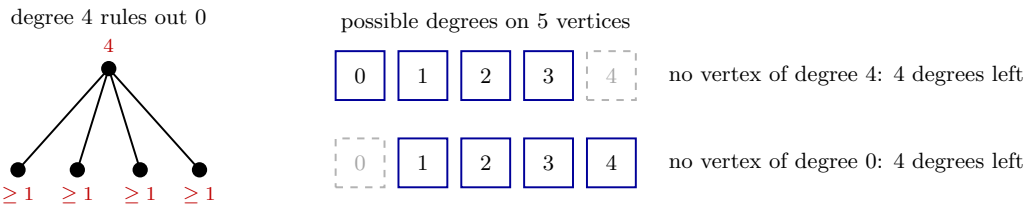


Figure 45: Why two vertices of a simple graph on 5 vertices have equal degree. The possible degrees are 0 to 4, five holes for five vertices, which forces nothing. But a vertex of degree 4 is joined to all four others, left, so each of them has degree at least 1 and none can have degree 0. So either no vertex has degree 4, top right, or none has degree 0, bottom right. In both cases only four degrees are available for five vertices, and two vertices share one.

- **Holes that don't force the property.** Two pigeons in one hole must give what is wanted. Pairs $\{1,2\},\{3,4\},\ldots$ force two consecutive numbers but not two that sum to 101.
- **Only half an answer.** For "what is the largest", the pigeonhole bound needs an example of that size as well, and the example needs the bound.
- **Off by one in the generalised form.** $k \cdot m$ pigeons can sit k to a hole. It takes $k \cdot m + 1$ to force $k + 1$ in one hole: 24 people can have no three sharing a birth month, 25 cannot.
- **A loose bound on the holes.** Counting more holes than can actually be used (sums up to 78 rather than 57, or degrees 0 to $n - 1$ when 0 and $n - 1$ exclude each other) can make an argument that should work fail.
- **Claiming to know which hole.** The principle says some hole has two pigeons. It does not say which.

See also

- cardinality[125] — no one-to-one function from a larger finite set to a smaller one, which is the principle for functions
- one-to-one-and-onto-functions[126] — what one-to-one means
- [graphs] — degree, used in equal degrees
- counting-selections[127] — counting the pigeons and the holes
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[128] — Lecture 33

[125] courses/math1061/cardinality.pdf
[126] courses/math1061/one-to-one-and-onto-functions.pdf
[127] courses/math1061/counting-selections.pdf
[128] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

- 2026-10-26-walks-trails-and-circuits[129] — Lecture 34, which opens with equal degrees again
- practice-problems[130] — §42, with full worked solutions

Practice Problems — the Semester-wide Set

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

Applied Classes start in **Week 2** and run to Week 13 — twelve of them, matching the "best 8 of 12" Applied Classes component worth 30% (see math1061[131]). Each week's class applies the *previous* week's lecture content, so the material a class covers runs roughly one week behind the lecture column below. Which sections a given Applied Class draws on is not stated in any of the source material.

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

How each section is laid out

1. Relevant textbook pages for Epp 4th edition and 5th (metric) edition
2. **Practice problems**
3. **Solutions** — full worked solutions, not just answers
4. Occasionally a non-assessable **Application** block (see the table below)

Errata

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

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

[129] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[130] courses/math1061/practice-problems.pdf
[131] courses/math1061/math1061.pdf

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

Section index

Every section is below, with its topic and textbook page ranges. Each section goes with one pre-work video (§1 with *Video 001*, and so on up to *Video 046*), and the Lecture (week) column places it in the schedule of math1061[132] by that video number. The Notes column links to the concept note covering that material where one exists; the rest are still ahead in the semester.

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
1	Logical Form	L2 (wk 1)	023–029	037–043	logical-connectives[133]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[134]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[135]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[136]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[137]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[138]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[139]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[140]

[132] courses/math1061/math1061.pdf
[133] courses/math1061/logical-connectives.pdf
[134] courses/math1061/logical-equivalence-laws.pdf
[135] courses/math1061/conditional-statements.pdf
[136] courses/math1061/valid-argument-forms.pdf
[137] courses/math1061/determining-argument-validity.pdf
[138] courses/math1061/quantified-statements.pdf
[139] courses/math1061/quantified-statements.pdf
[140] courses/math1061/quantified-statements.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[141]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[142]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[143]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[144]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[145]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[146]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[147]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[148]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[149]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[150]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[151]

[141] courses/math1061/proof-techniques.pdf
[142] courses/math1061/proof-techniques.pdf
[143] courses/math1061/proof-techniques.pdf
[144] courses/math1061/rational-and-irrational-numbers.pdf
[145] courses/math1061/divisibility-and-factorisation.pdf
[146] courses/math1061/modular-arithmetic.pdf
[147] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[148] courses/math1061/sequences-and-summations.pdf
[149] courses/math1061/mathematical-induction.pdf
[150] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[151] courses/math1061/recursive-definitions.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[152]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[153]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[154]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[155]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[156]
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	

[152] courses/math1061/solving-recurrence-relations.pdf
[153] courses/math1061/sets-and-set-notation.pdf
[154] courses/math1061/sets-and-set-notation.pdf
[155] courses/math1061/proving-set-properties.pdf
[156] courses/math1061/functions-on-general-sets.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
33	Definitions and Examples of Groups	L26 (wk 9)	—	—	
34	Elementary Properties of Groups	L27 (wk 10)	—	—	
35	Group Isomorphisms	*not scheduled*	—	—	
36	Definitions and Examples of Fields	L28 (wk 10)	—	—	
37	Introduction to Counting	L29 (wk 11)	516–553	564–604	
38	Counting Selections	L30 (wk 11)	516–553	564–604	
39	Introduction to Probability	L31 (wk 12)	516–553	564–604	
40	Binomial Coefficients	L31 (wk 12)	565–591	617–641	
41	Inclusion Exclusion	L32 (wk 12)	545–549	595–599	
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[157].

Problems

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

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

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[158].

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.

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

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

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

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

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

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

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

Solutions

1. (a) We have

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

   (b) We have

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

2. (a) We have

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

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

(b) We have

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

Hence the statement is a **tautology**.

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

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

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

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

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

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

4. (a) We have

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

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

(b) We have

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

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

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

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

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

Application — Applications to Computer Science

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

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

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

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

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

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

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

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

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

Application problems

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

   (a) 1011110, 0100001

   (b) 11110000, 10101010

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

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

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

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

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

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

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

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

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

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

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

Application solutions

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

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

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

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

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

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

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

4. (a) We have

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

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

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

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

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

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

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

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

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

Alternatively, by truth table:

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

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

§3 — Conditional Statements

Epp 4th ed. pp. 039–050 · 5th ed. (metric) pp. 053–066. Lecture 3 (week 1). Notes: conditional-statements[159].

Problems

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

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

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

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

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

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

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

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

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

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

5. Negate the following two statements.

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

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

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

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

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

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

Solutions

1. We have

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

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

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

   while

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

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

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

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

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

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

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

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

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

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

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

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

Therefore the truth table for the statement is:

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

The statement is a **tautology**.

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

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

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

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

$$R \wedge \sim U,$$

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

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

$$H \wedge \sim B,$$

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

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

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

§4 — Valid and Invalid Arguments

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 4 (week 2). Notes: valid-argument-forms[160].

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

Problems

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

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

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

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

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

   (a) **Elimination:**

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

   (b) **Generalisation:**

   1. $p \therefore p \vee q$

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

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

Solutions

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

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

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

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

3. (a)

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

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

(b)

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

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

4. We compute the truth table:

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

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

§5 — Methods for Determining Validity

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 5 (week 2). Notes: determining-argument-validity[161].

Problems

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

   (a)

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

   (b)

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

   (c)

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

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

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

   Please use the following variables:

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

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

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

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

Solutions

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

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

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

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

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

Therefore the argument is valid.

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

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

2. The argument has the symbolic form:

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

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

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

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

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

We can write the argument as follows:

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

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

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

Application — Applications of Valid and Invalid Arguments

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

Application problems

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

   Consider the following predicates and domains:

   Predicates:

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

   Domains:

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

   Express the system specifications below using quantifiers and logical connectives:

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

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

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

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

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

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

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

Application solutions

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

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

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

2. (a) Define the following variables:

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

Now we can express the specifications as follows:

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

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

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

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

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

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

(b) Define the following variables:

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

Now we can express the specifications as follows:

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

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

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

§6 — Quantified Statements

Epp 4th ed. pp. 096–108 · 5th ed. (metric) pp. 108–121. Lecture 5 (week 2). Notes: quantified-statements[162].

Problems

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

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

Solutions

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

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

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

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

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

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

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

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

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

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

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

§7 — Negation of Quantified Statements

Epp 4th ed. pp. 108–117 · 5th ed. (metric) pp. 122–131. Lecture 6 (week 2). Notes: quantified-statements[163].

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.

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

Solutions

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

   The original statement is **false**. For instance, take $x = -4$. Then $x^2 > 9$ but $x \not\geq 2$.

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

   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[164].

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:

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

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

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

do the following:

i. Write the statement in symbolic form.

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

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

Solutions

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

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

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

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

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

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

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

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

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

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

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

   iii. The **original** statement is true. For any given $x \in \mathbb{Q}$ and $y \in \mathbb{Z}^{<0}$, take $z = xy + 1$. This is a real number satisfying the inequality $z > xy$.

(b) i. **Original:** $\forall x \in \mathbb{R},\ \exists y \in \mathbb{R}$ s.t. $3y = x$.

ii. **Negation:** $\exists x \in \mathbb{R}$ s.t. $\forall y \in \mathbb{R},\ 3y \neq x$.

iii. The **original** statement is true. Given any $x \in \mathbb{R}$, choose $y = \frac{x}{3}$. This is a real number satisfying the equality $3y = x$.

§9 — Direct Proofs and Counterexamples

Epp 4th ed. pp. 145–163 · 5th ed. (metric) pp. 160–182. Lecture 7 (week 3). Notes: proof-techniques[165].

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*

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

(a) The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

(b) If a and b are even integers, then $4a + 2b$ is even.

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

(c) $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true.

(d) $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that $n^2 + 2n + 1$ is composite, so this means

$$n^2 + 2n + 1 = rs$$

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite.

Solutions

1. (a) **The sum of any pair of even integers is even.**

Proof. Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence

$$m + n = 2k + 2\ell = 2(k + \ell),$$

which is even. Therefore, the sum of any pair of even integers is even. □

(b) **There exist positive integers a, b and c such that $a^2 + b^2 = c^2$.**

Proof. Consider the positive integers $a = 3$, $b = 4$, $c = 5$. Then $a^2 + b^2 = 9 + 16 = 25 = c^2$. □

(c) **There is an even integer n such that $5n - 4$ is prime.** This statement is **false**. We prove the negation: $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

Proof. Suppose that n is an even integer. Thus $n = 2k$ for some integer k. Hence

$$5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2).$$

By definition, this means that $5n - 4$ is even. The only even prime is 2. If $2(5k - 2) = 2$, then $5k - 2 = 1$ and hence $k = \frac{3}{5}$ which is not an integer. Therefore $5n - 4$ is not a prime number. □

(d) **$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.**

Proof. Suppose n is a positive integer and $n \geq 4$. Let us factor

$$2n^2 - 5n + 2 = (2n - 1)(n - 2).$$

Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers > 1. Hence the expression is composite for all $n \geq 4$. □

(e) **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** This statement is **false**. Take $x = 1$ and $y = -2$. Then $y^2 = 4 > x^2 = 1$, but $y = -2 \not> 1 = x$.

2. Take $x = \frac{3}{2}$. Then $\lfloor x^2 \rfloor = \lfloor \frac{9}{4} \rfloor = 2$, while $\lfloor x \rfloor^2 = \lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$. Hence $\lfloor x^2 \rfloor \neq \lfloor x \rfloor^2$, so the statement is false.

3. (a) **Statement.** The difference between any odd integer and any even integer is odd.

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. **[Error: using k for both m and n means that the statement is only proved when $m = n + 1$.]** Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

Correct proof. Let m be any odd integer and let n be any even integer. Then there exist $k, \ell \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2\ell$. Hence

$$m - n = (2k + 1) - 2\ell = 2(k - \ell) + 1,$$

which is an odd integer by definition. □

(b) **Statement.** If a and b are even integers, then $4a + 2b$ is even. **[Error: the proof forgets to state its assumptions.]**

Proof. We have $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Then we want to show that $4a + 2b$ is even, so

$$\begin{aligned} 4a + 2b &= 2\ell \quad \textbf{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

therefore the statement is true.

Correct proof. Suppose a and b are even integers. Then $a = 2k$ and $b = 2j$ for some $k, j \in \mathbb{Z}$. Therefore

$$4a + 2b = 4(2k) + 2(2j) = 8k + 4j = 2(4k + 2j).$$

Since $k, j \in \mathbb{Z}$, we have $(4k + 2j) \in \mathbb{Z}$ and so, by definition, $4a + 2b$ is even. □

(c) **Statement.** $\forall x \in \mathbb{R}$, $\exists y \in \mathbb{R}$ such that $xy = 1$.

Proof. This is true, for example if $x = 10$ then let $y = \frac{1}{10}$ and $xy = 10 \cdot \frac{1}{10} = 1$. Therefore the statement is true. **[Error: the proof argues from a single example, which cannot establish a universal statement. Moreover, the statement is false.]**

Correct disproof. The statement is false. As a counterexample, let $x = 0$. We know that $0 \cdot y = 0$ for all $y \in \mathbb{R}$ and so there is no real number y such that $0 \cdot y = 1$. □

(d) **Statement.** $\forall n \in \mathbb{Z}$, if $n > 0$ then $n^2 + 2n + 1$ is composite.

Proof. Suppose n is an integer and $n > 0$, then we want to show that n^2+2n+1 is composite, so this means

$n^2+2n+1 = rs$ **[Error: forgets to define r, s — e.g. for some $r, s \in \mathbb{Z}$]**

where

$$1 < r, s < n^2 + 2n + 1$$

Clearly neither r nor s are equal to 1 so $n^2 + 2n + 1$ is not prime and hence must be composite. **[Error: this is jumping to the conclusion without showing what needs to be shown. The expression we need to show (the definition of composite) has been given but it has not been shown.]**

Correct proof. Let $n \in \mathbb{Z}$ with $n > 0$. Then we have

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

Now since $0 < n < n^2 + 2n$, we must have that $1 < n + 1 < n^2 + 2n + 1$. So by letting $r = s = n + 1$ we have shown that

$$n^2 + 2n + 1 = rs$$

for integers $1 < r, s < n^2 + 2n + 1$. By definition this means $n^2 + 2n + 1$ is composite. □

Application — Applications of Proofs to Computer Science

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 74–80.*

Computer programs have been developed to automate the task of reasoning and proving theorems. Many of these programs make use of a rule of inference known as **resolution**. This rule of inference is based on the tautology

$$((p \vee q) \wedge (\sim p \vee r)) \rightarrow (q \vee r) \tag{1}$$

Resolution can be used to build automatic theorem proving systems.

To construct proofs using resolution as the only rule of inference, the hypotheses and conclusion must be expressed as **clauses**. Clauses are logical expressions which only feature disjunctions of variables or their negations (i.e. expressions which only use $\vee$, $\sim$, so they do not use $\wedge$, $\rightarrow$). To express any statement as a clause, we can use the laws of logical equivalence.

Application problems

1. (a) Using a truth table, show that expression (1) is a tautology.

   (b) Write the following expressions as clauses.

   i. $\sim (\sim r \wedge w)$

   ii. $r \rightarrow u$

   iii. $\sim (u \wedge w)$

   (c) Use resolution only to show that the following argument is valid:

   If it is raining, then Yvette has their umbrella. It is not the case that Yvette has their umbrella and gets wet. It is not the case that Yvette gets wet while it is not raining. Therefore, Yvette does not get wet.

Application solutions

1. (a) The truth table is

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

Since the last column is always T, the statement is a tautology.

(b) Clause forms:

i. $\sim (\sim r \wedge w) \equiv r \vee \sim w$ (by De Morgan's law and double negative law).

ii. $r \rightarrow u \equiv \sim r \vee u$ (by definition of implication).

iii. $\sim (u \wedge w) \equiv \sim u \vee \sim w$ (by De Morgan's law).

(c) Define the following variables:

r	it is raining
u	Yvette has their umbrella
w	Yvette gets wet

Then we can express the argument as

1. $r \rightarrow u$
2. $\sim (u \wedge w)$
3. $\sim (\sim r \wedge w) \therefore \sim w$

Using the equivalences in (b), we can rewrite this as

1.	$\sim r \vee u$	
2.	$\sim u \vee \sim w$	
3.	$r \vee \sim w$	
4.	$\sim r \vee \sim w$	From 1 and 2 by Resolution
5.	$\sim w$	From 3 and 4 by Resolution.

§10 — Proof by Contradiction

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 8 (week 3). Notes: proof-techniques[166].

Problems

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

   For integers a and b, if $6a + 3b$ is odd, then b is odd.

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

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

Solutions

1. **For integers a and b, if $6a + 3b$ is odd, then b is odd.**

   Proof. Suppose the statement is false, that is, suppose that there exist integers a and b for which $6a + 3b$ is odd and b is even.

   Since b is even, $b = 2k$ for some integer k. Thus

   $$6a + 3b = 6a + 3(2k) = 6a + 6k = 2(3a + 3k).$$

   Since $a, k \in \mathbb{Z}$, $3a + 3k \in \mathbb{Z}$ so $6a + 3b$ is even. This contradicts our assumption that $6a + 3b$ is odd, so our assumption was incorrect and hence the original statement is true. □

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

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

   Proof. Suppose, for contradiction, that x and y are positive integers satisfying $x^2 - y^2 = 1$. Now, by factoring, we have

   $$1 = x^2 - y^2 = (x - y)(x + y).$$

   Since x and y are positive integers, we must have $x - y = 1$ and $x + y = 1$. This means $2x = 2$, so $x = 1$. But then we must have $y = 0$ which is not a positive integer; this is a contradiction. Therefore the original statement is true. □

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[167].

Problems

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

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

2. Prove the following statement:

   For any integer n, n^2 is odd if and only if n is odd.

   Use a direct proof for the reverse implication ($\Leftarrow$), and a proof by contraposition for the forward implication ($\Rightarrow$).

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

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

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

Solutions

1. **For all integers a and b, if $(ab)^2$ is odd then a is odd and b is odd.**

   Proof. We prove the contrapositive statement, which is:

   > For all integers a and b, if a is even or b is even, then $(ab)^2$ is even.

   Let a and b be integers and suppose a is even or b is even. Without loss of generality, suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ is even, and therefore $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, we know $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even by definition. □

2. **For any integer n, n^2 is odd if and only if n is odd.**

   Proof. To prove this "if and only if" statement, we must prove each of the following two statements:

   > ($\Leftarrow$) For any integer n, if n is odd, then n^2 is odd. ($\Rightarrow$) For any integer n, if n^2 is odd, then n is odd.

   ($\Leftarrow$) Let n be an integer and suppose n is odd. Then $n = 2k+1$ for some $k \in \mathbb{Z}$. Hence $n^2 = (2k+1)^2 = 2(2k^2+2k)+1$. Since $k \in \mathbb{Z}$, we have $2k^2+2k \in \mathbb{Z}$ and hence n^2 is odd by definition.

   ($\Rightarrow$) The contrapositive is: for any integer n, if n is even, then n^2 is even. Let n be an integer and suppose n is even. Then $n = 2k$ for some $k \in \mathbb{Z}$. Hence $n^2 = 4k^2 = 2(2k^2)$. Since $k \in \mathbb{Z}$, we have $2k^2 \in \mathbb{Z}$, so n^2 is even by definition.

   Therefore, for all integers n, n^2 is odd if and only if n is odd. □

3. **For all integers x and y, if $x^2(y^2-2y)$ is odd then x and y are odd.**

   Proof. We will prove the contrapositive statement, which is:

   > For all integers x and y, if x is even or y is even, then $x^2(y^2-2y)$ is even.

   Let $x, y \in \mathbb{Z}$ and suppose x or y is even. We consider the cases of x even or y even individually.

   Case 1. Suppose x is even. Then $x = 2k$ for some $k \in \mathbb{Z}$. Hence

   $$x^2(y^2-2y) = (2k)^2(y^2-2y) = 2(2k^2)(y^2-2y).$$

   Since $k, y \in \mathbb{Z}$, we have $(2k^2)(y^2-2y) \in \mathbb{Z}$, and hence $x^2(y^2-2y)$ is even, by definition.

Case 2. Suppose y is even. Then $y = 2\ell$ for some $\ell \in \mathbb{Z}$. Hence

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

Since $x, \ell \in \mathbb{Z}$, we have $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$ and thus $x^2(y^2 - 2y)$ is even, by definition. □

§12 — Rational Numbers

Epp 4th ed. pp. 163–170 · 5th ed. (metric) pp. 183–190. Lecture 9 (week 3). Notes: rational-and-irrational-numbers[168].

Problems

1. Prove the following statement:

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

2. Prove the following statement:

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

3. Prove the following statement:

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

4. Recall that $\sqrt{2}$ is irrational. Consider the statement

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

   (a) Write down the negation of the statement.

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

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

Solutions

1. **For real numbers m and n, if m is irrational and n is rational, then $m-n$ is irrational.**

   Proof. Let m and n be real numbers and suppose (for a contradiction) that m is an irrational number and n is rational, but $m-n$ is rational. Since n is rational, we have $n=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $m-n$ is rational, we have $m-n=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

   Notice that $m=(m-n)+n$. Hence

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

   Since $a,b,c,d\in\mathbb{Z}$ we have $bc+ad\in\mathbb{Z}$ and $bd\in\mathbb{Z}$. Further, since $b\neq 0$ and $d\neq 0$, we have $bd\neq 0$. Thus, by definition, m is rational. But this contradicts the assumption that m is irrational. □

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

   Proof. We prove the contrapositive statement: for a real number r, if r is rational, then $2r^2-3r$ is rational.

   Let r be a real number and suppose $r\in\mathbb{Q}$. Then $r=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. So

   $$2r^2-3r=2\left(\frac{a}{b}\right)^2-3\left(\frac{a}{b}\right)=\frac{2a^2-3ab}{b^2}.$$

   Since $a,b\in\mathbb{Z}$, we have $2a^2-3ab\in\mathbb{Z}$ and $b^2\in\mathbb{Z}$. Further, $b^2\neq 0$ because $b\neq 0$. This means $2r^2-3r$ is rational, by definition. □

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

   Proof. Suppose, for a contradiction, that the statement is false. Then there exist real numbers r, s and n such that r is an irrational number, s is rational, n is a positive integer, but $n(r-s)$ is rational. Since s is rational, $s=\frac{a}{b}$ for some $a,b\in\mathbb{Z}$ where $b\neq 0$. Since $n(r-s)$ is rational, we have $n(r-s)=\frac{c}{d}$ for some $c,d\in\mathbb{Z}$ where $d\neq 0$.

Now,

$$\begin{aligned} r - s &= n(r-s)\left(\frac{1}{n}\right) \quad \text{noting that } n \neq 0 \\ r - s &= \frac{c}{d} \cdot \frac{1}{n} \\ r &= s + \frac{c}{d} \cdot \frac{1}{n} \\ &= \frac{a}{b} + \frac{c}{dn} \\ &= \frac{adn + bc}{bdn} \end{aligned}$$

Since $a, b, c, d \in \mathbb{Z}$, we have $adn + bc \in \mathbb{Z}$ and $bdn \in \mathbb{Z}$. Further, since $b \neq 0$, $d \neq 0$ and $n \neq 0$, we have $bdn \neq 0$. This means r is rational, by definition, which is a contradiction. □

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

   (a) **Negation:** There exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

   (b)

   Proof. Suppose, for a contradiction, that the original statement is false. Then there exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$. Since r is rational, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and since $r \neq 0$, we have $a \neq 0$. Since we have assumed $r\sqrt{2}$ is rational, $r\sqrt{2} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Now

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \left(r\sqrt{2}\right)\left(\frac{1}{r}\right) = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad}.$$

   Since $a, b, c, d \in \mathbb{Z}$, we know $bc \in \mathbb{Z}$ and $ad \in \mathbb{Z}$. Further, since $a \neq 0$ and $d \neq 0$, we have $ad \neq 0$. Thus, by definition, $\sqrt{2}$ is rational. However, this is a contradiction, as $\sqrt{2}$ is irrational. Thus, the original statement is true. □

§13 — Divisibility

Epp 4th ed. pp. 170–179 · 5th ed. (metric) pp. 190–199. Lecture 10 (week 4). Notes: divisibility-and-factorisation[169].

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

Problems

1. Find the unique factorisation (in standard form) of the integer 27 720.
2. Prove or disprove the statement: for any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.
3. Prove the following statements.
   (a) If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.
   (b) The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.
4. Use proof by contradiction to prove this statement:

$$\text{For all integers } c, d \text{ and } e, \text{ if } c \mid d \text{ and } c \nmid e, \text{ then } c \nmid (d+e).$$

Solutions

1. By repeated division, we have $27\,720 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.
2. **For any integers m, n, and q, if $m \mid n$ and $n \mid q$ then $m^2 \mid nq$.** The statement is **true**, and we will prove it.

   Proof. Let m, n, and q be non-zero integers. Assume $m \mid n$ and $n \mid q$. Then, by definition, there exist integers a, b such that

   $$n = ma \quad \text{and} \quad q = nb.$$

   Then observe

   $$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2b).$$

   Since $a^2b \in \mathbb{Z}$, we conclude that $m^2 \mid nq$. □
3. (a) **If k is any even integer and m is any odd integer, then $(k+2)^2-(m-3)^2$ is divisible by 4.**

   Proof. Let k be even and m be odd. Then $k = 2a$ and $m = 2b+1$ for some $a, b \in \mathbb{Z}$. Hence

   $$(k+2)^2 = (2a+2)^2 = 4(a+1)^2 \quad \text{and} \quad (m-3)^2 = (2b-2)^2 = 4(b-1)^2.$$

   Therefore

   $$(k+2)^2-(m-3)^2 = 4\big[(a+1)^2-(b-1)^2\big].$$

   Since $a, b \in \mathbb{Z}$ we have $(a+1)^2-(b-1)^2 \in \mathbb{Z}$ so $4 \mid \big[(k+2)^2-(m-3)^2\big]$. □

(b) **The difference between the cube of two consecutive integers leaves the remainder 1 when it is divided by 6.**

Proof. Let n and $n+1$ be two consecutive integers. The difference between their cubes is

$$(n+1)^3 - n^3 = 3n^2 + 3n + 1 = 3n(n+1) + 1.$$

Now whether n is odd or even (so whatever integer n is), one of n, $n+1$ will be odd and the other one will be even. Thus the product $n(n+1)$ is even.

Since $n(n+1)$ is even, write $n(n+1) = 2t$ for some $t \in \mathbb{Z}$. Then

$$(n+1)^3 - n^3 = 3(2t) + 1 = 6t + 1 \equiv 1 \pmod 6.$$

Hence the remainder is 1 upon division by 6. □

4. **For all integers c, d and e, if $c \mid d$ and $c \nmid e$, then $c \nmid (d+e)$.**

Proof. Suppose for a contradiction that the statement is false. Then there exist integers c, d and e such that $c \mid d$ and $c \nmid e$ and $c \mid (d+e)$.

Now $c \mid d$ means that $d = cx$ for some integer x. And $c \mid (d+e)$ means that $d + e = cy$ for some integer y.

Hence $d + e = cx + e = cy$, so $e = cy - cx = c(y - x)$, and we have $y - x \in \mathbb{Z}$, because x and y are both integers. Thus $c \mid e$, a contradiction. So the original statement is true. □

§14 — Modular Arithmetic

Epp 4th ed. pp. 482–485 · 5th ed. (metric) pp. 528–531. Lecture 11 (week 4). Notes: modular-arithmetic[170].

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 $58 \bmod 11$.

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

(b) Find integers q and r, with $0 \leqslant r < d$ and $n = dq + r$, in the case that $n = -95$ and $d = 11$.

3. (a) An integer n, when divided by 7, leaves remainder 4. What is the remainder (between 0 and 6 inclusive) when $3n$ is divided by 7?

   (b) When the integer m is divided by 11, the remainder 9 is left. What remainder is left when $4m$ is divided by 22?

4. Prove or disprove the following statements.

   (a) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

   (b) For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.

Solutions

1. **If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.**

   Proof. Fix $y \in \mathbb{Z}$. By the division algorithm, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

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

   Let us compute the possible values for r^2 mod 5:

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

   Thus $y^2 \equiv 0, 1$, or $4 \pmod 5$, and never 2 or 3. □

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

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

   (b) We want $-95 = 11q + r$ with $0 \leq r < 11$. Taking $q = -9$ gives

   $$11(-9) = -99 \quad \Rightarrow \quad -95 = -99 + 4 = 11(-9) + 4,$$

   so $q = -9$ and $r = 4$.

3. (a) If n leaves remainder 4 upon division by 7, then $n = 7k + 4$ for some integer k. Hence

$$3n = 21k + 12 = 7(3k + 1) + 5,$$

so the remainder when $3n$ is divided by 7 is **5**. (The source PDF prints this step as $7(3k) + 5$, which equals $21k + 5$, not $21k + 12$ — the quotient is $3k + 1$, as above. The answer of 5 is unaffected.)

(b) If m leaves remainder 9 upon division by 11, then $m = 11k + 9$ for some integer k. Then

$$4m = 44k + 36 = 22(2k + 1) + 14,$$

so the remainder when $4m$ is divided by 22 is **14**.

4. (a) **For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** The statement is **false**. For a counterexample, take $x = \frac{3}{2}$. Then

$$\lfloor x^2 \rfloor = \left\lfloor \frac{9}{4} \right\rfloor = 2 \quad \text{but} \quad \lfloor x \rfloor^2 = \left\lfloor \frac{3}{2} \right\rfloor^2 = 1^2 = 1.$$

(b) **For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.** The statement is **true**.

Proof. Let n be an odd integer, so $n = 2k + 1$ for some integer k. Then

$$\frac{n^2}{4} = \frac{(2k+1)^2}{4} = \frac{4k^2 + 4k + 1}{4} = k(k+1) + \frac{1}{4},$$

so $\left\lfloor \frac{n^2}{4} \right\rfloor = k(k+1)$. Moreover, notice

$$\left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right) = \left(\frac{2k}{2}\right)\left(\frac{2k+2}{2}\right) = k(k+1).$$

Hence $\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right)$ for all odd integers n. □

§15 — The Euclidean Algorithm

Epp 4th ed. pp. 220–224 · 5th ed. (metric) pp. 250–254. Lecture 12 (week 4). Notes: gcd-lcm-and-euclidean-algorithm[171].

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

Problems

1. Use the Euclidean Algorithm to determine $\gcd(14, 3003)$.
2. Compute
   (a) $\operatorname{lcm}(12, 18)$
   (b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2)$
   (c) $\operatorname{lcm}(2800, 6125)$
3. Prove that for all positive integers a and b, we have

$$\gcd(a, b) = \operatorname{lcm}(a, b) \iff a = b.$$

4. Prove that for all positive integers a and b, we have

$$a \mid b \iff \operatorname{lcm}(a, b) = b.$$

5. (a) Use the Euclidean algorithm to determine $\gcd(931, 301)$. Show your working.
   (b) Write down the unique prime factorisation of 931 in standard form.
   (c) How many positive divisors does 931 have? (Hint: use part (b).)
6. (a) Using the Euclidean algorithm, compute $\gcd(116, 88)$. Show your working.
   (b) Using your answer to part (a), compute $\operatorname{lcm}(116, 88)$.

Solutions

1. We apply the Euclidean Algorithm:

$$3003 = 14 \cdot 214 + 7, \qquad 14 = 7 \cdot 2 + 0.$$

   Hence $\gcd(14, 3003) = 7$.

2. (a) We factor $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$ so $\operatorname{lcm}(12, 18) = 2^2 \cdot 3^2 = 36$.
   (b) Using the maximum exponents of each prime, we have

$$\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

   (c) We factor $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$. Thus

$$\operatorname{lcm}(2800, 6125) = 2^4 \cdot 5^3 \cdot 7^2 = 98000.$$

3. **For all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.**

   Proof. Let a and b be positive integers.

   ($\Longleftarrow$) It is clear that if $a = b$ then $\gcd(a, b) = \operatorname{lcm}(a, b)$.

   ($\Longrightarrow$) Assume $\gcd(a, b) = \operatorname{lcm}(a, b)$. Denoting $g = \gcd(a, b)$, we have $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$.

   Now notice gm and gn have no common prime factors beyond those in g, so the least common multiple uses all primes from both m and n. Therefore

   $$\operatorname{lcm}(a, b) = gmn.$$

   Now, we have $g = gmn$. Therefore $mn = 1$, and so $m = n = 1$. This lets us conclude $a = b$. □

4. **For all positive integers a and b, $a \mid b$ if and only if $\operatorname{lcm}(a, b) = b$.**

   Proof. Let us denote $g = \gcd(a, b)$ so that $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$. As explained in the previous question, we have

   $$\operatorname{lcm}(a, b) = gmn.$$

   ($\Longrightarrow$) If $a \mid b$, then $gm \mid gn$, hence $m \mid n$. Since $\gcd(m, n) = 1$, we conclude $m = 1$. Therefore $\operatorname{lcm}(a, b) = gmn = gn = b$.

   ($\Longleftarrow$) If $\operatorname{lcm}(a, b) = b$, then $gmn = gn$ which means $m = 1$. Therefore $a = gm = g$ and so $a \mid b$. □

5. (a) Using the Euclidean Algorithm:

   $$\begin{aligned} 931 &= 301 \cdot 3 + 28 \\ 301 &= 28 \cdot 10 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

   Hence $\gcd(931, 301) = 7$.

   (b) Since $\gcd(931, 301) = 7$, we know $7 \mid 931$, and we have $931 = 7 \cdot 133$. The number 133 has prime factorisation $7 \cdot 19$. Therefore the unique prime factorisation of 931 is $7^2 \cdot 19$.

(c) We have $931 = 7^2 \cdot 19^1$ from part (b). Any divisor of 931 must have a prime factorisation of the form $7^a \cdot 19^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. Thus the number of positive divisors is

$$(2 + 1)(1 + 1) = 6.$$

(There are 3 choices for the exponent a and 2 choices for the exponent b.)

6. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 116 &= 88 \cdot 1 + 28 \\ 88 &= 28 \cdot 3 + 4 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Hence $\gcd(116, 88) = 4$.

(b) Using $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{Z}^+$,

$$\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{\gcd(116, 88)} = \frac{116 \cdot 88}{4} = 116 \cdot 22 = 2552.$$

Application — Trace Tables for Algorithms

Not assessable for MATH1061. For reference, see S. Epp, Discrete Mathematics with Applications, *Section 4.8 (4th edition) or Section 4.10 (5th edition), Brooks/Cole, Belmont, CA.*

The following pseudo-code describes the **Division Algorithm**, with annotations to explain what each step is doing.

Input: a (a non-negative integer), d (a positive integer). This algorithm will take two inputs, a and d, and will find the quotient $a \operatorname{div} d$ and the remainder $a \bmod d$.

Algorithm body:

```
r := a          -- defining our variables
q := 0
                -- starting with a, repeatedly subtract lots of d until we reach
                -- a number less than d; each round adds 1 to the quotient count
while r >= d,
    r := r - d
    q := q + 1
end while
```

Output: q, r. Once we have obtained a number less than d, we are finished. The output q is the quotient ($a \operatorname{div} d$) and the output r is the remainder ($a \bmod d$).

The following pseudo-code describes the **Euclidean Algorithm**, with annotations to explain what each step is doing.

Input: A, B (integers with $A > B \geq 0$).

Algorithm body:

```
a := A          -- defining our variables
b := B
r := B
                -- if b /= 0, compute a mod b (call the algorithm above for this
                -- step) and set r to be this value; replace a with b and b with r
                -- and repeat until b = 0
while b /= 0,
    r := a mod b
    a := b
    b := r
end while
gcd := a
```

Output: gcd (a positive integer).

A **trace table** keeps track of the value of each variable at each step of an algorithm. For example, the trace table for the Division Algorithm with input variables $a = 19$ and $d = 4$ is:

Variable / iteration	0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

Output: $q = 4$, $r = 3$.

Application problems

1. Construct a trace table to trace the action of the Division Algorithm for the following inputs.

   (i) $a = 26$, $d = 7$

(ii) $a = 15$, $d = 6$

2. Construct a trace table to trace the action of the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$.

Application solutions

1. (i) Trace table for the Division Algorithm with $a = 26$, $d = 7$:

Variable / iteration	0	1	2	3
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

Output: $q = 3$, $r = 5$.

(ii) Trace table for the Division Algorithm with $a = 15$, $d = 6$:

Variable / iteration	0	1	2
a	15		
d	6		
r	15	9	3
q	0	1	2

Output: $q = 2$, $r = 3$.

2. Trace table for the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$:

Variable / iteration	0	1	2	3	4	5
A	1001					
B	871					
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Output: gcd = 13.

§16 — Sequences

Epp 4th ed. pp. 227–244 · 5th ed. (metric) pp. 258–275. Lecture 13 (week 5).

Problems

1. Write down the first four terms in the sequence defined by $a_k = \dfrac{k}{10+k}$ for $k = 1, 2, \ldots$.
2. Consider the sequences $a_k = 2k+1$ and $b_k = (k-1)^3 + k + 2$ where $k = 0, 1, 2, \ldots$. Show that the first three terms of these sequences are identical, but that their fourth terms differ.
3. (a) Find an explicit formula for a sequence c_n whose first six terms are $-1, 1, -1, 1, -1, 1$.
   (b) Find an explicit formula for a sequence d_n whose first six terms are $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$.
4. (a) Write $(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)$ in summation notation.
   (b) Evaluate $\displaystyle\prod_{i=1}^{5}(-1)^i \cdot i$.
   (c) Write $(y-1)(y^2-2)(y^3-3)(y^4-4)$ in product notation.
   (d) Evaluate $\displaystyle\sum_{j=1}^{n}(-1)^j\frac{1}{2^j}$ when $n = 5$.

Solutions

1. We have

$$a_1 = \frac{1}{11}, \qquad a_2 = \frac{2}{12} = \frac{1}{6}, \qquad a_3 = \frac{3}{13}, \qquad a_4 = \frac{4}{14} = \frac{2}{7}.$$

2. We compute

$$a_0 = 1, \quad a_1 = 3, \quad a_2 = 5, \quad a_3 = 7;$$

$$b_0 = (-1)^3+0+2 = 1, \quad b_1 = 0^3+1+2 = 3, \quad b_2 = 1^3+2+2 = 5, \quad b_3 = 2^3+3+2 = 13.$$

Hence the first three terms agree ($a_0 = b_0$, $a_1 = b_1$ and $a_2 = b_2$), but the fourth terms differ ($a_3 = 7$ while $b_3 = 13$).

3. (a) One explicit formula is

$$c_n = (-1)^n \qquad n = 1, 2, 3, ...$$

(b) The denominators are square numbers, so an explicit formula is

$$d_n = \frac{n}{(n+1)^2} \qquad n = 1, 2, 3, ...$$

4. (a) We have

$$(x^2 - 1) + (2x^3 - 1) + (3x^4 - 1) + (4x^5 - 1) + (5x^6 - 1) = \sum_{k=1}^{5} \left(kx^{k+1} - 1\right).$$

(b) We have

$$\prod_{i=1}^{5} (-1)^i \cdot i = \left(\prod_{i=1}^{5} (-1)^i\right) \left(\prod_{i=1}^{5} i\right) = (-1)^{1+2+3+4+5} \cdot 5! = (-1)^{15} \cdot 120 = -120.$$

(c) We have

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} \left(y^k - k\right).$$

(d) When $n = 5$, we have

$$\sum_{j=1}^{5} (-1)^j \frac{1}{2^j} = -\frac{1}{2} + \frac{1}{4} - \frac{1}{8} + \frac{1}{16} - \frac{1}{32} = -\frac{11}{32}.$$

§17 — Mathematical Induction

Epp 4th ed. pp. 244–268 · 5th ed. (metric) pp. 275–301. Lecture 13 (week 5).

Problems

1. Use mathematical induction to prove the following statements.

   (a) For every positive integer n, $n(n+1)$ is even.

   (b) For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.

   (c) For all integers $n \geq 7$, $3^n < n!$.

   (d) For each integer $n \geq 1$,

   $$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

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

Solutions

1. (a) **For every positive integer n, $n(n+1)$ is even.**

   Proof. Let $P(n)$ be the predicate "$n(n+1)$ is even".

   Basis: when $n = 1$, $n(n+1) = 2$ which is even, so $P(1)$ is true.

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

   Inductive hypothesis: suppose that for some integer $k \geq 1$, $P(k)$ is true. Thus $k(k+1) = 2a$ for some integer a.

   Now consider $n = k + 1$. Then

   $$(k+1)(k+2) = k(k+1) + 2(k+1) = 2a + 2(k+1) = 2(a+k+1).$$

   Since a and k are integers, $a + k + 1$ is an integer, so $(k+1)(k+2)$ is even and $P(k+1)$ is true.

   Thus, by the principle of mathematical induction, $n(n+1)$ is even for every positive integer n. □

   (b) **For every integer $n \geq 2$, $n^3 - n$ is a multiple of 6.**

Proof. Let $P(n)$ be the predicate $6 \mid (n^3 - n)$.

Basis: when $n = 2$, $n^3 - n = 8 - 2 = 6$. Since $6 \mid 6$, $P(2)$ is true.

(The inductive step is to show that for all integers $k \geq 2$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: suppose that for some integer $k \geq 2$, $P(k)$ is true. Thus $k^3 - k = 6a$ for some integer a.

Now consider $n = k + 1$. Then

$$(k+1)^3-(k+1) = k^3+3k^2+3k+1-k-1 = k^3-k+3k^2+3k = 6a+3k(k+1).$$

For the integer k, $k(k+1)$ is even from part (a), so let $k(k+1) = 2b$ for some integer b. Hence $(k+1)^3 - (k+1) = 6a + 3(2b) = 6(a+b)$. Thus $6 \mid ((k+1)^3 - (k+1))$ and so $P(k+1)$ is true.

Thus, by the principle of mathematical induction, $n^3 - n$ is a multiple of 6 for each integer $n \geq 2$. □

(c) **For all integers $n \geq 7$, $3^n < n!$.**

Proof. Let $P(n)$ be the predicate $3^n < n!$.

Basis: $P(7)$ is the statement $3^7 < 7!$. The left-hand side is $3^7 = 2187$ and the right-hand side is $7! = 5040$, so $P(7)$ holds.

(The inductive step is to show that for all integers $k \geq 7$, $P(k)$ implies $P(k+1)$.)

Inductive hypothesis: let $k \geq 7$ be an integer and assume that $P(k)$ is true; that is $3^k < k!$. We will now show that $P(k+1)$ holds, so we will show $3^{k+1} < (k+1)!$.

Taking the right-hand side, we have

$$\begin{aligned}(k+1)! &= (k+1) \cdot k! \\ &> (k+1) \cdot 3^k && \text{by the inductive hypothesis} \\ &> 3 \cdot 3^k && \text{since } k \geq 7 \\ &= 3^{k+1}\end{aligned}$$

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

Thus by the principle of mathematical induction, for all integers $n \geq 7$, $3^n < n!$. □

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

Proof. Let $P(n)$ be the predicate

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Basis: consider $n = 1$. We have $\sum_{i=1}^{1} i^3 = 1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ so $P(1)$ is true.

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

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(k)$ is true. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

Now consider $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 && \text{(splitting off the last term)} \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 && \text{by the inductive hypothesis} \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{(k+1)^2}{4}(k^2 + 4(k+1)) \\
&= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\
&= \frac{(k+1)^2}{4}(k+2)^2
\end{aligned}$$

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

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for every integer $n \geq 1$. □

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

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

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

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

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

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

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

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

Thus, by the principle of mathematical induction, $1 + 4n \leq 5^n$ for every integer $n \geq 0$. □

§18 — Strong Induction and the Well Ordering Principle

Epp 4th ed. pp. 268–279 · 5th ed. (metric) pp. 301–314. Lecture 14 (week 5).

Problems

1. Consider the statement

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

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

   (b) Prove the statement using strong mathematical induction.

2. The Lucas sequence $a_1, a_2, a_3, ...$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Use strong mathematical induction to prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

3. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Use strong mathematical induction to prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.

Solutions

1. **For every integer $n \geq 2$, there exist integers $a, b \geq 0$ such that $n = 2a + 3b$.**

   (a)

Proof (using the well-ordering principle). Consider the set of counterexamples

$$S = \{\, n \in \mathbb{Z}^{\geq 2} : \text{there do not exist integers } a, b \geq 0 \text{ with } n = 2a + 3b \,\}.$$

If S is empty, we are done. Otherwise, by the well-ordering principle, S has a least element. Let us call it N.

Notice that $2 \notin S$ because $2 = 2 \cdot 1 + 3 \cdot 0$, and $3 \notin S$ because $3 = 2 \cdot 0 + 3 \cdot 1$. Also $4 \notin S$ because $4 = 2 \cdot 2 + 3 \cdot 0$. Hence $N \geq 5$. By minimality of N, we must have $N - 2 \notin S$. Therefore there exist integers $a, b \geq 0$ such that

$$N - 2 = 2a + 3b.$$

In other words, we have

$$N = 2(a + 1) + 3b.$$

This means $N \notin S$, contradicting the assumption that $N \in S$. Hence S is empty, and the statement holds for all $n \geq 2$. $\square$

(b)

Proof (using strong induction). Let $P(n)$ be the predicate: "there exist integers $a, b \geq 0$ such that $n = 2a + 3b$."

Basis: we have

$$2 = 2 \cdot 1 + 3 \cdot 0, \qquad 3 = 2 \cdot 0 + 3 \cdot 1, \qquad 4 = 2 \cdot 2 + 3 \cdot 0,$$

so $P(2)$, $P(3)$, $P(4)$ are true.

(The inductive step is to show that for every integer $k \geq 4$, if $P(2), P(3), \ldots, P(k)$ are all true then $P(k + 1)$ is true.)

Inductive hypothesis: suppose $k \geq 4$ is an integer and assume $P(m)$ is true for every integer $m = 2, 3, \ldots, k$.

Consider $n = k + 1$. Since $k \geq 4$, we have $k - 1 \geq 3$, so by the inductive hypothesis $P(k - 1)$ is true. Thus there exist $a, b \geq 0$ such that

$$k - 1 = 2a + 3b.$$

Adding 2 gives

$$k + 1 = 2(a + 1) + 3b,$$

so $P(k + 1)$ holds. $\square$

2. **The Lucas sequence** $a_1, a_2, a_3, \ldots$ is defined by $a_1 = 1$, $a_2 = 3$ and $a_k = a_{k-1} + a_{k-2}$ for all integers $k \geqslant 3$. Prove that $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all $n \in \mathbb{Z}^+$.

Proof. Let $P(n)$ be the predicate $a_n \leqslant \left(\frac{7}{4}\right)^n$.

Basis: when $n = 1$, $a_1 = 1 \leqslant \left(\frac{7}{4}\right)^1 = 1\frac{3}{4}$ is true, so $P(1)$ is true. When $n = 2$, $P(2)$ holds because $a_2 = 3 \leqslant \left(\frac{7}{4}\right)^2 = \frac{49}{16} = 3\frac{1}{16}$.

(The inductive step is to show that for every integer $k \geq 1$, if $P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and that $P(m)$ is true for all m with $1 \leq m \leq k$.

Now consider $P(k+1)$, which we want to prove holds. We have

$$\begin{aligned}
a_{k+1} &= a_k + a_{k-1} \\
&\leqslant \left(\frac{7}{4}\right)^k + \left(\frac{7}{4}\right)^{k-1} && \text{by the inductive hypothesis} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4} + 1\right) \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{11}{4}\right) \\
&\leqslant \left(\frac{7}{4}\right)^{k-1}\left(\frac{49}{16}\right) && \text{noting } \tfrac{11}{4} = \tfrac{44}{16} < \tfrac{49}{16} \\
&= \left(\frac{7}{4}\right)^{k-1}\left(\frac{7}{4}\right)^2 \\
&= \left(\frac{7}{4}\right)^{k+1}.
\end{aligned}$$

Hence $P(k+1)$ holds. Therefore, by the principle of strong mathematical induction, $a_n \leqslant \left(\frac{7}{4}\right)^n$ for all integers $n \geqslant 1$. □

3. **Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Prove $a_n := x^n + \frac{1}{x^n}$ is an integer for all $n \geq 0$.**

Proof. Suppose x is a real number and $x + \frac{1}{x}$ is an integer. Let $P(n)$ be the predicate "a_n is an integer."

Basis: $P(0)$ holds since $a_0 = x^0 + \frac{1}{x^0} = 2$. $P(1)$ holds since $a_1 = x + \frac{1}{x}$, which is an integer by assumption.

(The inductive step is to show that for every integer $k \geq 1$, if $P(0), P(1), \ldots, P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(m)$ holds for all integers $m = 0, 1, \ldots, k$.

We now aim to show that $P(k+1)$ is true. Notice that

$$\begin{aligned} a_1 a_k &= \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) \\ &= \left(x^{k+1} + \frac{1}{x^{k+1}}\right) + \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_{k+1} + a_{k-1}. \end{aligned}$$

Therefore $a_{k+1} = a_1 a_k - a_{k-1}$. By the inductive hypothesis, a_k and a_{k-1} are integers, and a_1 is an integer, so a_{k+1} is an integer. Hence $P(k+1)$ holds.

Therefore, by the principle of strong mathematical induction, a_n is an integer for all $n \geq 0$. □

§19 — Recursive Definitions

Epp 4th ed. pp. 290–304 · 5th ed. (metric) pp. 325–340. Lecture 15 (week 6).

Problems

1. Define the sequence $b_1 = 2$, $b_2 = 6$ and

$$b_k = b_{k-1} + b_{k-2} + \gcd(b_{k-1}, b_{k-2})$$

for all $k \geq 3$. Use strong induction to prove b_n is even for all $n \geq 1$.

2. A sequence is defined by $a_1 = 2$ and

$$a_k = k(a_{k-1} + k - 1)$$

for all integers $k \geq 2$. Use mathematical induction to prove a_n is even for all $n \geq 1$.

3. Recursively define the set S of binary strings as follows.

   (a) *(Base rule)* $1 \in S$.

   (b) *(Recursion rule)* If $s \in S$ then $0s \in S$ and $1s \in S$ (e.g. if $s = 1$ then $0s = 01$).

   (c) *(Restriction rule)* No other strings lie in S besides those given by the rules above.

   What are the strings contained in S arising from the first three applications of the recursive rule?

Solutions

1. *Proof.* Let $P(n)$ be the predicate "b_n is even".

   Base case. The base cases are $n = 1, 2$. We have $b_1 = 2$ and $b_2 = 6$ so $P(1)$ and $P(2)$ are true.

   Inductive hypothesis. Assume $P(m)$ is true for all integers m with $1 \leq m \leq k$, where $k \geq 2$ is an integer. That is, we assume $b_1, b_2, \ldots, b_k$ are all even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. b_{k+1} is even. Using the recursive definition, we have

   $$b_{k+1} = b_k + b_{k-1} + \gcd(b_k, b_{k-1}).$$

   By the inductive hypothesis, b_k and b_{k-1} are even, so $2 \mid b_k$ and $2 \mid b_{k-1}$, hence $2 \mid \gcd(b_k, b_{k-1})$ as well. Therefore each term on the right-hand side is even, so their sum b_{k+1} is even. Thus $P(k+1)$ holds.

   Therefore, b_n is even for all integers $n \geq 1$. □

2. *Proof.* Let $P(n)$ be the predicate "a_n is even".

   Base case. The base case is $n = 1$. We have $a_1 = 2$, which is even, so $P(1)$ is true.

   Inductive hypothesis. Assume $P(k)$ is true for some integer $k \geq 1$. That is, assume a_k is even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. a_{k+1} is even. By the recursive definition, we have

   $$a_{k+1} = (k+1)(a_k + (k+1) - 1) = (k+1)(a_k + k).$$

   Note that a_k is even by the inductive hypothesis. We split into cases:

   - If k is even, then $a_k + k$ is even, hence a_{k+1} is even.
   - If k is odd, then $k+1$ is even, hence a_{k+1} is even.

   In all cases, a_{k+1} is even, so $P(k+1)$ is true.

   Therefore, a_n is even for all integers $n \geq 1$. □

3. By the base rule, we only know $1 \in S$.

   First application of the recursive rule:

   $$01 \in S, \qquad 11 \in S.$$

   Second application of the recursive rule:

$$001 \in S, \quad 101 \in S, \quad 011 \in S, \quad 111 \in S.$$

Third application of the recursive rule:

$$0001 \in S, \quad 1001 \in S, \quad 0101 \in S, \quad 1101 \in S,$$
$$0011 \in S, \quad 1011 \in S, \quad 0111 \in S, \quad 1111 \in S.$$

§20 — Solving Recurrence Relations

Epp 4th ed. pp. 304–328 · 5th ed. (metric) pp. 340–364. Lecture 16 (week 6).

Problems

1. Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that

$$a_n = 5a_{n-1} - 6a_{n-2}$$

for all integers $n \geq 2$.

2. Let $\{b_n\}_{n\geq 0}$ be the sequence defined by

$$b_0 = 2, \qquad b_1 = 5, \qquad \text{and} \qquad b_k = 2b_{k-1} - b_{k-2} \text{ for each integer } k \geq 2.$$

   (a) Write down the values of $b_0, b_1, b_2, b_3, b_4, b_5$.

   (b) Based on your answers for part (a), guess an explicit formula for this sequence.

   (c) Prove that your guess from part (b) is correct.

3. Let T_n be a sequence defined by $T_1 = 1$ and

$$T_{n+1} = 1 + (T_1 \times T_2 \times T_3 \times \cdots \times T_n)$$

for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.

4. Consider the Fibonacci sequence defined recursively by

$$\begin{aligned} a_0 &= 0 \\ a_1 &= 1 \\ a_n &= a_{n-2} + a_{n-1} \qquad \text{for all integers } n \geq 2. \end{aligned}$$

Use strong mathematical induction to prove the explicit formula

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

for all integers $n \geq 0$, where $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. (You may use the fact that $\phi^2 = \phi + 1$ and $\psi^2 = \psi + 1$.)

Solutions

1. **Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$.**

Proof. For $n \geq 2$, we have $n - 2 \geq 0$ so all three terms a_n, a_{n-1} and a_{n-2} are defined in the given formula. Then,

$$\begin{aligned} 5a_{n-1} - 6a_{n-2} &= 5\left(2^{n-1} + 5 \cdot 3^{n-1}\right) - 6\left(2^{n-2} + 5 \cdot 3^{n-2}\right) \\ &= \left(5 \cdot 2^{n-1} - 6 \cdot 2^{n-2}\right) + \left(25 \cdot 3^{n-1} - 30 \cdot 3^{n-2}\right) \\ &= (10 - 6)2^{n-2} + (75 - 30)3^{n-2} \\ &= 4 \cdot 2^{n-2} + 45 \cdot 3^{n-2} \\ &= 2^n + 5 \cdot 3^n \\ &= a_n. \end{aligned}$$

Hence $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. □

2. (a)

$$\begin{aligned} b_0 &= 2 \\ b_1 &= 5 \\ b_2 &= 2(5) - 2 = 8 \\ b_3 &= 2(8) - 5 = 11 \\ b_4 &= 2(11) - 8 = 14 \\ b_5 &= 2(14) - 11 = 17 \end{aligned}$$

(b) Guess that $b_n = 3n + 2$ for each integer $n \geq 0$.

(c)

Proof. The guess gives $b_0 = 3(0) + 2 = 2$ and $b_1 = 3(1) + 2 = 5$ so it gives the correct initial conditions. Now we substitute the guess into the recurrence relation. The LHS of the recurrence relation is $b_k = 3k + 2$. The RHS of the recurrence relation is

$$\begin{aligned} 2b_{k-1} - b_{k-2} &= 2(3(k-1)+2) - (3(k-2)+2) \\ &= 2(3k-1) - (3k-4) \\ &= 6k - 2 - 3k + 4 \\ &= 3k + 2 \end{aligned}$$

So the guess also satisfies the recurrence relation. Thus the guess is correct. □

Alternative proof (by strong induction). Let $P(n)$ be the predicate $b_n = 3n + 2$.

Basis: $b_0 = 2$ from the recursive definition and $3(0) + 2 = 2$ so $P(0)$ is true. $b_1 = 5$ from the recursive definition and $3(1) + 2 = 5$ so $P(1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are true.

Now

$$\begin{aligned} b_{k+1} &= 2b_k - b_{k-1} && \text{by the rec. rel. since } k+1 \geq 2 \\ &= 2(3k+2) - (3(k-1)+2) && \text{since } P(k) \text{ and } P(k-1) \text{ are true} \\ &= 6k + 4 - (3k - 1) \\ &= 3k + 5 \\ &= 3(k+1) + 2 \end{aligned}$$

So $P(k+1)$ is true. Therefore, by the principle of (strong) mathematical induction, the guess is correct for this recursively defined sequence. □

3. **Let T_n be a sequence defined by $T_1 = 1$ and $T_{n+1} = 1 + (T_1 \times \cdots \times T_n)$ for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.**

Proof. We can prove this simply by applying the recursive formula twice, once for T_{n+1} and once for T_n:

$$\begin{aligned} T_{n+1} &= 1 + (T_1 \cdot T_2 \cdot T_3 \cdots T_n) && \text{by the recursive definition} \\ &= 1 + T_n \cdot (T_1 \cdot T_2 \cdot T_3 \cdots T_{n-1}) \\ &= 1 + T_n \cdot (T_n - 1) && \text{since } T_n = 1 + (T_1 \cdots T_{n-1}) \text{ by rec. def.} \\ &= 1 + (T_n)^2 - T_n \\ &= (T_n)^2 - T_n + 1. \end{aligned}$$

Note that both applications of the recursive definition are valid, since $n-1 \geq 1$. $\square$

4. **Fibonacci explicit formula.**

Proof. Let $P(n)$ be the predicate

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}.$$

Basis. The base cases are $n = 0, 1$, which are true because

$$\frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = a_0,$$

and

$$\frac{\phi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = a_1.$$

Inductive hypothesis. Now suppose that for some integer $m \geq 1$, we have that $P(i)$ is true for all $0 \leq i \leq m$. In particular, $P(m)$ and $P(m-1)$ are true, that is,

$$a_m = \frac{\phi^m - \psi^m}{\sqrt{5}} \qquad \text{and} \qquad a_{m-1} = \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}}.$$

We need to show that $P(m+1)$ is true. That is, we aim to show

$$a_{m+1} = \frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}}.$$

Starting with the right-hand side of $P(m+1)$, we have

$$\begin{aligned}
\frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}} &= \frac{\phi^2\phi^{m-1} - \psi^2\psi^{m-1}}{\sqrt{5}} \\
&= \frac{(\phi+1)\phi^{m-1} - (\psi+1)\psi^{m-1}}{\sqrt{5}} && \text{since } \phi^2 = \phi + 1 \text{ and } \psi^2 = \psi + 1 \\
&= \frac{(\phi^m + \phi^{m-1}) - (\psi^m + \psi^{m-1})}{\sqrt{5}} \\
&= \frac{\phi^m - \psi^m}{\sqrt{5}} + \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}} \\
&= a_m + a_{m-1} && \text{by the inductive hypothesis} \\
&= a_{m+1} && \text{by definition.}
\end{aligned}$$

Hence $P(m+1)$ is true. $\square$

§21 — Set Theory Definitions

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Define the sets

$$\begin{aligned} V &= \{x \in \mathbb{Z} \mid 2 \leqslant x \leqslant 11 \text{ and } x \text{ is odd}\}, \\ X &= \{x \in \mathbb{Z} \mid -1 \leqslant x \leqslant 4\}, \\ Y &= \{2, 3, 7, 9\}, \\ Z &= \{x \in \mathbb{Z} \mid x \neq 0\}. \end{aligned}$$

   Write down the following sets, listing their elements and using brackets as appropriate.

   (a) $V \cap X$. (b) $V \cup Y$. (c) $X \cap Z$.

   (b) $X \cap (Z - Y)$. (e) $(X \cup Y) \cap V$. (f) $X \cup (Y \cap V)$.

2. For each of the following sets, write down its elements and then state the size of the set; that is, find $|A|$, $|B|$, $|C|$ and $|D|$.

   (a) $A = \{x \in \mathbb{Z} \mid \exists\, i \in \mathbb{Z} \text{ such that } x = 1 + (-1)^i\}$.

   (b) $B = \{y \in \mathbb{Z} \mid -8 < y \leqslant -5\}$.

   (c) $C = \{s \in \mathbb{Z} \mid s^2 + 1 = 0\}$.

   (d) $D = \{t \in \mathbb{Z} \mid t^4 = 1\}$.

3. Define the sets $A = \{0, 1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ and $C = \{1, 2, 4, 5, 7\}$. List the elements of the set

$$R = ((A - B) \cap (A - C)) \cup (B \cap C \cap A).$$

4. Are the following statements true or false? Justify in one or two sentences.

   (a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{\emptyset\} \in \{\{\emptyset\}\}$

   (b) $\emptyset \subseteq \{x\}$ (e) $\emptyset \in \{x\}$

Solutions

1. (a) $V \cap X = \{3\}$

   (b) $V \cup Y = \{2, 3, 5, 7, 9, 11\}$

   (c) $X \cap Z = \{-1, 1, 2, 3, 4\}$

   (d) $X \cap (Z - Y) = \{-1, 1, 4\}$

   (e) $(X \cup Y) \cap V = \{3, 7, 9\}$

   (f) $X \cup (Y \cap V) = \{-1, 0, 1, 2, 3, 4, 7, 9\}$

2. (a) Note that $(-1)^i$ is either $+1$ or -1 (according as i is even or odd). So x is either $1 + 1$ or $1 - 1$, that is, 2 or 0. So $A = \{2, 0\}$ and $|A| = 2$.

   (b) $B = \{-7, -6, -5\}$, so $|B| = 3$.

   (c) If $s^2 + 1 = 0$, we have $s^2 = -1$, and there are no such real numbers s, let alone integers! So $C = \emptyset$ and $|C| = 0$.

   (d) $D = \{-1, 1\}$, since $t^4 = 1$ with $t \in \mathbb{Z}$ implies $t = \pm 1$. Hence $|D| = 2$.

3. We have $A - B = \{0, 1, 2\}$ and $A - C = \{0, 3\}$, so $(A - B) \cap (A - C) = \{0\}$. Also $B \cap C \cap A = \{4\}$. Thus $R = \{0\} \cup \{4\} = \{0, 4\}$.

4. (a) **True:** $\{x\}$ is the set whose only element is x, so $x \in \{x\}$.

   (b) **True:** every set is a subset of itself, so $\{x\} \subseteq \{x\}$.

   (c) **True:** $\{\{\emptyset\}\}$ has the single element $\{\emptyset\}$, so $\{\emptyset\} \in \{\{\emptyset\}\}$.

   (d) **True:** $\emptyset \subseteq S$ for every set S, in particular $\emptyset \subseteq \{x\}$.

   (e) **False** (in general): $\emptyset \in \{x\}$ would require $\emptyset = x$.

Application — Computer Representations of Sets

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 134–138.*

There are various ways to represent sets using a computer. One such method involves the use of binary strings.

If we fix a finite universal set U with an arbitrary ordering, for example $U = \{a_1, a_2, \ldots, a_n\}$, we can represent subsets of U using binary strings of length n. A 1 in the ith position of the string indicates that element a_i is in the subset and a 0 indicates it is not.

For example if $U = \{1, 2, 3\}$ then the string 000 represents the empty set, 101 represents the subset $\{1, 3\}$ and 111 represents the entire set U.

The set operations union and intersection can be computed at the level of binary strings by utilising the bitwise OR and AND operations. The union of two sets corresponds to the bitwise OR operation on the strings and the intersection corresponds to bitwise AND.

Application problems

1. Define the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   (a) Express each of the following subsets of U using binary strings:

   i. $\{3, 4, 5\}$

   ii. $\{1, 3, 6, 10\}$

   iii. $\{a \in U \mid a \text{ is prime}\}$.

   (b) Using the same U, find the set represented by the following strings:

   i. 1111001111

   ii. 0101111000

   iii. 1000000001

   (c) Use binary strings to compute the following set operations.

   i. $\{1, 3, 4, 6, 10\} \cap \{2, 3, 6, 9, 10\}$

   ii. $\{2, 4, 6, 8\} \cup \{3, 4, 5\}$

Application solutions

1. (a) i. 0011100000

   ii. 1010010001

   iii. 0110101000 — the primes in U are $2, 3, 5, 7$. (The source PDF prints 1010111000 here, which decodes to $\{1, 3, 5, 6, 7\}$ and is not the set of primes; the string above is the correct one.)

   (b) i. $\{1, 2, 3, 4, 7, 8, 9, 10\}$

   ii. $\{2, 4, 5, 6, 7\}$

   iii. $\{1, 10\}$

   (c) i. 1011010001 AND 0110010011 = 0010010001, so the intersection is $\{3, 6, 10\}$.

   ii. 0101010100 OR 0011100000 = 0111110100, so the union is $\{2, 3, 4, 5, 6, 8\}$.

§22 — More Definitions and Examples of Sets

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Let $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$. List the elements of the following sets.
   (a) $A \cap C$
   (b) $(A \cup C) - B$
   (c) $(A \times B) \cap (A \times C)$
   (d) $\mathcal{P}(B \cap C)$
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\}$
2. Are the following statements true or false?
   (a) $\mathbb{Q} \in \mathbb{R}$.
   (b) $\{1, 2\} \subseteq \mathbb{Z}$.
   (c) $\{-3, 0\} \subseteq \mathcal{P}(\mathbb{Z})$.
   (d) $\{(1, 2), (0, 1)\} \in \mathbb{Z} \times \mathbb{Z}$.
3. Let $X = \mathcal{P}(\emptyset)$ and $Y = \mathcal{P}(\mathcal{P}(\emptyset))$. List the elements of each of the following sets.
   (a) X (b) Y (c) $X \cap Y$ (d) $X \cup Y$
4. Define sets $S = \{3, 5\}$ and $T = \{2, 3, 7\}$. Are the following statements true or false?
   (a) $S \subseteq T$
   (b) $\emptyset \in \mathcal{P}(S)$
   (c) $\emptyset \in T$
   (d) $(3, 3, 3) \in S \times T$

Solutions

1. (a) $A \cap C = \emptyset$.
   (b) $(A \cup C) - B = \{1, 4\}$.
   (c) $(A \times B) \cap (A \times C) = \{(1, 3), (2, 3)\}$.
   (d) $\mathcal{P}(B \cap C) = \{\emptyset, \{3\}\}$.
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\} = \{\emptyset, \{2\}\}$.
2. (a) **False.** ($\mathbb{Q}$ is a *subset* of $\mathbb{R}$, not an element of it.)
   (b) **True.**
   (c) **False.** (The elements of $\mathcal{P}(\mathbb{Z})$ are sets of integers; -3 and 0 are integers, not sets.)
   (d) **False.** (It is a *subset* of $\mathbb{Z} \times \mathbb{Z}$, not an element — the elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs.)
3. (a) $X = \mathcal{P}(\emptyset) = \{\emptyset\}$.
   (b) $Y = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
   (c) $X \cap Y = \{\emptyset\}$.
   (d) $X \cup Y = \{\emptyset, \{\emptyset\}\}$.
4. (a) **False.** ($5 \in S$ but $5 \notin T$.)
   (b) **True.** (The empty set is an element of every power set.)
   (c) **False.** (T's elements are 2, 3 and 7.)
   (d) **False.** (The elements of $S \times T$ are ordered *pairs*, not triples.)

§23 — Properties of Sets

Epp 4th ed. pp. 352–366 · 5th ed. (metric) pp. 391–407. Lecture 18 (week 7).

Problems

1. (a) Use the element method to prove that for all sets A and B

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

   (b) Use the element method to prove that for all sets X, Y and Z,

$$(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset.$$

   (c) Use set identities to prove that for all sets A, B and C

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

2. Prove or disprove the following:

   (a) For all sets A and B, we have $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

   (b) For all sets A and B, we have $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.

   (c) There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

   (d) Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$.

3. Let A, B and C be sets. Prove that

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

Solutions

1. (a) **For all sets A and B, $A \cup (B - A) = A \cup B$.**

   Proof. First we show that $A \cup (B - A) \subseteq A \cup B$.

   Consider an arbitrary element $x \in A \cup (B - A)$. Then we know $x \in A$ or $x \in B - A$. This means $x \in A$, or $x \in B$ and $x \notin A$. If $x \in A$, then $x \in A \cup B$. Similarly if $x \in B - A$, then it must be in B and so $x \in A \cup B$. In either case, we have $x \in A \cup B$, thus $A \cup (B - A) \subseteq A \cup B$.

   Now we show that $A \cup B \subseteq A \cup (B - A)$.

   Let $x \in A \cup B$, then $x \in A$ or $x \in B$ or it is in both A and B. If $x \in A$, then $x \in A \cup (B - A)$. If $x \notin A$ then $x \in B$ since $x \in A \cup B$. So we have that $x \in B$ and $x \notin A$, hence $x \in B - A$ and thus $x \in A \cup (B - A)$. This proves that $A \cup B \subseteq A \cup (B - A)$, and together this proves that $A \cup B = A \cup (B - A)$. $\square$

(b) **For all sets X, Y and Z, $(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset$.**

Proof. Assume that $(X - Z) \cap (Y - Z) \cap (X - Y) \neq \emptyset$.

So let $x \in (X - Z) \cap (Y - Z) \cap (X - Y)$. Then, in particular, $x \in Y - Z$ and $x \in X - Y$. The former implies $x \in Y$, but the latter implies $x \notin Y$. No such x exists. Therefore the set is empty. □

(c) **For all sets A, B and C, $(A - B) - C = A - (B \cup C)$.**

Proof. Using $A - B = A \cap B^c$, $(S - T) = S \cap T^c$, and De Morgan's law, we have

$$(A-B)-C = (A\cap B^c)\cap C^c = A\cap(B^c\cap C^c) = A\cap(B\cup C)^c = A-(B\cup C). \qquad \square$$

2. (a) **For all sets A and B, $\mathcal{P}(A\cup B) = \mathcal{P}(A)\cup\mathcal{P}(B)$. False.** Counterexample: $A = \{1\}$, $B = \{2\}$. Then

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \neq \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}.$$

(b) **For all sets A and B, $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$. True.**

($\Longleftarrow$) If $A = B$ then clearly $\mathcal{P}(A) = \mathcal{P}(B)$.

($\Longrightarrow$) We next show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Suppose (for a contradiction) that $\mathcal{P}(A) = \mathcal{P}(B)$ but $A \neq B$. Then (without loss of generality), there exists an element x in A that is not in B. Therefore, there is an element $\{x\}$ in $\mathcal{P}(A)$ that is not in $\mathcal{P}(B)$. Therefore $\mathcal{P}(A) \neq \mathcal{P}(B)$ — a contradiction. Thus, for all sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$. □

(c) **There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. False.**

No such set exists. The power set of any set must contain the empty set — that is, $\emptyset \in \mathcal{P}(A)$, where A is any set. Also, the power set of any set of size n has cardinality 2^n. The power set above contains 7 elements, and there does not exist any integer n such that $2^n = 7$.

(d) **Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$. True.**

First note that if $A = \emptyset$ then $A \times B = A \times C = \emptyset$ and the statement is true. Also, if $B = \emptyset$ then $A \times B = \emptyset$ and $\emptyset \subseteq A \times C$ for any C, so the statement is true.

Suppose A, B and C are non-empty sets with $B \subseteq C$. Thus if $b \in B$, then $b \in C$. Consider any element $(a, b) \in A \times B$, where $a \in A$ and $b \in B$. Since

$b \in B$, $b \in C$. As such, $a \in A$ and $b \in C$ for all a or b, so $(a, b) \in A \times C$. Therefore $A \times B \subseteq A \times C$. □

3. **For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.**

   Proof Option 1. For any x, we have

   $$x \in A - (B \cup C) \iff x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge (x \notin B) \wedge (x \notin C).$$

   Also, we have

   $$x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff (x \in A \wedge x \notin B) \wedge x \notin C.$$

   The statements on the right-hand side are equivalent. Hence $A - (B \cup C) = (A - B) - C$. □

   Proof Option 2.

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

§24 — Functions Defined on General Sets

Epp 4th ed. pp. 383–396 · 5th ed. (metric) pp. 425–439. Lecture 18 (week 7).

Problems

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 1$.
   (a) What is the domain, codomain and range of f?
   (b) What is the image of $\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$ under f?
   (c) What is the preimage of $\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}$ under f?
2. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$ be sets. Define $f : X \to Y$ by the arrow diagram

   $$1 \mapsto v, \qquad 3 \mapsto s, \qquad 5 \mapsto v$$

   (the elements t and u of Y receive no arrows).

(a) Write the domain of f and the co-domain of f.

(b) Determine $f(1)$, $f(3)$, and $f(5)$.

(c) Determine the range of f.

(d) Is 3 an inverse image of s? Is 1 an inverse image of u?

(e) What is the inverse image of s? of u? of v?

(f) Represent f as a set of ordered pairs.

3. Let D be the set of all finite subsets of $\mathbb{Z}^+$. Consider the function $T : \mathbb{Z}^+ \to D$ defined by $T(n) := \{d \mid d \in \mathbb{Z}^+ \text{ and } d \text{ divides } n\}$. Find the following:

(a) $T(1)$ (b) $T(15)$ (c) $T(17)$ (d) $T(5)$ (e) $T(18)$ (f) $T(21)$

4. Let S be the set of all strings of a's and b's.

(a) Define the function $f : S \to \mathbb{Z}$ by

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s, & \text{if } s \text{ contains an } a, \\ 0, & \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

(b) Define the function $g : S \to S$ by

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

Solutions

1. (a) The domain is $\mathbb{R}$, the codomain is $\mathbb{R}$, and the range is $[-1, \infty)$.

(b) $f(\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}) = [-1, 3]$.

(c) $f^{-1}(\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} = [-2, -1] \cup [1, 2]$.

2. (a) The domain is $X = \{1, 3, 5\}$ and the codomain is $Y = \{s, t, u, v\}$.

(b) $f(1) = v$, $f(3) = s$, $f(5) = v$.

(c) $\text{range}(f) = \{s, v\}$.

(d) **Yes**, 3 is an inverse image of s. **No**, 1 is not an inverse image of u.

(e) $f^{-1}(s) = \{3\}$, $f^{-1}(u) = \emptyset$, $f^{-1}(v) = \{1, 5\}$.

(f) $f = \{(1, v), (3, s), (5, v)\}$.

3. (a) $T(1) = \{1\}$.

(b) $T(15) = \{1, 3, 5, 15\}$.

(c) $T(17) = \{1, 17\}$.

(d) $T(5) = \{1, 5\}$.

(e) $T(18) = \{1, 2, 3, 6, 9, 18\}$.

(f) $T(21) = \{1, 3, 7, 21\}$.

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

(b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, $\text{range}(g) = S$.

§25 — one-to-one, Onto, and Inverse Functions

Epp 4th ed. pp. 397–416 · 5th ed. (metric) pp. 439–461. Lecture 19 (week 7).

Problems

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \left\lfloor \dfrac{1 - 6n}{3} \right\rfloor$.

(a) Is f one-to-one?

(b) Is f onto?

(c) Is f bijective?

(d) Prove or disprove that for all $m, n \in \mathbb{Z}$, we have $f(mn) = f(m)f(n)$.

2. Define the set $A = \{0, 1, 2, 3, 4\}$ and the functions $f : A \to A$ and $g : A \to A$ by

$$f(a) = (a + 4)^2 \pmod 5, \qquad g(a) = (a^2 + 3a + 1) \pmod 5.$$

Is $f = g$?

3. Consider the function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f((m, n)) = 2^m 3^n$.

(a) Determine $f((3, 1))$.

(b) Determine the pre-image of $\{36\}$.

(c) Prove f is one-to-one.

4. Consider the function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x^2 \rfloor$.

   (a) What is the image $f([-1, 1])$?

   (b) What is the preimage $f^{-1}(\{1\})$?

   (c) Is f one-to-one?

   (d) Is f onto?

   (e) Is f bijective?

Solutions

1. First, we note that, for $n \in \mathbb{Z}$,

$$f(n) = \left\lfloor \frac{1 - 6n}{3} \right\rfloor = \left\lfloor -2n + \frac{1}{3} \right\rfloor = -2n$$

   since $-2n \in \mathbb{Z}$ and $\frac{1}{3} \in [0, 1)$.

   (a) **Yes.** If $f(m) = f(n)$ then $-2m = -2n$, hence $m = n$. Therefore f is one-to-one.

   (b) **No.** Since $f(n) = -2n$ we see that f never maps to any odd integer; for example, there is no integer w with $f(w) = 1$. Therefore f is not onto.

   (c) **No**, f is not a bijection. (It is injective but not surjective.)

   (d) This is **false**; take $m = n = 1$. Then $f(mn) = -2$ but $f(m)f(n) = 4$.

2. **Yes.** First note f and g have the same domain and codomain. This means we just need to show $f(a) = g(a)$ for all $a \in A$. Notice that we have

$$(a + 4)^2 = a^2 + 8a + 16 \equiv a^2 + 3a + 1 \pmod 5,$$

   so $f(a) = g(a)$ for all $a \in A$, and hence $f = g$.

3. (a) $f((3, 1)) = 2^3 3^1 = 24$.

   (b) $36 = 2^2 3^2$, so $f((m, n)) = 36$ if and only if $(m, n) = (2, 2)$. Hence $f^{-1}(\{36\}) = \{(2, 2)\}$.

   (c) If $f((m, n)) = f((m', n'))$, then $2^m 3^n = 2^{m'} 3^{n'}$, so $2^{m-m'} = 3^{n'-n}$. By unique prime factorisation, this forces $m - m' = 0$ and $n' - n = 0$. That is, $m = m'$ and $n = n'$, and hence $(m, n) = (m', n')$. So f is one-to-one.

4. (a) Note that if $x \in [-1, 1]$ then $x^2 \in [0, 1]$. This means we have $\lfloor x^2 \rfloor \in \{0, 1\}$. Both values occur because $\lfloor 0^2 \rfloor = 0$ and $\lfloor 1^2 \rfloor = 1$. Thus $f([-1, 1]) = \{0, 1\}$.

(b) $f^{-1}(\{1\}) = \{x \in \mathbb{R} : 1 \leq x^2 < 2\} = (-\sqrt{2}, -1] \cup [1, \sqrt{2})$.

(c) **No**, f is not one-to-one. For example, $f\left(\frac{1}{2}\right) = 0 = f\left(-\frac{1}{2}\right)$ but $\frac{1}{2} \neq -\frac{1}{2}$.

(d) **No**, f is not onto since $f(x) = \lfloor x^2 \rfloor \geq 0$ for all x. This means, for instance, that -1 is not in the image of f.

(e) **No**, f is not bijective.

§26 — Composition of Functions

Epp 4th ed. pp. 416–427 · 5th ed. (metric) pp. 461–472. Lecture 20 (week 7).

Problems

1. Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^3 - 1$ and $g(x) = x + 5$.

   (a) Determine the functions $(g \circ f)(x)$ and $(f \circ g)(x)$.

   (b) Is $g \circ f$ a bijection?

2. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(x) = 2\lfloor x + 1 \rfloor$.

   (a) What is the range of f?

   (b) Is f one-to-one?

   (c) Is f onto?

   (d) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = 2x - 1$. Determine the composition $(g \circ f)(x)$.

   (e) Calculate $(g \circ f)\left(-\frac{3}{4}\right)$.

   (f) What is the range of $g \circ f$?

3. Let f and g be functions. Prove or disprove the following statements:

   (a) If f and $f \circ g$ are one-to-one, then g is one-to-one.

   (b) If f and $f \circ g$ are onto, then g is onto.

Solutions

1. (a) We have

$$(g \circ f)(x) = g(x^3 - 1) = x^3 + 4$$

and

$$(f \circ g)(x) = f(x + 5) = (x + 5)^3 - 1 = x^3 + 15x^2 + 75x + 124.$$

(b) **No**, $g \circ f$ is not a bijection. The map $x \mapsto x^3 + 4$ is one-to-one on $\mathbb{Z}$, but it is not onto (e.g. 0 is not in its image since $x^3 = -4$ has no integer solution).

2. (a) The range is a subset of the even integers because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. If $2m$ is an even integer then $f(m - 1) = 2\lfloor m - 1 + 1 \rfloor = 2m$, so the range is the set of all even integers.

(b) **No**, f is not one-to-one. For example,

$$f(0) = 2\lfloor 0 + 1 \rfloor = 2\lfloor 1 \rfloor = 2 \times 1 = 2, \quad \text{and}$$
$$f\left(\tfrac{1}{2}\right) = 2\left\lfloor \tfrac{1}{2} + 1 \right\rfloor = 2\left\lfloor \tfrac{3}{2} \right\rfloor = 2 \times 1 = 2,$$

but $0 \neq \frac{1}{2}$.

(c) **No**, f is not onto since $\text{range}(f) \neq \mathbb{Z}$ (e.g. there is no $x \in \mathbb{Q}$ such that $f(x) = 1$ because 1 is odd).

(d) We have

$$(g \circ f)(x) = g(f(x)) = 2(2\lfloor x + 1 \rfloor) - 1 = 4\lfloor x + 1 \rfloor - 1.$$

(e) We have

$$(g \circ f)\left(-\frac{3}{4}\right) = 4 \cdot 0 - 1 = -1.$$

(f) The range is a subset of $\{4n - 1 \mid n \in \mathbb{Z}\}$ because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. This *is* the range because, given an integer $4n - 1$, we have $f(n - 1) = 4\lfloor n - 1 + 1 \rfloor - 1 = 4n - 1$. Note that you can also write the range as $\{n \in \mathbb{Z} \mid n \equiv -1 \pmod 4\}$ which is the same as $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 4\}$.

3. (a) The statement is **true**.

Proof. Suppose that f and $f \circ g$ are one-to-one functions. Suppose for a contradiction that g is not one-to-one. Thus there exist two distinct elements in the domain of g, say x_1 and x_2, for which $g(x_1) = g(x_2)$. Let $g(x_1) = y = g(x_2)$. Thus $f(g(x_1)) = f(y) = f(g(x_2))$, but $x_1 \neq x_2$, which contradicts the fact that $f \circ g$ is one-to-one. Therefore g must be one-to-one. □

(b) The statement is **false**.

Counterexample. Consider the functions $g : \{1\} \to \{2, 3\}$ defined by $g(1) = 2$, and $f : \{2, 3\} \to \{4\}$ defined by $f(2) = 4$ and $f(3) = 4$. Then f is onto, and $f \circ g$ is onto (since $f \circ g : \{1\} \to \{4\}$ and $f(g(1)) = 4$). However, g is not onto. □

§27 — Cardinalities

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 21 (week 8).

Problems

1. Let $A = \{-2, -1, 0, 1\}$ and $B = \{3, 4, 5, 6\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.
2. Prove that $|\{1, 2, 3\}| \leq |\mathbb{Z}|$ by providing an appropriate injective (one-to-one) function.
3. Consider the intervals

$$[6, 12] = \{x \in \mathbb{R} \mid 6 \leq x \leq 12\} \quad \text{and} \quad (6, 12) = \{x \in \mathbb{R} \mid 6 < x < 12\}.$$

   Prove that $|[6, 12]| \leq |(6, 12)|$ by providing an appropriate injective (one-to-one) function.
4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.

Solutions

1. Define the function $f : A \to B$ by

$$f(-2) = 3, \qquad f(-1) = 4, \qquad f(0) = 5, \qquad f(1) = 6.$$

   Then f is bijective, hence $|A| = |B|$.
2. Define the function $g : \{1, 2, 3\} \to \mathbb{Z}$ by $g(1) = 1$, $g(2) = 2$, and $g(3) = 3$. Then g is injective (one-to-one), so $|\{1, 2, 3\}| \leq |\mathbb{Z}|$.

3. Define $h : [6, 12] \to (6, 12)$ by

$$h(x) = \frac{x}{2} + 4.$$

For each $x \in [6, 12]$ we have

$$\begin{aligned} \frac{6}{2} + 4 \leq h(x) &\leq \frac{12}{2} + 4 \\ 7 \leq h(x) &\leq 10. \end{aligned}$$

Thus h is indeed a function from $[6, 12]$ to $(6, 12)$, and h has range $[7, 10] \subseteq (6, 12)$.

Suppose $x, y \in [6, 12]$ and $h(x) = h(y)$. Then $\frac{x}{2} + 4 = \frac{y}{2} + 4$, so $x = y$. Therefore h is injective (one-to-one).

Thus $|[6, 12]| \leq |(6, 12)|$.

4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$.

Consider the function $f : A \to B$ where $f(x) = 2x + 5$. Since $x \geq -1$, $f(x) = 2x + 5 \geq 2(-1) + 5 = 3$, and since $x \leq 1$, $f(x) = 2x + 5 \leq 2(1) + 5 = 7$. Also each value of x gives a unique value of $2x + 5$. Thus f is a function with the correct domain and codomain.

We now prove that f is one-to-one. Suppose that $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Thus $2x_1 + 5 = 2x_2 + 5$, and so $x_1 = x_2$. Thus f is one-to-one.

We now prove that f is onto. Suppose $y \in [3, 7]$. Let $x = \frac{y-5}{2}$. Since $y \leq 7$, we have $x \leq 1$ and since $y \geq 3$, we have $x \geq -1$. So $x \in [-1, 1]$. Furthermore $f(x) = f\left(\frac{y-5}{2}\right) = 2\left(\frac{y-5}{2}\right) + 5 = y - 5 + 5 = y$. Thus f is onto.

Hence f is a bijection and so $|A| = |B|$.

§28 — Countable and Uncountable Sets

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 22 (week 8).

Note that this content will not be assessed in MATH1061.

Problems

1. Determine whether each of the following sets is countable or uncountable.
   (a) $\{1, 2, \ldots, n\}$.
   (b) $\mathbb{Z} \times \mathbb{Z}$.
   (c) $\mathbb{Q} \times \mathbb{Q}$.
   (d) $\mathbb{Z} \times \mathbb{Z} \times \cdots$ (infinitely many copies of $\mathbb{Z}$).
2. (a) Is $|\mathbb{Z}| = |\mathbb{Q}|$?
   (b) Is $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$?
   (c) Is $|\mathbb{R}| = |\mathbb{Q} \times \mathbb{Q}|$?
3. (a) Show that the union of a countable number of countable sets is countable.
   (b) Show that the set of all finite binary strings is countable.
   (c) Use (a) to show that the set of all irrational numbers is uncountable.

Solutions

1. (a) The set is **countable** because the function $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ defined by $f(i) = i$ is injective.
   (b) The set $\mathbb{Z} \times \mathbb{Z}$ is **countable**. Define the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ by

$$f(a,b) = \begin{cases} 2^a 3^b, & a > 0,\ b > 0, \\ 5^{-a} 7^{-b}, & a < 0,\ b < 0, \\ 11^a 13^{-b}, & a > 0,\ b < 0, \\ 17^{-a} 19^b, & a < 0,\ b > 0, \\ 23^b, & a = 0,\ b > 0, \\ 29^a, & a > 0,\ b = 0, \\ 31^{-b}, & a = 0,\ b < 0, \\ 37^{-a}, & a < 0,\ b = 0, \\ 1, & (a,b) = (0,0). \end{cases}$$

   We claim f is injective. Suppose $f(a,b) = f(c,d)$. By unique prime factorisation, the set of primes dividing $f(a,b)$ and the set of primes dividing $f(c,d)$ must be equal. Hence (a,b) and (c,d) lie in the same case. Again, by unique prime factorisation, the corresponding exponents must agree, so $a = c$ and $b = d$. Therefore f is injective.

(c) The set $\mathbb{Q} \times \mathbb{Q}$ is **countable**. First define an injection $e : \mathbb{Z} \to \mathbb{N}$ by

$$e(z) = \begin{cases} 2z, & z \geq 0, \\ -2z - 1, & z < 0. \end{cases}$$

Next define an injection $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$c(m, n) = 2^m 3^n.$$

Write each rational in lowest terms with positive denominator: $x = \frac{p}{q}$, $y = \frac{r}{s}$ with $p, r \in \mathbb{Z}$ and $q, s \in \mathbb{N}$. Define $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$ by

$$F\left(\frac{p}{q}, \frac{r}{s}\right) = 2^{\,c(e(p),\, q)}\, 3^{\,c(e(r),\, s)}.$$

If $F\left(\frac{p}{q}, \frac{r}{s}\right) = F\left(\frac{p'}{q'}, \frac{r'}{s'}\right)$, then by unique prime factorisation we get $c(e(p), q) = c(e(p'), q')$ and $c(e(r), s) = c(e(r'), s')$. Since c is injective, we have $e(p) = e(p')$, $q = q'$, $e(r) = e(r')$, $s = s'$. Moreover, since e is injective, we have $p = p'$ and $r = r'$. Therefore $\frac{p}{q} = \frac{p'}{q'}$ and $\frac{r}{s} = \frac{r'}{s'}$, so F is injective.

(d) The set $\mathbb{Z} \times \mathbb{Z} \times ...$ is **not countable**. We will prove this by giving an injection $\mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$.

For each $x \in \mathbb{R}$, write $x = n + r$ with $n = \lfloor x \rfloor \in \mathbb{Z}$ and $r \in [0, 1)$. Choose the unique decimal expansion of r that does not end with an infinite tail of 9's. Write this decimal expansion as

$$r = 0.d_1 d_2 d_3 \cdots, \qquad d_k \in \{0, 1, \ldots, 9\}.$$

Then define the function $\iota : \mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$ by

$$\iota(x) = (n, d_1, d_2, d_3, \ldots) \in \mathbb{Z} \times \mathbb{Z} \times \cdots.$$

This is injective; if $\iota(x) = \iota(y)$ then the decimals of x and y are equal, so $x = y$.

2. (a) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Q}$ are countable and infinite.

   (b) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are countable and infinite.

   (c) **No.** $\mathbb{Q} \times \mathbb{Q}$ is countable, while $\mathbb{R}$ is uncountable.

3. (a) Let $A_1, A_2, A_3, ...$ be countable. Then for each n we can list A_n as

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

Now list the union by going along diagonals:

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

Every element of every A_n appears somewhere in this list, so $\bigcup_{n=1}^{\infty} A_n$ can be listed in a sequence. Hence $\bigcup_{n=1}^{\infty} A_n$ is countable.

(b) Let B_n be the set of all binary strings of length n. Each B_n is finite (there are 2^n such strings), hence countable. Every finite binary string has some length, so

$$B = \{\text{all finite binary strings}\} = \bigcup_{n=0}^{\infty} B_n.$$

By (a), a countable union of countable sets is countable, so B is countable.

(c) Suppose, for contradiction, that the set of irrationals $\mathbb{R} \setminus \mathbb{Q}$ were countable. We already know $\mathbb{Q}$ is countable. Then by part (a),

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

would be a union of two countable sets, hence countable. But $\mathbb{R}$ is uncountable. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

Application — Computability of Functions

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 170–177.*

An important application of the topic of countability to computer science is examining the **computability** of functions. In computer science, a function is **computable** if there is a computer program in some programming language that can find the values of the function. If there is no such program, we say the function is **uncomputable**.

Application problems

1. (a) Show the set of all computer programs in any given computer language is countable.

   Hint: a computer program written in a programming language can be thought of as a string of symbols from a finite alphabet.

   (b) Let T be the set of all functions from $\mathbb{Z}^+$ to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.

   Hint: start by finding an injection between the interval $(0, 1)$ *and a subset of* T*.*

   (c) Hence show that there are uncomputable functions.

Application solutions

1. (a) Given a computer language with a finite alphabet A, we let P be the set of all computer programs in the language. If P is finite, then it is countable and we are done, so assume P is infinite.

   Now we use the fact that we can think of each computer program as a series of strings made using the alphabet A. Consider all strings of length m made from alphabet A, and denote this set by A_m. It is easy to show that there are $|A|^m$ distinct strings of this type, and since A is finite, $|A|^m$ is also finite. Now P is a subset of $\bigcup_{i=1}^{\infty} A_m$. Since the union of a countable number of countable sets is also countable (see Question 3(a) from earlier in this section) it follows that $\bigcup_{i=1}^{\infty} A_m$ is countable and hence P is countable.

   (b) We use the hint and start by defining a function from $(0, 1)$ to T as follows. Recall that every real number in the interval $(0, 1)$ can be written in decimal notation as $0.a_1a_2a_3 \ldots a_n \ldots$ where each a_i is an integer from 0 to 9. Also recall that T is the set of all functions from $\mathbb{Z}^+$ to $\{0, 1, \ldots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

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

   where g is the function in T such that $g(n) = a_n$ for all $n \in \mathbb{Z}^+$.

   So for example, if $f(0.457013) = g$ then g is the function where $g(1) = 4$, $g(2) = 5$, $g(3) = 7$, $g(4) = 0$, $g(5) = 1$, $g(6) = 3$ and $g(n) = 0$ for all $n \geq 7$.

   Now we will prove that this function is one-to-one. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in (0, 1)$. Then for these functions to be equal, they map every integer to the same value. For this to happen, every decimal digit of x_1 must be equal to the same decimal digit of x_2 and so we must have $x_1 = x_2$.

   Now denote the set of all outputs of f as S. Hence $S \subseteq T$. Now if we set the codomain of f to be S, which is the range of f, we have made this function surjective and hence a

bijection. This means that the subset $S \subseteq T$ is in bijection with the interval $(0, 1)$. Since the interval $(0, 1)$ is uncountable, we must have that S is also uncountable and since $S \subseteq T$, T must also be uncountable.

(c) Part (a) showed us that the set of all computer programs in a given language is countable. This means that there are a countable number of computable functions. However part (b) showed us that there is an uncountable number of functions in the set T, so we must have that some functions are uncomputable.

§29 — Relations on Sets

Epp 4th ed. pp. 442–449 · 5th ed. (metric) pp. 487–494. Lecture 23 (week 8).

Problems

1. Define a relation P on $\mathbb{Z}$ as follows: for every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \; P \; n \iff m \text{ and } n \text{ have a common prime factor.}$$

   (a) Is $15 \; P \; 25$?

   (b) Is $22 \; P \; 27$?

   (c) Is $0 \; P \; 5$?

   (d) Is $8 \; P \; 8$?

2. Let $X = \{a, b, c\}$. Define a relation S on the power set $\mathcal{P}(X)$ as follows: for all sets A and B in $\mathcal{P}(X)$,

$$A \; S \; B \iff A \text{ has the same number of elements as } B.$$

   (a) Is $\{a, b\} \; S \; \{b, c\}$?

   (b) Is $\{a\} \; S \; \{a, b\}$?

   (c) Is $\{c\} \; S \; \{b\}$?

3. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ be sets. Let R be the 'divides' relation. That is, for every ordered pair (a, b) in $A \times B$, we have $a \; R \; b$ if and only if $a \mid b$. Draw an arrow diagram (i.e. the directed graph) of this relation.

Solutions

1. (a) **Yes**, since $15 = 3 \cdot 5$ and $25 = 5 \cdot 5$ share the prime factor 5.

   (b) **No**, since $22 = 2 \cdot 11$ and $27 = 3^3$ share no common prime factor.

   (c) **Yes**, since 0 is divisible by every prime; in particular $5 \mid 0$ and $5 \mid 5$, so 0 and 5 have a common prime factor.

   (d) **Yes**, since $8 = 2^3$ and 2 is a prime factor of 8 (so they share the prime factor 2).

2. (a) **Yes**, since $|\{a, b\}| = 2 = |\{b, c\}|$.

   (b) **No**, since $|\{a\}| = 1 \neq 2 = |\{a, b\}|$.

   (c) **Yes**, since $|\{c\}| = 1 = |\{b\}|$.

3. We have $A \times B = \{(3,4), (3,5), (3,6), (4,4), (4,5), (4,6), (5,4), (5,5), (5,6)\}$. The pairs (a, b) satisfying $a \mid b$ are

$$\{(3,6),\ (4,4),\ (5,5)\} \subseteq A \times B.$$

   So the directed graph has an arrow from 3 (in A) to 6 (in B), an arrow from 4 to 4, and an arrow from 5 to 5 — and no other arrows.

§30 — Reflexivity, Symmetry, Transitivity

Epp 4th ed. pp. 449–459 · 5th ed. (metric) pp. 495–505. Lecture 23 (week 8).

Problems

1. Let $X = \{1, 2, 3, 4, 5\}$ and consider the subset $R \subseteq X \times X$ given by

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3), (3,4), (4,5), (5,1)\}.$$

   (a) Draw an arrow diagram for the binary relation R.

   (b) Draw an arrow diagram for the binary relation R^{-1}.

   (c) Draw an arrow diagram for the binary relation $R \cup R^{-1}$.

   (d) Is R symmetric? Is R^{-1} symmetric? Is $R \cup R^{-1}$ symmetric?

   (e) Is R transitive? Is R^{-1} transitive? Is $R \cup R^{-1}$ transitive?

2. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

- $(1, 2) \in R$
- $(2, 3) \in R$
- R is reflexive
- R is transitive

What is the minimum number of arrows required in an arrow diagram for a relation R that satisfies these criteria?

Solutions

1. (a) The arrow diagram for R has the five vertices $1, 2, 3, 4, 5$ drawn around a circle, with a **loop at every vertex** (from the pairs $(1, 1), \ldots, (5, 5)$) together with the directed 5-cycle

$$1 \to 2 \to 3 \to 4 \to 5 \to 1.$$

(b) The arrow diagram for R^{-1} is the same picture with every non-loop arrow reversed: a loop at every vertex, together with the directed 5-cycle

$$1 \to 5 \to 4 \to 3 \to 2 \to 1,$$

that is, $R^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$.

(c) The arrow diagram for $R \cup R^{-1}$ has a loop at every vertex and a **double-headed arrow** between each consecutive pair around the cycle — that is, both $(i, i + 1)$ and $(i + 1, i)$ for the cycle $1, 2, 3, 4, 5, 1$.

(d) R is **not** symmetric because $(1, 2) \in R$ but $(2, 1) \notin R$.

R^{-1} is **not** symmetric because $(2, 1) \in R^{-1}$ but $(1, 2) \notin R^{-1}$.

$R \cup R^{-1}$ **is** symmetric. If $(a, b) \in R \cup R^{-1}$ then $(a, b) \in R$ or $(a, b) \in R^{-1}$, which means $(b, a) \in R^{-1}$ or $(b, a) \in R$, and thus, in either case, $(b, a) \in R \cup R^{-1}$.

(e) R is **not** transitive because $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

R^{-1} is **not** transitive because $(3, 2), (2, 1) \in R^{-1}$ but $(3, 1) \notin R^{-1}$.

$R \cup R^{-1}$ is **not** transitive because $(1, 2), (2, 3) \in R \cup R^{-1}$ but $(1, 3) \notin R \cup R^{-1}$.

2. R is reflexive, so $(1,1),(2,2),(3,3) \in R$ — a loop on each point of the arrow diagram. We are also given $(1,2),(2,3) \in R$, and R is transitive, so $(1,3) \in R$. R is *not* required to be symmetric, so no further arrows are forced.

$$R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$$

So the **minimum number of arrows required is 6**.

§31 — Equivalence Relations

Epp 4th ed. pp. 459–478 · 5th ed. (metric) pp. 505–523. Lecture 24 (week 9).

Problems

1. Define the binary relations α, β and γ on $\mathbb{Z}$ as follows:

$$\begin{aligned} x\ \alpha\ y &\iff x+y \text{ is an even integer,} \\ x\ \beta\ y &\iff x \text{ is a multiple of } y, \\ x\ \gamma\ y &\iff 3 \text{ is a factor of } x^2-y^2. \end{aligned}$$

   (a) Fill in the table with 'Yes'/'No' to indicate the properties satisfied by each relation.

	α	β	γ
Reflexive			
Symmetric			
Transitive			
Equivalence relation			

   (b) For each equivalence relation, state its equivalence classes.

2. Let $A = \{a,b,c,d,e\}$ be a set and ρ be a binary relation defined by

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

   For instance, $(a,b) \in \rho$ means $a\ \rho\ b$.

   (a) Draw the directed graph representing ρ.

   (b) Is ρ reflexive? Is ρ symmetric? Is ρ transitive?

(c) Is ρ an equivalence relation on A? If so, give its equivalence classes.

(d) What is the smallest subset τ of ρ which forms an equivalence relation on A?

(e) Give the equivalence classes for τ.

3. Consider a positive integer n and any set of strings S. Define a relation R_n on S by the condition $s\ R_n\ t$ if and only if $s = t$ or both s and t have at least n characters and the first n characters are the same. Show that R_n is an equivalence relation.

Solutions

1. (a)

	α	β	γ
Reflexive	Yes	Yes	Yes
Symmetric	Yes	No	Yes
Transitive	Yes	Yes	Yes
Equivalence relation	Yes	No	Yes

(b) The equivalence relations are α and γ.

For α, notice $x\ \alpha\ y \iff x + y$ is even $\iff x$ and y have the same parity. This means the equivalence classes are $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

For γ, notice $x\ \gamma\ y \iff 3 \mid (x^2 - y^2) \iff x^2 \equiv y^2 \pmod 3$. But modulo 3 the only possible square residues are

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 1 \pmod 3.$$

Hence $x^2 \equiv 0 \pmod 3$ exactly when $3 \mid x$, and $x^2 \equiv 1 \pmod 3$ exactly when $3 \nmid x$. Therefore $x\ \gamma\ y$ iff either both x and y are multiples of 3, or neither is. So the equivalence classes are $\{n \in \mathbb{Z} : 3 \mid n\}$ and $\{n \in \mathbb{Z} : 3 \nmid n\}$. Note that another way to write the equivalence classes is $\{3n \mid n \in \mathbb{Z}\}$ and $\{3n + 1,\ 3n + 2 \mid n \in \mathbb{Z}\}$.

2. (a) A digraph for ρ (vertex set $A = \{a, b, c, d, e\}$) has a **loop at every vertex**, double-headed arrows between each pair of $\{a, b, d\}$ — that is between a and b, between a and d, and between b and d — and a double-headed arrow between c and e. There are no arrows between $\{a, b, d\}$ and $\{c, e\}$.

(b) ρ is **reflexive**: we have $(x, x) \in \rho$ for all $x \in A$ (loops on all vertices).

ρ is **symmetric**: whenever $(x, y) \in \rho$, we have $(y, x) \in \rho$ (no single-direction arrow between any two distinct vertices).

ρ is **transitive**: within $\{a, b, d\}$ all relations occur, within $\{c, e\}$ all relations occur, and there are no relations between $\{a, b, d\}$ and $\{c, e\}$. That is, whenever (x, y) and (y, z) are in ρ, then (x, z) is also in ρ (and $x = z$ is possible).

(c) **Yes**, ρ is an equivalence relation. Its equivalence classes are

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

(d) An equivalence relation $\tau \subseteq \rho$ must be reflexive, so $(x, x) \in \tau$ for all $x \in A$. But notice if τ is the relation

$$\tau = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$$

then τ is an equivalence relation. Therefore this is the smallest relation which is an equivalence relation.

(e) The equivalence classes for τ are the singletons:

$$[a] = \{a\},\ [b] = \{b\},\ [c] = \{c\},\ [d] = \{d\},\ [e] = \{e\}.$$

3. Let S be any set of strings and fix $n \in \mathbb{Z}^+$.

   R_n **is reflexive:** for any $s \in S$, since $s = s$, by definition $s\ R_n\ s$.

   R_n **is symmetric:** let $s, t \in S$, and assume $s\ R_n\ t$. If $s = t$ then $t\ R_n\ s$; otherwise both s and t must have at least n characters and, since $s\ R_n\ t$, they must have the same first n characters, so $t\ R_n\ s$.

   R_n **is transitive:** let $s, t, u \in S$ and assume $s\ R_n\ t$ and $t\ R_n\ u$. Since $s\ R_n\ t$ we either have $s = t$, or s and t both have at least n characters and have the same first n characters. Similarly, since $t\ R_n\ u$, either $t = u$, or t and u both have at least n characters and have the same first n characters. Thus either $s = t = u$, or s and u both have at least n characters and they both share the first n characters with t (and hence each other). Thus $s\ R_n\ u$ and so R_n is transitive.

   Since R_n is reflexive, symmetric and transitive it is an equivalence relation. □

Application — Identifiers

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 608–618.*

In the C programming language, an **identifier** is the name of a variable, a function or another type of entity.

Each identifier is a nonempty string of characters where each character is a lowercase or uppercase English letter, a digit, or an underscore.

There is no limit on the number of characters used in the identifier; however, for some compilers for some versions of C, there is a limit on the number of characters checked when two names are compared.

For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. We see that two identifiers will be considered the same if and only if they are related under the relation R_n when $n = 31$ (defined in a previous question).

Application problems

1. Using R_{31} on the set of all possible identifiers, determine the equivalence classes of each of the following identifiers:

   (a) `file_1`

   (b) `Number_of_tropical_storms`

   (c) `Number_of_named_tropical_storms`

   (d) `Number_of_named_tropical_storms_in_the_Atlantic_in_2005`

Application solutions

1. Let I be the set of all possible identifiers (strings over letters, digits and underscores).

   (a) Since `file_1` has length $6 < 31$, its equivalence class is just

   $$[\texttt{file_1}]_{R_{31}} = \{\texttt{file_1}\}.$$

   (b) Since `Number_of_tropical_storms` has length $25 < 31$, its equivalence class is

   $$[\texttt{Number_of_tropical_storms}]_{R_{31}} = \{\texttt{Number_of_tropical_storms}\}.$$

(c) The identifier `Number_of_named_tropical_storms` has length exactly 31, so two identifiers are R_{31}-equivalent to it iff they have at least 31 characters and their first 31 characters equal this string. Hence

$$[\texttt{Number_of_named_tropical_storms}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 31 characters of} \\ t \text{ are } \texttt{Number_of_named_tropical_storms} \end{array} \right\}.$$

(d) The identifier `Number_of_named_tropical_storms_in_the_Atlantic_in_2005` begins with the same first 31 characters `Number_of_named_tropical_storms`, so it has the same R_{31}-equivalence class as in (c):

$$[\texttt{Number_of_named_tropical_storms_in_the_Atlantic_in_2005}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 3} \\ t \text{ are } \texttt{Number_of_name} \end{array} \right.$$

§32 — Partial Order Relations

Epp 4th ed. pp. 498–515 · 5th ed. (metric) pp. 546–563. Lecture 25 (week 9).

Problems

1. Let ρ be a relation on $\mathbb{Z}$ defined by $x \rho y$ if and only if $x^3 - 1 < y^3$.
   (a) Prove ρ is a partial order relation.
   (b) Is ρ a total order?
2. Let S be the set of binary strings of length 6. Define the **weight** of a binary string as the number of ones it contains. (For example, weight(110110) = 4.) Define a relation ρ on S by

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

   (a) Prove that ρ is not an equivalence relation.
   (b) Prove that ρ is not a partial order relation.
3. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:
   - $(2, 3) \in R$
   - $(3, 2) \in R$
   - $(1, 1) \notin R$

- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) To show that ρ is a partial order, we need to show that ρ is reflexive, antisymmetric and transitive.

   Reflexive: let $x \in \mathbb{Z}$. Then $x^3 - 1 < x^3$ and so $x \rho x$, so ρ is reflexive.

   Antisymmetric: suppose $x \rho y$ where $x \neq y$. (We must show that then $y \not\rho x$.) Now $x \rho y$ means that $x^3 - 1 < y^3$. And since $x \neq y$ we must have $x^3 < y^3$ and so $x^3 \leqslant y^3 - 1$. Hence $y^3 - 1 \not< x^3$ and so we do not have $y \rho x$. Therefore ρ is antisymmetric.

   Transitive: suppose that $x \rho y$ and $y \rho z$. Then we know that $x^3 - 1 < y^3$ and $y^3 - 1 < z^3$. So $x^3 - 1 \leqslant y^3 - 1 < z^3$, that is, $x^3 - 1 < z^3$ so that $x \rho z$, which means that ρ is transitive.

   Hence ρ is a partial order. □

   (b) To check whether ρ is a total order, let x and y be any two distinct integers. Then $x^3 \neq y^3$ and so either $x^3 < y^3$ or else $y^3 < x^3$.

   If $x^3 < y^3$ then $x^3 - 1 < y^3$ and so $x \rho y$.

   If $y^3 < x^3$ then $y^3 - 1 < x^3$ and so $y \rho x$.

   So for any integers $x \neq y$, we have either $x \rho y$ or else $y \rho x$. So any two integers are comparable under ρ. Hence ρ **is** a total order.

2. (a) It is **not an equivalence relation** because it is not symmetric. For instance, let $s = 000000$ and $t = 111111$. Then $\text{weight}(s) = 0 \leq 6 = \text{weight}(t)$, so $(s, t) \in \rho$, but $(t, s) \notin \rho$.

   (b) It is **not a partial order** because it is not antisymmetric. For instance, let $s = 100000$ and $t = 010000$. Then $\text{weight}(s) = \text{weight}(t) = 1$, so $s \rho t$ and $t \rho s$, but $s \neq t$.

3. One relation on $\{1, 2, 3\}$ satisfying all conditions is

$$R = \{(1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3, 2)\}.$$

(It contains $(2,3)$ and $(3,2)$; it is transitive; it is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$; it is not antisymmetric since $2 \neq 3$ and $(2,3),(3,2) \in R$; and $(1,1) \notin R$.)

An arrow diagram for this R has vertices $1,2,3$ with: arrows $1 \to 2$ and $1 \to 3$; loops at 2 and at 3; and a double-headed arrow between 2 and 3. There is no loop at vertex 1.

§33 — Definitions and Examples of Groups

No relevant textbook pages. Lecture 26 (week 9).

Problems

1. Show $\mathbb{Z}_9 - \{0\} = \{1,2,3,\ldots,7,8\}$ is not a group under multiplication modulo 9.
2. Let G be the set of all odd integers. Define the binary operation $\star$ on G by

$$x \star y = x + y - 1.$$

   Show that $(G, \star)$ is an abelian group.
3. Show $\mathbb{Z}_9 - \{0,3,6\} = \{1,2,4,5,7,8\}$ is a group under multiplication modulo 9. Is the group abelian?
4. Define the group $H = \mathbb{Z}_5 - \{0\} = \{1,2,3,4\}$ under multiplication modulo 5. Write the Cayley table for H.
5. Define the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ under component-wise addition modulo 2. That is,

$$(a,b) + (c,d) = (a + c \bmod 2,\ b + d \bmod 2).$$

   Write the Cayley table for G.

Solutions

1. It is not a group under multiplication mod 9 because, for example, it is **not closed** ($3 \cdot 3 = 0 \notin \mathbb{Z}_9 - \{0\}$).

2. **Closure:** if x and y are odd, then $x+y$ is even, so $x+y-1$ is odd. Hence $x \star y \in G$.

   Associativity: for $x, y, z \in G$,

$$(x \star y) \star z = (x+y-1)+z-1 = x+y+z-2 = x+(y+z-1)-1 = x \star (y \star z).$$

   Commutativity: for $x, y \in G$,

$$x \star y = x+y-1 = y+x-1 = y \star x.$$

   Identity: we seek $e \in G$ such that $x \star e = x = e \star x$ for all x. Now the requirement $x \star e = x+e-1 = x$ implies that $e = 1$. Note 1 lies in G. Moreover, commutativity implies that $e \star x = x$ as well. Thus the identity is 1.

   Inverses: given $x \in G$, we want $y \in G$ with $x \star y = 1$. This means $x+y-1 = 1$, so $y = 2-x$. Since x is odd, $2-x$ is odd, hence $2-x \in G$. Thus the inverse of x is $x^{-1} = 2-x$.

   Therefore $(G, \star)$ is an abelian group. $\square$

3. **Closure:** if $a, b \in \{1,2,4,5,7,8\}$, then $3 \nmid a$ and $3 \nmid b$, hence $3 \nmid ab$, so $ab \not\equiv 0, 3, 6 \pmod 9$; thus $\{1,2,4,5,7,8\}$ is closed under multiplication modulo 9.

   Associativity and commutativity: normal multiplication between integers is associative and commutative, so multiplication modulo 9 in the set $\{1,2,4,5,7,8\}$ is also associative and commutative. This means the group **is abelian**.

   Identity: $1 \in G$ is the identity because $1 \cdot x \equiv x \pmod 9$.

   Inverse: every element has an inverse. We explicitly calculate the inverses:

$$\begin{aligned}
1^{-1} &= 1 \quad \text{because } 1 \cdot 1 \equiv 1 \pmod 9, \\
2^{-1} &= 5 \quad \text{because } 2 \cdot 5 = 10 \equiv 1 \pmod 9, \\
4^{-1} &= 7 \quad \text{because } 4 \cdot 7 = 28 \equiv 1 \pmod 9, \\
5^{-1} &= 2 \quad \text{because } 5 \cdot 2 = 10 \equiv 1 \pmod 9, \\
7^{-1} &= 4 \quad \text{because } 7 \cdot 4 = 28 \equiv 1 \pmod 9, \\
8^{-1} &= 8 \quad \text{because } 8 \cdot 8 = 64 \equiv 1 \pmod 9.
\end{aligned}$$

4. For $H = \mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ under multiplication mod 5, the Cayley table is:

$\cdot$	1	2	3	4
1	1	2	3	4

$\cdot$	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition mod 2, the Cayley table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(\mathbf{1},\mathbf{0})$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

§34 — Elementary Properties of Groups

No relevant textbook pages. Lecture 27 (week 10).

Problems

1. Let $H = \{3n \mid n \in \mathbb{Z}\}$ be the set of multiples of 3. Prove H is a subgroup of $(\mathbb{Z}, +)$.
2. Fix elements g and h in a group G where e is the group identity. Prove the following statements:
   (a) If $g^{-1} = h$ then $h^{-1} = g$.
   (b) $(g^{-1})^{-1} = g$.
   (c) $(gh)^{-1} = h^{-1}g^{-1}$.
3. Prove $K = \{(0,0),(0,1),(2,0),(2,1)\}$ is a subgroup of $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ where the group operation is componentwise addition:

$$(a,b) + (c,d) = (a + c \pmod 4,\ b + d \pmod 2).$$

4. Consider the group $(\mathbb{Z}_{11} - \{0\}, \cdot)$. Show that this group is cyclic.
   Hint: express every element of $\mathbb{Z}_{11} - \{0\}$ as a power of 2.

Solutions

1. First we note that $H \subseteq \mathbb{Z}$, and $H \neq \emptyset$.

   Closure: if $x, y \in H$ then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}$. Therefore $x + y = 3a + 3b = 3(a + b) \in H$.

   Identity: the identity of $(\mathbb{Z}, +)$ is 0, and since $0 = 3 \cdot 0$, we have $0 \in H$.

   Inverse: in $\mathbb{Z}$, the inverse of x is $-x$. In H, if $x \in H$ then $x = 3a$ for some $a \in \mathbb{Z}$. This means $-x = -3a = 3 \cdot (-a)$, and so $-x \in H$ also.

   Note that we do not need to check associativity for subgroups, since this property is automatically inherited from the parent group $(\mathbb{Z}, +)$. □

2. (a) Suppose $g^{-1} = h$. Now $gh = gg^{-1} = e$ and $hg = g^{-1}g = e$. Thus $h^{-1} = g$.

   (b) By definition, $gg^{-1} = e = g^{-1}g$, so $(g^{-1})^{-1} = g$.

   (c) Notice we have

   $$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = e$$

   and

   $$(h^{-1}g^{-1})(gh) = h^{-1}g^{-1}gh = e.$$

   This means $(gh)^{-1} = h^{-1}g^{-1}$.

3. We draw the Cayley table of $K = \{(0,0), (0,1), (2,0), (2,1)\}$ under componentwise addition in $\mathbb{Z}_4 \times \mathbb{Z}_2$:

$+$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(2,1)$	$(2,0)$
$(\mathbf{2},\mathbf{0})$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(\mathbf{2},\mathbf{1})$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$

   Notice the operation is closed in K and every element of K has an inverse in K. Therefore K is a subgroup. □

4. Note that 2 is a generator of $(\mathbb{Z}_{11} - \{0\}, \cdot)$, so it is cyclic:

   $$1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ 8 = 2^3,\ 5 = 2^4,\ 10 = 2^5,\ 9 = 2^6,\ 7 = 2^7,\ 3 = 2^8,\ 6 = 2^9.$$

§35 — Group Isomorphisms

No relevant textbook pages. No lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36).

This content is optional and will not be assessed. The source document carries no practice problems or solutions for this section.

§36 — Definitions and Examples of Fields

No relevant textbook pages. Lecture 28 (week 10).

Problems

1. (a) Solve $3x + 4 = 2$ in the field $(\mathbb{Z}_5, +, \cdot)$.
   (b) Solve $8x - 9 = 6$ in the field $(\mathbb{Z}_{11}, +, \cdot)$.
   (c) Solve $4(1 - x) = 10$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.
   (d) Solve $16(x - 6) = 15$ in the field $(\mathbb{Z}_{19}, +, \cdot)$.
2. Prove $\mathbb{Z}_{12}$ with addition modulo 12 and multiplication modulo 12 is not a field.
3. Define addition and multiplication on $\mathbb{Q} \times \mathbb{Q}$ by

$$(a, b) + (c, d) = (a + c,\ b + d)$$

   and

$$(a, b) \cdot (c, d) = (ac + 3bd,\ ad + bc)$$

   for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$. Prove that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field.

Solutions

1. (a)

$$\begin{aligned} 3x + 4 &= 2 \\ \rightarrow 3x &= -2 \end{aligned}$$

Now, since $3 \times 2 = 6 \equiv 1 \pmod 5$, 2 is the multiplicative inverse of 3, and so we multiply both sides by 2 and obtain $x = -4$. That is, $x = 1$.

Check: $3 \cdot 1 + 4 = 7 \equiv 2 \pmod 5$.

(b)

$$\begin{aligned} 8x - 9 &= 6 \\ \rightarrow 8x &= 15 = 4 \end{aligned}$$

Now, since $8 \times 7 = 56 \equiv 1 \pmod{11}$, 7 is the multiplicative inverse of 8, and so we multiply both sides by 7 and obtain $x = 28$. That is, $x = 6$.

Check: $8 \cdot 6 - 9 = 39 \equiv 6 \pmod{11}$.

(c) Since $4 \times 10 = 40 \equiv 1 \pmod{13}$, 10 is the multiplicative inverse of 4, and so we multiply both sides by 10 and obtain $1 - x = 100 = 9$. That is, $x = 1 - 9 = 14 - 9 = 5$.

Check: $4(1 - 5) = -16 \equiv 10 \pmod{13}$.

(d) Since $16 \times 6 = 96 \equiv 1 \pmod{19}$, 6 is the multiplicative inverse of 16, and so we multiply both sides by 6 and obtain $x - 6 = 90 = 14$. That is, $x = 20 = 1$.

Check: $16(1 - 6) = -80 \equiv 15 \pmod{19}$.

2. $\mathbb{Z}_{12}$ is not a field because 2 has no multiplicative inverse modulo 12. Indeed $2 \cdot k \equiv 1 \pmod{12}$ has no solution since $2k$ is always even.

3. We show that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field in three steps.

Step 1 — $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Closure: for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Q} \times \mathbb{Q}$.

Associative: for all $(a, b), (c, d), (e, f) \in \mathbb{Q} \times \mathbb{Q}$ we have $\big((a, b) + (c, d)\big) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) = (a, b) + (c + e, d + f) = (a, b) + \big((c, d) + (e, f)\big)$.

Identity: for all $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0) + (a, b)$.

Inverses: for all $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a,b) + (-a,-b) = (a-a, b-b) = (0,0)$ and $(-a,-b) + (a,b) = (-a+a, -b+b) = (0,0)$. So $(-a,-b)$ is the inverse of (a,b).

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b)$.

Thus $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Step 2 — $((\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\},\ \cdot)$ is an abelian group.

Closure: for all $(a,b),(c,d) \in (\mathbb{Q}\times\mathbb{Q}) - \{(0,0)\}$, we have $(a,b)\cdot(c,d) = (ac+3bd, ad+bc) \in \mathbb{Q} \times \mathbb{Q}$. So we only need to show that $(ac+3bd, ad+bc) \neq (0,0)$. For a contradiction, suppose $(ac+3bd, ad+bc) = (0,0)$. That is, $ac+3bd = 0$ and $ad+bc = 0$. Multiplying the first equation by d and the second by c we obtain $acd + 3bd^2 = 0$ and $acd + bc^2 = 0$, from which it follows that $3bd^2 = bc^2$.

Now, if $b = 0$, then $ac = 0$, $ad = 0$ and $a \neq 0$, and so $c = d = 0$; a contradiction. Thus $b \neq 0$ and we have $3d^2 = c^2$. This is a contradiction because if $d = 0$, then $c \neq 0$ and the equation does not hold, and if $d \neq 0$, then we have $3 = \frac{c^2}{d^2}$, which implies $\sqrt{3} = \frac{c}{d}$ is rational. Thus $(ac+3bd, ad+bc) \neq (0,0)$ and we have closure.

Associative: for all $(a,b),(c,d),(e,f) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have

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

and

$$\begin{aligned}\big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac+3bd,\ ad+bc)\cdot(e,f)\\ &= \big((ac+3bd)e+3(ad+bc)f,\ (ac+3bd)f+(ad+bc)e\big)\\ &= (ace+3bde+3adf+3bcf,\ acf+3bdf+ade+bce)\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf).\end{aligned}$$

Identity: for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have $(a,b)\cdot(1,0) = (a,b)$ and $(1,0)\cdot(a,b) = (a,b)$, so $(1,0)$ is a multiplicative identity.

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have

$$(a,b)\cdot(c,d) = (ac+3bd,\ ad+bc) = (ca+3db,\ cb+da) = (c,d)\cdot(a,b).$$

Inverses: we check that for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2-3b^2},\ \frac{-b}{a^2-3b^2}\right).$$

First, note that $a^2-3b^2 \neq 0$, because $a^2-3b^2=0$ implies either $(a,b)=(0,0)$ or $\sqrt{3}=\frac{a}{b}$, both of which are contradictions (the second because $\sqrt{3}$ is not rational). Thus $(a,b)^{-1} \in (\mathbb{Q}\times\mathbb{Q})-\{(0,0)\}$, and notice

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2-3b^2},\frac{-b}{a^2-3b^2}\right) &= \left(a\cdot\frac{a}{a^2-3b^2}+3b\cdot\frac{-b}{a^2-3b^2},\ a\cdot\frac{-b}{a^2-3b^2}+b\cdot\frac{a}{a^2-3b^2}\right)\\ &= \left(\frac{a^2-3b^2}{a^2-3b^2},\ \frac{-ab+ab}{a^2-3b^2}\right)\\ &= (1,0).\end{aligned}$$

So every nonzero element has an inverse. Thus $((\mathbb{Q}\times\mathbb{Q})-\{(0,0)\},\cdot)$ is an abelian group.

Step 3 — the distributive laws. For all $(a,b),(c,d),(e,f)\in\mathbb{Q}\times\mathbb{Q}$ we have

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,\ d+f)\\ &= (a(c+e)+3b(d+f),\ a(d+f)+b(c+e))\\ &= ((ac+3bd)+(ae+3bf),\ (ad+bc)+(af+be))\\ &= (ac+3bd,\ ad+bc)+(ae+3bf,\ af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)\end{aligned}$$

and (since we have already shown that multiplication and addition are commutative)

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f) &= (e,f)\cdot((a,b)+(c,d))\\ &= (e,f)\cdot(a,b)+(e,f)\cdot(c,d) \quad \text{(by the first distributive law)}\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f).\end{aligned}$$

Thus $(\mathbb{Q}\times\mathbb{Q},+,\cdot)$ is a field. □

§37 — Introduction to Counting

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 29 (week 11).

Problems

1. The UQ drama club is auditioning for its annual production of *Romeo and Juliet*. Six people are auditioning for the role of Romeo, and eight other people are auditioning for the role of Juliet. In how many ways can the director cast the lead couple?
2. There are eleven questions on the final exam, but you decide — based on your successful grade for your in-semester exam — that you will only do five of them. How many combinations of questions are there which you could complete?
3. (a) How many permutations of $\{1, 2, \dots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \dots, 15\}$ contain exactly two numbers from $\{1, 2, 3, 4\}$?

Solutions

1. There are 6 choices for Romeo and 8 choices for Juliet, so $6 \cdot 8 = 48$ ways.
2. Since the order in which you do the 5 questions does not matter, there are $\binom{11}{5} = 462$ combinations of questions.
3. (a) There are 8 odd numbers in the set $\{1, \dots, 15\}$. Choose the first entry in 8 ways, then permute the remaining 14 numbers, so $8 \cdot 14!$ permutations.

   (b) We choose exactly 2 numbers from the set $\{1, 2, 3, 4\}$ and exactly 3 numbers from the remaining 11 numbers, so the number of subsets is

$$\binom{4}{2}\binom{11}{3}.$$

Application — Runtime

Not assessable for MATH1061. Taken from S. Epp, Discrete Mathematics with Applications, *5th edition, pages 787–799.*

In many algorithms, the runtime is well approximated by counting how many times the basic instructions are executed.

For programs with nested `for`-loops and no early exits, the total number of executions of the inner loop body equals the number of choices of the outer-loop index multiplied by the number of choices of the inner-loop index.

Concretely, if i runs through M values and, for each fixed i, the variable j runs through N values, then the inner loop body is executed exactly MN times.

Application problems

1. The following algorithms are written in pseudo-code and contain nested loops. For each algorithm, count the total number of iterations of the inner loop that the algorithm will run.

   (a)

```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (b)

```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (c) (Fix integers $a, b, c, d \in \mathbb{Z}^+$ with $a \leq b$ and $c \leq d$.)

```
for i := a to b
    for j := c to d
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

Application solutions

1. (a) $i = 1, \ldots, 30$ gives 30 iterations and $j = 1, \ldots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

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

   (c) $i = a, \ldots, b$ gives $b - a + 1$ iterations and $j = c, \ldots, d$ gives $d - c + 1$ iterations, so the inner loop runs $(b - a + 1)(d - c + 1)$ times.

§38 — Counting Selections

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 30 (week 11).

Problems

1. (a) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY?

   (b) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with R and end with P?

   (c) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with I and end with Y?

   (d) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that have all four Os next to each other?

2. (a) How many distinct arrangements can be made of the letters of the word WOOLLOONGABBA?

   (b) How many distinct arrangements are there of the letters of the word WOOLLOONGABBA such that **exactly one** of the following is true?

   - The two As are not next to each other.
   - The two Bs are not next to each other.
   - The two Ls are not next to each other.

3. (a) How many one-to-one (injective) functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

   (b) How many onto (surjective) functions are there from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$?

Solutions

1. (a) There are 13 letters in INDOOROOPILLY, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!} = 64\,864\,800.$$

   (b) Fix R in the first position and P in the last position. There are 11 letters remaining, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!\,2!} = 415\,800.$$

(c) Fix I in the first position and Y in the last position. There are 11 letters remaining, with four O's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!} = 831\,600.$$

(d) Treat the four O's as one 'letter'. There are 10 'letters' with two I's, two L's, and the remaining 'letters' appearing once each. Therefore the number of distinct arrangements is

$$\frac{10!}{2!\,2!} = 907\,200.$$

2. (a) There are 13 letters in WOOLLOONGABBA, with four O's, two L's, two A's, two B's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!\,2!} = 32\,432\,400.$$

(b) We want exactly one of the pairs AA, BB, LL to be non-adjacent. That is, there are three cases to consider:

- **Case 1:** the two A's are not adjacent but BB and LL are adjacent.
- **Case 2:** the two B's are not adjacent but AA and LL are adjacent.
- **Case 3:** the two L's are not adjacent but AA and BB are adjacent.

Note that the number of ways Case 1 can occur is exactly the same as the number of ways Case 2 can occur (and similarly for Case 3).

To count the number of ways Case 1 can occur, we first count arrangements with BB adjacent and LL adjacent. Treat BB as one 'letter' and LL as one 'letter'. Then there are 11 'letters' (W, O, O, LL, O, O, N, G, A, BB, A) to arrange, with four O's, two A's, and the remaining 'letters' appearing once each. Therefore the number of such arrangements is

$$\frac{11!}{4!\,2!}.$$

In order to determine the number of these for which the two A's are not adjacent, we take this total and subtract those where AA is also adjacent. For this, treat AA, BB, and LL as 'letters'. Then there are 10 'letters' to arrange, with four O's and the remaining 'letters' appearing once each. Therefore the number of arrangements with AA adjacent and BB adjacent and LL adjacent is

$$\frac{10!}{4!}.$$

Hence, the number of ways that Case 1 can occur is

$$\frac{11!}{4!\,2!} - \frac{10!}{4!}.$$

Case 2 and Case 3 have exactly the same number of occurrences as Case 1. Also note that the three cases are mutually exclusive (you cannot have both Case 1 and Case 2 occurring at the same time, for example).

So the number of arrangements of the word WOOLLOONGABBA for which exactly one of the three cases occurs is

$$3\left(\frac{11!}{4!\,2!} - \frac{10!}{4!}\right).$$

3. (a) An injective function $f : \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ is determined by choosing distinct images for a, b, c. The number of choices is

$$5 \cdot 4 \cdot 3 = {}^5P_3 = 60.$$

(b) The number of surjective functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ is the total number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ minus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ which are not surjective. The former number is 3^5. A function which is not surjective must have image of size 1 or 2.

- In the first case, there are 3 such functions (one for each of the three choices for the image).
- In the latter case, first choose which 2 elements of $\{a, b, c\}$ will be in the image. There are $\binom{3}{2}$ such choices. For this fixed two-element image, the number of functions with this image is

$$2^5 - 2,$$

since there are 2^5 total functions from a 5-element set to a 2-element set, and we subtract the 2 constant ones (which fall into the first case, having image of size 1). Thus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ with an image of size 2 is

$$\binom{3}{2}(2^5 - 2) = 3 \cdot 30 = 90.$$

This means there are 93 functions which are not surjective, so the number of surjective functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ is

$$3^5 - 93 = 150.$$

§39 — Introduction to Probability

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 31 (week 11).

Problems

1. To form a committee, five people are to be chosen from a group of ten people.
   (a) How many different committees of five can be chosen?
   (b) Amongst the ten people, we have Alice, Bob, Eve and Oscar. Alice and Bob are extremely talkative during meetings, and so at most one of these two can be chosen. Eve and Oscar are inseparable, and so a committee must either contain both of them or neither of them. With these constraints, how many different five-person committees can be formed?
   (c) What is the probability that none of Alice, Bob, Eve and Oscar are on a committee, given that a random committee of five is chosen subject to the constraints in part (b)?
2. (a) How many positive two-digit integers are multiples of 3?
   (b) What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
   (c) What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

Solutions

1. (a) Number of different committees of five is

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252.$$

   (b) Let A, B be Alice and Bob, and let E, O be Eve and Oscar. There are 6 other people. We split into cases.

   Case 1: the committee contains both E and O. Then we choose 3 more people from the remaining 8 with the restriction that we cannot choose both A and B. There are $\binom{8}{3}$ ways to choose 3 more people from the remaining 8 to be on the committee; of these, there are $\binom{6}{1}$ ways in which both A and B are chosen (such a committee must have E, O, A, B so there is only one more person to choose from the remaining 6 people). Thus the number of committees for this case is

$$\binom{8}{3} - \binom{6}{1} = 56 - 6 = 50.$$

   Case 2: the committee contains neither E nor O. Then we choose 5 people from the remaining 8, again not allowing both A and B. There are $\binom{8}{5}$ ways to choose 5 people from the remaining 8 people to be on the committee; of these, there are $\binom{6}{3}$ ways in which both A and B are chosen. Thus the number of committees for this case is

$$\binom{8}{5} - \binom{6}{3} = 56 - 20 = 36.$$

   Hence the total number is $50 + 36 = 86$.

   (c) To have none of Alice, Bob, Eve, or Oscar on the committee, we must choose all 5 members from the other 6 people, which can be done in $\binom{6}{5} = 6$ ways. Therefore the probability is

$$\frac{6}{86} = 0.069767\ldots$$

2. (a) The positive two-digit multiples of 3 occur as every third number from 12 to 99, so there are

$$\frac{99 - 12}{3} + 1 = 30$$

such numbers.

(b) There are 90 positive two-digit integers (9 choices for the first digit and 10 choices for the second digit). Thus, by part (a), the probability that a randomly selected positive two-digit number is a multiple of 3 is

$$\frac{30}{90} = \frac{1}{3}.$$

(c) The positive two-digit multiples of 4 occur as every fourth number from 12 to 96, so there are

$$\frac{96-12}{4} + 1 = 22$$

such numbers. Hence the probability that a randomly selected positive two-digit number is a multiple of 4 is

$$\frac{22}{90} = \frac{11}{45}.$$

§40 — Binomial Coefficients

Epp 4th ed. pp. 565–591 · 5th ed. (metric) pp. 617–641. Lecture 31 (week 11).

Problems

1. What is the coefficient of x^4 in $(2+3x)^7$?
2. (a) What is the coefficient of x^{12} in $(3-x^3)^6$?
   (b) What is the coefficient of x^8 in $(3-x^3)^6$?
3. What is the coefficient of x^2 in the expansion of $(3-x)^6$?
4. What is the coefficient of x^5 in the expansion of $(2x+1)^{20}$?
5. What is the coefficient of x^5 in the expansion of $\left(3x^2 - \dfrac{2}{x}\right)^7$?

Solutions

1. By the binomial theorem,

$$(2+3x)^7 = \sum_{k=0}^{7} \binom{7}{k} 2^{7-k}(3x)^k.$$

The term x^4 appears only when $k=4$. This term is $\binom{7}{4}2^3(3x)^4$. Therefore the coefficient of x^4 is

$$\binom{7}{4}2^3 3^4 = 35 \times 8 \times 81 = 22\,680.$$

2. By the binomial theorem,

$$(3-x^3)^6 = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-x^3)^k = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-1)^k x^{3k}.$$

(a) The term involving x^{12} is $\binom{6}{4}3^2(-1)^4 x^{3\cdot 4}$, so the coefficient of x^{12} is

$$15 \times 9 \times (-1)^4 = 135.$$

(b) Every power of x that appears is a multiple of 3. Since 8 is not a multiple of 3, there is no x^8 term, so the coefficient of x^8 is $\mathbf{0}$.

3. By the binomial theorem,

$$(3-x)^6 = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-x)^i = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-1)^i x^i.$$

The term x^2 appears only when $i=2$, so the coefficient of x^2 is

$$\binom{6}{2}3^{6-2}(-1)^2 = \binom{6}{2}3^4 = 1215.$$

4. By the binomial theorem,

$$(2x+1)^{20} = \sum_{k=0}^{20} \binom{20}{k} (2x)^{20-k}(1)^k.$$

The term x^5 appears only when $k = 15$, where the term is $\binom{20}{15}(2x)^5$, so the coefficient of x^5 is

$$\binom{20}{5} 2^5 = 496\,128.$$

5. By the binomial theorem,

$$\left(3x^2 - \frac{2}{x}\right)^7 = \sum_{i=0}^{7} \binom{7}{i} (3x^2)^{7-i} \left(-\frac{2}{x}\right)^i = \sum_{i=0}^{7} \binom{7}{i} 3^{7-i}(-2)^i x^{14-3i}.$$

The term x^5 appears only when $14 - 3i = 5$, i.e. $i = 3$. Therefore the coefficient of x^5 is

$$\binom{7}{3} 3^4(-2)^3 = -22\,680.$$

§41 — Inclusion Exclusion

Epp 4th ed. pp. 545–549 · 5th ed. (metric) pp. 595–599. Lecture 32 (week 12).

Problems

1. Out of 100 people surveyed, 40 people like apples, 50 like bananas and 40 like cherries. 15 like apples and bananas, 16 like bananas and cherries, 17 like cherries and apples and 10 people like all three. How many people do not like any of the three fruits?
2. How many integers between 1 and 600 inclusive are coprime with 15? That is, how many integers n satisfy $1 \leq n \leq 600$ and $\gcd(n, 15) = 1$?
3. Seven friends, named Alice, Bob, Charlie, Delia, Edward, Fred and George, stand in a line for a photograph. How many different arrangements are there of the seven friends standing in a line such that Alice is not next to Charlie and Bob is not next to Delia?

Solutions

1. Let A be the set of people who like apples, B the set of people who like bananas, and C the set of people who like cherries. We are given

$$|A| = 40,\ |B| = 50,\ |C| = 40, \quad |A \cap B| = 15,\ |B \cap C| = 16,\ |C \cap A| = 17, \quad |A \cap B \cap C| = 10.$$

   By inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \\ &= 40 + 50 + 40 - 15 - 17 - 16 + 10 \\ &= 92. \end{aligned}$$

   Hence the number of people who do not like any of the three fruits is

$$100 - |A \cup B \cup C| = 100 - 92 = 8.$$

2. Let $U = \{1, 2, \ldots, 600\}$. Define

$$A = \{n \in U : 3 \mid n\}, \qquad B = \{n \in U : 5 \mid n\}.$$

   Then n is not coprime to 15 if and only if $n \in A \cup B$. We have

$$|A| = \frac{600}{3} = 200, \qquad |B| = \frac{600}{5} = 120, \qquad |A \cap B| = \frac{600}{15} = 40.$$

   By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 200 + 120 - 40 = 280.$$

   Therefore the number of n with $\gcd(n, 15) = 1$ is

$$|U| - |A \cup B| = 600 - 280 = 320.$$

3. Let U be the set of all linear arrangements of the 7 friends, so $|U| = 7!$. Define

$$A = \{\text{arrangements in which Alice is next to Charlie}\},$$
$$B = \{\text{arrangements in which Bob is next to Delia}\}.$$

We want to count the number of arrangements in U which are neither in A nor in B. The required number is $|U \setminus (A \cup B)| = |U| - |A \cup B|$.

To count $|A|$, treat {Alice, Charlie} as a single block. There are 6! ways to arrange the 6 "objects", and for each of these there are 2 ways to order Alice and Charlie within their block (either Alice or Charlie to the left). Hence

$$|A| = 2 \cdot 6!.$$

Similarly, $|B| = 2 \cdot 6!$.

To count $|A \cap B|$, treat both pairs {Alice, Charlie} and {Bob, Delia} as two single blocks. There are 5! ways to arrange the 5 objects (two blocks plus the other three people), and for each of these there are $2 \cdot 2$ internal orders of the two blocks. Hence

$$|A \cap B| = 4 \cdot 5!.$$

By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!.$$

Therefore

$$|U \setminus (A \cup B)| = 7! - (2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!) = 2640.$$

§42 — The Pigeonhole Principle

Epp 4th ed. pp. 554–565 · 5th ed. (metric) pp. 604–616. Lecture 33 (week 12).

Problems

1. (a) Explain why, in a group of 50 people, at least five people were born in the same month.

   (b) How many people do you need to ensure that at least seven people were born in the same month?

2. Show that, if we select six distinct integers from the set $\{1, 2, \ldots, 10\}$, two of these must add to give 11.

3. A computer network consists of six computers. Each computer is directly connected to zero or more of the other computers. Show that there are at least two computers in the network that are directly connected to the same number of other computers.

4. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

5. Let $S = \{1, 2, \ldots, 100\}$. What is the minimum number of integers you must pick from S to be sure that at least one pair has a difference which is divisible by 3?

Solutions

1. (a) There are 12 months (pigeonholes) and 50 people (pigeons). If each month had at most 4 birthdays, then there would be at most $12 \cdot 4 = 48$ people. Since $50 > 48$, by the pigeonhole principle some month must contain at least 5 people.

   (b) To guarantee at least 7 people are born in the same month, note that if each month had at most 6 birthdays, then there could be at most $12 \cdot 6 = 72$ people. Therefore with **73** people, by the pigeonhole principle some month has at least 7 people. Moreover, 72 people is not enough (take 6 born in each month), so the minimum is 73.

2. Partition $A = \{1, 2, \ldots, 10\}$ into the 5 pairs

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\},\ \{5, 6\},$$

   each summing to 11. In order for a selection of distinct integers from the set A to **not** have two that add to give 11, at most one integer can be chosen from each of the subsets. Choosing 6 distinct integers from A forces us to select two numbers from the same pair (there are 5 pairs but 6 choices), by the pigeonhole principle. Those two numbers then add to 11.

3. For each computer, let its **degree** be the number of other computers it is directly connected to. With 6 computers, each degree is an integer in $\{0, 1, 2, 3, 4, 5\}$. It is impossible to have both a computer of degree 0 and a computer of degree 5 (if one is connected to everyone, then none has degree 0). Hence the degrees must all lie in one of the two 5-element sets

$$\{0, 1, 2, 3, 4\} \quad \text{or} \quad \{1, 2, 3, 4, 5\}.$$

So, in either case, there are only 5 possible degree values available for 6 computers. By the pigeonhole principle, at least two computers have the same degree, i.e. are connected to the same number of other computers.

4. Let g_i be the total number of games played in the first i days, for $i = 1, 2, \ldots, 30$. Then

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

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

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

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

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

all lying in the set $\{1, 2, \ldots, 59\}$ of size 59. By the pigeonhole principle, two of these 60 integers are equal. Since the g_i are strictly increasing, no equality can occur among the g_i themselves, and likewise no equality can occur among the $g_i + 14$ themselves. Therefore we must have

$$g_j = g_i + 14$$

for some $i, j \in \{1, \ldots, 30\}$. Then the number of games played from day $i + 1$ through day j is

$$g_j - g_i = 14,$$

so there is a period of consecutive days during which exactly 14 games are played.

5. First, we note that two integers have a difference that is divisible by 3 if and only if they are congruent modulo 3 (have the same remainder when divided by 3). Now, the set S can be partitioned into three sets based on their congruence class modulo 3. By the pigeonhole principle, if we select **4** numbers from S, at least two of them must belong to the same congruence class. These two will have difference that is divisible by 3. Note that 4 is the minimum number of selections that guarantees this, since it is possible to select 3 numbers where no two of them have difference divisible by 3 (select one from each congruence class).

§43 — Introduction to Graph Theory

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 33 (week 12).

Problems

1. For each of the following, state whether or not there exists a simple graph with the stated number of vertices and degrees. Draw the graph, or explain why one does not exist.
   (a) Five vertices with degrees 3, 3, 2, 2, 2.
   (b) Seven vertices with degrees 4, 2, 3, 1, 1, 1, 1.
   (c) Five vertices with degrees 5, 4, 3, 1, 1.
2. A graph has 10 edges and 6 vertices. Five of the vertices have degree 3. What is the degree of the remaining vertex?
3. Let n be a positive integer and let K_n be the complete graph with n vertices. How many edges does K_n have?
4. A graph has 27 edges and every vertex has degree 2, 3 or 4. If there are 7 vertices that have degree 4 and 4 vertices that have degree 3, then how many vertices of degree 2 are there?

Solutions

1. (a) **Yes**, such a simple graph exists. One drawing has vertices a, b, c, d, e and the six edges

$$ab, \quad ac, \quad ad, \quad bc, \quad be, \quad de,$$

   giving $\deg(a) = 3$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 2$, $\deg(e) = 2$ as required.

   (b) **No** such graph exists. If the degrees are 4, 2, 3, 1, 1, 1, 1, then the sum of degrees is

$$4 + 2 + 3 + 1 + 1 + 1 + 1 = 13,$$

which is odd. Remember (by the Handshake Theorem) that the sum of the degrees in any graph equals twice the number of edges, and so is always even. So such a graph cannot exist.

(c) **No** such graph exists. In a simple graph on 5 vertices, the largest possible degree is 4, but the sequence contains a vertex of degree 5, which is impossible. So there is no such simple graph.

2. Since the graph has 10 edges, the sum of all the degrees is $2 \cdot 10 = 20$. If five vertices have degree 3, the sum of their degrees is $5 \cdot 3 = 15$, so the remaining vertex has degree

$$20 - 15 = 5.$$

3. In K_n, an edge is determined by choosing 2 distinct vertices, so the number of edges is

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

4. Let x be the number of vertices of degree 2. Since the graph has 27 edges, the sum of degrees is $2 \cdot 27 = 54$. Given that there are seven vertices of degree 4 and four vertices of degree 3, and all other vertices have degree 2, we have

$$2x + 4 \cdot 7 + 3 \cdot 4 = 54.$$

This means $x = 7$.

§44 — Walks, Trails and Circuits

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 34 (week 12).

Problems

1. Let G and H be the graphs below.

   G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is drawn with a **loop at** v_2, a **loop at** v_5, and **two parallel edges between** v_1 **and** v_2. Its degree sequence is

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   so G is connected with 10 edges.

   H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is a simple connected graph drawn as the 4-cycle $v_1v_2v_3v_4v_1$ with a single pendant edge v_3v_5, giving degrees

   $$\deg(v_1) = 2, \quad \deg(v_2) = 2, \quad \deg(v_3) = 3, \quad \deg(v_4) = 2, \quad \deg(v_5) = 1.$$

   For each of the following statements, explain why it is true or false.

   (a) G is a simple graph.

   (b) The sum of the degrees of the vertices of G is 18.

   (c) G contains an Euler circuit.

   (d) H contains an Euler trail.

2. Does the following graph contain an Euler circuit? (The graph shown is connected and has exactly two vertices of degree 3.)

3. Let G be a simple, connected, Eulerian graph with eight vertices and let e be the number of edges in G. Prove that $8 \leq e \leq 24$.

Solutions

1. (a) This statement is **false**. The graph G has loops (at v_2 and v_5) and it also has multiple edges between v_1 and v_2, so G is not simple.

   (b) This statement is **false**. A loop contributes 2 to the degree, so we have

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   and thus the sum of the degrees is $4 + 6 + 4 + 2 + 4 = 20 \neq 18$.

   (c) This statement is **true**. The graph G is connected and every vertex has even degree (as computed above), so G contains an Euler circuit.

(d) This statement is **true**. In H, the degrees are

$$\deg(v_1) = 2,\ \deg(v_2) = 2,\ \deg(v_4) = 2,\ \deg(v_3) = 3,\ \deg(v_5) = 1,$$

so exactly two vertices have odd degree (namely v_3 and v_5). Therefore H has an Euler trail (starting at one of v_3, v_5 and ending at the other).

2. **No.** The graph is connected, but has two vertices of degree 3, so not all vertices have even degree. Hence there is no Euler circuit.

3. Since G is connected and Eulerian, every vertex has even degree, and (because G is simple and connected with 8 vertices) each vertex has degree at least 2. Hence

$$2e = \sum_{v} \deg(v) \geq 8 \cdot 2 = 16,$$

so $e \geq 8$. Moreover, in a simple graph on 8 vertices we have $\deg(v) \leq 7$, and because G is Eulerian all degrees are even, so in fact $\deg(v) \leq 6$ for every vertex. Therefore

$$2e = \sum_{v} \deg(v) \leq 8 \cdot 6 = 48,$$

so $e \leq 24$. Hence $8 \leq e \leq 24$. □

§45 — Matrix Representations of Graphs

Epp 4th ed. pp. 661–675 · 5th ed. (metric) pp. 698–712. Lecture 35 (week 13).

Problems

1. Let G be the graph with vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{a, b, c, d, e, f\}$, where the edges are

edge	endpoints
a	$v_1 v_2$
b	$v_2 v_3$
c	$v_2 v_3$ (parallel to b)
d	$v_3 v_4$
e	$v_2 v_4$
f	loop at v_4

(a) Write down an adjacency matrix for G. Make sure you clearly label the rows and columns of your matrix.

(b) Write down an incidence matrix for G. Make sure you clearly label the rows and columns of your matrix.

(c) Does G have an Euler circuit? If yes, write it out as a sequence of vertices and edges. If not, determine the fewest number of edges that would need to be added to G to create a new graph that does have an Euler circuit.

2. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(a) Draw the graph G.

(b) Explain whether or not G has an Euler circuit or an Euler trail.

3. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Explain whether or not G is Eulerian.

Solutions

1. (a) The labelled adjacency matrix for G is

	v_1	v_2	v_3	v_4
$\mathbf{v_1}$	0	1	0	0
$\mathbf{v_2}$	1	0	2	1
$\mathbf{v_3}$	0	2	0	1
$\mathbf{v_4}$	0	1	1	1

(where the entry 1 on the diagonal at v_4 records the single loop at v_4).

(b) The labelled incidence matrix for G is

	a	b	c	d	e	f
$\mathbf{v_1}$	1	0	0	0	0	0
$\mathbf{v_2}$	1	1	1	0	1	0
$\mathbf{v_3}$	0	1	1	1	0	0
$\mathbf{v_4}$	0	0	0	1	1	2

(where the entry 2 in the bottom right indicates the loop that is incident twice with v_4).

(c) The degrees are

$$\deg(v_1) = 1, \quad \deg(v_2) = 4, \quad \deg(v_3) = 3, \quad \deg(v_4) = 4,$$

so G does **not** have an Euler circuit (since v_1 and v_3 have odd degree).

The fewest edges to add to make all degrees even is **1**; for example, adding an edge g between vertices v_1 and v_3 creates a new connected graph in which all of the vertices have even degree.

An example of an Euler circuit in the new graph is

$$v_1,\ a,\ v_2,\ b,\ v_3,\ d,\ v_4,\ f,\ v_4,\ e,\ v_2,\ c,\ v_3,\ g,\ v_1.$$

2. (a) Reading the matrix off (with vertices $v_1, \ldots, v_5$ in matrix order), G has the edges

- v_1v_2 — a single edge,
- v_1v_5 — **three** parallel edges,
- v_2v_3 — **two** parallel edges,
- v_3v_4 — a single edge,
- v_3v_5 — a single edge,
- v_4v_5 — a single edge.

(b) The degrees are

$$\deg(v_1) = 4,\ \deg(v_2) = 3,\ \deg(v_3) = 4,\ \deg(v_4) = 2,\ \deg(v_5) = 5,$$

so there is **no Euler circuit** (since v_2 and v_5 have odd degree), but there **is an Euler trail** (exactly two odd-degree vertices) from v_2 to v_5.

3. Let the vertices be $v_1, v_2, v_3, v_4, v_5, v_6$ in the order of the matrix. Reading the matrix off, G has edges

$$v_1v_2, \quad v_1v_4, \quad v_2v_4, \quad v_3v_5, \quad v_3v_6, \quad v_5v_6,$$

that is, two disjoint triangles: one on $\{v_1, v_2, v_4\}$ and one on $\{v_3, v_5, v_6\}$.

The graph is **not connected** (e.g. there is no walk from vertex v_1 to vertex v_3). Hence G is not Eulerian.

(Errata note: the source document's solution to 1(b) was corrected on 11 August 2026 — the note in brackets had previously copied the note from 1(a). The corrected note is the one given above.)

§46 — Trees

Epp 4th ed. pp. 683–701 · 5th ed. (metric) pp. 720–742. Lecture 36 (week 13).

Problems

1. A tree has 11 vertices, of which exactly four vertices have degree 1 and exactly one vertex has degree 4. Determine the degrees of the remaining six vertices.
2. Let T be a tree with p vertices, where $p \geq 11$. Suppose T has precisely six vertices of degree 1 and precisely four vertices of degree 3. Determine the degree of each of the remaining $p - 10$ vertices of T.
3. Let T be a tree on 12 vertices. Suppose T has exactly three vertices of degree 3 and each of the remaining vertices has degree 1 or 5. Using theorems that were given in lectures, determine the number of vertices of degree 5.
4. Two trees with the same vertex set $\{1, 2, \ldots, n\}$ are **distinct** if their edge sets are not equal. Use mathematical induction to prove that for each integer $n \geq 2$, the number of distinct trees with vertex set $\{1, 2, \ldots, n\}$ is at least $(n-1)!$.

Solutions

1. A tree with 11 vertices has $e = 10$ edges, so by the Handshake Theorem, the sum of degrees is $2e = 20$. We are given that exactly four vertices have degree 1 and exactly one vertex has degree 4. Let $v_1, v_2, \ldots, v_6$ be the remaining vertices whose degrees are to be determined. We have

$$\sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20$$

$$\sum_{i=1}^{6} \deg(v_i) = 12.$$

None of these six vertices $v_1, v_2, \ldots, v_6$ can have degree 1 (since there are exactly four vertices of degree 1, already accounted for). Hence each has degree at least 2. Because six vertices of degree at least 2 have total degree 12, each must have degree exactly 2.

Thus the remaining six vertices all have **degree 2**.

2. T is a tree with p vertices and so must have $p-1$ edges. Now by the Handshake Theorem we know

$$2(p-1) = \sum_{i=1}^{p} \deg(v_i).$$

Using the known degrees we can write this as

$$\begin{aligned} 2(p-1) &= 6 \cdot 1 + 4 \cdot 3 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-1) &= 18 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2p - 2 - 18 &= \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-10) &= \sum_{i=1}^{p-10} \deg(v_i). \end{aligned}$$

Rewriting the final line as

$$\frac{\sum_{i=1}^{p-10} \deg(v_i)}{p-10} = 2, \qquad \text{i.e.} \qquad \frac{\deg(v_1) + \deg(v_2) + \cdots + \deg(v_{p-10})}{p-10} = 2,$$

we see that the average degree of the remaining $p-10$ vertices is 2. However, we know that there are no more vertices of degree 1. Thus each of the remaining $p-10$ vertices must have **degree exactly 2**.

3. Let x be the number of vertices of degree 5 and y the number of vertices of degree 1. Then, because the tree has 12 vertices, we have

$$x + y + 3 = 12.$$

This simplifies to give $x + y = 9$.

Now, since T is a tree on 12 vertices, it must have $e = 11$ edges. By the Handshake Theorem, the sum of degrees is $2e = 22$, so

$$3 \cdot 3 + 5x + 1 \cdot y = 22.$$

This simplifies to give $5x + y = 13$.

Subtracting $x + y = 9$ from $5x + y = 13$ gives $4x = 4$, hence $x = 1$. Therefore there is exactly **one** vertex of degree 5.

4. We prove by induction that the number of distinct trees with vertex set $\{1, 2, \dots, n\}$ is at least $(n-1)!$.

Basis: let $n = 2$. Here $(n-1)! = (2-1)! = 1$. There is exactly one tree on $\{1, 2\}$, namely the single edge $\{1, 2\}$. So the base case is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and there are at least $(k-1)!$ distinct trees on $\{1, 2, \dots, k\}$.

Now consider $n = k + 1$. We aim to show that there are at least $k!$ distinct trees on vertex set $\{1, 2, \dots, k, k+1\}$.

Let T be a tree on vertex set $\{1, 2, \dots, k\}$. For any choice of $m \in \{1, 2, \dots, k\}$, we form a graph T_m on vertex set $\{1, 2, \dots, k, k+1\}$ as follows: start with tree T, add a new vertex $k+1$, and the edge $\{k+1, m\}$.

Note that T_m is connected (since $k+1$ is joined to m, and T was connected). Also, T_m has no circuit because T is a tree and adding a new leaf does not create a circuit. Thus T_m is a tree. Moreover, different choices of m give rise to distinct trees T_m, because their edge sets are different.

By the inductive hypothesis, there are at least $(k-1)!$ choices for the tree T. Since there are k choices for the vertex m, there are at least $k \cdot (k-1)! = k!$ trees T_m on vertex set $\{1, 2, \dots, k+1\}$.

By the principle of mathematical induction, this completes the proof. $\square$

See also

- math1061[172] — assessment weights and the full lecture schedule
- Logic: logical-connectives[173] · logical-equivalence-laws[174] · conditional-statements[175] · valid-argument-forms[176] · determining-argument-validity[177] · quantified-statements[178]
- Number theory and proof: proof-techniques[179] · rational-and-irrational-numbers[180] · divisibility-and-factorisation[181] · modular-arithmetic[182] · gcd-lcm-and-euclidean-algorithm[183]
- Graph theory (§43–§46): [graphs] · walks-trails-and-circuits[184] · euler-circuits-and-trails[185] · adjacency-matrices[186] · incidence-matrices[187] · [trees]

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)
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 $s = 1)$

[172] courses/math1061/math1061.pdf
[173] courses/math1061/logical-connectives.pdf
[174] courses/math1061/logical-equivalence-laws.pdf
[175] courses/math1061/conditional-statements.pdf
[176] courses/math1061/valid-argument-forms.pdf
[177] courses/math1061/determining-argument-validity.pdf
[178] courses/math1061/quantified-statements.pdf
[179] courses/math1061/proof-techniques.pdf
[180] courses/math1061/rational-and-irrational-numbers.pdf
[181] courses/math1061/divisibility-and-factorisation.pdf
[182] courses/math1061/modular-arithmetic.pdf
[183] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[184] courses/math1061/walks-trails-and-circuits.pdf
[185] courses/math1061/euler-circuits-and-trails.pdf
[186] courses/math1061/adjacency-matrices.pdf
[187] courses/math1061/incidence-matrices.pdf

Term	Definition
n is **composite**	$n \in \mathbb{Z}$, $n > 1$, and $\exists r, s \in \mathbb{Z}^+$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$
r is **rational**	$\exists a, b \in \mathbb{Z}$ such that $r = \frac{a}{b}$ and $b \neq 0$
$d \mid n$	$d \neq 0$ and $n = dk$ for some integer k

Two facts used constantly, and worth naming explicitly when you lean on them:

- **Fact**: the sum, difference, and product of integers is an integer.
- **Fact**: every integer is either even or odd.

Parity

Almost every early proof in this course turns on whether something is even or odd, so the consequences of those two definitions are worth having ready rather than re-deriving:

	Result
even + even, odd + odd	even
even + odd	odd
even× anything	even
odd × odd	odd
consecutive integers	opposite parity — so two integers **two apart share their parity**

Each row follows from the two definitions by a one-line substitution. Subtraction behaves like addition throughout, since $m - n$ and $m + n$ differ by $2n$.

The "two apart" row is the whole content of the warm-up in 2026-07-27-welcome-and-intro-problems[188], where consecutive $p < q < r$ forces $p + r$ to be even and $r - p$ to be exactly 2, while pr is free to be either.

Prime vs. not-prime. For $n \in \mathbb{Z}^{>1}$, "n is not prime" means "n is composite". For $n \in \mathbb{Z}$ generally, "n is not prime" means "n is composite **or** $n \leq 1$" — the integers split into $\mathbb{Z}^{\leq 1}$, $\mathbb{Z}^{\text{prime}}$, and $\mathbb{Z}^{\text{composite}}$, and 1 and everything below it is in none of the latter two. This is why $n = 1$ is the standard counterexample to "every positive integer is prime or composite".

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

[188] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf

The four methods

All four target $\forall x \in D, P(x) \to Q(x)$. Recall the truth table for $p \to q$ — the only row that makes it false is p true, q false:

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

Every method below is a different way of attacking that one row.

Direct proof (shows the statement is true)

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

Why suppose $P(x)$ is true, when $P(x) \to Q(x)$ holds anyway if $P(x)$ is false? Because the only case that could make the statement false is $P(x)$ true and $Q(x)$ false. Ruling that out is the whole job — the $P(x)$-false rows are true for free.

Disproof by counterexample (shows the statement is false)

> Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true. However, $Q(x)$ is false. So x is a counterexample and the statement is false.

A counterexample to $p \to q$ needs p **true** and q **false** — a value where the hypothesis fails proves nothing.

Proof by contradiction (shows the statement is true)

> Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true. That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false. ... Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$. This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. $\square$

The set-up comes straight from quantified-statements[189]: the negation of $\forall x \in D, P(x) \to Q(x)$ is $\exists x \in D$ such that $P(x) \wedge \sim Q(x)$.

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

Proofs of the statement $\forall x \in D,\ P(x) \to Q(x)$

Direct proof:

Let $x \in D$ and suppose $P(x)$.

...

Hence $Q(x)$. □

Shows the statement is true.

Disproof by counterexample:

Let $x = \cdots$. Then $x \in D$ and $P(x)$ is true.

However, $Q(x)$ is false.

So x is a counterexample and the statement is false.

Shows the statement is false.

Proof by contradiction:

Suppose the negation of $\forall x \in D, P(x) \to Q(x)$ is true.

That is, suppose $\exists x \in D$ such that $P(x)$ is true but $Q(x)$ is false.

...

Hence something that is obviously wrong, like $P(x)$ is false, or $Q(x)$ is true, or $1 = 0$.

This is a contradiction, and we conclude that $\forall x \in D, P(x) \to Q(x)$ is true. □

Shows the statement is true.

Proof by contraposition:

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

Let $x \in D$ and suppose $\sim Q(x)$.

...

Hence, $\sim P(x)$. □

Figure 46: The skeletons of the four methods for a statement of the form x D, P(x) → Q(x). Three of the four establish the statement and one demolishes it, which is what the red verdict lines record.

Useful negations to have ready (see logical-equivalence-laws[190]):

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

Proof by contraposition (shows the statement is true)

> We prove the contrapositive of $\forall x \in D, P(x) \to Q(x)$, namely that $\forall x \in D, \sim Q(x) \to \sim P(x)$. Let $x \in D$ and suppose $\sim Q(x)$. ... Hence, $\sim P(x)$. $\square$

This is valid because $p \to q \equiv \sim q \to \sim p$ (see conditional-statements[191]).

Choosing a method

- **Contradiction is the most versatile**, but it needs more set-up, so a direct proof is often easier when one is available.
- **Contraposition** is the natural choice when $\sim Q(x)$ gives you something concrete to work with and $P(x)$ doesn't — typically when the conclusion is a negative statement ("r is irrational", "n is odd") whose negation is a definition you can expand.
- **Contradiction vs. contraposition**: a contraposition proof is a contradiction proof that never actually needs the assumption $P(x)$ — you derive $\sim P(x)$ from $\sim Q(x)$ alone. If your "contradiction" proof only ever uses the $\sim Q(x)$ half of the assumption, write it as a contraposition instead.
- **Counterexample vs. contradiction**: counterexample is a **disproof**, contradiction is a **proof**. They are not variants of each other.

Worked comparisons on the same statements live in the lecture notes: 2026-08-13-proof-by-contradiction[192] 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[193] 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.

[190] courses/math1061/logical-equivalence-laws.pdf
[191] courses/math1061/conditional-statements.pdf
[192] courses/math1061/2026-08-13-proof-by-contradiction.pdf
[193] courses/math1061/2026-08-13-proof-by-contraposition.pdf

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

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

Since $k \in \mathbb{Z}$, we have $3k + 2 \in \mathbb{Z}$, and hence $3n + 2$ is odd. □

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

Let $x \in \mathbb{Z}$ and suppose $x + 6 = 4y$ for some $y \in \mathbb{Z}$. Then $x = 4y - 6 = 2(2y - 3)$, so

$$\frac{x}{2} = \frac{2(2y-3)}{2} = 2y - 3 = 2(y-1) - 1.$$

Since $y \in \mathbb{Z}$ we have $2y - 3 \in \mathbb{Z}$, so $\frac{x}{2} \in \mathbb{Z}$; and $y - 1 \in \mathbb{Z}$, so by definition $\frac{x}{2}$ is odd. □

The sum of any pair of even integers is even.

Let $m, n \in \mathbb{Z}$ be even. Then $m = 2k$ and $n = 2\ell$ for some $k, \ell \in \mathbb{Z}$. Hence $m + n = 2k + 2\ell = 2(k + \ell)$, which is even. □

$\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

Suppose $n \in \mathbb{Z}^+$ and $n \geq 4$. Factor $2n^2 - 5n + 2 = (2n-1)(n-2)$. Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers greater than 1. Hence the expression is composite. □

Disproof by counterexample

- **For all integers m and n, if $2m + n$ is odd then m and n are both odd.** Counterexample $m = 4, n = 5$: $2(4) + 5 = 13$ is odd, but m is even. (Not $m = 3, n = 5$ — there the conclusion holds; not $m = 3, n = 6$ or $m = 4, n = 6$ — there the hypothesis fails.)
- **$\forall n \in \mathbb{Z}^{\geq 2}$, n is composite or $n+1$ is composite.** Take $n = 2$: both 2 and 3 are prime.
- **For each integer $n \geq 2$, the product of the first n primes minus 1 is prime.** Take $n = 4$: $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, composite.
- **$\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.** Take $x = 1, y = -2$: $4 > 1$ but $-2 \not> 1$.
- **$\forall x \in \mathbb{R}, \lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** Take $x = \frac{3}{2}$: $\lfloor \frac{9}{4} \rfloor = 2$ but $\lfloor \frac{3}{2} \rfloor^2 = 1$. (See modular-arithmetic[194] for the floor function.)

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

Disproof by proving the negation

When the statement to disprove is existential, a single counterexample isn't available — you must prove the universal negation.

$\exists n \in \mathbb{Z}^+$ **such that** $n^2 + 5n + 6$ **is prime.** This is false; the negation is $\forall n \in \mathbb{Z}^+$, $n^2 + 5n + 6$ is composite.

> Let $n \in \mathbb{Z}^+$. Now $n^2 + 5n + 6 = (n + 2)(n + 3)$. Since $n \geq 1$ we have $n + 2 > 1$ and $n + 3 > 1$, so $n^2 + 5n + 6$ is composite. □

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

There is an even integer n **such that** $5n - 4$ **is prime.** False; prove $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

> Suppose n is even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $5n - 4 = 10k - 4 = 2(5k - 2)$, which is even. The only even prime is 2; if $2(5k-2) = 2$ then $k = \frac{3}{5} \notin \mathbb{Z}$. Therefore $5n - 4$ is not prime. □

Proof by contradiction

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

> Suppose $\exists m, n \in \mathbb{Z}$ such that mn is even and both m and n are odd. Since m is odd, $m = 2k + 1$ for some $k \in \mathbb{Z}$; since n is odd, $n = 2\ell + 1$ for some $\ell \in \mathbb{Z}$ — **a new variable**, since m and n need not be equal. Now
>
> $$mn = (2k + 1)(2\ell + 1) = 4k\ell + 2k + 2\ell + 1 = 2(2k\ell + k + \ell) + 1.$$
>
> Since $k, \ell \in \mathbb{Z}$, $2k\ell + k + \ell \in \mathbb{Z}$, so mn is odd. It is impossible for mn to be both even and odd, a contradiction. Therefore the original statement is true. □

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

> Suppose the statement is false: $\exists n \in \mathbb{Z}$ such that $3n^3 - 2$ is odd and n is even. Since n is even, $n = 2a$ for some $a \in \mathbb{Z}$. Then
>
> $$3n^3 - 2 = 3(2a)^3 - 2 = 24a^3 - 2 = 2(12a^3 - 1).$$
>
> Since $a \in \mathbb{Z}$, $12a^3 - 1 \in \mathbb{Z}$, so $3n^3 - 2$ is even — a contradiction. Therefore the original statement is true. □

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

Suppose the statement is false. Then $\exists m, n \in \mathbb{Z}$ such that $m+n$ is even but exactly one of m, n is even. **Without loss of generality**, assume m is even and n is odd — the other case (m odd, n even) follows because $m+n = n+m$. Thus $m = 2a$ for some $a \in \mathbb{Z}$ and $n = 2b+1$ for some $b \in \mathbb{Z}$. Now $m+n = 2a+2b+1 = 2(a+b)+1$, and $a+b \in \mathbb{Z}$, so $m+n$ is odd. This contradicts the assumption that $m+n$ is even. Therefore the original statement is true. □

For integers a and b, if $6a+3b$ is odd, then b is odd.

Suppose there exist integers a, b with $6a+3b$ odd and b even. Then $b = 2k$ for some $k \in \mathbb{Z}$, so $6a+3b = 6a+6k = 2(3a+3k)$, which is even — contradicting that $6a+3b$ is odd. □

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

Suppose $x, y \in \mathbb{Z}^+$ with $x^2 - y^2 = 1$. Factoring, $1 = (x-y)(x+y)$. Since x, y are positive integers we must have $x-y = 1$ and $x+y = 1$, so $2x = 2$ and $x = 1$; then $y = 0$, which is not a positive integer — a contradiction. □

Proof by contraposition

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

We prove the contrapositive: $\forall r \in \mathbb{R}$, if $r \in \mathbb{Q}$ then $r^2 \in \mathbb{Q}$. Suppose $r \in \mathbb{R}$ with $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$. Now $r^2 = \frac{a^2}{b^2}$. Since $a, b \in \mathbb{Z}$ we have $a^2, b^2 \in \mathbb{Z}$, and $b^2 \neq 0$ since $b \neq 0$. So $r^2 \in \mathbb{Q}$. □

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

We prove the contrapositive: $\forall m, n \in \mathbb{Z}$, if at least one of m, n is even then mn is even. Without loss of generality, assume m is even, so $m = 2k$ for some $k \in \mathbb{Z}$. Now $mn = (2k)n = 2(kn)$, and $kn \in \mathbb{Z}$, so mn is even. □

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

Contrapositive: if a is even or b is even, then $(ab)^2$ is even. WLOG suppose a is even, so $a = 2k$ for some $k \in \mathbb{Z}$. Then $ab = 2kb$ and $(ab)^2 = 4k^2b^2 = 2(2k^2b^2)$. Since $k, b \in \mathbb{Z}$, $2k^2b^2 \in \mathbb{Z}$, so $(ab)^2$ is even. □

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

Contrapositive: if x is even or y is even, then $x^2(y^2-2y)$ is even. Here the two cases need separate treatment.

Case 1: x even. $x = 2k$ for some $k \in \mathbb{Z}$, so $x^2(y^2-2y) = 4k^2(y^2-2y) = 2(2k^2(y^2-2y))$, and $2k^2(y^2-2y) \in \mathbb{Z}$.

Case 2: y even. $y = 2\ell$ for some $\ell \in \mathbb{Z}$, so $x^2(y^2 - 2y) = x^2(4\ell^2 - 4\ell) = 2(x^2(2\ell^2 - 2\ell))$, and $x^2(2\ell^2 - 2\ell) \in \mathbb{Z}$.

In both cases $x^2(y^2 - 2y)$ is even. □

For any integer n, n^2 is odd if and only if n is odd. A biconditional needs both directions, and they want different methods:

($\Leftarrow$, direct) Suppose n is odd, so $n = 2k+1$. Then $n^2 = 4k^2+4k+1 = 2(2k^2+2k)+1$ is odd.

($\Rightarrow$, contraposition) The contrapositive is: if n is even then n^2 is even. Suppose $n = 2k$. Then $n^2 = 4k^2 = 2(2k^2)$ is even. □

This lemma — **for all integers n, if n^2 is even then n is even** — is used in the proof that $\sqrt{2}$ is irrational (see rational-and-irrational-numbers[195]).

Common proof errors

The course explicitly tests spotting these. The seven below are the list given with the practice problems' §9 Q3 (see practice-problems[196], where the four proofs you are asked to find the errors in are worked):

- **Arguing from examples** — a single example never establishes a universal statement. ("$\forall x \in \mathbb{R}, \exists y \in \mathbb{R}$ s.t. $xy = 1$. Proof: if $x = 10$ take $y = \frac{1}{10}$." Not a proof — and the statement is false, since $x = 0$ has no such y.)
- **Using the same variable to mean two different things** — "let $m = 2k + 1$ and $n = 2k$" only proves the case $m = n + 1$. Use a fresh variable for each quantity.
- **Jumping to the conclusion** — writing down the definition you need to satisfy and then asserting it holds, without exhibiting the witnesses.
- **Assuming what is to be proved** — starting from "$4a + 2b = 2\ell$" and manipulating both sides assumes the conclusion. Derive the conclusion; don't begin with it.
- **Confusion between what is known and what is to be shown.**
- **Use of the word *any* instead of *some*.**
- **Misuse of the word *if*.**

One more, not on that list: **forgetting to state your assumptions**, or forgetting to say where a variable lives ("for some $r, s \in \mathbb{Z}$"). Introduce every existential witness with its domain.

[195] courses/math1061/rational-and-irrational-numbers.pdf
[196] courses/math1061/practice-problems.pdf

See also

- quantified-statements[197] — the negations these proofs are built on
- conditional-statements[198] · logical-equivalence-laws[199]
- 2026-07-27-welcome-and-intro-problems[200] — the parity warm-up, the course's first proof-shaped problem
- proving-set-properties[201] — the element method, and these techniques applied to sets
- rational-and-irrational-numbers[202] · divisibility-and-factorisation[203]
- practice-problems[204] — §9 Direct Proofs and Counterexamples, with full worked solutions
- practice-problems[205] — §10 Proof by Contradiction, with full worked solutions
- practice-problems[206] — §11 Proof by Contraposition, with full worked solutions

Strong Induction and the Well-Ordering Principle

Strong mathematical induction, the well-ordering principle for the integers, and the sense in which these two and ordinary induction are all the same tool. See mathematical-induction[207] for ordinary induction and the four-step proof template both methods share.

Strong mathematical induction

Let $P(n)$ be a predicate written in terms of some integer n. The difference from ordinary induction is entirely in what the inductive step is allowed to assume: **every** earlier case, not just the immediately preceding one — and, to pay for that, a basis step that establishes several cases rather than one.

	Ordinary induction (MI)	Strong induction (SMI)
Basis step	$P(2)$	$P(2) \wedge P(3) \wedge P(4)$
Inductive step	$\forall k \in \mathbb{Z}$ with $k \geq 2$, if $P(k)$ then $P(k+1)$	$\forall k \in \mathbb{Z}$ with $k \geq 4$, if $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$ then $P(k+1)$
Conclusion	$P(n)$ for each integer $n \geq 2$	$P(n)$ for each integer $n \geq 2$

[197] courses/math1061/quantified-statements.pdf
[198] courses/math1061/conditional-statements.pdf
[199] courses/math1061/logical-equivalence-laws.pdf
[200] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[201] courses/math1061/proving-set-properties.pdf
[202] courses/math1061/rational-and-irrational-numbers.pdf
[203] courses/math1061/divisibility-and-factorisation.pdf
[204] courses/math1061/practice-problems.pdf
[205] courses/math1061/practice-problems.pdf
[206] courses/math1061/practice-problems.pdf
[207] courses/math1061/mathematical-induction.pdf

Both reach the same conclusion by the same kind of chain. For MI, $P(5)$ follows from $P(2)$ by three applications of the implication; for SMI with the basis above, $P(6)$ follows in two.

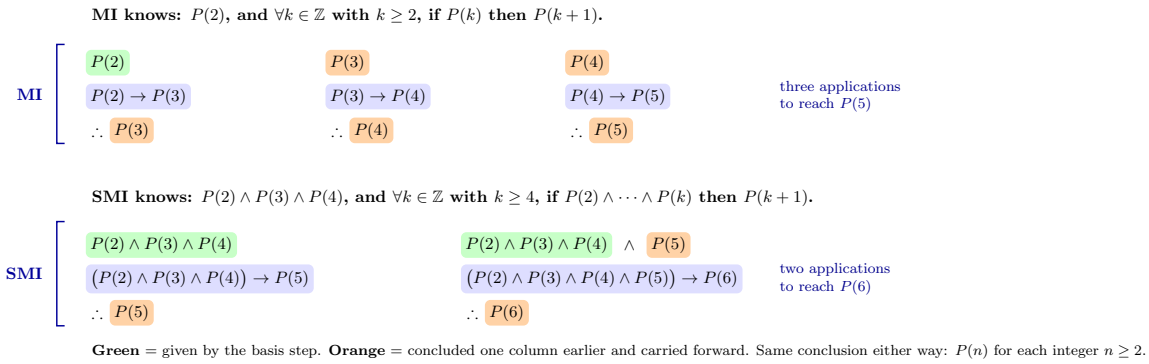


Figure 47: Mathematical induction and strong mathematical induction as chains of inferences. Each column is an argument — premises stacked, conclusion prefixed by $\therefore$, no rule line. MI climbs one rung at a time from a single base case; SMI starts from three base cases and each step may lean on everything established so far, which is why it lands on P(6) in two moves rather than four. Colour tracks one expression as it moves: green is what the basis step supplies, orange is a statement concluded one column earlier and carried forward. There are no arrows between columns — the repeated colour alone shows where a statement moves.

How many base cases?

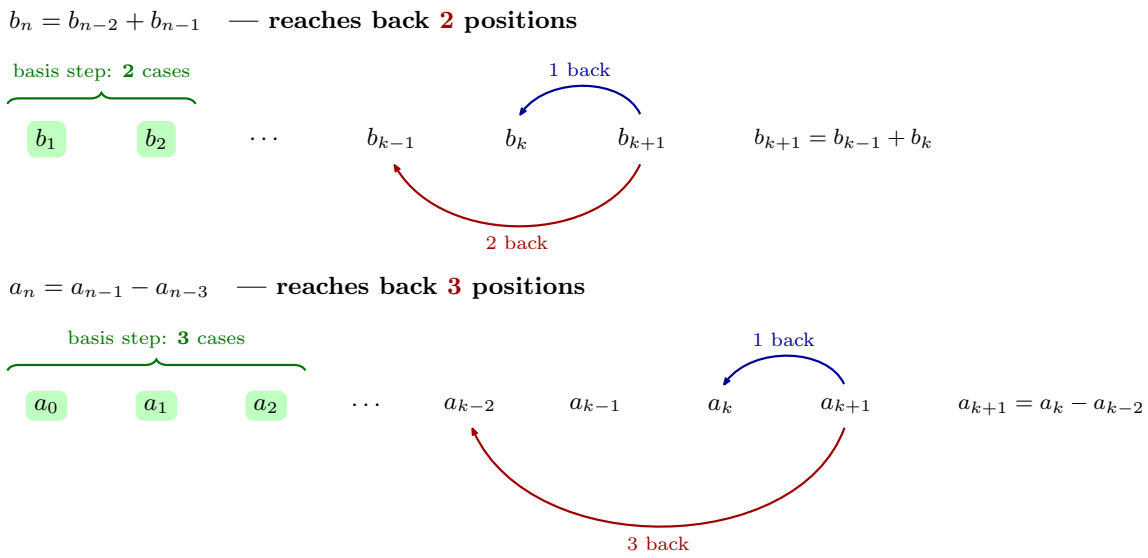
As many as the inductive step reaches back for. This is the whole reason the basis step of an SMI proof is not a single case, and the answer to "why two values and not three?"

Count *how far back* the recurrence reaches, not how many terms it uses — those differ. $a_n = a_{n-1} - a_{n-3}$ uses only two earlier terms, but the deepest is three positions back, so all three of $P(0), P(1), P(2)$ must be established or the step could reach for an unproven case.

If the basis step establishes fewer cases than the inductive step consumes, the chain has a hole in it: the first few applications of the inductive step would reach for a case nobody ever proved.

Worked example — a two-term recurrence

Suppose $b_1, b_2, b_3, \ldots$ is defined by $b_1 = 4$, $b_2 = 12$, and $b_n = b_{n-2} + b_{n-1}$ for each integer $n \geq 3$. Prove that $4 \mid b_n$ for each integer $n \geq 1$.



The longest arrow sets the count, not the number of arrows: both recurrences use exactly two earlier terms, but the second reaches three positions back, so it needs three base cases.

Figure 48: How many base cases a strong induction needs, on the two sequences worked below: b_n = b_{n-2} + b_{n-1} and a_n = a_{n-1} − a_{n-3}. Both use exactly two earlier terms, so counting terms gives the wrong answer; what settles it is the longest arrow. Reaching two positions back means the basis step must cover two cases; reaching three means three. The terms sit in a row, and each short curved arrow is labelled with what it does.

Proof. Let $P(n)$ be the predicate $4 \mid b_n$.

Basis step. We know that $b_1 = 4$ and $b_2 = 12$. Since $4 \mid 4$ and $4 \mid 12$, $P(1)$ is true and $P(2)$ is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(1), P(2), \ldots, P(k)$ are true. Since $P(k)$ is true, $b_k = 4x$ for some $x \in \mathbb{Z}$. Since $P(k-1)$ is true, $b_{k-1} = 4y$ for some $y \in \mathbb{Z}$.

Inductive step. Consider $n = k + 1$:

$$\begin{aligned} b_{k+1} = b_{k-1} + b_k &= 4y + 4x \qquad \text{(by the inductive hypothesis)} \\ &= 4(y + x) \end{aligned}$$

Thus $4 \mid b_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 1$, $4 \mid b_n$. □

Note where strong induction actually earns its keep: the step uses $P(k)$ **and** $P(k-1)$. Ordinary induction only hands you $P(k)$, which is not enough to say anything about b_{k-1}.

Worked example — every integer $n > 1$ is a product of primes

Theorem. Every integer $n > 1$ can be written as a product of primes.

Proof. Let $P(n)$ be the predicate *n can be written as a product of primes*, for $n \geq 2$.

Basis step. $n = 2$ is prime and thus is a product of primes, so $P(2)$ is true.

Inductive step. Suppose that for some integer $k \geq 2$, every integer $2, 3, \ldots, k$ can be written as a product of primes — that is, $P(2) \wedge P(3) \wedge \cdots \wedge P(k)$. We now need to prove that $k + 1$ is a product of primes. Since $k + 1 > 1$, either $k + 1$ is prime or $k + 1$ is composite.

- *Case 1: $k + 1$ is prime.* Then $k + 1$ is a product of primes.
- *Case 2: $k + 1$ is composite.* Then $k + 1 = rs$ for some positive integers $r \neq 1$ and $s \neq 1$. This implies $1 < r < k + 1$ and $1 < s < k + 1$. So by the inductive hypothesis — specifically $P(r)$ and $P(s)$ — both r and s are products of primes. Let $r = p_1 p_2 \ldots p_a$ and $s = q_1 q_2 \ldots q_b$ where the p_i and q_j are primes; thus $k + 1 = rs = p_1 p_2 \ldots p_a q_1 q_2 \ldots q_b$ is a product of primes.

In either case, $k + 1$ is a product of primes.

Therefore, by SMI, every integer $n > 1$ can be written as a product of primes. □

Why strong induction and not ordinary induction? Because r and s can be *any* integers from 2 to k — the factorisation gives no control over which — so the proof needs the inductive hypothesis available at all of those values, not just at k.

The well-ordering principle for the integers

> Let S be a **non-empty** set of integers, each of which is **greater than some fixed integer**. Then S has a **least element**.

Four pieces of terminology, all load-bearing:

- **non-empty** — the empty set has no least element, trivially.
- **of integers** — not of rationals or reals. This clause is not decoration: the positive rationals are non-empty *and* bounded below by 0, and still have no least element, because between any candidate and 0 there is always another one (halve it). See 2026-08-27-strong-induction-and-well-ordering[208].
- **greater than some fixed integer** — S must be bounded below. Without this the principle fails: $\mathbb{Z}^-$ is a non-empty set of integers with no least element.
- **a least element** — an element *of* S that is $\leq$ every element of S. It lives inside the set, not outside it.

Example — integers congruent to 1 mod 4

True or false? The set of all integers congruent to 1 mod 4 **has a least element.**

False. The set is $\{\dots, -7, -3, 1, 5, 9, \dots\}$.

> Suppose this set did have a least element, call it x. Then, since $x \equiv 1 \pmod 4$, we have $x - 4 \equiv 1 \pmod 4$, so $x - 4$ is also in the set. But $x - 4$ is smaller than x — a contradiction. $\square$

The set is non-empty, but it fails the "bounded below" condition, so the well-ordering principle simply does not apply to it.

MI, SMI and the WOP are equivalent

Anything provable by one is provable by the other two. Two of the translations:

SMI $\to$ MI: reword the statement. A strong-induction proof of $P(n)$ becomes an ordinary-induction proof of the *accumulated* predicate

[208] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf

$$Q(n) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$$

Assuming $Q(k)$ in ordinary induction gives you exactly what assuming $P(0), \ldots, P(k)$ gave you in strong induction. (Epp, Q27 p. 279.)

MI $\rightarrow$ WOP: argue by contradiction. Suppose the set of integers $\geq a$ for which $P(n)$ is *false* is non-empty. It is bounded below by a, so by the WOP it has a least element; derive a contradiction from that least element. (Epp, Q31 p. 279.)

The same theorem, three ways

Suppose $a_0, a_1, a_2, \ldots$ is defined by $a_0 = 6$, $a_1 = 9$, $a_2 = 12$ and $a_n = a_{n-1} - a_{n-3}$ for each integer $n \geq 3$. Prove that for all integers $n \geq 0$, $3 \mid a_n$.

By SMI.

Let $P(n)$ be the predicate $3 \mid a_n$.

Basis step. $a_0 = 6$, $a_1 = 9$ and $a_2 = 12$. Since $3 \mid 6$, $3 \mid 9$ and $3 \mid 12$, $P(0)$, $P(1)$ and $P(2)$ are true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $P(0), P(1), \ldots, P(k)$ are true. Since $P(k-2)$ is true, $a_{k-2} = 3y$ for some $y \in \mathbb{Z}$; since $P(k)$ is true, $a_k = 3x$ for some $x \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$, so $P(k+1)$ is true.

Therefore, by PSMI, for each integer $n \geq 0$, $3 \mid a_n$. $\square$

By MI, on the reworded predicate.

Let $Q(n)$ be the predicate $3 \mid a_j$ *for all integers* j *where* $0 \leq j \leq n$ — that is, $Q(n) \equiv P(0) \wedge P(1) \wedge \cdots \wedge P(n)$.

Basis step. Consider $n = 2$. Since $3 \mid a_0$, $3 \mid a_1$ and $3 \mid a_2$, $Q(2)$ is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and that $Q(k)$ is true. Since $Q(k)$ is true and $k \geq 2$, $a_k = 3x$ and $a_{k-2} = 3y$ for some $x, y \in \mathbb{Z}$.

Inductive step. Consider $n = k+1$: $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$. Thus $3 \mid a_{k+1}$. Since $Q(k)$ already gives $3 \mid a_i$ for every $0 \leq i \leq k$, adding $3 \mid a_{k+1}$ gives $Q(k+1)$.

(That last step is the point of rewording the predicate: $Q(k+1)$ is a conjunction over *all* indices up to $k+1$, so it needs $Q(k)$ **and** the new case — $3 \mid a_{k+1}$ alone would not establish it.)

Therefore, by PMI, for each integer $n \geq 0$, $3 \mid a_n$. $\square$

The two proofs have the *same* algebraic core: the line $a_{k+1} = a_k - a_{k-2} = 3x - 3y = 3(x-y)$ is identical in each. All the reworded predicate does is let a single assumption, $Q(k)$, carry the several earlier facts the algebra needs.

Two details of the MI proof are easy to get wrong:

- **The basis is $n = 2$, not $n = 0$.** $Q(2)$ already asserts $3 \mid a_0$, $3 \mid a_1$ *and* $3 \mid a_2$, so verifying $Q(2)$ discharges all three of the SMI proof's base cases in one statement. Three base cases have not disappeared; they have been packed into one predicate.
- **The step concludes $Q(k+1)$, not $P(k+1)$.** An ordinary induction on Q has to deliver $Q(k+1)$, and $3 \mid a_{k+1}$ on its own does not — it needs $Q(k)$ alongside it.

The conjunction in Q starts at $P(0)$, not $P(1)$. The predicate is $3 \mid a_j$ *for all integers j where* $0 \leq j \leq n$, so $Q(2) \equiv P(0) \wedge P(1) \wedge P(2)$ — which is also what the basis step checks.

By the WOP, by contradiction.

> Suppose the statement is false, so there exists an integer $n \geq 0$ such that 3 does not divide a_n. Let
>
> $$A = \{\, n \in \mathbb{Z}^{\geq 0} \;:\; 3 \nmid a_n \,\}$$
>
> By the WOP and our assumption, A has a least element — the smallest n for which $3 \nmid a_n$. Call it k. Thus $3 \nmid a_k$, but $3 \mid a_i$ for all $0 \leq i \leq k-1$.
>
> Note that $k \geq 3$, since a_0, a_1 and a_2 are all divisible by 3.
>
> Thus $a_{k-1} = 3x$ and $a_{k-3} = 3y$ for some $x, y \in \mathbb{Z}$, so
>
> $$a_k = a_{k-1} - a_{k-3} = 3x - 3y = 3(x-y)$$
>
> Thus $3 \mid a_k$, which is a contradiction.
>
> Therefore, for each integer $n \geq 0$, $3 \mid a_n$. $\square$

Reading the WOP proof next to the SMI one: "let k be the least counterexample" plays the role of the inductive hypothesis (everything below k works), and "$3 \mid a_k$, contradiction" plays the role of the inductive step. Drawn on the index line, the whole proof is one picture:

Note which term the WOP proof reaches for. The SMI proof used a_k and a_{k-2} to build a_{k+1}; the WOP proof is standing at k rather than at $k+1$, so the same recurrence reads $a_k = a_{k-1} - a_{k-3}$ and it reaches for a_{k-1} and a_{k-3}. Same recurrence, index shifted by one — and that shift is why the "$k \geq 3$" line has to be there.

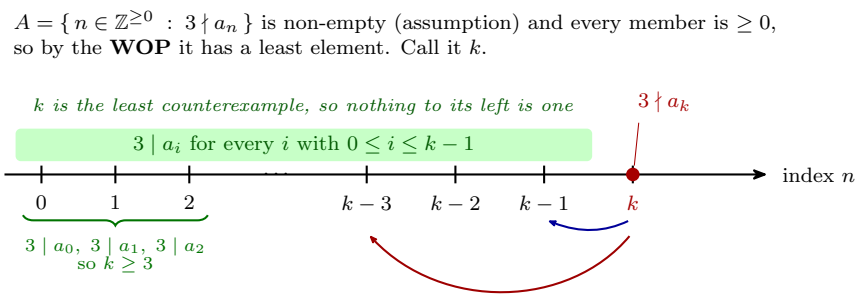


Figure 49: The well-ordering proof of 3 | a_n as a picture of its own least counterexample. Everything to the left of k is green not because it was proved, but because k was chosen least — that single step is the only place the WOP is used, and it is exactly what the strong inductive hypothesis supplies in the SMI proof. The least element here is the smallest number that gives a contradiction. k 3 is what guarantees both arrows land inside the green stretch, since a_{k-3} has to be a term of the sequence at all.

Spotting a WOP proof

A proof is using the well-ordering principle whenever it says **"choose the smallest such n"** about a set it has just argued is non-empty. That phrase is not free — it is the WOP being invoked, and it needs the set to be non-empty and bounded below.

For instance, the primes theorem above can be rewritten as a contradiction proof: suppose some integer $n > 1$ is not a product of primes; by the WOP, choose the smallest such n; then n is prime (done) or $n = rs$ with $1 < r, s < n$, and both r and s *are* products of primes precisely because n was chosen smallest — contradicting the choice of n. Structurally it is the SMI proof with the induction turned inside out.

See also

- mathematical-induction[209] · proof-techniques[210] · sequences-and-summations[211]
- recursive-definitions[212] · solving-recurrence-relations[213] — where a two-term recurrence forces the strong hypothesis

[209] courses/math1061/mathematical-induction.pdf
[210] courses/math1061/proof-techniques.pdf
[211] courses/math1061/sequences-and-summations.pdf
[212] courses/math1061/recursive-definitions.pdf
[213] courses/math1061/solving-recurrence-relations.pdf

- trees[214] — strong induction on the number of vertices: a tree with n vertices has $n-1$ edges
- 2026-08-27-strong-induction-and-well-ordering[215] — Lecture 14
- practice-problems[216] — §18, with full worked solutions

Trees

A tree is a connected graph with no non-trivial circuits. Trees are the connected graphs with as few edges as possible, and the circuit-free graphs with as many edges as possible, and the two facts meet in one theorem: a graph with n vertices is a tree exactly when it is simple, connected and has $n-1$ edges. With the Handshake Theorem (graphs[217]) that theorem turns questions about the degrees in a tree into equations. Walks, trails, circuits and connectedness are in walks-trails-and-circuits[218]. First met in 2026-10-29-trees[219], which has the full proofs and the 11 trees with 7 vertices.

Circuit-free graphs

A circuit is a trail that ends where it starts (walks-trails-and-circuits[220]). A single vertex with no edges counts as one.

> A **trivial circuit** is a circuit consisting of a single vertex and no edges. A **non-trivial circuit** is a circuit that has edges.
>
> A graph is **circuit-free** if there are no non-trivial circuits.

Every vertex is a trivial circuit, so the definition has to say *non-trivial*: otherwise no graph would be circuit-free.

Every circuit-free graph is simple. A loop e at v is the non-trivial circuit $v\,e\,v$. Two edges $e_1 \neq e_2$ joining u and v make the non-trivial circuit $u\,e_1\,v\,e_2\,u$. So a circuit-free graph has neither (graphs[221]).

[214] courses/math1061/trees.pdf
[215] courses/math1061/2026-08-27-strong-induction-and-well-ordering.pdf
[216] courses/math1061/practice-problems.pdf
[217] courses/math1061/graphs.pdf
[218] courses/math1061/walks-trails-and-circuits.pdf
[219] courses/math1061/2026-10-29-trees.pdf
[220] courses/math1061/walks-trails-and-circuits.pdf
[221] courses/math1061/graphs.pdf

Trees

Definition. A graph is a **tree** if and only if it is connected and circuit-free.

- A single vertex is a tree. So is a single edge, and so is a line of vertices.
- A triangle is not a tree: it is a circuit.
- Two edges with no vertex in common are not a tree: the graph is not connected.
- Every tree is simple, since it is circuit-free.

Small trees

Counting trees means counting **essentially different** ones: two trees count as the same if one becomes the other by renaming its vertices (they are **isomorphic**). Up to renaming there is 1 tree with each of 1, 2 and 3 vertices, 2 with 4 vertices, 3 with 5, 6 with 6 and 11 with 7. The 11 are drawn and checked in 2026-10-29-trees[222].

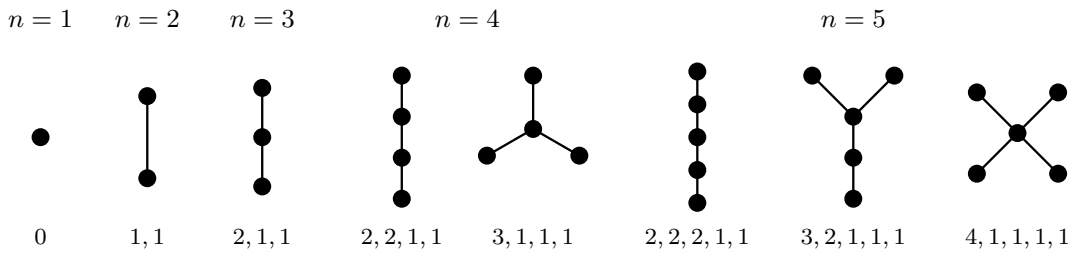


Figure 50: Every tree with 1 to 5 vertices, up to renaming the vertices, each labelled with its degree sequence. With 4 vertices there are two: a line, and one vertex joined to the other three. With 5 there are three: a line, a vertex of degree 3 with one of its branches two long, and one vertex joined to the other four. Each tree with n vertices has $n - 1$ edges, and each with at least 2 vertices has at least two vertices of degree 1.

Deleting an edge

If any edge is deleted from a tree then the result is a disconnected graph. This disconnected graph consists of two trees.

Say the edge e joins u and v. If u could still reach v without e, a shortest such route repeats no vertex, and together with e it would be a non-trivial circuit in the tree. So nothing joins the side of u to the side of v, and every vertex is on one side or the other, because its route to u in

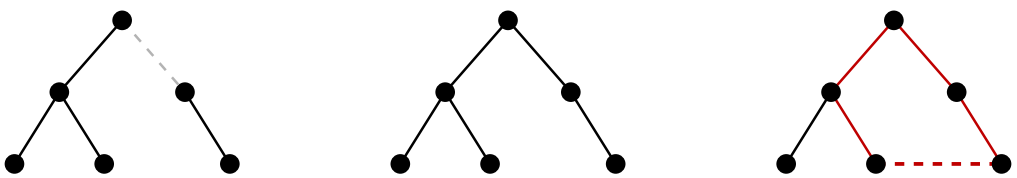
[222] courses/math1061/2026-10-29-trees.pdf

the tree either avoids e or ends by crossing e from v. Each side is connected, and has no circuit since the tree has none, so each side is a tree. The careful proof is in 2026-10-29-trees[223].

Minimally connected, maximally circuit-free

A tree sits exactly on the line between too few edges and too many.

- **Remove any edge and it is no longer connected.** That is the last section. Conversely, a connected graph in which every edge disconnects it when deleted is a tree: if it had a non-trivial circuit, deleting an edge of that circuit would leave it connected, since the rest of the circuit still joins the edge's two endpoints.
- **Add any edge and it gets a circuit.** A new loop is a circuit on its own. A new edge f joining two different vertices x and y: the tree is connected, so there is a walk from x to y, and a shortest one never repeats a vertex, so it is a trail. That trail followed by f back to x is a non-trivial circuit. Conversely, a circuit-free graph in which every new edge makes a circuit is connected: if x could not reach y, add a new edge f joining them. Any circuit it creates must use f, since the graph had none before, and the rest of that circuit would be a walk from y to x in the old graph. So no circuit is created.



delete an edge:
two pieces

a tree:
6 vertices, 5 edges

add an edge:
a circuit

Figure 51: A tree with 6 vertices and 5 edges, in the middle. Left: deleting any one edge, here the dashed one, leaves two pieces with no walk between them, so a tree has no edge to spare. Right: adding any edge, here the dashed red one, closes a non-trivial circuit, in red, so a tree has no room for another edge. 5 edges is the only number of edges a tree with 6 vertices can have.

A tree with n vertices has $n-1$ edges

Theorem. A graph G with n vertices is a tree if and only if it is simple, connected and has $n-1$ edges.

[223] courses/math1061/2026-10-29-trees.pdf

($\Rightarrow$) A tree is connected by definition and simple because it is circuit-free. For the edges, use strong induction on n. One vertex: no edges, since an edge would be a loop, which is a circuit. For a tree T with $k+1 \geq 2$ vertices, delete any edge. That leaves two trees with p and q vertices, where $p+q = k+1$ and $1 \leq p, q \leq k$. By the inductive hypothesis they have $p-1$ and $q-1$ edges, so T has $(p-1)+(q-1)+1 = p+q-1 = k$ edges. The induction is strong because p and q can be any sizes below $k+1$.

($\Leftarrow$) Let G be simple and connected with n vertices and $n-1$ edges, and suppose it has a non-trivial circuit. Deleting an edge of a circuit keeps a graph connected, because the rest of the circuit still joins that edge's endpoints. Keep deleting edges of circuits until none is left. The result is connected and circuit-free, a tree with n vertices and at most $n-2$ edges, which contradicts ($\Rightarrow$). So G has no non-trivial circuit, and is a tree.

Both directions written out in full, with the two facts about deleting edges proved, are in 2026-10-29-trees[224].

Two consequences:

- **Simple is automatic.** The proof of ($\Leftarrow$) never uses it: any connected graph with n vertices and $n-1$ edges is a tree.
- **Connected is not.** A triangle together with one more vertex on its own has 4 vertices and 3 edges, and is not a tree. To use the theorem in the ($\Leftarrow$) direction, check connectedness.

Vertices of degree 1

A **leaf** is a vertex of degree 1.

Leaf is the standard word, and it appears in the practice problems, but results in this course are stated as "vertex of degree 1". In an exam answer, say "vertex of degree 1", or define leaf before using it.

Theorem. Every tree with at least two vertices has at least two vertices of degree 1.

Proof (handshake). Let T have $n \geq 2$ vertices. It has $n-1$ edges, so its degrees add to $2n-2$. It is connected with at least two vertices, so no vertex has degree 0. If at most one vertex had degree 1, all the others would have degree at least 2, and the degrees would add to at least $1 + 2(n-1) = 2n-1 > 2n-2$. $\square$

Proof (longest walk). Among the walks in T that visit no vertex twice, take one with the most edges, $w_0\, f_1\, w_1 \cdots f_k\, w_k$. T is connected with at least two vertices, so it has an edge, and $k \geq 1$. Suppose w_0 had another edge $f \neq f_1$, joining it to x (f is not a loop, since T is simple). If x is not on the walk, $x\, f\, w_0\, f_1 \cdots w_k$ is longer and still visits no vertex twice. If $x = w_j$, then

[224] courses/math1061/2026-10-29-trees.pdf

$w_0\, f_1 \cdots f_j\, w_j\, f\, w_0$ is a non-trivial circuit: its edges are all different, since $f \neq f_1$ and no other f_i meets w_0. Both are impossible, so $\deg(w_0) = 1$, and likewise $\deg(w_k) = 1$. $\square$

The full proof by contradiction is worked in 2026-10-29-trees[225].

- **"At least two vertices" is needed.** The tree with one vertex has no vertex of degree 1: its only vertex has degree 0.
- **"Two" cannot be improved.** A line of vertices has exactly two vertices of degree 1, its ends.

How many vertices of degree 1. Subtract 2 from every degree. In a tree with $n \geq 2$ vertices the total is $(2n-2) - 2n = -2$. A vertex of degree 1 gives -1, a vertex of degree 2 gives 0, and every other vertex gives $\deg(v) - 2 > 0$. So

$$\text{number of vertices of degree 1} \;=\; 2 + \sum_{\deg(v) \geq 3} (\deg(v) - 2).$$

Every vertex of degree 3 adds one more vertex of degree 1, every vertex of degree 4 adds two, and vertices of degree 2 add nothing. A tree whose other vertices all have degree 2 is a line, with exactly 2.

Counting with the Handshake Theorem

Most questions about trees give some of the degrees and ask for a count. Two facts settle them:

1. **The theorem:** a tree with n vertices has $n-1$ edges.
2. **The Handshake Theorem:** the degrees add to twice the number of edges, so in a tree they add to $2(n-1)$.

The method:

1. Name the unknown count, x.
2. Write the number of vertices n in terms of x.
3. Write the number of edges as $n-1$.
4. Write the degree sum two ways, from the degrees and as $2(n-1)$, and set them equal.
5. Solve, then check that the degrees add to twice the edges.

Two more facts often finish the job: every vertex of a tree with at least two vertices has degree at least 1, and there are at least two of degree 1.

[225] courses/math1061/2026-10-29-trees.pdf

Worked: degrees 4, 3 and 1

> A tree has three vertices of degree 4, two vertices of degree 3, and every other vertex has degree 1. How many vertices does it have?

Let x be the number of vertices of degree 1. Then $n = x + 5$, and the tree has $n - 1 = x + 4$ edges. The degree sum is

$$3 \cdot 4 + 2 \cdot 3 + x = 2(x + 4), \qquad 18 + x = 2x + 8, \qquad x = 10.$$

So the tree has $n = 15$ vertices. Check: $12 + 6 + 10 = 28 = 2 \cdot 14$, and $14 = 15 - 1$. The formula for vertices of degree 1 agrees: $2 + 3 \cdot (4 - 2) + 2 \cdot (3 - 2) = 10$.

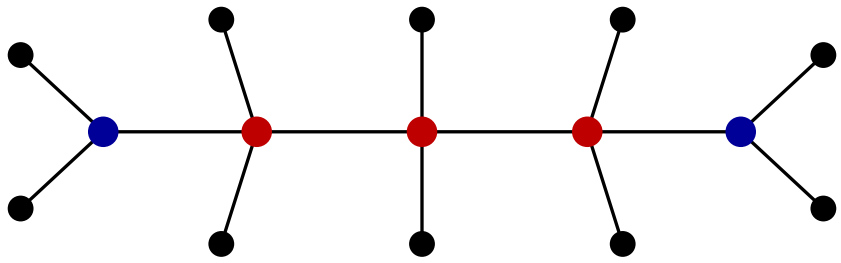


Figure 52: A tree with three vertices of degree 4, in red, two of degree 3, in blue, and every other vertex of degree 1. The red vertices lie in a line, each blue vertex hangs off an end of it, and each of the five has two vertices of degree 1 joined to it. That is $5 + 10 = 15$ vertices and 14 edges, and the degrees add to $12 + 6 + 10 = 28 = 2 \cdot 14$.

More worked examples, with figures: 2026-10-29-trees[226] (every degree 3 or 1, with 15 edges) and 2026-10-29-trees[227] (two of degree 4, one of degree 2).

Common mistakes

- **Using $n - 1$ edges for a graph that is not a tree.** The count needs connected and circuit-free. In the other direction, $n - 1$ edges alone is not enough: a triangle and a separate vertex have 4 vertices and 3 edges.
- **Off by one.** n vertices go with $n - 1$ edges, so 15 edges means 16 vertices, not 14.
- **Miscounting the vertices.** If x is the number of vertices of degree 1 and three other vertices are named, there are $x + 3$ vertices, not x.

[226] courses/math1061/2026-10-29-trees.pdf
[227] courses/math1061/2026-10-29-trees.pdf

- **Forgetting why no degree is 0.** In a tree with at least two vertices every vertex has degree at least 1 because the tree is connected. Say so: the bounds on the degree sum depend on it.
- **Calling a single vertex a leaf.** The one-vertex tree has a vertex of degree 0 and no vertex of degree 1. The two-leaves theorem needs at least two vertices.
- **Deleting an edge from any graph and expecting two pieces.** That is true for trees. An edge on a circuit can be deleted without disconnecting anything.
- **Reading "circuit-free" as "no circuits at all".** Every vertex is a trivial circuit. Circuit-free means no circuit with edges.
- **Judging two trees by their degree sequences.** Different degree sequences mean different trees, but the same degree sequence does not mean the same tree: with 7 vertices, three different trees all have degrees $3, 2, 2, 2, 1, 1, 1$ (2026-10-29-trees[228]).

See also

- walks-trails-and-circuits[229] — circuits, trails and walks, and connected graphs
- graphs[230] — the degrees add to twice the number of edges
- strong-induction-and-the-well-ordering-principle[231] — the induction behind the $n-1$ theorem
- proof-techniques[232] — proof by contradiction, used for ($\Leftarrow$) and for the vertices of degree 1
- 2026-10-29-trees[233] — Lecture 36, with the full proofs and the 11 trees with 7 vertices
- practice-problems[234] — §46, with full worked solutions

Walks, Trails and Circuits

A walk is a way of getting around a graph: start at a vertex and keep moving along edges. A trail is a walk that never uses an edge twice, and a circuit is a trail that finishes where it started. The difference that matters is **edges versus vertices**: a trail may come back to a vertex it has already visited, as long as it leaves along a new edge. The last definition here, connected, says that a walk can get from any vertex to any other. These words are what euler-circuits-and-trails[235] and [trees] are built from. Graphs, degree and the rest of the basic vocabulary are in [graphs]. First met in 2026-10-26-walks-trails-and-circuits[236].

[228] courses/math1061/2026-10-29-trees.pdf
[229] courses/math1061/walks-trails-and-circuits.pdf
[230] courses/math1061/graphs.pdf
[231] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[232] courses/math1061/proof-techniques.pdf
[233] courses/math1061/2026-10-29-trees.pdf
[234] courses/math1061/practice-problems.pdf
[235] courses/math1061/euler-circuits-and-trails.pdf
[236] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf

Walks

A **walk** is a sequence

$$v_0\, e_1\, v_1\, e_2\, v_2 \cdots v_{i-1}\, e_i\, v_i \cdots e_{n-1}\, v_{n-1}\, e_n\, v_n$$

where each v_i is a vertex, and each e_i is an edge with endpoints v_{i-1} and v_i.

It alternates vertex, edge, vertex, edge, …, and starts and ends with a vertex. Each edge joins the vertex before it to the vertex after it. This is a **walk from v_0 to v_n**, and it has n edges, counted with repeats.

- **Anything can repeat.** A walk can go back along the edge it just used, and pass through the same vertex many times.
- **A walk can have no edges.** With $n = 0$ the walk is the single vertex v_0. That is a walk from v_0 to itself.
- **A loop can be used.** If e is a loop at v, its endpoints are v and v, so $v\, e\, v$ is a walk.
- **Why the edges are written in.** If two vertices are joined by multiple edges, the vertices alone do not say which edge was used. In a simple graph two vertices are joined by at most one edge (graphs[237]), so the vertices determine the edges and a walk can be written $v_0 v_1 \cdots v_n$, or $a, b, c, \ldots$.

Trails

A **trail** is a walk where $e_1, e_2, \ldots, e_n$ are pairwise distinct.

No edge is used twice. That is the only condition. **Vertices may repeat**: a trail can come back to a vertex it has visited before, provided it arrives and leaves along edges it has not used yet. Every trail is a walk; a walk that uses some edge twice is not a trail.

Circuits

A **circuit** is a trail $v_0\, e_1\, v_1\, e_2 \cdots v_{n-1}\, e_n\, v_n$ where $v_0 = v_n$.

A circuit is a trail that finishes where it started. Like any trail it uses no edge twice, and it can pass through other vertices more than once.

A **trivial circuit** is a circuit consisting of a single vertex and no edges.
A **non-trivial circuit** is a circuit that has edges.
A graph is **circuit-free** if there are no non-trivial circuits.

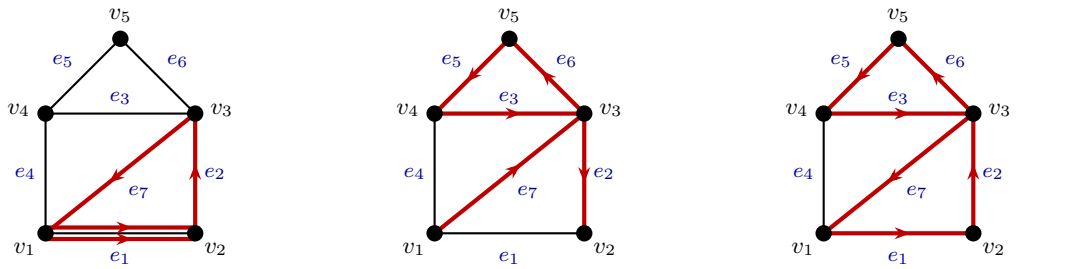
[237] courses/math1061/graphs.pdf

Every vertex v gives a trivial circuit, the walk v with $n = 0$: it is a trail (it has no edges to repeat) and it starts and ends at v. Every graph has these, so "circuit-free" has to mean free of the non-trivial ones.

The smallest non-trivial circuits:

- **One edge:** a loop e at v gives the circuit $v\,e\,v$. An ordinary edge e joining v and w does not give one, because $v\,e\,w\,e\,v$ uses e twice.
- **Two edges:** two edges e_1, e_2 that both join v and w give the circuit $v\,e_1\,w\,e_2\,v$.
- **In a simple graph** there are no loops and no multiple edges, so a non-trivial circuit has at least 3 edges. A triangle $a\,b\,c\,a$ is the smallest.

	Edge repeated?	Vertex repeated?	Ends where it starts?
Walk	allowed	allowed	allowed, not required
Trail	**no**	allowed	allowed, not required
Circuit	**no**	allowed	**yes**



walk, not a trail

$v_1\,e_1\,v_2\,e_2\,v_3\,e_7\,v_1\,e_1\,v_2$

e_1 used twice

trail, not a circuit

$v_1\,e_7\,v_3\,e_6\,v_5\,e_5\,v_4\,e_3\,v_3\,e_2\,v_2$

v_3 twice, no edge twice, ends at $v_2 \neq v_1$

circuit

$v_1\,e_1\,v_2\,e_2\,v_3\,e_6\,v_5\,e_5\,v_4\,e_3\,v_3\,e_7\,v_1$

v_3 twice, no edge twice, back at v_1

Figure 53: The three definitions on one graph, with the route in red and arrows showing the direction of travel. Left: a walk that is not a trail, since it uses e_1 twice, drawn as the doubled red line. Middle: a trail that is not a circuit. It visits v_3 twice, arriving along e_7 and e_3 and leaving along e_6 and e_2, but uses every edge at most once, and it ends at v_2, not at v_1 where it started. Right: a circuit. It also passes through v_3 twice, uses no edge twice, and returns to v_1.

Two things about circuits used later, in the proofs in euler-circuits-and-trails[238]:

- **A circuit can be started anywhere on it.** If $v_0\,e_1\,v_1 \cdots e_n\,v_n$ is a circuit and $1 \leq k \leq n$, then

$$v_k\,e_{k+1}\,v_{k+1} \cdots e_n\,v_n\,e_1\,v_1 \cdots e_k\,v_k$$

[238] courses/math1061/euler-circuits-and-trails.pdf

is a circuit too. Since $v_n = v_0$, each edge still joins the vertices beside it, it uses the same edges, and it starts and ends at v_k.

- **A circuit can be read backwards.** $v_n\, e_n\, v_{n-1} \cdots e_1\, v_0$ is a circuit with the same edges.

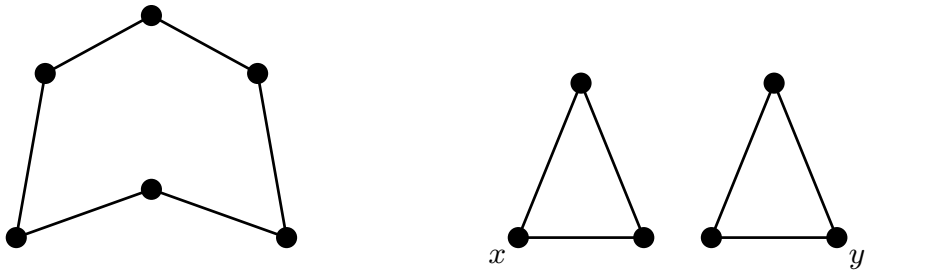
Connected

A graph is **connected** if and only if there is a walk from any given vertex to any other given vertex.

A graph that is not connected is **disconnected**: there are two vertices with no walk from one to the other. A drawing of a disconnected graph falls into separate pieces with no edge between them.

- **A graph with one vertex is connected.** There is no other vertex to reach.
- **An isolated vertex disconnects a graph** with two or more vertices. A walk from it would have to start along an edge, and it has none.
- **A crossing in a drawing is not a connection.** Two lines that cross without a dot do not meet, so a drawing that looks like one piece can be a disconnected graph.

To check, pick a vertex, mark every vertex that can be reached from it along edges, then everything reachable from those, and so on. The graph is connected exactly when every vertex ends up marked.



connected **disconnected**: no walk from x to y

Figure 54: Two graphs with the same degrees, six vertices of degree 2 each. Left: one circuit through all six vertices, a connected graph, since from any vertex there is a walk to any other around the circuit. Right: two separate triangles, a disconnected graph. There is no walk from x to y, since every walk from x stays inside its triangle. So the degrees alone do not decide whether a graph is connected.

Common mistakes

- **Thinking a trail cannot revisit a vertex.** A trail can pass through a vertex as often as it likes. It is the **edges** that may not repeat.
- **Thinking a circuit cannot revisit a vertex.** Same again: the circuit in the figure above passes through v_3 twice.
- **Going out and back along one edge and calling it a circuit.** $v\,e\,w\,e\,v$ ends where it starts, but uses e twice, so it is not a trail and not a circuit. It is only a walk.
- **Forgetting the trivial circuit.** A single vertex with no edges is a circuit. That is why circuit-free is defined by having no **non-trivial** circuits.
- **Reading a crossing as a vertex.** Only dots are vertices, so lines that cross do not join two pieces of a graph.

See also

- [graphs] — graphs, loops, multiple edges, simple graphs and degree
- euler-circuits-and-trails[239] — a circuit or trail that uses every edge exactly once
- [trees] — connected, circuit-free graphs
- 2026-10-26-walks-trails-and-circuits[240] — Lecture 34, where these definitions are introduced
- practice-problems[241] — §44, with full worked solutions

[239] courses/math1061/euler-circuits-and-trails.pdf
[240] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[241] courses/math1061/practice-problems.pdf