MATH1061 — Week 12 Notes

Table of contents

Lecture 31 — Probability, Binomial Coefficients **1**
- Goals . . . 1
- Finishing BARBARA . . . 2
- Worked: a committee with at least one mathematician . . . 2
- Worked: 5 not next to 6 . . . 3
- Worked: dividing 400 students into two groups . . . 4
- Pascal's formula . . . 5
- The Binomial Theorem . . . 6
- Worked: coefficients in binomial expansions . . . 7
- Worked: the sum of a row of Pascal's triangle . . . 10
- See also . . . 11

Lecture 32 — Inclusion/Exclusion **11**
- Goals . . . 12
- Two sets . . . 12
- Three sets . . . 12
- Worked: the three-set rule from the two-set rule . . . 13
- Worked: divisible by neither 7 nor 11 . . . 14
- The general rule . . . 17
- Worked: words containing "a" and "b" . . . 19
- Worked: attendance and exam marks . . . 20
- Worked: divisible by none of 3, 5, 7 . . . 20
- Worked: 1 and 2 first or 5 last . . . 23
- See also . . . 24

Lecture 33 — Pigeonhole Principle, Introduction to Graph Theory **24**
- Goals . . . 25
- The pigeonhole principle . . . 25
- Worked: no two consecutive . . . 26
- Worked: two numbers that sum to 101 . . . 27

Worked: no three consecutive . . . 27
Worked: two subsets with the same sum . . . 29
Graphs . . . 31
The Handshake Theorem . . . 32
Worked: which statement about degrees is true . . . 32
Worked: degree sequences . . . 33
See also . . . 36

Reference material **36**
Binomial Coefficients . . . 36
Counting Principles . . . 48
Counting Selections . . . 56
The Examination Formula Page . . . 66
Graphs . . . 70
Inclusion/Exclusion . . . 79
The Pigeonhole Principle . . . 89
Practice Problems — the Semester-wide Set . . . 97
Probability . . . 222
Sets and Set Notation . . . 228

Lecture 31 — Probability, Binomial Coefficients

Probability as a ratio of two counts when the outcomes are equally likely, and the identities that binomial coefficients satisfy: the symmetry $\binom{n}{r} = \binom{n}{n-r}$, Pascal's formula, the Binomial Theorem, and the sum of a row of Pascal's triangle. Pre-work: Video 039 (Introduction to Probability) and Video 040 (Binomial Coefficients). Sample spaces, events, the formula $P(E) = \frac{|E|}{|S|}$ and the complement are collected in [probability]. The identities, their combinatorial proofs, Pascal's triangle and the method for picking a coefficient out of an expansion are in binomial-coefficients[1]. The note starts by finishing the BARBARA question from 2026-10-13-counting-selections[2].

Goals

1. Learn how to calculate probabilities by counting when there are equally likely outcomes.
2. Gain a better understanding of the combinatorial proofs of Pascal's formula and the Binomial Theorem.
3. Learn how to evaluate coefficients in binomial expansions.
4. Gain confidence with solving counting problems.

Three questions to keep in mind:

[1] courses/math1061/binomial-coefficients.pdf
[2] courses/math1061/2026-10-13-counting-selections.pdf

- **To find a coefficient in an expansion, how do you work out what k should be?** Finding k: set the power of x in the general term equal to the power wanted.
- **Why is Pascal's formula true?** Its combinatorial proof, which splits subsets by whether they contain one particular element.
- **Why is the Binomial Theorem true?** Its combinatorial proof, which counts a, b-sequences by their number of b's.

Finishing BARBARA

> How many distinct arrangements of the letters in the word BARBARA are there?

The full working is in 2026-10-13-counting-selections[3]. In short: tag the copies so every letter is different, $\mathrm{B}_1\mathrm{B}_2$, $\mathrm{A}_1\mathrm{A}_2\mathrm{A}_3$, $\mathrm{R}_1\mathrm{R}_2$, and there are 7! arrangements of the 7 tagged letters. Removing the tags merges arrangements that differ only in how the copies of each letter are ordered among themselves: 2! orders for the B's, $3! = 6$ for the A's ($\mathrm{A}_1\mathrm{A}_2\mathrm{A}_3$, $\mathrm{A}_1\mathrm{A}_3\mathrm{A}_2$, $\mathrm{A}_2\mathrm{A}_1\mathrm{A}_3$, $\mathrm{A}_2\mathrm{A}_3\mathrm{A}_1$, $\mathrm{A}_3\mathrm{A}_1\mathrm{A}_2$, $\mathrm{A}_3\mathrm{A}_2\mathrm{A}_1$, all giving the same word) and 2! for the R's. So

$$\#(\text{arrangements}) = \frac{7!}{2!\,3!\,2!} = \frac{(\text{total number of letters})!}{(\#\text{B's})!\,(\#\text{A's})!\,(\#\text{R's})!} = \frac{5040}{24} = 210.$$

Worked: a committee with at least one mathematician

> If a committee of 5 is chosen at random from a group of 25 mathematicians and 25 physicists, what is the probability that at least one mathematician will be chosen?

Answer: $\frac{1283}{1316} \approx 97.5\%$**.**

A committee is an unordered selection of 5 from the 50 people, and every committee is equally likely. Let

- T = the total number of ways to choose 5 people = $\binom{50}{5} = 2\,118\,760$,
- N = the number of choices with no mathematicians = $\binom{25}{5} = 53\,130$, all five chosen from the 25 physicists.

"At least one mathematician" is five cases (1 to 5 mathematicians), but its complement, "no mathematicians", is one. So count the complement and subtract:

$$\begin{aligned} P(\text{at least one mathematician}) &= \frac{\#(\text{choices with} \geq 1 \text{ mathematician})}{\text{total number of choices}} = \frac{T-N}{T} = 1 - \frac{N}{T} \\ &= 1 - \frac{\binom{25}{5}}{\binom{50}{5}} = 1 - \frac{53\,130}{2\,118\,760} = 1 - \frac{33}{1316} = \frac{1283}{1316} \approx 97.5\% \text{ (to 1 dp).} \end{aligned}$$

[3] courses/math1061/2026-10-13-counting-selections.pdf

The fraction $\frac{N}{T} \approx 2.5\%$ is the probability of **no** mathematicians; it is the quantity being subtracted, not the answer. The sample space split into the two events is drawn in probability[4].

maths	physics	ways	committees	
0	5	$\binom{25}{0}\binom{25}{5}$	53 130	no mathematicians: one case, $53\,130 = \binom{25}{5}$
1	4	$\binom{25}{1}\binom{25}{4}$	316 250	at least one mathematician: five cases, 2 065 630
2	3	$\binom{25}{2}\binom{25}{3}$	690 000	
3	2	$\binom{25}{3}\binom{25}{2}$	690 000	
4	1	$\binom{25}{4}\binom{25}{1}$	316 250	
5	0	$\binom{25}{5}\binom{25}{0}$	53 130	
		all six rows: $\binom{50}{5} = 2\,118\,760$		

Figure 1: All committees of 5, sorted by how many mathematicians they contain. With k mathematicians there are $\binom{25}{k}$ ways to pick them and $\binom{25}{5-k}$ ways to pick the $5-k$ physicists. The event wanted, at least one mathematician, is the five rows $k = 1, \dots, 5$; its complement is the single row $k = 0$. The six rows together are every committee, so the five-row sum is the total minus the one row: $2,118,760 - 53,130 = 2,065,630$.

Worked: 5 not next to 6

> What is the probability that a randomly chosen permutation of $\{1, 2, \dots, 9\}$ has 5 not next to 6?

Answer: $\frac{7}{9} \approx 77.8\%$**.**

A permutation is ordered with no repeats. Let

- T = the total number of permutations = 9!,
- A = the number of permutations containing "56" = 8!.

To count A, glue 5 and 6 into a single tile "56". Then there are 8 objects to arrange, the tile and the other 7 numbers, so 8! arrangements. Equivalently, the tile can start in any of 8 positions (1 to 8), and the other seven numbers fill the remaining positions in 7! ways: $8 \cdot 7! = 8!$. By the same argument there are 8! permutations containing "65". "5 next to 6" means "56" or "65", which cannot both happen, so $2A = 2 \cdot 8!$ permutations have 5 next to 6. Then

[4] courses/math1061/probability.pdf

$$P(\text{5 not next to 6}) = \frac{T - 2A}{T} = \frac{9! - 2 \cdot 8!}{9!} = \frac{9 \cdot 8! - 2 \cdot 8!}{9 \cdot 8!} = \frac{9-2}{9} = \frac{7}{9} = 0.\dot{7} \approx 77.8\% \text{ (to 1 dp)}.$$

The tile is drawn, and the answer checked a second way, in probability[5]. The factor of 2 is the easy thing to lose: without the "65" permutations the answer would come out as $\frac{8}{9}$.

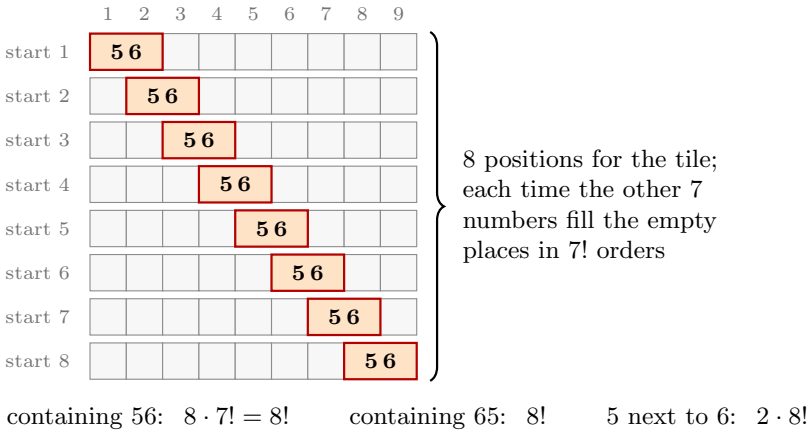


Figure 2: Counting the permutations of $1, \ldots, 9$ that contain 56 by where the pair sits. The tile 56 covers two neighbouring places out of nine, and its left end can be at any of places 1 to 8, so there are 8 positions for it. Whichever is used, the other seven numbers fill the seven empty places in 7! orders. That gives $8 \cdot 7! = 8!$ permutations with 5 immediately before 6, and another 8! with 6 immediately before 5.

Worked: dividing 400 students into two groups

How many ways are there to divide 400 students into a group of 150 and a group of 250?

Answer: $\binom{400}{150} = \binom{400}{250} = \dfrac{400!}{150!\,250!}$, about 3.47×10^{113}.

Choose which 150 students go in the first group: $\binom{400}{150}$ ways. The 250 left over are the second group, with no further choice, so that is the whole count. Choosing the group of 250 first instead gives $\binom{400}{250}$ ways, and it must be the same number, since it counts the same divisions. Both equal $\frac{400!}{150!\,250!}$.

[5] courses/math1061/probability.pdf

Because the groups have different sizes, a division is fixed by saying who is in the group of 150. There is nothing to multiply by for the second group, and nothing to divide by either.

The general fact. For $0 \le r \le n$,

$$\binom{n}{r} = \binom{n}{n-r},$$

because the number of ways of choosing an r-element subset of an n-element set equals the number of ways of choosing the $n-r$ elements that are *not* in the subset. Each subset is paired with its complement. For $n = 5$, $r = 2$ the pairing is

$$\{1,2\} \leftrightarrow \{3,4,5\}, \quad \{1,3\} \leftrightarrow \{2,4,5\}, \quad \{1,4\} \leftrightarrow \{2,3,5\}, \quad \{1,5\} \leftrightarrow \{2,3,4\}, \quad \{2,3\} \leftrightarrow \{1,4,5\},$$
$$\{2,4\} \leftrightarrow \{1,3,5\}, \quad \{2,5\} \leftrightarrow \{1,3,4\}, \quad \{3,4\} \leftrightarrow \{1,2,5\}, \quad \{3,5\} \leftrightarrow \{1,2,4\}, \quad \{4,5\} \leftrightarrow \{1,2,3\},$$

so $\binom{5}{2} = \binom{5}{3} = 10$. See binomial-coefficients[6].

Pascal's formula

Pascal's formula. For integers $1 \le r \le n$,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

With $n = 8$ and $r = 3$ it says $\binom{9}{3} = \binom{8}{2} + \binom{8}{3}$, that is, $84 = 28 + 56$.

Why it is true. $\binom{9}{3}$ is the number of 3-element subsets of $\{1, 2, \dots, 9\}$. Pick out one element, 9, and sort the subsets by whether they contain it.

- **The subsets that contain 9**, like $\{1, 7, 9\}$. With 9 already in, the subset is decided by its other two elements, which can be any two of $1, \dots, 8$. So these subsets are $\{9\}$ joined to a 2-element subset of $\{1, \dots, 8\}$, and there are $\binom{8}{2} = 28$ of them.
- **The subsets that do not contain 9**, like $\{1, 7, 8\}$. All three elements come from $\{1, \dots, 8\}$, so these are just the 3-element subsets of $\{1, \dots, 8\}$, and there are $\binom{8}{3} = 56$.

[6] courses/math1061/binomial-coefficients.pdf

Every 3-element subset of $\{1, \dots, 9\}$ is in exactly one of the two groups, so $\binom{9}{3} = \binom{8}{2} + \binom{8}{3}$. Nothing here depended on the numbers 8 and 3. In general, sort the r-element subsets of $\{1, \dots, n+1\}$ by whether they contain $n+1$. Those that do are $\{n+1\}$ joined to an $(r-1)$-element subset of $\{1, \dots, n\}$, $\binom{n}{r-1}$ of them, and those that don't are r-element subsets of $\{1, \dots, n\}$, $\binom{n}{r}$ of them. That is the whole proof: **one side counts a collection directly, the other counts it in two disjoint pieces**. It is drawn, with the general proof written out, in binomial-coefficients[7].

Pascal's triangle. Writing $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$ as row n and centring the rows gives

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1 \\
 & 1 & & 8 & & 28 & & 56 & & 70 & & 56 & & 28 & & 8 & & 1
\end{array}$$

The top row is $\binom{0}{0}$, the next is $\binom{1}{0}, \binom{1}{1}$, and so on down to row 8. Pascal's formula is the rule that builds it: each entry inside the triangle is the sum of the two above it. For example $4 + 6 = 10$ is $\binom{4}{1} + \binom{4}{2} = \binom{5}{2}$. Each row also reads the same in both directions, which is the symmetry $\binom{n}{r} = \binom{n}{n-r}$. The triangle is drawn with these additions picked out in binomial-coefficients[8].

The Binomial Theorem

The Binomial Theorem. For any $a, b \in \mathbb{R}$ and any nonnegative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k = a^n + \binom{n}{1} a^{n-1} b^1 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

a, b-sequences. A sequence of n terms, each either a or b, is an **a, b-sequence of length n**; $aabab$ is one of length 5. Expanding

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n \text{ factors}}$$

[7] courses/math1061/binomial-coefficients.pdf
[8] courses/math1061/binomial-coefficients.pdf

without collecting terms means choosing a or b from each factor in turn and writing the choices down in order. So **the expansion of $(a+b)^n$ is the sum of every a,b-sequence of length n**:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = aa+ab+ba+bb,\\ (a+b)^3 &= (a+b)(a+b)(a+b) = (aa+ab+ba+bb)(a+b)\\ &= aaa+aba+baa+bba+aab+abb+bab+bbb.\end{aligned}$$

Why it is true. Collect the sequences by their number of b's.

1. **Each sequence is a monomial.** An a,b-sequence of length n with k occurrences of b has $n-k$ occurrences of a, so it equals $a^{n-k}b^k$. For example $aabab = a^3b^2$, and in $(a+b)^3$ the three sequences aba, baa, aab each equal a^2b, which gives the term $3a^2b$.
2. **Counting them.** A sequence of length n with k b's is decided by which k of the n positions hold the b's. There are $\binom{n}{k}$ choices of where to put the b's, so $\binom{n}{k}$ such sequences.
3. **Adding up.** The term $a^{n-k}b^k$ therefore appears $\binom{n}{k}$ times, for each k from 0 to n, which is the theorem. At the ends, a^n (no b's) has coefficient $\binom{n}{0} = 1$ and b^n (all b's) has coefficient $\binom{n}{n} = 1$.

For example, the terms of $(a+b)^5$ with three a's and two b's are the ten sequences

$$aaabb + aabab + aabba + abaab + ababa + abbaa + baaab + baaba + babaa + bbaaa = 10a^3b^2,$$

and $10 = \binom{5}{2}$, the number of ways to choose where the two b's go among the five positions. Choosing where the three a's go, as in $\boxed{a}\boxed{a}\boxed{\ }\boxed{a}\boxed{\ }$, gives $\binom{5}{3}$, and $\binom{5}{3} = \binom{5}{2} = 10$, so it doesn't matter which letter's positions are chosen.

The full proof, with the a,b-sequences of length 3 drawn as a tree and all ten of these length-5 sequences drawn as choices of positions for the b's, is in binomial-coefficients[9].

Worked: coefficients in binomial expansions

(1) What is the coefficient of x^3 in the expansion of $(x+9)^7$?

(2) What is the coefficient of x^8 in the expansion of $(3-x)^{12}$?

(3) What is the coefficient of x^2 in the expansion of $(3x-2)^5$?

Answers: (1) 229 635**, (2)** 40 095**, (3)** -720**.**

Each uses the Binomial Theorem, $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$, and only one of its terms.

[9] courses/math1061/binomial-coefficients.pdf

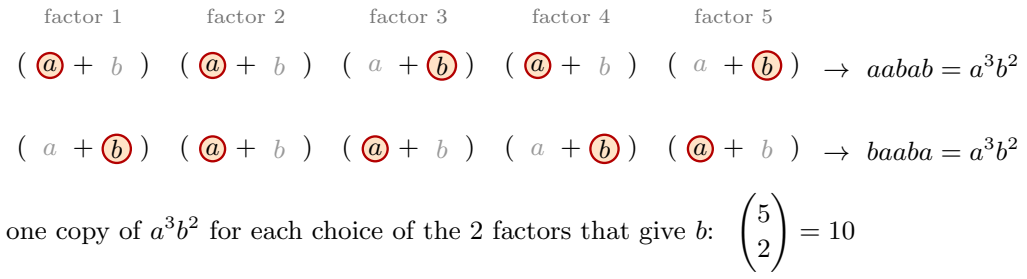


Figure 3: Where the coefficient of a^3b^2 in $(a+b)^5$ comes from. Expanding the product means picking one letter from each of the five factors, and the result is the a, b-sequence of the picks. Picking b from factors 3 and 5 and a from the rest gives $aabab$; picking b from factors 1 and 4 gives $baaba$. Both equal a^3b^2. Every way of choosing which 2 of the 5 factors supply a b gives one more copy of a^3b^2, so the coefficient is $\binom{5}{2} = 10$.

Finding k

Match the expression to $(a+b)^n$, taking each constant and each minus sign along with the letter it belongs to. Then the general term is $\binom{n}{k}a^{n-k}b^k$, and k **is whatever value makes the power of x in that term equal to the power asked for.** Where x sits decides the equation:

- if x is in a, it is raised to the power $n-k$, so solve \$n - k = \$ (the power wanted);
- if x is in b, it is raised to the power k, so k is the power wanted.

Which of the two terms is called a doesn't affect the answer. Swapping them turns k into $n-k$, and $\binom{n}{k} = \binom{n}{n-k}$. In (1), $k=4$ with x as a, or $k=3$ with x as b, and $\binom{7}{4} = \binom{7}{3} = 35$ either way. What does matter is that the power $n-k$ goes on whatever was called a and the power k on whatever was called b.

(1) x^3 in $(x+9)^7$

Here $a=x$, $b=9$, $n=7$. The power of x is $n-k=7-k$, so $7-k=3$ and $k=4$. The term is

$$\binom{7}{4}x^3 \cdot 9^4,$$

so the coefficient of x^3 is $\binom{7}{4} \cdot 9^4 = 35 \cdot 6561 = 229\,635$.

		in place of a	in place of b	
general term	$\binom{n}{k}$	$a^{\,n-k}$	$b^{\,k}$	**power of x = wanted** $\Rightarrow$ k
(1) $(x+9)^7$	$\binom{7}{k}$	$x^{\,7-k}$	$9^{\,k}$	$7-k=3 \;\Rightarrow\; k=4$
(2) $(3-x)^{12}$	$\binom{12}{k}$	$3^{\,12-k}$	$(-x)^k$	$k=8$
(3) $(3x-2)^5$	$\binom{5}{k}$	$(3x)^{5-k}$	$(-2)^k$	$5-k=2 \;\Rightarrow\; k=3$

Figure 4: Finding k by lining each expansion up against the general term $\binom{n}{k}a^{n-k}b^k$. Whatever stands in the place of a is raised to the power $n-k$, and whatever stands in the place of b to the power k. The power of x comes from whichever of the two contains x, outlined in red: in (1) and (3) x is part of a, so its power is $n-k$; in (2) it is part of b, so its power is k. Setting that power equal to the one wanted gives k.

(2) x^8 in $(3-x)^{12}$

Here $a=3$, $b=-x$, $n=12$. The power of x is k, so $k=8$ and $n-k=4$. The term is

$$\binom{12}{8}\cdot 3^4\cdot(-x)^8=\binom{12}{8}\cdot 3^4\cdot x^8,$$

since an even power of $-x$ is positive. So the coefficient of x^8 is $\binom{12}{8}\cdot 3^4=\binom{12}{4}\cdot 81=495\cdot 81=40\,095$.

(3) x^2 in $(3x-2)^5$

Here $a=3x$, $b=-2$, $n=5$. The power of x is $n-k=5-k$, so $5-k=2$ and $k=3$. The term is

$$\binom{5}{3}\cdot(3x)^2\cdot(-2)^3=-\binom{5}{3}\cdot 2^3\cdot 9\cdot x^2,$$

since $(3x)^2=9x^2$ and $(-2)^3=-8$. So the coefficient of x^2 is $-\binom{5}{3}\cdot 2^3\cdot 9=-10\cdot 8\cdot 9=-720$.

The traps are the 3 and the sign: writing $3x^2$ for $(3x)^2$ gives -240, and dropping the minus gives 720. More on both, and a case where x is in both terms, in binomial-coefficients[10].

Worked: the sum of a row of Pascal's triangle

Find a combinatorial proof that $\displaystyle\sum_{r=0}^{n} \binom{n}{r} = 2^n$.

The idea is to find one collection that has 2^n elements and can also be counted as a sum of binomial coefficients. The subsets of an n-element set are such a collection.

01-sequences. Let $N = \{1, 2, \ldots, n\}$. Represent each subset of N by a 01-sequence of length n: a 1 in position i if i is in the subset, a 0 if not. For $n = 6$,

$$\{2, 3, 6\} \subseteq \{1, 2, 3, 4, 5, 6\} \quad \longleftrightarrow \quad 0\,1\,1\,0\,0\,1.$$

Each subset gives exactly one 01-sequence and each 01-sequence gives exactly one subset.

Proof. Count the subsets of N in two ways.

- **All at once.** The number of subsets of N is $|\mathcal{P}(N)| = 2^{|N|} = 2^n$ (sets-and-set-notation[11]): each of the n positions of the 01-sequence is a 0 or a 1, independently.
- **By cardinality.** Every subset has some cardinality k with $0 \le k \le n$, so

$$\begin{aligned} \#(\text{subsets of } N) &= \sum_{k=0}^{n} \#(\text{subsets of cardinality } k) \\ &= \sum_{k=0}^{n} \#(\text{01-sequences with exactly } k \text{ ones}) \\ &= \sum_{k=0}^{n} \binom{n}{k}, \end{aligned}$$

since a 01-sequence with exactly k ones is fixed by choosing which k of the n positions hold the ones.

Both expressions count the subsets of N, so

$$2^n = \sum_{r=0}^{n} \binom{n}{r}. \qquad \square$$

[10] courses/math1061/binomial-coefficients.pdf
[11] courses/math1061/sets-and-set-notation.pdf

For $n = 6$: $1+6+15+20+15+6+1 = 64 = 2^6$, the sum of row 6 of Pascal's triangle. The case $n = 3$, with all eight subsets of $\{1, 2, 3\}$ grouped by size, is drawn in binomial-coefficients[12].

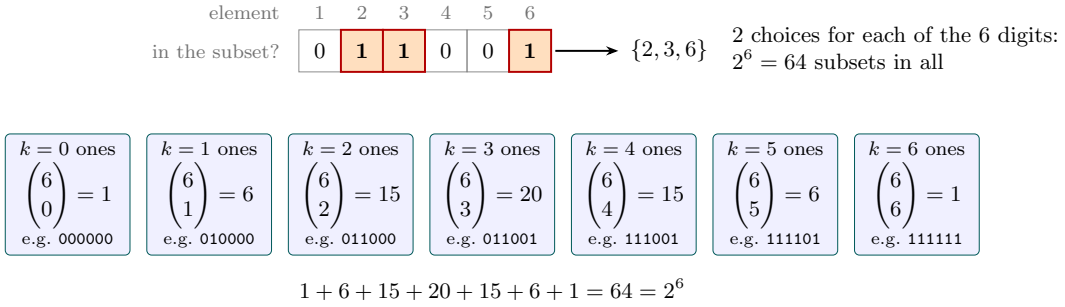


Figure 5: Both counts of the subsets of $1, \ldots, 6$. Top: a subset is recorded as a 01-sequence, one digit per element, 1 for in and 0 for out, so $2, 3, 6$ is 011001. Six digits, each 0 or 1, give $2^6 = 64$ sequences. Bottom: the same 64 sorted by their number of ones, which is the size of the subset. A sequence with k ones is a choice of k of the 6 positions, so each group has $\binom{6}{k}$ members, one example shown for each. The group sizes are row 6 of Pascal's triangle, and they add up to 64.

See also

- [probability] — sample spaces, events, equally likely outcomes, and the complement
- binomial-coefficients[13] — symmetry, Pascal's formula and triangle, the Binomial Theorem, finding coefficients, and the row sum
- counting-selections[14] — n choose r, gluing, and arrangements of words with repeated letters
- 2026-10-13-counting-selections[15] — Lecture 30 · 2026-10-20-inclusion-exclusion[16] — Lecture 32
- practice-problems[17] — §39, with full worked solutions
- practice-problems[18] — §40, with full worked solutions

[12] courses/math1061/binomial-coefficients.pdf
[13] courses/math1061/binomial-coefficients.pdf
[14] courses/math1061/counting-selections.pdf
[15] courses/math1061/2026-10-13-counting-selections.pdf
[16] courses/math1061/2026-10-20-inclusion-exclusion.pdf
[17] courses/math1061/practice-problems.pdf
[18] courses/math1061/practice-problems.pdf

Lecture 32 — Inclusion/Exclusion

Counting a union of sets that are not disjoint. The addition rule only adds sizes when no element is in two of the sets; when they overlap, adding the sizes counts the shared elements more than once, and **inclusion/exclusion** subtracts the overlaps back out. The rule for two and three sets, why it counts every element exactly once, a proof of the three-set rule from the two-set one, and the general rule for n sets, then five counting questions, the last of them a probability. Pre-work: Video 041 (Inclusion/Exclusion). The principle, the complement for "none of them", counting multiples with the floor function and the probability form are collected in inclusion-exclusion[19]. The addition and difference rules it extends are in counting-principles[20].

Goals

1. Understand the inclusion/exclusion principle for two and three sets.
2. Know how to use the inclusion/exclusion principle to solve counting problems.

Two questions to keep in mind:

- **In the three-set rule, why is $|A \cap B \cap C|$ added back once and not twice?** The region counts show it.
- **Could the two-set rule be applied twice instead of learning a three-set rule?** Yes, and doing it proves the three-set rule.

Two sets

Inclusion/exclusion for two sets. For finite sets A and B,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

$|A|$ counts every element of A, including those also in B. $|B|$ counts every element of B, including those also in A. So $|A| + |B|$ counts each element of $A \cap B$ twice and everything else in $A \cup B$ once. Subtracting $|A \cap B|$ takes one of the two counts away.

When A and B are disjoint, $|A \cap B| = 0$ and this is the addition rule (counting-principles[21]). Inclusion/exclusion is what the addition rule becomes when the sets are allowed to overlap.

[19] courses/math1061/inclusion-exclusion.pdf
[20] courses/math1061/counting-principles.pdf
[21] courses/math1061/counting-principles.pdf

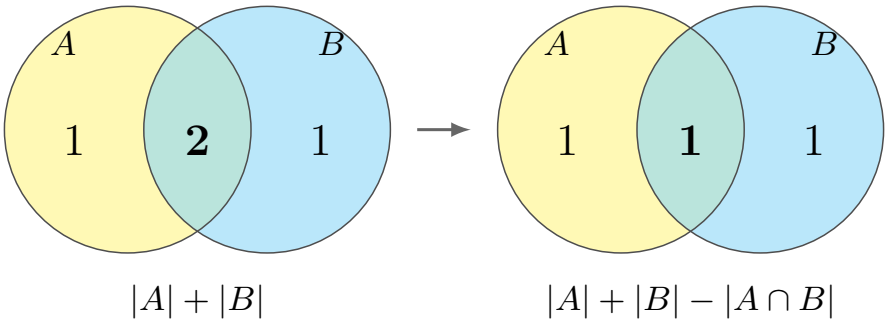


Figure 6: How many times each region of $A \cup B$ is counted. Adding $|A|$ and $|B|$ counts the two outer regions once each but the overlap twice, once inside A and once inside B. Subtracting $|A \cap B|$ removes one count from the overlap only, so every element of $A \cup B$ ends up counted exactly once.

Three sets

Inclusion/exclusion for three sets. For finite sets A, B and C,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.$$

Three circles cut the plane into seven regions inside the union, and the formula is right exactly when each of the seven ends up counted once. Track the counts term by term.

- **Add the single sets.** $|A|+|B|+|C|$ counts an element once for each set it is in. Regions in one set are counted once, regions in exactly two sets twice, and the centre, $A \cap B \cap C$, three times.
- **Subtract the pairs.** An element in exactly two sets, say A and B but not C, is in only one of the three pairwise intersections, $A \cap B$, so it loses one count and drops from 2 to 1. An element of the centre is in all three pairwise intersections, so it loses three counts and drops from 3 to 0.
- **Add the triple.** Only the centre is in $A \cap B \cap C$. Adding $|A \cap B \cap C|$ once brings it from 0 to 1 and leaves every other region alone.

So the triple intersection is added back **once** because once is exactly what the centre is short after the pairs are subtracted. Adding it twice would leave the centre counted twice.

Worked: the three-set rule from the two-set rule

Could the inclusion/exclusion rule for two sets be used twice instead of a separate rule for three sets?

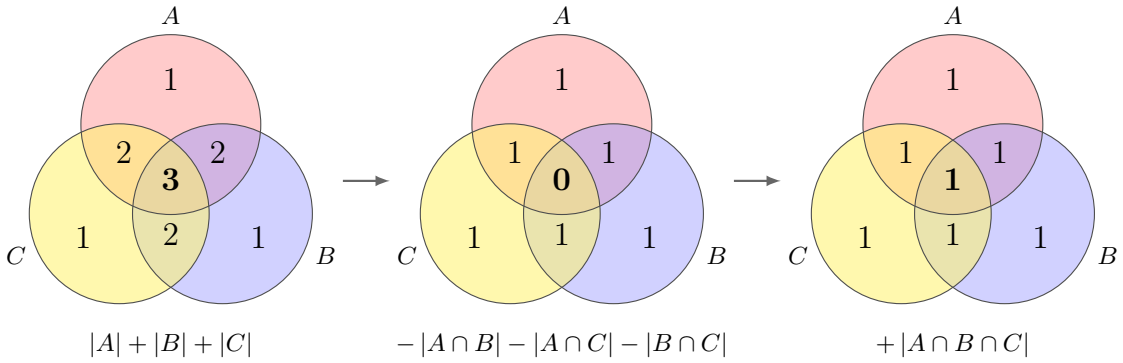


Figure 7: The number of times each of the seven regions is counted after each stage of the three-set formula. The three single-set sizes count a region once for each circle it lies in, so the centre is counted three times. Subtracting the three pairwise intersections removes one count from each two-set region but three from the centre, which drops to 0. Adding the triple intersection once restores the centre, and every region is counted exactly once.

Yes. Treat $B \cup C$ as a single set, apply the two-set rule to A and $B \cup C$, and the three-set rule falls out. The laws are cited by their numbers in the table of set identities on the formula-sheet[22]. The two-set rule is used with different sets in the role of X and Y in

$$|X \cup Y| = |X| + |Y| - |X \cap Y|.$$

$$\begin{aligned}
|A \cup B \cup C| &= |A \cup (B \cup C)| && \text{by the associative law (2} \\
&= |A| + |B \cup C| - |A \cap (B \cup C)| && \text{two-set rule, } X = A,\ Y = \\
&= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| && \text{two-set rule, } X = B,\ Y = \\
&= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| && \text{by the distributive law (} \\
&= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |(A \cap B) \cap (A \cap C)|) && \text{two-set rule, } X = A \cap B, \\
&= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|) && \text{see below} \\
&= |A| + |B| + |C| - |B \cap C| - |A \cap B| - |A \cap C| + |A \cap B \cap C| && \text{expanding the bracket} \\
&= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| && \text{rearranging.}
\end{aligned}$$

The step marked "see below" simplifies $(A \cap B) \cap (A \cap C)$. Regroup with the commutative and associative laws (1b, 2b) to get $(A \cap A) \cap (B \cap C)$, and $A \cap A = A$ by the idempotent law (7b), leaving $A \cap B \cap C$.

[22] courses/math1061/formula-sheet.pdf

The sign of the triple term comes from the bracket. The rule for $A \cap B$ and $A \cap C$ *subtracts* their overlap, and that whole bracket is itself subtracted, so the overlap ends up added. This is the same "once, not twice" seen in the region counts, reached by algebra.

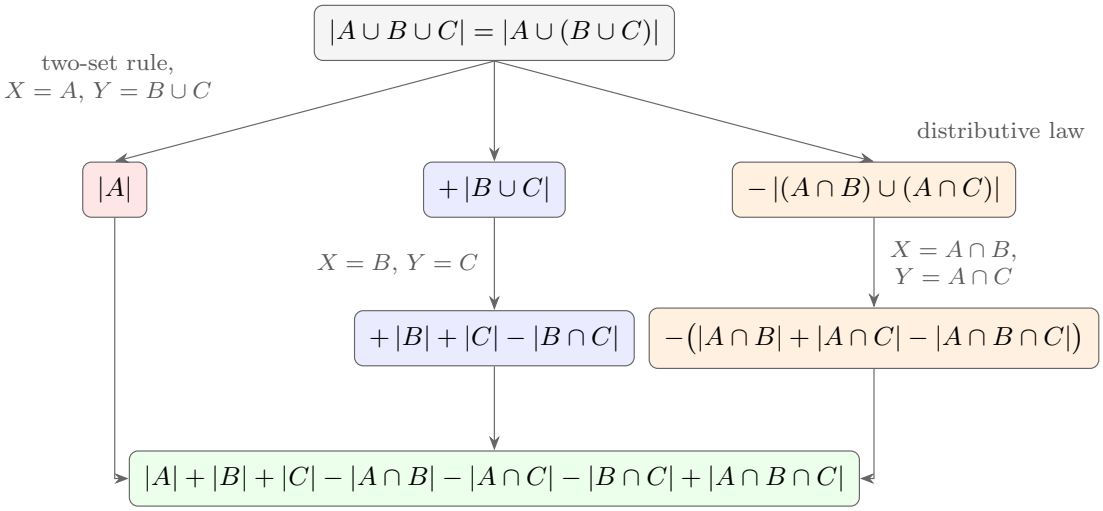


Figure 8: The three-set rule as three uses of the two-set rule. First A is separated from $B \cup C$. That leaves two unions to count: $B \cup C$, and the part of A inside $B \cup C$, which the distributive law writes as $(A \cap B) \cup (A \cap C)$. Each of those is a union of two sets and gets the two-set rule. The overlap of $A \cap B$ and $A \cap C$ is $A \cap B \cap C$, and because it sits inside a bracket that is subtracted, it ends up added.

Worked: divisible by neither 7 nor 11

> Among the integers $1, 2, \ldots, 77$, seven are divisible by 11, eleven are divisible by 7, and one is divisible by both 7 and 11. How many of the integers $1, 2, \ldots, 77$ are divisible by neither 7 nor 11?

Let A be the set of integers from $1, 2, \ldots, 77$ that are divisible by 11, and B the set of those divisible by 7. Then

$$A = \{11, 22, 33, 44, 55, 66, 77\}, \qquad B = \{7, 14, 21, 28, 35, 42, 49, 56, 63, 70, 77\},$$

so $|A| = 7$, $|B| = 11$, and $A \cap B = \{77\}$, since $77 = 7 \cdot 11$ is the only multiple of both that is at most 77.

$A \cup B$ is the set of integers from $1, \ldots, 77$ divisible by at least one of 7 and 11. By inclusion/exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 7 + 11 - 1 = 17.$$

The integers divisible by neither are the ones outside $A \cup B$, so there are

$$77 - |A \cup B| = 77 - 17 = 60.$$

Adding $7 + 11 = 18$ would count 77 twice, once as a multiple of 11 and once as a multiple of 7, and give 59. Checking every integer from 1 to 77 directly also gives 60.

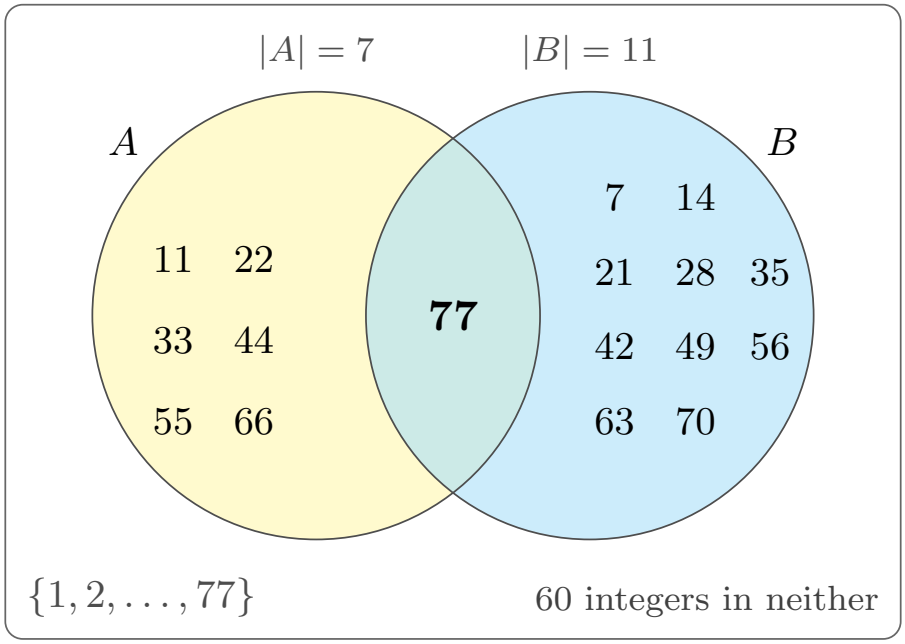


Figure 9: The integers from 1 to 77, with the multiples of 11 in A and the multiples of 7 in B. The only integer in both is $77 = 7 \cdot 11$, so the union has $7 + 11 - 1 = 17$ elements. The 60 integers outside both circles are the ones divisible by neither 7 nor 11.

The general rule

The pattern continues for any number of finite sets: add the sizes of the single sets, subtract the sizes of the pairwise intersections, add the sizes of the triple intersections, subtract the four-way intersections, and so on, alternating, until the intersection of all n sets.

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$
$$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_1 \cap A_3| - |A_2 \cap A_3| + |A_1 \cap A_2 \cap A_3|$$

Adding a fourth set A_4 brings one more term into each group and a new last group: $+|A_4|$ with the singles; $-|A_1 \cap A_4| - |A_2 \cap A_4| - |A_3 \cap A_4|$ with the pairs; $+|A_1 \cap A_2 \cap A_4| + |A_1 \cap A_3 \cap A_4| + |A_2 \cap A_3 \cap A_4|$ with the triples; and the four-way term $-|A_1 \cap A_2 \cap A_3 \cap A_4|$. Four singles, six pairs, four triples and one four-way intersection, 15 terms in all.

Inclusion/exclusion for n sets. For finite sets $A_1, A_2, \ldots, A_n$,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

The conditions $i < j$ and $i < j < k$ make each pair and each triple appear once: $A_1 \cap A_2$ is in the second sum, and $A_2 \cap A_1$, the same set, is not counted again.

The same rule can be written as one sum over the sets of indices. For a set S of indices, $\bigcap_{t \in S} A_t$ is the intersection of the sets whose index is in S; with $S = \{2, 3, 6\}$ it is $A_2 \cap A_3 \cap A_6$. Then

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\substack{S \subseteq \{1,2,\ldots,n\} \\ S \neq \emptyset}} (-1)^{|S|+1} \left| \bigcap_{t \in S} A_t \right|.$$

The sign $(-1)^{|S|+1}$ is $+$ when S has an odd number of indices and $-$ when it has an even number, which is the alternation above. S has to be non-empty: an intersection of no sets at all is not one of the terms. Why every element of the union is counted exactly once, for any n, is in inclusion-exclusion[23].

Worked: words containing "a" and "b"

> In a list of 100 words, there are 47 that contain an "a" and 18 that contain a "b". If there are 51 that contain neither an "a" nor a "b", then how many contain both an "a" and a "b"?

Let A be the set of words that contain an "a" and B the set of words that contain a "b". The question wants $|A \cap B|$.

This runs inclusion/exclusion backwards: the union is found first and the intersection is the unknown. The words containing an "a" or a "b" are all the words except the 51 that contain neither, so

[23] courses/math1061/inclusion-exclusion.pdf

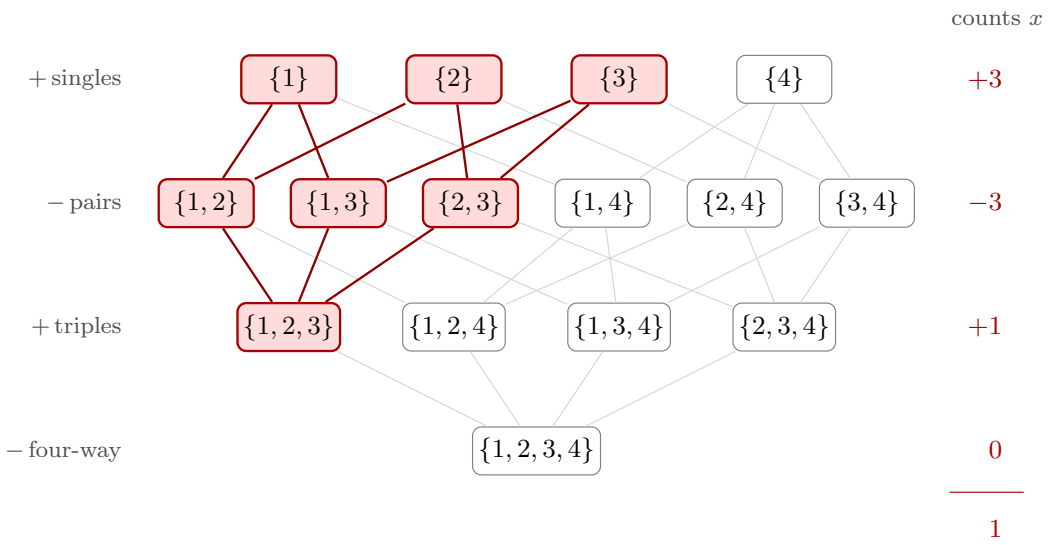


Figure 10: The fifteen terms of inclusion/exclusion for four sets, one for each non-empty set S of indices, in rows by the size of S with the sign each row carries. A line joins S to each index set with one more index. An element x lying in A_1, A_2 and A_3 but not in A_4 is counted by a term exactly when every set in that term contains x, that is, when $S \subseteq 1, 2, 3$; those are the highlighted terms. Three of them are added, three subtracted and one added, so x is counted $3 - 3 + 1 = 1$ time. Any S containing 4 misses x altogether.

$$|A \cup B| = 100 - |(A \cup B)^c| = 100 - 51 = 49.$$

Rearranging $|A \cup B| = |A| + |B| - |A \cap B|$,

$$|A \cap B| = |A| + |B| - |A \cup B| = 47 + 18 - 49 = 16.$$

So **16 words** contain both. Check by filling in the four regions: $47 - 16 = 31$ contain an "a" but no "b", $18 - 16 = 2$ contain a "b" but no "a", 16 contain both and 51 neither, and $31 + 16 + 2 + 51 = 100$.

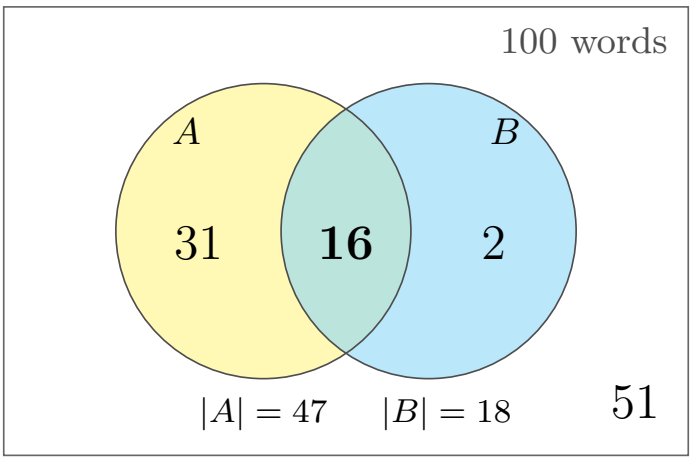


Figure 11: The 100 words split into the four regions of a two-set Venn diagram. The 51 outside both circles fix the union at $100 - 51 = 49$. The two circles hold $47 + 18 = 65$ counts between them, 16 more than the 49 words they contain, and those 16 extra counts are the words in both. The circles are not drawn to scale.

Worked: attendance and exam marks

> In 2015, there were 411 students enrolled in MATH1061. Of these, 270 did not come to class regularly and 118 scored at least 60% on the final exam. If 31 came to class regularly and got less than 60% on the final exam, then how many did not come to class regularly and scored at least 60% on the final exam?

Let A be the set of students who did not come to class regularly, and B the set of students who scored at least 60% on the final exam. The question wants $|A \cap B|$.

The 31 students who came regularly *and* scored below 60% are in neither A nor B: coming regularly puts them outside A, and scoring below 60% puts them outside B. So $|(A \cup B)^c| = 31$ and $|A \cup B| = 411 - 31 = 380$. Then

$$\begin{aligned} |A \cap B| &= |A| + |B| - |A \cup B| \\ &= |A| + |B| - (411 - |(A \cup B)^c|) \\ &= 270 + 118 - (411 - 31) \\ &= 388 - 380 = 8. \end{aligned}$$

So **8 students** did not come to class regularly and still scored at least 60%. The four regions are $270 - 8 = 262$ in A only, 8 in both, $118 - 8 = 110$ in B only and 31 in neither, which add to 411.

The step to be careful with is reading "came regularly and got less than 60%" as the complement of the union. It is the negation of both conditions, $A^c \cap B^c$, which by De Morgan's law (9a) is $(A \cup B)^c$.

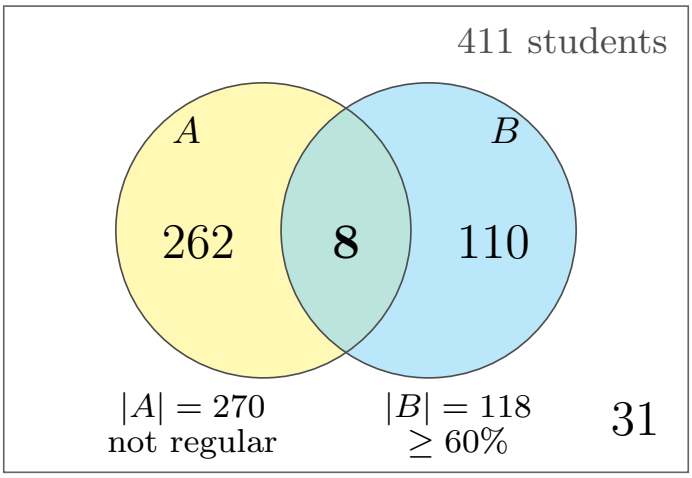


Figure 12: The 411 students by attendance and exam result. A is the students who did not come to class regularly and B those who scored at least 60%. The 31 who came regularly and scored below 60% are outside both circles, so the union holds 380, and the overlap is the $270 + 118 - 380 = 8$ students counted in both circles. The circles are not drawn to scale.

Worked: divisible by none of 3, 5, 7

How many of the integers $\{1, 2, \ldots, 105\}$ are divisible by none of 3, 5 or 7?

Let $S = \{1, 2, \ldots, 105\}$. Let A be the set of integers in S divisible by 3, B those divisible by 5, and C those divisible by 7.

Single sets. Every third integer is a multiple of 3, so $|A|$ is $105 \div 3$. Since $105 = 3 \cdot 5 \cdot 7$, each division is exact.

$$|A| = \frac{105}{3} = 35, \qquad |B| = \frac{105}{5} = 21, \qquad |C| = \frac{105}{7} = 15.$$

Pairs. An integer divisible by both 3 and 5 is divisible by 15, because 3 and 5 are different primes, so $A \cap B = \{x \in S : 15 \mid x\}$. The same holds for every pair and for all three.

$$|A \cap B| = \frac{105}{15} = 7, \qquad |A \cap C| = \frac{105}{21} = 5, \qquad |B \cap C| = \frac{105}{35} = 3, \qquad |A \cap B \cap C| = \frac{105}{105} = 1.$$

The union. By inclusion/exclusion for three sets,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C| \\ &= 35 + 21 + 15 - 7 - 5 - 3 + 1 \\ &= 71 - 15 + 1 = 57. \end{aligned}$$

None of them. The integers divisible by none of 3, 5 and 7 are the ones outside the union:

$$|(A \cup B \cup C)^c| = |S| - |A \cup B \cup C| = 105 - 57 = 48.$$

So **48** of the integers are divisible by none of 3, 5 or 7. Checking all 105 directly gives the same.

Worked: 1 and 2 first or 5 last

> What is the probability that a randomly chosen permutation of $\{1, 2, 3, 4, 5\}$ has 1 and 2 in the first two positions (not necessarily in that order), or has 5 in the last position?

With every permutation equally likely, the probability of an event is the number of permutations in it divided by the number of permutations, $5! = 120$ (probability[24]). Let A be the set of permutations with 1 and 2 in the first two positions, and B the set of permutations with 5 in the last position. The event is $A \cup B$.

[24] courses/math1061/probability.pdf

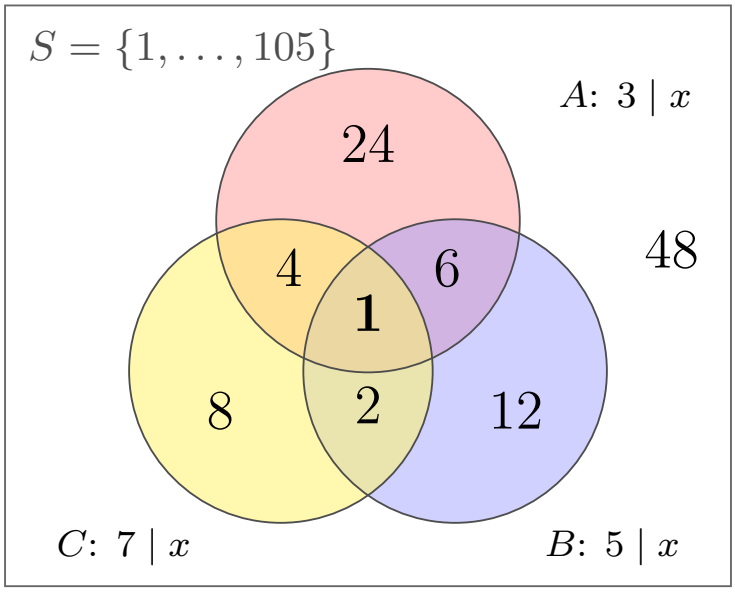


Figure 13: The integers from 1 to 105, sorted by which of 3, 5 and 7 divide them. Only 105 is in all three sets. The two-set regions hold the multiples of 15, 21 and 35 other than 105, and the single-set regions what is left of each set. The seven regions inside add to 57, so 48 integers lie outside every circle.

- $|A|$**.** The first two positions hold 1 and 2 in one of 2 orders, 12 or 21. The other three numbers fill the last three positions in 3! ways. So $|A| = 2 \cdot 3! = 12$.
- $|B|$**.** 5 is fixed in the last position, and the other four numbers fill the first four in any order: $|B| = 4! = 24$.
- $|A \cap B|$**.** 1 and 2 in front in 2 orders, 5 last, and 3 and 4 in the middle two positions in 2! ways: $|A \cap B| = 2 \cdot 2! = 4$.

By inclusion/exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 12 + 24 - 4 = 32,$$

and

$$P(A \cup B) = \frac{|A \cup B|}{5!} = \frac{32}{120} = \frac{4}{15} \approx 26.7\%.$$

Dividing the inclusion/exclusion identity through by 120 gives the same answer in terms of probabilities,

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{1}{10} + \frac{1}{5} - \frac{1}{30} = \frac{4}{15}.$$

Listing all 120 permutations and counting confirms 32. The four in $A \cap B$ are 12345, 12435, 21345 and 21435, and adding $12 + 24$ without subtracting them would count each of them twice.

See also

- inclusion-exclusion[25] — the principle for two, three and n sets, why it counts each element once, "none of them" through the complement, counting multiples, and probabilities
- counting-principles[26] — the addition rule for disjoint sets and the difference rule, which inclusion/exclusion extends
- [probability] — probability by counting equally likely outcomes, used in the last question
- 2026-10-19-probability-binomial-coefficients[27] — Lecture 31 · 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[28] — Lecture 33
- practice-problems[29] — §41, with full worked solutions

[25] courses/math1061/inclusion-exclusion.pdf
[26] courses/math1061/counting-principles.pdf
[27] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf
[28] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[29] courses/math1061/practice-problems.pdf

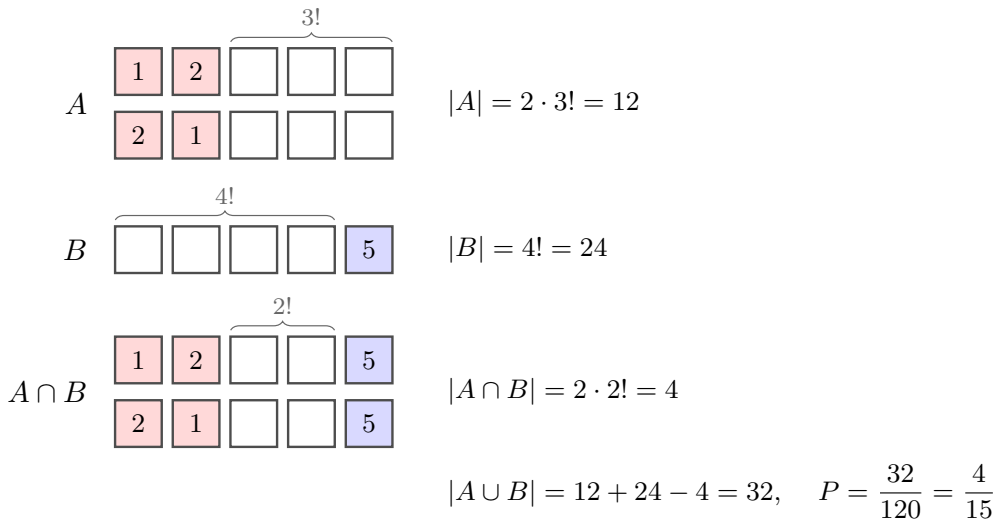


Figure 14: Counting the permutations of $1, \ldots, 5$ in A, in B and in both, position by position. In A, 1 and 2 take the first two positions in either order and the other three numbers fill the rest. In B, 5 is fixed last and the other four are free. A permutation in both has all three restrictions, leaving only 3 and 4 to arrange in the middle.

Lecture 33 — Pigeonhole Principle, Introduction to Graph Theory

Two topics: the pigeonhole principle, used to prove that a selection of numbers must contain a pair (or a triple, or two subsets) of a certain kind, and the first definitions of graph theory: graphs, loops, multiple edges, simple graphs, degree, the Handshake Theorem and degree sequences. Pre-work: Video 042 (The Pigeonhole Principle) and Video 043 (Introduction to Graph Theory). The principle, its generalised form, how to choose the pigeons and the holes, and more examples are in pigeonhole-principle[30]. Graphs, degree, the Handshake Theorem and its corollary, and degree sequences are in [graphs].

Goals

1. Learn how to use the pigeonhole principle to solve various problems.
2. Understand the basic terminology and definitions of graph theory.

Two questions to keep in mind:

[30] courses/math1061/pigeonhole-principle.pdf

- **What does the pigeonhole principle look like in practice?** Four arguments below (no two consecutive, a pair summing to 101, no three consecutive, equal subset sums), and more examples, with a guide to choosing the holes, in pigeonhole-principle[31].
- **Why does every graph have an even number of vertices of odd degree?** It follows from the Handshake Theorem, and it settles which statement about degrees is true.

The pigeonhole principle

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

Ten pigeons and nine holes: if every hole held at most one pigeon, the holes would hold at most nine pigeons, and there are ten. So some hole holds two. That is the whole proof, for any $n > m$.

In a proof the pigeons are the objects chosen and the holes are categories that every object falls into. The skill is choosing the holes so that **two pigeons in one hole is exactly the thing to be proved**. In each problem below the holes are a partition of the set the numbers come from, built so that two chosen numbers in the same part give the pair that is wanted.

Many of these problems ask for the **largest** selection with some property. The answer then needs two halves:

1. **A selection of that size exists.** Write one down.
2. **No larger selection exists.** This is the pigeonhole half.

Worked: no two consecutive

> What is the largest number of integers that can be selected from $\{1, 2, \ldots, 100\}$ such that no two selected integers are consecutive?
> A. 49
> B. 50
> C. 51
> D. 52
> E. 99

Answer: B, 50.

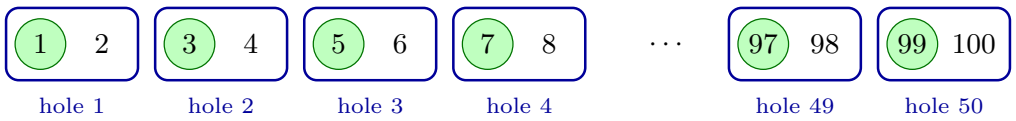
50 is possible. Take the odd numbers $1, 3, 5, \ldots, 99$. There are 50 of them, and any two differ by at least 2, so no two are consecutive.

More than 50 is impossible. Split $\{1, 2, \ldots, 100\}$ into the 50 pairs

[31] courses/math1061/pigeonhole-principle.pdf

$$\{1,2\},\ \{3,4\},\ \{5,6\},\ \ldots,\ \{99,100\}.$$

Every number is in exactly one pair, and each pair is two consecutive numbers. Choose more than 50 numbers. They are the pigeons, the 50 pairs are the holes, and by the pigeonhole principle some pair has both of its numbers chosen. Those two are consecutive.



50 holes, at most one chosen number in each: at most 50 numbers

Figure 15: The numbers 1 to 100 split into 50 pairs of consecutive numbers, the holes. A selection with no two consecutive numbers takes at most one number from each pair, so it has at most 50 numbers. The odd numbers, shaded, take exactly one from each pair and reach 50. A 51st number would have to go into a pair that already has one, and would sit next to it.

The other options:

- **A, 49**, can be done (drop one odd number), but it is not the largest.
- **C, 51**, and **D, 52**, are both more than 50, so the pigeonhole argument rules them out.
- **E, 99**, leaves out only one number. Whichever number k is left out, at least one of $\{1,\ldots,k-1\}$ and $\{k+1,\ldots,100\}$ has two or more numbers in it, and each of those is a run of consecutive numbers.

Worked: two numbers that sum to 101

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

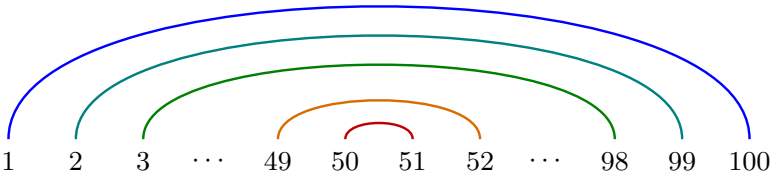
Pair each number with the number it adds to 101 with:

$$P_1 = \{1,100\},\ P_2 = \{2,99\},\ P_3 = \{3,98\},\ \ldots,\ P_{50} = \{50,51\}.$$

In general $P_i = \{i, 101-i\}$ for $1 \le i \le 50$. These 50 sets are disjoint and between them contain every number from 1 to 100 exactly once, since i runs over $1,\ldots,50$ and $101-i$ runs over $100,\ldots,51$.

Proof. Choose 51 numbers from $\{1, 2, \ldots, 100\}$. Each lies in exactly one of the 50 sets $P_1, \ldots, P_{50}$. Since $51 > 50$, by the pigeonhole principle there is some i with $1 \le i \le 50$ such that both numbers in P_i were chosen. Those two numbers are i and $101 - i$, and $i + (101 - i) = 101$. $\square$

51 is the smallest number that works. The 50 numbers $1, 2, \ldots, 50$ contain no such pair, since the largest sum of two of them is $49 + 50 = 99$.



$P_1 = \{1, 100\}$, $P_2 = \{2, 99\}$, $P_3 = \{3, 98\}$, $\ldots$, $P_{49} = \{49, 52\}$, $P_{50} = \{50, 51\}$

Figure 16: The holes for the sum-101 problem. Each arc joins two numbers that add to 101, i and $101 - i$, and the arcs nest because as one end moves in by one the other moves in by one too. There are 50 arcs and every number from 1 to 100 is the end of exactly one. 51 chosen numbers are more than the 50 arcs, so some arc has both of its ends chosen, and those two numbers sum to 101.

Worked: no three consecutive

> What is the maximum number of integers that can be chosen from $\{1, 2, \ldots, 60\}$ such that no three of the chosen numbers are consecutive?

"No three consecutive" means there is no integer a with a, $a + 1$ and $a + 2$ all chosen.

Answer: 40.

40 is possible. Choose every number that is not a multiple of 3, that is, every number congruent to 1 or 2 mod 3:

$$1, 2,\ 4, 5,\ 7, 8,\ \ldots,\ 58, 59.$$

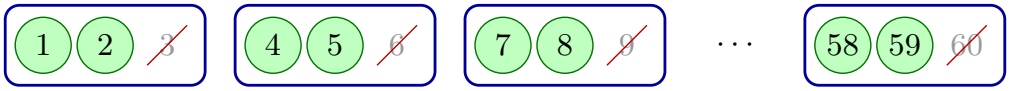
Any three consecutive integers include a multiple of 3, which was not chosen, so no three chosen numbers are consecutive. Two of every three numbers are chosen, $60 \cdot \frac{2}{3} = 40$ in all.

41 or more is impossible. Split $\{1, 2, \ldots, 60\}$ into the 20 blocks

$$\{1, 2, 3\},\ \{4, 5, 6\},\ \{7, 8, 9\},\ \ldots,\ \{58, 59, 60\}.$$

A block with all three of its numbers chosen gives three consecutive chosen numbers, so a good selection takes at most 2 from each block, at most $2 \cdot 20 = 40$ in all. If 41 or more numbers are chosen then, since $41 > 40 = 2 \cdot 20$, some block has all 3 of its numbers chosen.

This last step is the pigeonhole principle with "more than one" replaced by "more than two": if more than $2m$ pigeons go into m holes, some hole gets at least 3. If every hole had at most 2 there would be at most $2m$ pigeons. It is the generalised form in pigeonhole-principle[32].



20 blocks, at most 2 chosen from each: at most $2 \cdot 20 = 40$

Figure 17: The numbers 1 to 60 split into 20 blocks of three consecutive numbers. A block with all three chosen breaks the rule, so a good selection takes at most 2 from each block, at most 40 in all, and 41 numbers force some block to be full. Taking the first two of every block, shaded, and leaving out the multiples of 3, struck through, reaches 40. Two blocks side by side never make a run of three, because the multiple of 3 between them is missing.

Worked: two subsets with the same sum

> Show that if A is any 6-element subset of $\{1, 2, \ldots, 12\}$, then A has distinct subsets X and Y such that the sum of the elements in X equals the sum of the elements in Y.

For example, $A = \{2, 4, 6, 8, 10, 12\}$ has $X = \{6\}$ and $Y = \{2, 4\}$, both summing to 6. The task is to show such a pair exists for **every** A, without knowing what A is.

The pigeons are the subsets of A, the holes are the possible sums.

Pigeons. Write $A = \{a_1, a_2, \ldots, a_6\}$ with $1 \le a_1 < a_2 < \cdots < a_6 \le 12$, all integers. A has

$$|\mathcal{P}(A)| = 2^{|A|} = 2^6 = 64$$

subsets, counting $\emptyset$ and A itself (sets-and-set-notation[33]).

Holes. For a subset $S \subseteq A$ let $\Sigma(S)$ be the sum of its elements, with $\Sigma(\emptyset) = 0$. Every element is positive, so a subset's sum is at least 0 and at most the sum of all of A:

[32] courses/math1061/pigeonhole-principle.pdf
[33] courses/math1061/sets-and-set-notation.pdf

$$0 \le \Sigma(S) \le a_1 + a_2 + \cdots + a_6.$$

The six elements of A are six different integers that are at most 12, so the largest they can be is $7, 8, 9, 10, 11, 12$:

$$a_1 + a_2 + \cdots + a_6 \le 7 + 8 + 9 + 10 + 11 + 12 = 57.$$

So every subset sum is one of the 58 integers $0, 1, 2, \ldots, 57$.

Conclusion. 64 subsets, each with a sum among 58 possible values. Since $64 > 58$, by the pigeonhole principle two different subsets $X \neq Y$ of A have the same sum. □

The bound on the sum is the step that needs care. Bounding it by the sum of the whole of $\{1, \ldots, 12\}$, which is 78, gives 79 holes for 64 pigeons, and the argument says nothing.

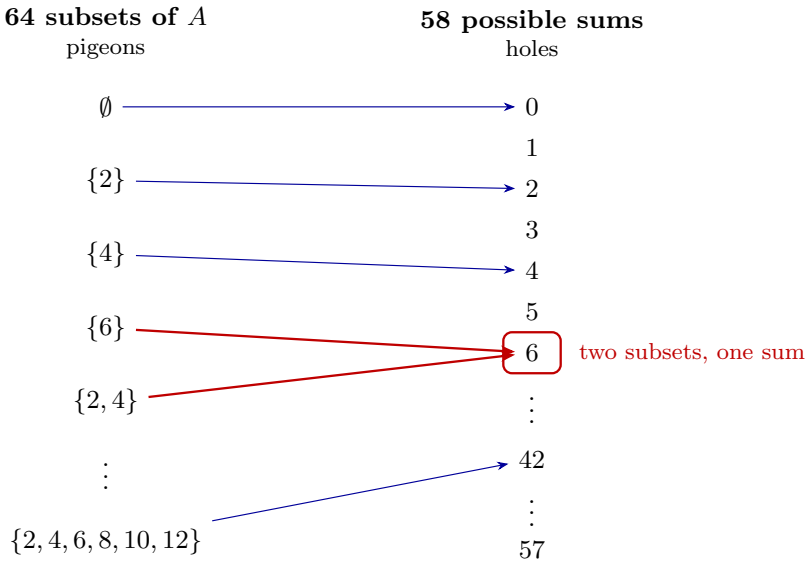


Figure 18: The subset-sum argument for $A = 2, 4, 6, 8, 10, 12$. Each of the 64 subsets of A, on the left, goes to its sum, on the right. However A is chosen, its sum is at most $7+8+\cdots+12 = 57$, so the sums lie among the 58 values 0 to 57. Sending 64 subsets to 58 values must send two subsets to the same value. Here 6 and $2, 4$ both go to 6.

Disjoint subsets. If X and Y share elements, take the shared ones out of both. The sums both drop by the same amount, so they stay equal, and $X - Y$ and $Y - X$ are disjoint. Neither is empty: if $X - Y$ were empty then X would be a proper subset of Y, and Y would have the larger sum, since every element is positive.

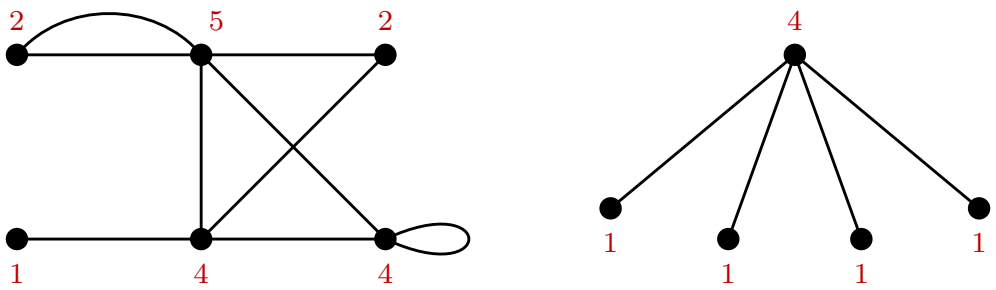
Graphs

> 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**. A graph is drawn with a dot for each vertex and, for each edge, a line joining its two endpoints, or, for an edge with a single endpoint, a line from that dot back to itself. A graph can have no edges at all, just dots, but it must have at least one vertex.

- A **loop** is an edge with only one endpoint.
- **Multiple edges** (also called parallel edges) are two or more edges with the same endpoints.
- A graph is **simple** if it has no loops and no multiple edges.

The **degree** of a vertex v, written $\deg(v)$, is the number of edge ends incident with it. An ordinary edge has one end at each of its endpoints. A loop has both of its ends at the same vertex, so **a loop adds 2 to the degree**.



$2+5+2+1+4+4=18$
$=2\cdot 9$ edges

$4+1+1+1+1=8$
$=2\cdot 4$ edges

Figure 19: Degrees counted as edge ends. Left: a graph with a pair of multiple edges between the two top-left vertices and a loop at the bottom-right vertex. The bottom-right vertex has degree 4: one end each from the edges to its two neighbours, and two from the loop. The top-middle vertex has degree 5, two of them from the multiple edges. The degrees add to 18, and there are 9 edges. Right: a simple graph, one vertex joined to four others. The centre has degree 4 and each of the others degree 1, a total of 8 for 4 edges.

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 $V(G) = \{v_1, v_2, \ldots, v_n\}$ and $|E(G)| = e$, then

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

Why. Adding up the degrees counts every edge end in the graph once, at the vertex it touches. Every edge has exactly two ends, an ordinary edge one at each endpoint and a loop both at its one endpoint. So the total number of ends is $2e$. In the left graph above, 9 edges give 18 ends, and the degrees add to 18.

So the sum of the degrees is always even. That gives the corollary:

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

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

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

The first sum adds even numbers, so it is even. The left side is even. So the second sum, the difference of two even numbers, is even too. It is a sum of odd numbers, and a sum of odd numbers is even only when there is an even number of them. So the number of vertices of odd degree is even. □

In the left graph above the odd-degree vertices are the ones of degree 5 and 1, two of them. In the right graph they are the four vertices of degree 1.

The proof of the theorem, and more on degree, are in graphs[34].

Worked: which statement about degrees is true

Which of the following is true?
(a) In any graph there is an even number of vertices of even degree.
(b) In any graph there is an odd number of vertices of even degree.
(c) In any graph there is an even number of vertices of odd degree.
(d) In any graph there is an odd number of vertices of odd degree.

[34] courses/math1061/graphs.pdf

Answer: (c). It is the corollary of the Handshake Theorem just proved:

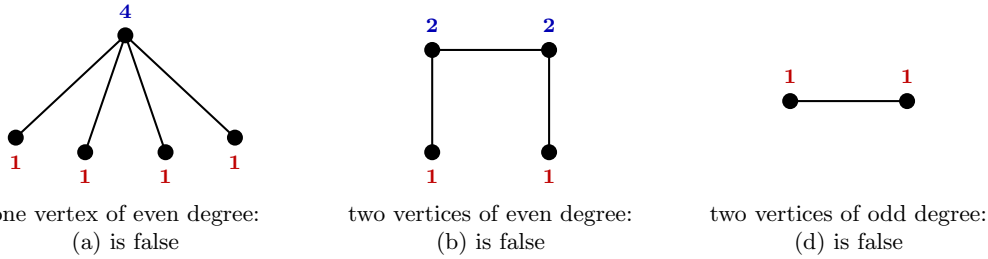
$$\sum_{i=1}^{n} \deg(v_i) = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) = 2e$$

is even, so the odd degrees among $\deg(v_1), \ldots, \deg(v_n)$ must come in an even number.

Each of the others says "in any graph", so one graph where it fails is enough to show it is false.

- **(a) is false.** One vertex joined to four others has degrees $4, 1, 1, 1, 1$: one vertex of even degree. (A graph with a single vertex and no edges, one vertex of degree 0, also works.)
- **(b) is false.** Four vertices in a path have degrees $1, 2, 2, 1$: two vertices of even degree.
- **(d) is false.** Two vertices joined by one edge have degrees $1, 1$: two vertices of odd degree. In fact (d) is false for **every** graph, by (c).

Statements (a) and (b) fail because the number of even-degree vertices can be anything: the corollary controls only the odd ones.



one vertex of even degree: (a) is false

two vertices of even degree: (b) is false

two vertices of odd degree: (d) is false

Figure 20: Three graphs that each break one of the false statements. Even degrees are blue and odd degrees red. Left: one vertex joined to four others has just one vertex of even degree, so the number of even-degree vertices need not be even. Middle: a path of four vertices has two vertices of even degree, so it need not be odd either. Right: a single edge has two vertices of odd degree, so the number of odd-degree vertices is not odd. In every graph, as in these three, the red labels come in an even number.

Worked: degree sequences

The list of the degrees of the vertices of a graph is its **degree sequence**.

> For each of the following lists, draw a **simple** graph with vertices whose degrees are the numbers in the list, or explain why no such graph exists.
> (a) 2, 2, 2, 2
> (b) 3, 2, 1

(c) 4, 3, 2, 2, 2, 2, 1, 1
(d) 1, 1, 1, 1
(e) 5, 5, 5, 5, 5, 5

Two checks rule a list out straight away:

- **The sum must be even**, by the Handshake Theorem. Equivalently, the list must contain an even number of odd entries.
- **In a simple graph with n vertices every degree is at most $n-1$.** With no loops and no multiple edges, a vertex has at most one edge to each of the other $n-1$ vertices.

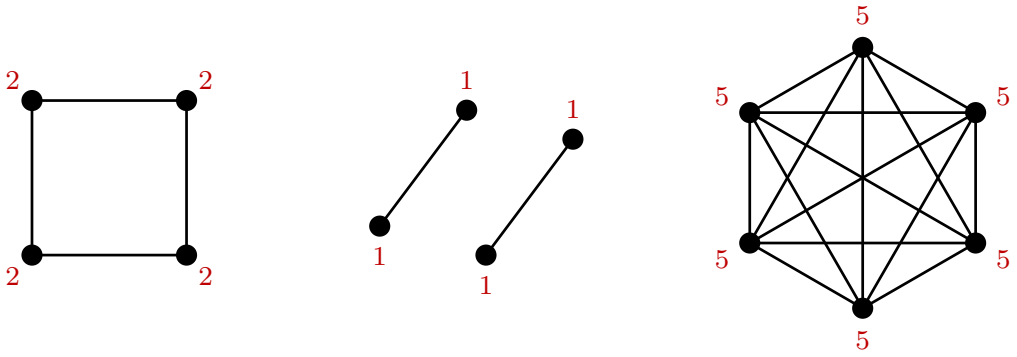
Passing both checks does not guarantee a graph, so for a list that passes, draw one.

List	Sum	Largest entry vs $n-1$	Simple graph?
(a) 2, 2, 2, 2	8	$2 \leq 3$	yes: a square, 4 edges
(b) 3, 2, 1	6	$3 > 2$	**no**
(c) 4, 3, 2, 2, 2, 2, 1, 1	17, odd	$4 \leq 7$	**no**
(d) 1, 1, 1, 1	4	$1 \leq 3$	yes: two separate edges
(e) 5, 5, 5, 5, 5, 5	30	$5 \leq 5$	yes: every pair of the 6 vertices joined, 15 edges

- **(a)** Four vertices around a square, each joined to its two neighbours. Each has degree 2, and $8 = 2 \cdot 4$ edges.
- **(b)** There are only three vertices, so in a simple graph a vertex can be joined to at most the other two, and degree 3 is impossible. The sum, 6, is even, so the Handshake Theorem alone does not rule it out. Without the word *simple* there is a graph: join the degree-3 vertex to the degree-2 vertex by two multiple edges and to the degree-1 vertex by one edge. That graph has multiple edges, so it is not simple.
- **(c)** The odd entries are 3, 1 and 1, three of them. A graph must have an even number of vertices of odd degree, so no graph exists, simple or not. Equivalently, the sum is 17, which is not $2e$ for any e.
- **(d)** Two edges with no vertex in common. Each vertex is the end of one edge.
- **(e)** Six vertices, every pair joined by an edge. Each vertex is joined to the other 5. There are $\binom{6}{2} = 15$ edges, and $6 \cdot 5 = 30 = 2 \cdot 15$.

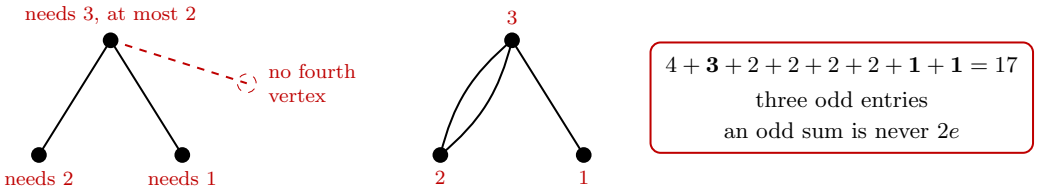
More on degree sequences, including a list that passes both checks and still has no simple graph, is in graphs[35].

[35] courses/math1061/graphs.pdf



(a) 2, 2, 2, 2 (d) 1, 1, 1, 1 (e) 5, 5, 5, 5, 5, 5

Figure 21: Simple graphs for the three lists that can be realised, each vertex labelled with its degree. (a) 2, 2, 2, 2: a square, each vertex joined to its two neighbours. (d) 1, 1, 1, 1: two edges sharing no vertex. (e) 5, 5, 5, 5, 5, 5: six vertices with every pair joined, 15 edges, so each vertex is joined to all 5 others.



(b) simple: impossible (b) with multiple edges: a graph, but not simple (c) no graph at all

Figure 22: Why lists (b) and (c) have no simple graph. (b) 3, 2, 1: each vertex is labelled with the degree it needs. With three vertices, the vertex that needs degree 3 can be joined to only the 2 others, since a simple graph allows at most one edge to each. A third edge would need a fourth vertex, or a second edge to a vertex it already meets. Allowing multiple edges gives a graph, in the middle, but it is not simple. (c) 4, 3, 2, 2, 2, 2, 1, 1: three entries are odd, and the number of odd-degree vertices in any graph is even.

See also

- pigeonhole-principle[36] — the principle, its generalised form, choosing the holes, and more examples
- [graphs] — graphs, loops and multiple edges, degree, the Handshake Theorem and degree sequences
- 2026-07-27-welcome-and-intro-problems[37] — the five friends with equal friend counts, and the bridges of Königsberg as a graph
- 2026-10-20-inclusion-exclusion[38] — Lecture 32
- practice-problems[39] — §42, with full worked solutions
- practice-problems[40] — §43, with full worked solutions

Reference material

Binomial Coefficients

The numbers $\binom{n}{r}$ count subsets, and they are also the coefficients that appear when $(a+b)^n$ is multiplied out, which is where the name **binomial coefficient** comes from. This note collects the identities they satisfy and the way each is proved by counting: the symmetry $\binom{n}{r} = \binom{n}{n-r}$, **Pascal's formula** and the triangle it builds, the **Binomial Theorem**, how to pick a single coefficient out of an expansion such as $(3x-2)^5$, and why every row of Pascal's triangle adds up to a power of 2. The definition and the formula $\frac{n!}{r!\,(n-r)!}$ are in counting-selections[41]. Using these counts to work out probabilities is in [probability]. First met in 2026-10-19-probability-binomial-coefficients[42].

n **choose** r

$\binom{n}{r}$, read "n choose r", is the number of r-element subsets of a set with n elements:

$$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 1}, \qquad 0 \le r \le n.$$

[36] courses/math1061/pigeonhole-principle.pdf
[37] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[38] courses/math1061/2026-10-20-inclusion-exclusion.pdf
[39] courses/math1061/practice-problems.pdf
[40] courses/math1061/practice-problems.pdf
[41] courses/math1061/counting-selections.pdf
[42] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf

Why it divides by $r!$, and how to calculate it without large factorials, is in counting-selections[43]. Two values come up constantly: $\binom{n}{0} = \binom{n}{n} = 1$ (one way to take nothing, one way to take everything) and $\binom{n}{1} = n$.

Everything below rests on reading $\binom{n}{r}$ as a **count**, not as a formula. Most identities about binomial coefficients can be proved by grinding through factorials, but each one is also the statement that two ways of counting the same collection agree, and that version explains *why* it is true.

Combinatorial proofs

A **combinatorial proof** of an identity LHS = RHS finds one collection of objects and counts it twice: once in a way that gives the left side, once in a way that gives the right side. Both counts are counts of the same thing, so they are equal. No algebra is needed. The work is in choosing the collection, and in checking that each count really counts every object exactly once.

There are two common shapes.

- **A pairing.** Match the objects counted by the left side one-to-one with the objects counted by the right side. That is how the symmetry is proved: each subset is paired with its complement.
- **Splitting into cases.** Count a collection directly for one side, and split it into disjoint cases, added up, for the other. That is how Pascal's formula and the row sum are proved.

Symmetry: $\binom{n}{r} = \binom{n}{n-r}$

For $0 \le r \le n$,

$$\binom{n}{r} = \binom{n}{n-r}.$$

Why. Choosing which r elements of an n-element set go *into* a subset is the same act as choosing which $n-r$ elements are left *out*. Every r-element subset A has a complement, the $n-r$ elements not in A, and every $(n-r)$-element subset is the complement of exactly one r-element subset. So the subsets of the two sizes pair off exactly, and there are the same number of each.

Using it. Calculate whichever of the two has the smaller bottom number:

$$\binom{12}{8} = \binom{12}{4} = \frac{12 \cdot 11 \cdot 10 \cdot 9}{4 \cdot 3 \cdot 2 \cdot 1} = 495, \qquad \binom{7}{4} = \binom{7}{3} = \frac{7 \cdot 6 \cdot 5}{3 \cdot 2 \cdot 1} = 35.$$

[43] courses/math1061/counting-selections.pdf

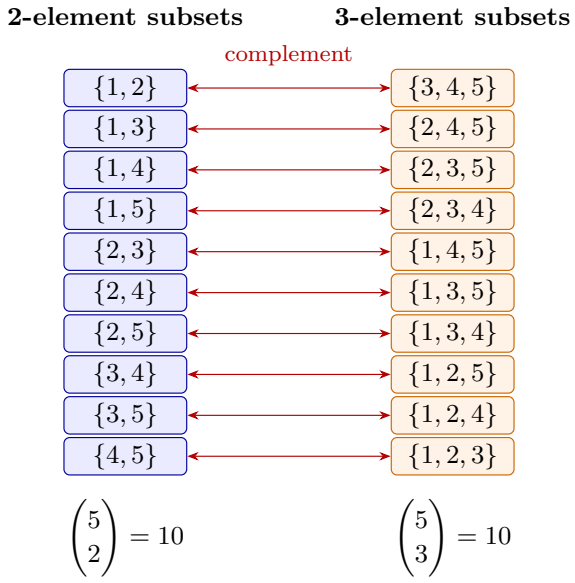


Figure 23: The ten 2-element subsets of $1, 2, 3, 4, 5$, each joined to its complement, the three elements it leaves out. Every 2-element subset has exactly one complement, and every 3-element subset is the complement of exactly one 2-element subset, so the two lists pair off with nothing left over. That pairing is the proof that $\binom{5}{2} = \binom{5}{3} = 10$, and the same pairing of each r-element subset with its complement proves $\binom{n}{r} = \binom{n}{n-r}$.

Dividing into two groups. The number of ways to split 400 students into a group of 150 and a group of 250 is $\binom{400}{150}$: choose who goes in the group of 150, and the other 250 make up the second group. Choosing the group of 250 first gives $\binom{400}{250}$, and the symmetry says these are the same number,

$$\binom{400}{150} = \binom{400}{250} = \frac{400!}{150!\,250!}.$$

It is about 3.47×10^{113}, a 114-digit number, so the factorial form is the answer. Choosing one group settles the other, so there is a single binomial coefficient, not a product of two.

Pascal's formula

Pascal's formula. For integers n and r with $1 \le r \le n$,

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

A case first. Take $n = 8$ and $r = 3$. The formula says

$$\binom{9}{3} = \binom{8}{2} + \binom{8}{3}, \qquad 84 = 28 + 56.$$

The left side counts the 3-element subsets of $\{1, 2, \dots, 9\}$. Split them according to whether they contain the largest element, 9.

- **Subsets that contain 9**, such as $\{1, 7, 9\}$. The 9 is already in, so the subset is decided by its other two elements, which are any two of $1, \dots, 8$. Each such subset is $\{9\}$ joined to a 2-element subset of $\{1, \dots, 8\}$, and there are $\binom{8}{2} = 28$ of them.
- **Subsets that do not contain 9**, such as $\{1, 7, 8\}$. All three elements come from $1, \dots, 8$, so these are exactly the 3-element subsets of $\{1, \dots, 8\}$: $\binom{8}{3} = 56$ of them.

Every 3-element subset of $\{1, \dots, 9\}$ is in exactly one of the two cases, so by the addition rule (counting-principles[44]) $\binom{9}{3} = \binom{8}{2} + \binom{8}{3}$.

The proof in general. Let $1 \le r \le n$. The left side $\binom{n+1}{r}$ counts the r-element subsets of $\{1, 2, \dots, n+1\}$. Split them by whether they contain $n + 1$.

[44] courses/math1061/counting-principles.pdf

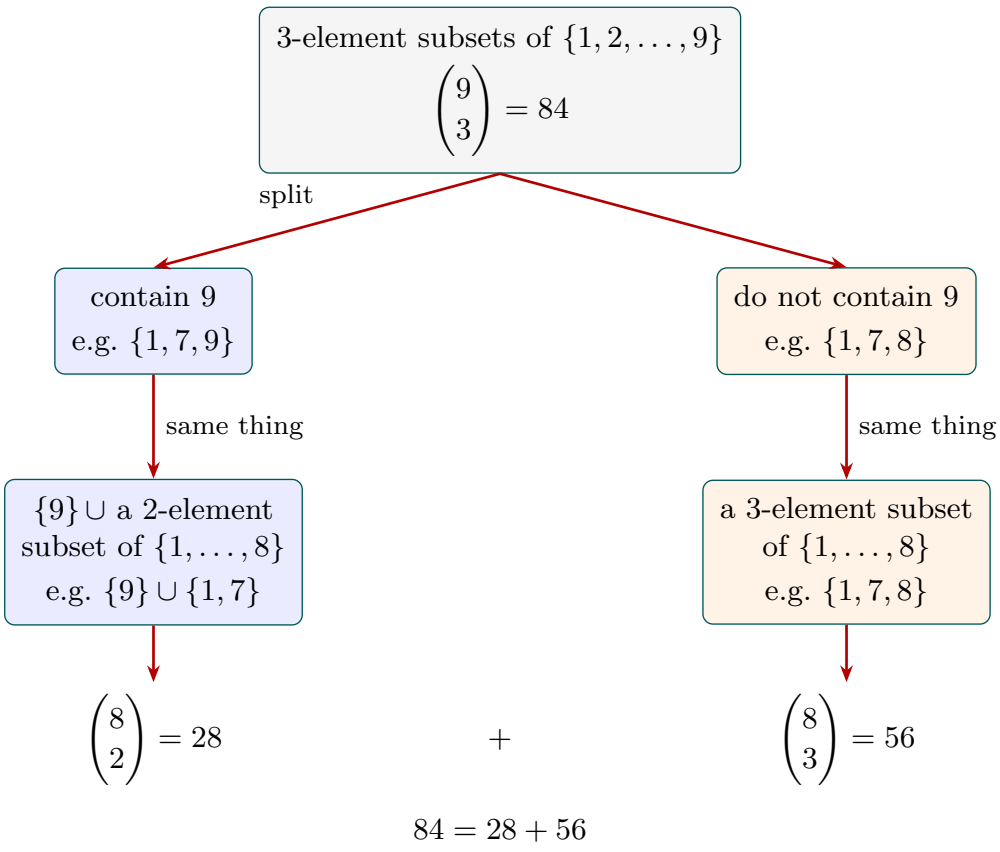


Figure 24: The combinatorial proof of Pascal's formula with $n = 8$ and $r = 3$. The 3-element subsets of $1, \ldots, 9$ either contain 9 or they don't, never both. One that contains 9, like $1, 7, 9$, is decided by its other two elements, a 2-element subset of $1, \ldots, 8$. One that doesn't, like $1, 7, 8$, is a 3-element subset of $1, \ldots, 8$. Counting the two cases and adding gives $\binom{9}{3} = \binom{8}{2} + \binom{8}{3}$.

1. **Those that contain $n+1$.** Removing $n+1$ leaves an $(r-1)$-element subset of $\{1, \dots, n\}$, and adding $n+1$ to any $(r-1)$-element subset of $\{1, \dots, n\}$ gives one of these back. So there are $\binom{n}{r-1}$ of them.
2. **Those that do not contain $n+1$.** These are exactly the r-element subsets of $\{1, \dots, n\}$, and there are $\binom{n}{r}$ of them.

Every r-element subset of $\{1, \dots, n+1\}$ falls in exactly one case, so $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$. $\square$

The one idea to remember is **fix one element and ask whether it is in or out**. "In" uses up one of the r places, which is where the $r-1$ comes from. "Out" uses up none of the places but removes the element from the pool, which is where the n in place of $n+1$ comes from.

Algebraic check. The same identity follows from the factorial formula, by putting both terms over the common denominator $r!\,(n-r+1)!$:

$$\binom{n}{r-1} + \binom{n}{r} = \frac{n!\,r}{r!\,(n-r+1)!} + \frac{n!\,(n-r+1)}{r!\,(n-r+1)!} = \frac{n!\,(n+1)}{r!\,(n+1-r)!} = \binom{n+1}{r}.$$

It is correct but says nothing about why the identity holds.

Pascal's triangle

Write the binomial coefficients in rows, row n holding $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{n}$, centred under one another. The result is **Pascal's triangle**. Each row starts and ends with 1, since $\binom{n}{0} = \binom{n}{n} = 1$, and Pascal's formula says that **every other entry is the sum of the two entries diagonally above it**. So the triangle can be built row by row with nothing but addition.

What to read off the triangle:

- **Row n is the list of coefficients of** $(a+b)^n$ (below). Row 3 is $1, 3, 3, 1$ and $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.
- **Each row is a palindrome**: that is the symmetry.
- **Each row adds up to a power of 2**: $1+4+6+4+1 = 16 = 2^4$. That is the row sum.

Row 8, for reference, is $1, 8, 28, 56, 70, 56, 28, 8, 1$.

a, b-sequences

> A sequence of n terms, each of which is either a or b, is an **a, b-sequence of length n**. For example, $aabab$ is an a, b-sequence of length 5.

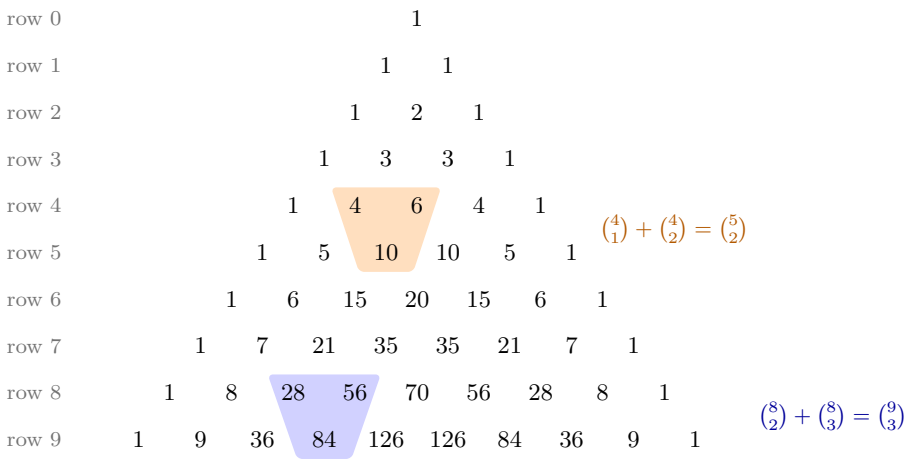


Figure 25: Pascal's triangle, rows 0 to 9. The entry in row n, position k (counting from 0 at the left) is $\binom{n}{k}$. Each entry inside the triangle is the sum of the two above it, which is Pascal's formula. Two additions are picked out: $4+6=10$ is $\binom{4}{1}+\binom{4}{2}=\binom{5}{2}$, and $28+56=84$ is $\binom{8}{2}+\binom{8}{3}=\binom{9}{3}$. Each row reads the same backwards as forwards, because $\binom{n}{k}=\binom{n}{n-k}$, and the entries of row n add up to 2^n.

There are 2^n of them, since each of the n terms is one of 2 letters.

Why they matter. Multiply out $(a+b)^n = (a+b)(a+b)\cdots(a+b)$, n factors, *without* collecting like terms and without reordering the letters in each product. Each term of the result is made by picking one letter from each factor, in order, so each term is an a,b-sequence of length n, and every a,b-sequence appears exactly once. So

$$(a+b)^n = \sum (\text{every } a,b\text{-sequence of length } n).$$

For $n=2$ and $n=3$:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = aa+ab+ba+bb,\\ (a+b)^3 &= (aa+ab+ba+bb)(a+b)\\ &= aaa+aba+baa+bba+aab+abb+bab+bbb.\end{aligned}$$

Since the letters are numbers, they commute, and a sequence is the same as the product of its letters: $aba = baa = aab = a^2b$, and $aabab = a^3b^2$. In general, **an a,b-sequence of length n with k copies of b equals $a^{n-k}b^k$.** Collecting like terms is then counting sequences by how many b's they have.

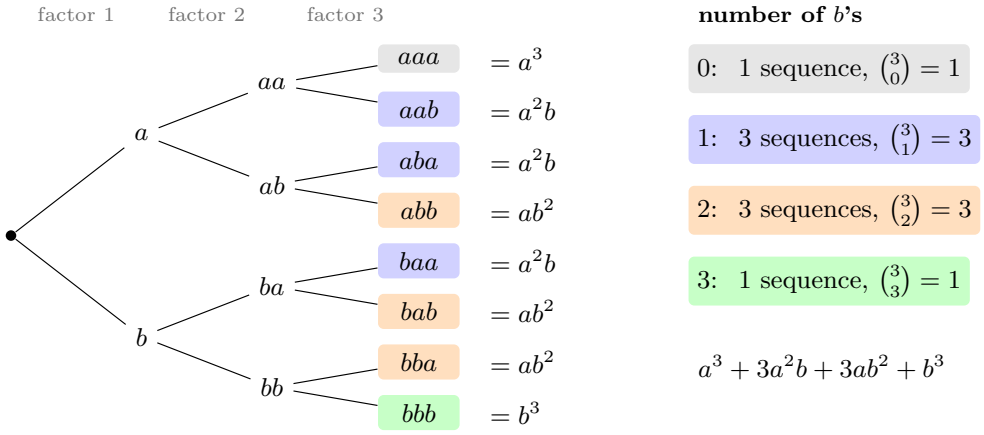


Figure 26: Multiplying out $(a+b)^3$ one factor at a time. Each factor contributes either a or b, so every path from the left to a leaf is one a,b-sequence of length 3, and the eight leaves are all eight of them. The colour of a leaf is its number of b's, and a sequence with k b's equals $a^{3-k}b^k$. There is 1 sequence with no b, 3 with one, 3 with two and 1 with three, which are the numbers of ways to choose where the b's go: $\binom{3}{0}, \binom{3}{1}, \binom{3}{2}, \binom{3}{3}$. Collecting them gives $(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$.

The Binomial Theorem

The Binomial Theorem. For any $a, b \in \mathbb{R}$ and any nonnegative integer n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k = a^n + \binom{n}{1} a^{n-1}b^1 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

The statement is printed on the exam formula-sheet[45]; the proof is not.

Combinatorial proof. $(a+b)^n$ is the sum of all the a,b-sequences of length n (above). Group them by their number of b's.

1. A sequence with exactly k b's has $n-k$ a's, so it equals $a^{n-k}b^k$.
2. **How many sequences of length n have exactly k b's?** Such a sequence is fixed by choosing which k of its n positions hold a b; the rest hold a. So there are $\binom{n}{k}$ of them.
3. So the term $a^{n-k}b^k$ appears $\binom{n}{k}$ times, and k can be anything from 0 to n. Adding up gives $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$. $\square$

The end terms fit the pattern: a^n is the single sequence with no b's, coefficient $\binom{n}{0} = 1$, and b^n is the single sequence of all b's, coefficient $\binom{n}{n} = 1$.

[45] courses/math1061/formula-sheet.pdf

An example to hold onto: $(a+b)^5$ and a^3b^2. The sequences of length 5 with three a's and two b's are

$$aaabb,\ aabab,\ aabba,\ abaab,\ ababa,\ abbaa,\ baaab,\ baaba,\ babaa,\ bbaaa,$$

ten of them, so the expansion of $(a+b)^5$ contains $10a^3b^2$. Ten is $\binom{5}{2}$, the number of ways to choose the 2 positions for the b's out of 5. Choosing the 3 positions for the a's instead gives $\binom{5}{3}$, which is also 10: placing the a's settles where the b's go, and that is the symmetry again. The full expansion is

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5,$$

with row 5 of Pascal's triangle as its coefficients.

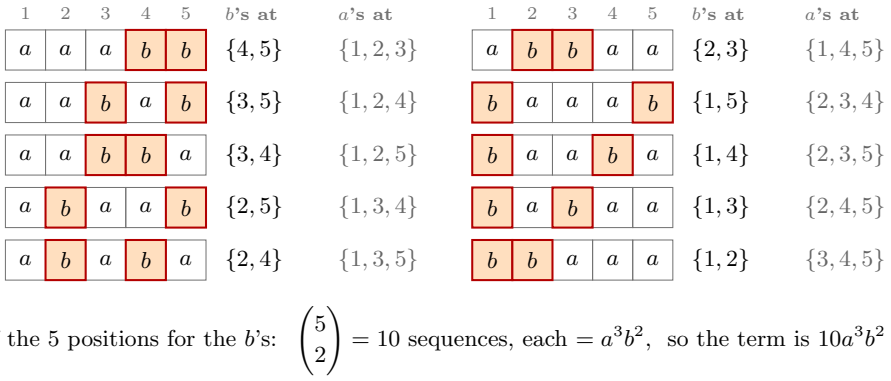


Figure 27: The ten a,b-sequences of length 5 with two b's, each drawn as five positions with the two b's shaded. A sequence is decided by which two positions hold its b's, and every pair of positions from $1,\dots,5$ appears exactly once, so there are $\binom{5}{2} = 10$ sequences, each equal to a^3b^2, and $(a+b)^5$ contains $10a^3b^2$. The pairs are the ten 2-element subsets of $1,2,3,4,5$, and the a's sit in the complementary 3 positions, so choosing the a-positions instead counts the same ten sequences as $\binom{5}{3}$.

Another way to see step 2. Multiplying out the product means choosing, from each of the n factors $(a+b)$, either its a or its b. A term equal to $a^{n-k}b^k$ comes from choosing b from some k of the factors and a from the rest, and there are $\binom{n}{k}$ ways to choose which k factors. The positions in the sequence and the factors in the product are the same thing.

Finding a coefficient in an expansion

To find the coefficient of one power of x in something like $(3x-2)^5$, don't expand the whole thing. Find the one term of the Binomial Theorem that contains that power.

1. **Match to $(a+b)^n$, signs and constants included.** In $(3x-2)^5$, $a=3x$, $b=-2$ and $n=5$. The minus sign belongs to b, and the 3 belongs to a.
2. **Write the general term** $\binom{n}{k}a^{n-k}b^k$ with these substituted: $\binom{5}{k}(3x)^{5-k}(-2)^k$.
3. **Find k.** Work out the power of x in the general term as a function of k, set it equal to the power wanted, and solve. Here x is inside a, so it is raised to $5-k$. For x^2, $5-k=2$, so $k=3$.
4. **Substitute k and simplify, keeping the constants and the sign.** $\binom{5}{3}(3x)^2(-2)^3 = 10\cdot 9x^2\cdot(-8) = -720x^2$. The coefficient is -720.

The question "what should k be?" always has the same answer: whatever makes the power of x come out right. Where x sits decides the equation.

- x **in the first term,** a**.** Its power is $n-k$. So for x^3 in $(x+9)^7$, $7-k=3$ and $k=4$.
- x **in the second term,** b**.** Its power is k. So for x^8 in $(3-x)^{12}$, $a=3$, $b=-x$ and $k=8$ directly.
- x **in both terms.** Collect the powers. In $\left(x^2+\frac{1}{x}\right)^5$ the general term is $\binom{5}{k}(x^2)^{5-k}(x^{-1})^k = \binom{5}{k}x^{10-3k}$. For x^4, $10-3k=4$ gives $k=2$, and the coefficient is $\binom{5}{2}=10$. For x^5, $10-3k=5$ has no whole-number solution, so there is no x^5 term and its coefficient is 0.

Which letter is called a and which b is a free choice. Swapping them changes k to $n-k$, and $\binom{n}{k}=\binom{n}{n-k}$, so the answer is the same either way. What must stay consistent is that the power $n-k$ goes on whatever was called a and the power k on whatever was called b.

Expansion	a	b	Power of x in the general term	Wanted	k	Term	Coefficient
$(x+9)^7$	x	9	$7-k$	x^3	4	$\binom{7}{4}x^3 9^4$	$35\cdot 6561 = 229\,635$
$(3-x)^{12}$	3	$-x$	k	x^8	8	$\binom{12}{8}3^4(-x)^8$	$495\cdot 81 = 40\,095$
$(3x-2)^5$	$3x$	-2	$5-k$	x^2	3	$\binom{5}{3}(3x)^2(-2)^3$	$10\cdot 9\cdot(-8) = -720$

These three are worked in full in 2026-10-19-probability-binomial-coefficients[46].

Signs. With $b=-c$, the general term carries $(-1)^k$. It is positive when k is even and negative when k is odd. In $(3-x)^{12}$, $(-x)^8 = x^8$, so the x^8 coefficient is positive. In $(3x-2)^5$, $(-2)^3=-8$, so the x^2 coefficient is negative.

[46] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf

Scaled terms. $(3x)^2 = 9x^2$, not $3x^2$. The constant inside the bracket is raised to the power too.

The sum of a row: $\sum_{r=0}^{n} \binom{n}{r} = 2^n$

For every nonnegative integer n,

$$\sum_{r=0}^{n} \binom{n}{r} = \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n.$$

Combinatorial proof. Count the subsets of $N = \{1, 2, \ldots, n\}$ in two ways.

- **All at once.** The number of subsets of N is the size of its power set, $|\mathcal{P}(N)| = 2^{|N|} = 2^n$ (sets-and-set-notation[47]). To see why, write each subset as a **01-sequence of length** n: put a 1 in position i if i is in the subset and a 0 if it isn't. For $N = \{1, \ldots, 6\}$, the sequence 011001 is the subset $\{2, 3, 6\}$. Every subset gives one 01-sequence and every 01-sequence gives one subset, and there are 2^n 01-sequences of length n, since each position is 0 or 1.
- **By size.** Every subset has some cardinality k between 0 and n, and the subsets of cardinality k are the 01-sequences with exactly k ones. Such a sequence is fixed by choosing which k positions hold the ones, so there are $\binom{n}{k}$ of them. Adding over all sizes, the number of subsets is $\sum_{k=0}^{n} \binom{n}{k}$.

Both count the subsets of N, so $2^n = \sum_{r=0}^{n} \binom{n}{r}$. □

A check from the Binomial Theorem. Put $a = b = 1$: $(1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 1^k$, which is the same identity. With $a = 1$ and $b = -1$ instead, $0 = (1-1)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k}$ for $n \geq 1$: the alternating sum of a row is 0, as in $1 - 4 + 6 - 4 + 1 = 0$. That alternating sum is what makes inclusion-exclusion[48] count every element exactly once.

Common mistakes

- **Leaving the constant behind.** In $(3x-2)^5$ the term is $\binom{5}{3}(3x)^2(-2)^3$, and $(3x)^2 = 9x^2$. Writing $3x^2$ gives -240 in place of -720.
- **Dropping the sign.** The $-$ belongs to b, so it is raised to the power k: $(-2)^3 = -8$ but $(-x)^8 = +x^8$. Forgetting it gives $+720$ for the x^2 coefficient of $(3x-2)^5$.
- **Putting k on the wrong letter.** When x is in a, its power is $n-k$, not k. In $(x+9)^7$, solving $k = 3$ and then writing $\binom{7}{3} x^4 9^3$ finds the x^4 coefficient, not the x^3 one. The binomial $\binom{7}{3} = \binom{7}{4}$ is the same either way; the powers on a and b are what go wrong.

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

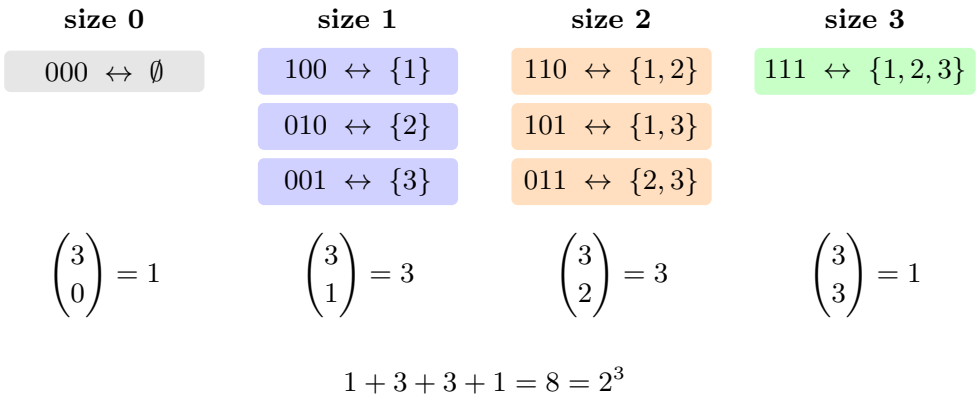


Figure 28: The eight subsets of $1, 2, 3$, each written as a 01-sequence, where a 1 in position i means i is in the subset. Grouped by size there are $\binom{3}{0} = 1$ with no elements, $\binom{3}{1} = 3$ with one, $\binom{3}{2} = 3$ with two and $\binom{3}{3} = 1$ with three: a subset of size k is a choice of k positions for the 1s. Counted all at once there are $2^3 = 8$, two choices for each position. So row 3 of Pascal's triangle adds up to 2^3.

- **Expecting every power to appear.** In $\left(x^2 + \frac{1}{x}\right)^5$ the powers are x^{10-3k}, so x^5 never appears and its coefficient is 0. A k that is not a whole number between 0 and n means the term isn't there.
- **Pascal's formula with the wrong indices.** It is $\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$: the two entries **diagonally above**, both from row n. Not $\binom{n}{r} + \binom{n}{r+1}$ in row $n + 1$, and not two entries from different rows.
- **Treating two groups as a product.** Splitting 400 people into groups of 150 and 250 is $\binom{400}{150}$, not $\binom{400}{150}\binom{400}{250}$: once the 150 are chosen the other group is already decided. (If it were written as stages, the second stage would be $\binom{250}{250} = 1$.)
- **A combinatorial proof that only computes.** Showing $84 = 28 + 56$ checks one case. The proof has to say what is being counted and why each side counts it.

See also

- counting-selections[49] — n choose r as the count of subsets, its formula, and the other three kinds of selection
- counting-principles[50] — the addition and multiplication rules that the combinatorial proofs use
- [probability] — probabilities worked out by counting, many of them with binomial coefficients

[49] courses/math1061/counting-selections.pdf
[50] courses/math1061/counting-principles.pdf

- sets-and-set-notation[51] — subsets, complements and the power set
- inclusion-exclusion[52] — counting a union, which rests on the alternating row sum
- 2026-10-19-probability-binomial-coefficients[53] — Lecture 31
- practice-problems[54] — §40, coefficients in expansions, with full worked solutions

Counting Principles

The rules for counting the outcomes of a process without listing them. The **multiplication rule** counts outcomes built in steps. The **addition rule** counts something that splits into cases that cannot happen together. **Subtracting from the total** counts what you want by counting what you don't. Applied to putting objects in order they give **permutations**, $n!$ arrangements of n objects, and **r-permutations**, the $\frac{n!}{(n-r)!}$ ordered selections of r of them. Selections where order does not matter, and the other kinds of selection, are in counting-selections[55]. First met in 2026-10-12-introduction-to-counting[56].

The multiplication rule

> **The multiplication rule.** Suppose each outcome is built by k steps carried out one after another, and that step i can always be done in n_i ways, whatever was chosen at the earlier steps. Then the number of outcomes is
>
> $$n_1 \times n_2 \times \cdots \times n_k.$$

Each outcome needs exactly one choice at *every* step, which is why the counts multiply. If step 1 has n_1 options and each of them can be followed by n_2 options at step 2, there are n_1 groups of n_2, which is $n_1 \times n_2$ two-step beginnings.

"Whatever was chosen at the earlier steps" is the condition to check. It is the *number* of options that must not depend on earlier choices. The options themselves may change. Arranging $1, 2, 3, 4, 5$: if 3 goes first, the second position can take 1, 2, 4 or 5, and if 1 goes first it can take 2, 3, 4 or 5. Those are different sets of options, but there are four of them either way, so the rule applies and gives $5 \times 4 \times 3 \times 2 \times 1 = 120$. When the number of options *does* change, split into cases first (below).

With two steps, one choice from a set A and one from a set B, the outcomes are the ordered pairs of $A \times B$, and the rule is the familiar $|A \times B| = |A| \times |B|$ (sets-and-set-notation[57]).

[51] courses/math1061/sets-and-set-notation.pdf
[52] courses/math1061/inclusion-exclusion.pdf
[53] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf
[54] courses/math1061/practice-problems.pdf
[55] courses/math1061/counting-selections.pdf
[56] courses/math1061/2026-10-12-introduction-to-counting.pdf
[57] courses/math1061/sets-and-set-notation.pdf

Choosing one odd and one even number from $1, \ldots, 9$ is $|D \times E| = 5 \times 4 = 20$, where D is the odd numbers and E the even ones. The order the two numbers are picked in does not matter there, but each choice still matches exactly one pair (odd, even), so the count is right (2026-10-12-introduction-to-counting[58]).

Possibility trees

A **possibility tree** draws a stepwise process. Each level is a step, each branch is one option at that step, and each path from the start to a leaf is one complete outcome. Counting outcomes is counting leaves.

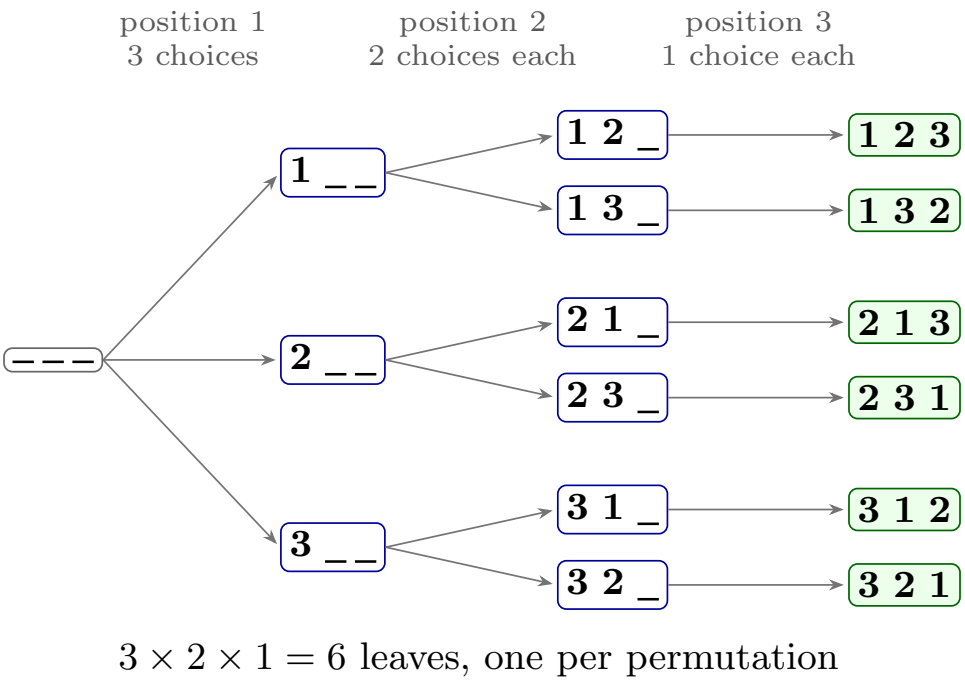


Figure 29: The possibility tree for arranging $1, 2, 3$, built one position at a time. Every node at the first level has 2 branches and every node at the second has 1, whichever numbers were used. Because each level splits evenly, the number of leaves is the product of the branch counts, $3 \times 2 \times 1 = 6$, one for each permutation. If the branch counts at a level differed, the leaves would have to be added up branch by branch.

A tree is worth drawing for a small case even when it is too big to finish, because it shows whether every node at a level has the same number of branches. If it does, multiply. If it

[58] courses/math1061/2026-10-12-introduction-to-counting.pdf

doesn't, as for a permutation of $\{1, \dots, 7\}$ that starts with a prime followed by an odd number, the leaves have to be added branch by branch (2026-10-12-introduction-to-counting[59]).

Worked: casting two roles

From practice-problems[60], Q1. Six people audition for Romeo, and eight *other* people audition for Juliet. How many ways can the lead couple be cast?

Step 1, choose Romeo: 6 ways. Step 2, choose Juliet: 8 ways, whoever was cast as Romeo, because nobody is in both groups. So there are $6 \times 8 = 48$ ways. If the same person could audition for both roles, step 2's count would depend on step 1 and the rule could not be used as it stands.

The addition rule

> **The addition rule.** If a finite set A is the union of mutually disjoint subsets $A_1, A_2, \dots, A_k$, then
> $$|A| = |A_1| + |A_2| + \cdots + |A_k|.$$

In counting terms: when every outcome falls into **exactly one** of several cases, count each case and add. "Mutually disjoint" is the condition of a partition (equivalence-classes-and-partitions[61]): no outcome is in two cases. "Union is A" means no outcome is left out.

- **One number from $\{1, \dots, 8\}$ that is prime or composite.** The primes $\{2, 3, 5, 7\}$ and the composites $\{4, 6, 8\}$ are disjoint, because no number is both, so there are $4 + 3 = 7$.
- **Number plates of four, five or six symbols.** Every plate has exactly one length, so the counts for the three lengths add (2026-10-12-introduction-to-counting[62]).
- **The symbols themselves.** 26 letters and 10 digits make $26 + 10 = 36$ symbols, since no symbol is both.

The cases must not overlap. Count the permutations of $\{1, \dots, 60\}$ with at least one even number in the first two positions as "first is even" plus "second is even", and the permutations whose first two numbers are *both* even are counted twice.

When the sets do overlap, the sum can be corrected rather than abandoned. Adding $|A|$ and $|B|$ counts each element of $A \cap B$ twice, so subtracting it once gives

$$|A \cup B| = |A| + |B| - |A \cap B|,$$

[59] courses/math1061/2026-10-12-introduction-to-counting.pdf
[60] courses/math1061/practice-problems.pdf
[61] courses/math1061/equivalence-classes-and-partitions.pdf
[62] courses/math1061/2026-10-12-introduction-to-counting.pdf

which is the addition rule when $A \cap B = \emptyset$. For the permutations, in multiples of 58!, that is $1770 + 1770 - 870 = 2670$, the right answer. This is **inclusion/exclusion**, which extends to three or more sets in inclusion-exclusion[63].

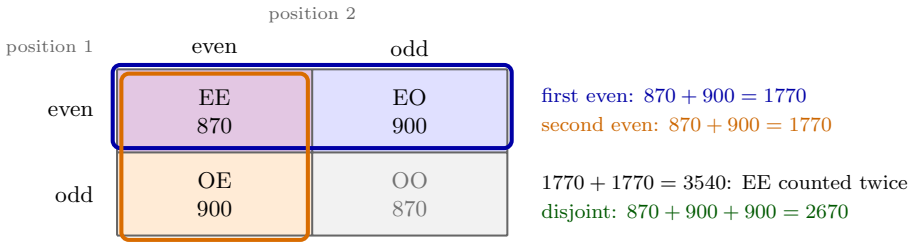


Figure 30: Why the addition rule needs disjoint cases. Each cell counts the permutations of $1, \ldots, 60$ whose first two numbers have the given parities, as a multiple of 58!. The blue band, first number even, and the orange band, second number even, overlap in the cell EE. Adding the two bands counts EE twice and gets 3540, every permutation, although the 870 in OO have no even number in front. Disjoint cases, EE, EO and OE, give the right answer, 2670.

When to add and when to multiply

	Multiply	**Add**
Shape	One outcome is built in steps, and every outcome makes one choice at every step.	The outcomes split into cases, and every outcome is in exactly one case.
Signals	"followed by", "then", "one from each", positions in an arrangement	an "or" between alternatives that exclude each other; "of length 4, 5 or 6"
Check	Is the number of options at each step the same whatever came before?	Do the cases overlap? Do they cover everything?
Example	one odd and one even from $1, \ldots, 9$: $5 \times 4 = 20$	one number from $\{1, \ldots, 8\}$ that is prime or composite: $4 + 3 = 7$

Most problems use both: **multiply within each case, add across the cases**. The plates with exactly one digit are an example. Within a length, choose the digit's position, then the digit, then the letters, and multiply. Across the three lengths, add.

[63] courses/math1061/inclusion-exclusion.pdf

Splitting into cases

The multiplication rule fails when the number of options at a step depends on what was chosen earlier. The fix is to split on that earlier choice, so that inside each case the counts are fixed.

1. Find the step whose count varies, and the earlier choice it depends on.
2. Split the outcomes into cases according to that choice. The cases must be disjoint and cover everything.
3. Apply the multiplication rule inside each case.
4. Add the cases.

Worked: a prime followed by an odd number. Permutations of $\{1, \dots, 7\}$. The primes are $2, 3, 5, 7$ and the odd numbers $1, 3, 5, 7$. The number of odd numbers left for position 2 depends on whether the prime in position 1 was odd.

- First number 2: $1 \times 4 \times 5!$, since all four odd numbers remain.
- First number 3, 5 or 7: $3 \times 3 \times 5!$, since the first number used up an odd number.

Total $(4 + 9) \times 5! = 1560$. Multiplying straight through, $4 \times 4 \times 5! = 1920$, overcounts.

Worked: an even number followed by a multiple of 3. Permutations of $\{1, \dots, 60\}$. There are 30 even numbers and 20 multiples of 3, and 10 of the even numbers, the multiples of 6, are also multiples of 3.

- First number a multiple of 6: $10 \times 19 \times 58!$, since it used up a multiple of 3.
- First number even but not a multiple of 3: $20 \times 20 \times 58!$.

Total $(190 + 400) \times 58! = 590 \times 58!$ (2026-10-12-introduction-to-counting[64]).

In both, the split comes from an *overlap*. A first choice that also belongs to the set the second choice is drawn from uses up one of its options, so it goes in one case, and a first choice outside that set goes in the other.

Counting the complement

If A is a finite set and $B \subseteq A$, then

$$|A - B| = |A| - |B|.$$

This is the addition rule turned round. A is the union of the disjoint sets B and $A - B$, so $|A| = |B| + |A - B|$. It is sometimes called the **difference rule**.

To count the outcomes with some property, count all outcomes and subtract those without it. It pays off whenever the unwanted outcomes are simpler than the wanted ones, which is typical of **"at least one"**: the opposite of "at least one" is "none", a single case.

[64] courses/math1061/2026-10-12-introduction-to-counting.pdf

- **Prime or composite from $\{1, \ldots, 8\}$.** Only 1 is neither: $|X - \{1\}| = 8 - 1 = 7$.
- **At least one even number in the first two positions** of a permutation of $\{1, \ldots, 60\}$. The opposite is "both odd": $60! - 30 \times 29 \times 58! = 2670 \times 58!$. Counting EE, EO and OE separately gives the same, with three cases instead of one.
- **Number plates with at least one repeated symbol.** The opposite is "no repeats", so subtract the plates with no repeats from all plates: $2\,238\,928\,128 - 1\,449\,063\,000 = 789\,865\,128$.

Subtract inside the same universe. B has to be a subset of A, counted under the same conditions. For the plates, both counts use lengths 4, 5 and 6 and the same 36 symbols. Subtracting the no-repeat four-symbol plates from all plates of every length would be meaningless.

Permutations

A **permutation** of a set of objects is an arrangement of the objects into an order.

Theorem. The number of permutations of a set of n distinct objects is

$$n \times (n-1) \times (n-2) \times \cdots \times 2 \times 1 = n!.$$

Why. Fill the positions in turn. The first can hold any of the n objects. Whatever went there, $n-1$ objects remain for the second, then $n-2$ for the third, and so on until 1 object remains for the last position. Every step's count is independent of what was chosen, so the multiplication rule gives $n!$.

$n!$ is "n factorial", also read "n bang":

$$n! = \prod_{i=1}^{n} i \quad \text{for } n \in \mathbb{Z}^+, \qquad 0! = 1.$$

$0! = 1$ is a definition, and it is the one that makes $n! = n \times (n-1)!$ true at $n = 1$ (recursive-definitions[65]). The values grow faster than any power: $5! = 120$, $6! = 720$, $10! = 3\,628\,800$, and $58!$ has 79 digits. Answers to permutation problems are usually left in factorial form for that reason.

n	0	1	2	3	4	5	6	7	8
$n!$	1	1	2	6	24	120	720	5040	40320

A bijection f from $\{1, \ldots, n\}$ to itself is the same thing as the arrangement $f(1), f(2), \ldots, f(n)$, so the symmetric group S_n has $n!$ elements (symmetric-group[66]).

[65] courses/math1061/recursive-definitions.pdf
[66] courses/math1061/symmetric-group.pdf

Restricted positions: fill them first

When some positions have conditions on them and the rest are free, choose for the restricted positions first. Each later position then has one fewer object than the last, whatever was chosen, and the $n-k$ free positions are an arrangement of the $n-k$ objects left: $(n-k)!$ ways.

Permutations of	that	Count
$\{1,\dots,5\}$	start with an even number	$2\times 4! = 48$
$\{1,\dots,7\}$	start with a prime	$4\times 6! = 2880$
$\{1,\dots,7\}$	start with a prime followed by a composite	$4\times 2\times 5! = 960$
$\{1,\dots,15\}$	start with an odd number	$8\times 14!$

The last line is Q3(a) of practice-problems[67]: $\{1,\dots,15\}$ has 8 odd numbers.

Why the restricted position goes first. Filling a free position first makes the count for the restricted one depend on what was used. In "starts with an even number", if position 2 were filled first, position 1 would have 2 options or only 1, depending on whether position 2 took an even number. Filling position 1 first keeps every count fixed. The second row of the table, $4\times 6!$, also shows the most common slip: 4×6 forgets that the remaining positions have to be filled too.

r-permutations

> An **r-permutation** of a set of n elements is an ordered selection of r of the elements, with no element used more than once.
>
> **The number of r-permutations** of a set of n elements, for $0\le r\le n$, is
>
> $$n\times(n-1)\times\cdots\times(n-r+1) = \frac{n!}{(n-r)!}.$$

Why. It is the permutation count stopped after r positions. The first position has n options, the second $n-1$, and the rth has $n-r+1$, so there are r factors. Multiplying top and bottom by the missing factors $(n-r)\times\cdots\times 1 = (n-r)!$ gives the fraction. With $r=n$ it is $\frac{n!}{0!} = n!$, the permutations of the whole set, which is one place $0! = 1$ is needed.

If repetition is allowed, every position has all n options and the count is n^r. Which of the two applies is the first thing to settle.

Worked: a four-symbol plate. The symbols are the 26 letters and 10 digits, 36 in all.

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

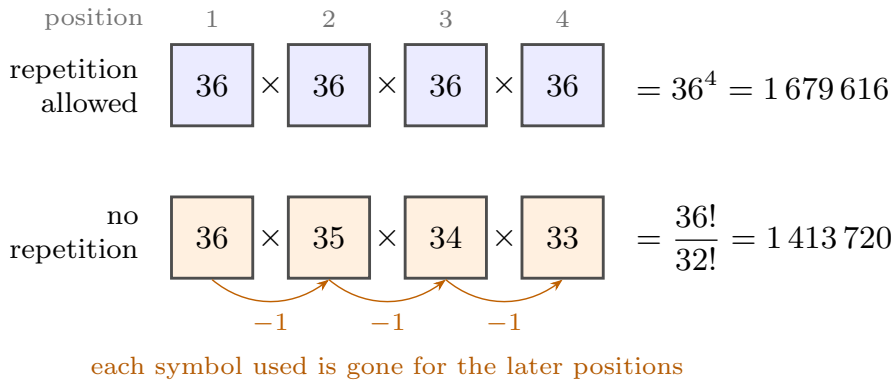


Figure 31: A four-symbol plate filled one position at a time, from 36 symbols. With repetition allowed, every position has all 36 symbols available, giving 36^4. Without repetition, each symbol placed is unavailable afterwards, so each position has one option fewer than the one before. That is a 4-permutation of the 36 symbols, $36\times35\times34\times33 = \frac{36!}{32!}$.

Over all three lengths these give $36^4+36^5+36^6$ plates with repetition and $\frac{36!}{32!}+\frac{36!}{31!}+\frac{36!}{30!}$ without (2026-10-12-introduction-to-counting[68]). Unordered selections, where only *which* elements are chosen matters, are counted in counting-selections[69].

Common mistakes

- **Adding steps, or multiplying cases.** One prime *and* one composite is $4 \times 3 = 12$. One number that is prime *or* composite is $4 + 3 = 7$. Getting these the wrong way round gives 7 and 12, swapped.
- **Multiplying when a count depends on an earlier choice.** "A prime followed by an odd number" is not $4 \times 4 \times 5!$. After an odd prime only three odd numbers are left. Split into cases.
- **Treating an unordered choice as ordered.** Choosing one odd and one even number from $1, \dots, 9$ is 20 ways. Counting "first pick, second pick" gives $5 \times 4 + 4 \times 5 = 40$, each pair twice.
- **Cases that overlap or leave something out.** "First is even" plus "second is even" counts the EE permutations twice. Check that each outcome is in exactly one case.
- **Forgetting the free positions.** Permutations of $\{1, \dots, 7\}$ starting with a prime are $4 \times 6!$, not 4×6. The other six positions still have to be arranged.
- **Mixing up n^r and $\frac{n!}{(n-r)!}$.** The first allows repeats, the second doesn't. Read the question for which.

[68] courses/math1061/2026-10-12-introduction-to-counting.pdf
[69] courses/math1061/counting-selections.pdf

- **Subtracting across different universes.** The complement has to be counted under the same conditions as the total.
- **Counting 1 as a prime or a composite.** It is neither, and several of the questions above turn on it.

See also

- 2026-10-12-introduction-to-counting[70] — Lecture 29, with every question worked in full
- counting-selections[71] — ordered and unordered selections, with and without repeats, and more on restrictions
- inclusion-exclusion[72] — counting a union of sets that overlap, where the addition rule does not apply
- probability[73] — the difference rule divided through: $P(E) = 1 - P(E^c)$
- pigeonhole-principle[74] — counting pigeons and holes to prove that two must share a hole
- sets-and-set-notation[75] — $|A \times B| = |A| \times |B|$, the two-step multiplication rule
- equivalence-classes-and-partitions[76] — mutually disjoint sets, the condition in the addition rule
- cardinality[77] — finite sets matched by a bijection have the same size, which is what counting by correspondence relies on
- recursive-definitions[78] — $n!$ defined recursively, with $0! = 1$
- symmetric-group[79] — the $n!$ bijections of $\{1, \dots, n\}$
- practice-problems[80] — §37, with full worked solutions

Counting Selections

Choosing r objects from a pool of n can be counted four ways, depending on two questions: **does the order of the choices matter**, and **can the same object be chosen more than once**? Each pair of answers has its own formula. This note collects the four, how to tell which one a problem needs, and the standard ways of handling a restriction: forcing part of the selection, splitting the pool into categories, and counting "at least" through the complement. It ends with arrangements of a word that has repeated letters, which are counted by choosing

[70] courses/math1061/2026-10-12-introduction-to-counting.pdf
[71] courses/math1061/counting-selections.pdf
[72] courses/math1061/inclusion-exclusion.pdf
[73] courses/math1061/probability.pdf
[74] courses/math1061/pigeonhole-principle.pdf
[75] courses/math1061/sets-and-set-notation.pdf
[76] courses/math1061/equivalence-classes-and-partitions.pdf
[77] courses/math1061/cardinality.pdf
[78] courses/math1061/recursive-definitions.pdf
[79] courses/math1061/symmetric-group.pdf
[80] courses/math1061/practice-problems.pdf

positions. The rules all of this is built from, the multiplication, addition and difference rules, and permutations, are in counting-principles[81]. First met in 2026-10-13-counting-selections[82].

The two questions

A **selection of r objects from n** is a choice of r objects, made one after another, from a set of n distinct objects. Before counting, settle two things.

- **Ordered or unordered?** In an ordered selection, the same objects chosen in a different order make a different selection: the password *cat* is not the password *cta*. In an unordered selection only *which* objects are chosen counts: the subset $\{1, 2, 3\}$ is the subset $\{3, 1, 2\}$. The test is to swap two of the chosen objects. If that changes the outcome, the selection is ordered.
- **With or without repeats?** With repeats, an object that has been chosen can be chosen again, as a letter can appear twice in a password. Without repeats, each object is used at most once, as each runner finishes a race in one place only.

	without repeats	**with repeats**
ordered	$\dfrac{n!}{(n-r)!} = n(n-1)\cdots(n-r+1)$	n^r
unordered	$\dbinom{n}{r} = \dfrac{n!}{r!\,(n-r)!}$	$\dbinom{n+r-1}{r}$ (extension)

Ordered, without repeats

There are n choices for the first object and $n-1$ for the second, because the first cannot be used again. Each choice has one fewer option than the one before, and the rth has $n-r+1$. By the multiplication rule (counting-principles[83]) the number of ordered selections without repeats is

$$n(n-1)(n-2)\cdots(n-r+1) = \frac{n!}{(n-r)!}.$$

The product has exactly r factors. The fraction is the same number written another way: $n! = n(n-1)\cdots 1$, and dividing by $(n-r)!$ cancels every factor from $n-r$ down to 1, leaving

[81] courses/math1061/counting-principles.pdf
[82] courses/math1061/2026-10-13-counting-selections.pdf
[83] courses/math1061/counting-principles.pdf

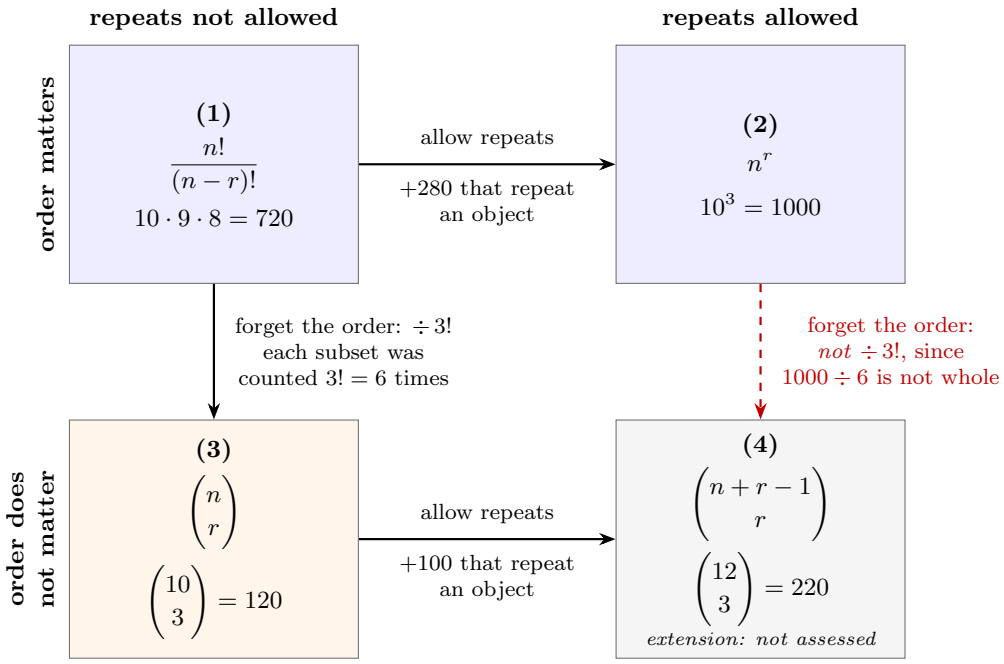


Figure 32: How the four cases are related, with the count for $n = 10$ and $r = 3$ in each. Moving right allows an object to be chosen again, which adds the selections that use some object more than once: $1000 - 720 = 280$ ordered ones and $220 - 120 = 100$ unordered ones. Moving down forgets the order. Without repeats, each subset was counted once for each of its $3! = 6$ orders, so the count divides by 3!. With repeats that fails, because a selection with a repeated object has fewer orders: 1, 1, 2 has only 3. There $1000 \div 6$ is not even a whole number. The bottom-right case is extension material.

the top r. For example $36 \cdot 35 \cdot 34 \cdot 33 = \frac{36!}{32!} = \frac{36!}{(36-4)!}$. These are the r-permutations of counting-principles[84], and with $r = n$ they are the $n!$ arrangements of all n objects.

Example. First, second and third place in a race of 10 people: $10 \cdot 9 \cdot 8 = 720$.

Compute with the product, which never needs a large factorial. The fraction is the compact form for writing the answer down.

Ordered, with repeats

Every one of the r choices has all n objects available, so there are

$$n \cdot n \cdots n = n^r$$

ordered selections with repeats. **Example.** 3-digit passwords: $10^3 = 1000$, the strings 000 to 999.

The base is the number of objects to choose from and the exponent is the number of choices made. An 8-letter password from a 26-letter alphabet has 26^8 possibilities, not 8^{26}.

Unordered, without repeats: n choose r

An unordered selection without repeats is a subset.

> The number of r-element subsets of an n-element set is written $\binom{n}{r}$, read "n **choose** r", and also written $C(n, r)$:
>
> $$\binom{n}{r} = \frac{n!}{r!\,(n-r)!} = \frac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 1}.$$

Why divide by $r!$. Count the ordered selections first: $n(n-1)\cdots(n-r+1)$. Every r-element subset appears among them $r!$ times, once for each order its r elements can be listed in. So the number of ordered selections is $r!$ times the number of subsets. For 3 objects from $\{1, 2, 3, 4\}$ there are $4 \cdot 3 \cdot 2 = 24$ ordered selections, each subset accounts for $3! = 6$ of them, and $\binom{4}{3} = \frac{24}{6} = 4$. It is drawn in 2026-10-13-counting-selections[85].

How to calculate it. Use the second form: r factors counting down from n on top, r factors counting down from r underneath, and cancel before multiplying.

[84] courses/math1061/counting-principles.pdf
[85] courses/math1061/2026-10-13-counting-selections.pdf

$$\binom{6}{3} = \frac{6\cdot 5\cdot 4}{3\cdot 2\cdot 1} = 20, \qquad \binom{10}{3} = \frac{10\cdot 9\cdot 8}{3\cdot 2\cdot 1} = 120, \qquad \binom{21}{7} = \frac{21\cdot 20\cdot 19\cdot 18\cdot 17\cdot 16\cdot 15}{7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1} = 116\,280.$$

The answer is always a whole number, because it counts something. A fraction left over means a slip.

Three facts worth knowing.

- $\binom{n}{r} = \binom{n}{n-r}$. Choosing the r objects to take is the same as choosing the $n-r$ to leave behind: each r-element subset pairs off with its complement, the $n-r$ elements not in it. So $\binom{10}{7} = \binom{10}{3} = 120$, and $\binom{11}{7} = \binom{11}{4} = \frac{11\cdot 10\cdot 9\cdot 8}{4\cdot 3\cdot 2\cdot 1} = 330$. Use whichever has the smaller bottom number. The pairing is drawn in binomial-coefficients[86], along with the other identities binomial coefficients satisfy.
- $\binom{n}{n} = \binom{n}{0} = 1$, using $0! = 1$. For instance $\binom{2}{2} = \frac{2!}{2!\,0!} = 1$: there is one way to take everything.
- $\binom{n}{1} = n$.

Unordered, with repeats

Extension material: not assessable in MATH1061. It is Section 9.6 of Epp, and it is covered in MATH2302.

The number of unordered selections of r objects from n with repeats allowed is

$$\binom{n+r-1}{r} = \frac{n(n+1)\cdots(n+r-1)}{r(r-1)\cdots 1}.$$

The top now counts **up** from n, still for r factors.

Why: stars and bars. Choose 7 candies from 4 colours, red, blue, yellow and pink, where candies of the same colour are identical and a colour can be taken any number of times, including not at all. A selection is settled by how many of each colour are taken. Write an X for each candy, colour by colour, with a bar | between one colour and the next. Four colours need three bars. Two red, one blue, four yellow and no pink is

$$\text{XX}\,|\,\text{X}\,|\,\text{XXXX}\,|$$

Every string of 7 X's and 3 bars describes exactly one selection, and every selection gives exactly one such string. So the selections can be counted as strings: 10 positions, of which

[86] courses/math1061/binomial-coefficients.pdf

3 are bars, and $\binom{10}{3} = 120$ ways to choose them. In general there are r X's and $n-1$ bars, $n+r-1$ positions in all, and the selection is fixed by which r of them hold X's.

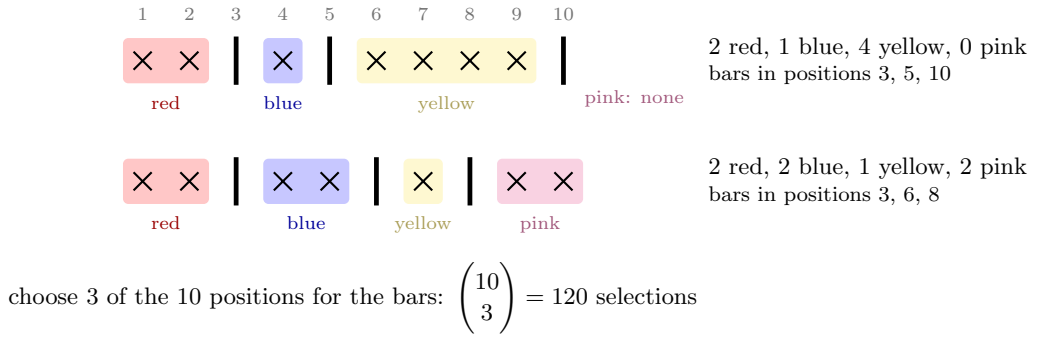


Figure 33: Choosing 7 candies from 4 colours, written as strings of 7 X's and 3 bars. The bars cut the string into four stretches, and the stretches, from left to right, are the red, blue, yellow and pink candies. Top: two red, one blue, four yellow and no pink, so the last stretch is empty. Bottom: two red, two blue, one yellow and two pink. A selection is decided by which 3 of the 10 positions hold the bars, so there are $\binom{10}{3} = 120$ selections.

Example. Choosing 3 chocolate bars when there are 10 kinds: 3 X's and 9 bars, so

$$\binom{12}{3} = \frac{12 \cdot 11 \cdot 10}{3 \cdot 2 \cdot 1} = \frac{10 \cdot 11 \cdot 12}{3 \cdot 2 \cdot 1} = 220.$$

Why not $n^r/r!$? Dividing by $r!$ works only when every selection has $r!$ different orderings, and a selection with a repeat has fewer: $\{1,1\}$ has one ordering, not two. For 2 objects from $\{1,2,3,4\}$, $4^2/2! = 8$, but the true count is $\binom{5}{2} = 10$.

Which case?

The same $n = 10$, $r = 3$ in four questions, one for each case:

Question	Ordered?	Repeats?	Count
First, second and third in a race of 10 people	yes	no	$10 \cdot 9 \cdot 8 = 720$
3-digit passwords	yes	yes	$10^3 = 1000$
3-element subsets of $\{1, 2, \ldots, 10\}$	no	no	$\binom{10}{3} = 120$

Question	Ordered?	Repeats?	Count
3 chocolate bars from 10 kinds	no	yes	$\binom{12}{3} = 220$

Wording that usually settles it:

- **Subset, committee, hand of cards, "choose 5 of the 11 questions"**: unordered, without repeats.
- **Password, string, number plate, sequence of digits**: ordered, and with repeats unless the problem rules them out.
- **First, second and third, or "arrange"**: ordered, without repeats.

When the wording is unclear, use the swap test from the two questions and ask whether anything stops an object being picked twice.

Restrictions

A restriction narrows down which selections count. Three moves handle most of them.

Force the restricted part, then fill in the rest. Decide the restricted part first and count the ways it can go, then count the ways to fill whatever is left, and multiply. Ordered selections of 4 from $\{1, 2, \dots, 10\}$ in which 5 is immediately followed by 6: the block "5 then 6" starts in position 1, 2 or 3 (not 4, where the 6 would have no room), and the two free positions take two of the other 8 numbers in order, $8 \cdot 7$ ways. So there are $3 \cdot 8 \cdot 7 = 168$ (2026-10-13-counting-selections[87]). Number plates with exactly one digit go the same way: a k-symbol plate has k places for the digit, 10 digits to put there, and 26 letters for each of the other $k - 1$ places, $k \cdot 10 \cdot 26^{k-1}$ in all.

Split the pool into categories and choose from each. 5-element subsets of $\{1, 2, \dots, 11\}$ with 3 even numbers and 2 odd: there are 5 evens and 6 odds, and the two choices are independent, so

$$\binom{5}{3}\binom{6}{2} = 10 \cdot 15 = 150.$$

The binomials are multiplied because every choice of evens goes with every choice of odds.

Split into cases and add. When the count depends on a case, such as the length of a number plate, count each case on its own and add, by the addition rule (counting-principles[88]). The cases must not overlap.

[87] courses/math1061/2026-10-13-counting-selections.pdf
[88] courses/math1061/counting-principles.pdf

"At least": count the complement

Counting "at least one" directly means adding up exactly one, exactly two, and so on. The opposite, "none", is usually a single product. So

$$\#(\text{at least one}) = \#(\text{all}) - \#(\text{none}),$$

which is counting the complement, the difference rule of counting-principles[89].

How many …	All	The opposite	At least one
8-letter passwords contain a vowel?	26^8	no vowel: 21^8	$26^8 - 21^8 = 171\,004\,205\,215$
integers from 0 to 9999 contain the digit 5?	10^4	no 5: 9^4	$10^4 - 9^4 = 3439$
number plates of 4, 5 or 6 symbols repeat a symbol?	$36^4 + 36^5 + 36^6$	no repeat: $\frac{36!}{32!} + \frac{36!}{31!} + \frac{36!}{30!}$	$789\,865\,128$

At least two. Take away both "none" and "exactly one". For 7-element subsets of $\{1, 2, \dots, 21\}$ with at least two even numbers (10 evens, 11 odds):

$$\binom{21}{7} - \binom{11}{7} - \binom{11}{6}\binom{10}{1} = 116\,280 - 330 - 4620 = 111\,330.$$

"Exactly one even" is itself a categories count: one even from the 10, which is $\binom{10}{1} = 10$ ways, and six odds from the 11.

Checking with a direct count. The long way gives the same answer and is a good check. Integers from 0 to 9999 with exactly k fives: choose the k places for the fives and fill the others from the 9 other digits, $\binom{4}{k}9^{4-k}$. Then

$$\binom{4}{1}9^3 + \binom{4}{2}9^2 + \binom{4}{3}9 + \binom{4}{4} = 2916 + 486 + 36 + 1 = 3439.$$

Fixing one doesn't work. "Put a vowel in one of the 8 places, then anything anywhere else" gives $8 \cdot 5 \cdot 26^7 = 321\,272\,407\,040$, which is more than the $26^8 = 208\,827\,064\,576$ passwords there are. A password with two vowels is counted once for each vowel that could be "the" vowel.

[89] courses/math1061/counting-principles.pdf

Arrangements of a word with repeated letters

An arrangement uses every letter of the word exactly once, so a word of n different letters has $n!$ arrangements. Repeated letters spoil this. Swapping the two B's of BARBARA gives the same string, so $7! = 5040$ counts every arrangement more than once.

Count by choosing positions. Place one kind of letter at a time. BARBARA has 7 positions.

1. The two B's go in 2 of the 7 positions: $\binom{7}{2} = 21$ ways. This is a choice of positions, not an ordered selection, because the B's are identical: once two positions are chosen it makes no difference which B goes in which.
2. The three A's go in 3 of the 5 positions left: $\binom{5}{3} = 10$ ways.
3. The two R's fill the last 2 positions: $\binom{2}{2} = 1$ way.

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = 21 \cdot 10 \cdot 1 = 210.$$

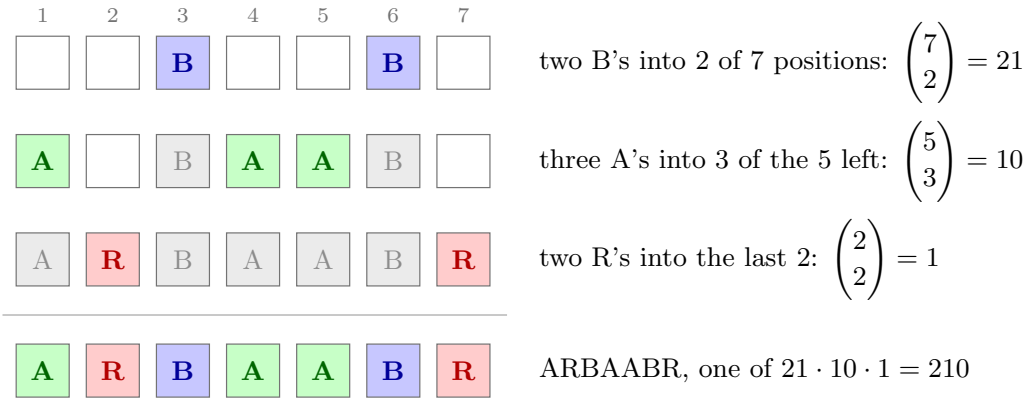


Figure 34: Building one arrangement of BARBARA by choosing positions. First the two B's take 2 of the 7 positions, here 3 and 6, in one of $\binom{7}{2} = 21$ ways. Then the three A's take 3 of the 5 positions still free, here 1, 4 and 5, in one of $\binom{5}{3} = 10$ ways. The two R's must take the last two positions, so there is $\binom{2}{2} = 1$ way. Positions already taken are greyed. The result is ARBAABR, one of $21 \cdot 10 \cdot 1 = 210$ arrangements.

The general formula. Writing the binomials out as factorials, almost everything cancels:

$$\binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!\,5!} \cdot \frac{5!}{3!\,2!} \cdot \frac{2!}{2!\,0!} = \frac{7!}{2!\,3!\,2!} = \frac{5040}{24} = 210.$$

In general, a word of n letters made of k different letters, appearing $n_1, n_2, \ldots, n_k$ times (so $n_1 + n_2 + \cdots + n_k = n$), has

$$\frac{n!}{n_1!\, n_2! \cdots n_k!}$$

distinct arrangements. It also explains the division. Tag the copies so that every letter is different, $\mathrm{B}_1\mathrm{A}_1\mathrm{R}_1\mathrm{B}_2\mathrm{A}_2\mathrm{R}_2\mathrm{A}_3$, and there are 7! arrangements. Removing the tags merges $2!\,3!\,2! = 24$ of them into one word, because the tags can be shuffled among the B's, among the A's and among the R's without changing the word.

The order the letters are placed in doesn't matter. Placing the A's first gives $\binom{7}{3}\binom{4}{2}\binom{2}{2} = 35 \cdot 6 \cdot 1 = 210$ again.

Example: BANANAS. Seven letters: one B, three A's, two N's and one S.

$$\frac{7!}{1!\,3!\,2!\,1!} = \frac{5040}{12} = 420.$$

A letter that appears once contributes $1! = 1$ and can be left out of the denominator.

Restrictions on arrangements use the same moves as before. Letters fixed at the ends are placed first, and the rest of the word is arranged in the positions between. Letters that must sit together are glued into a single tile, which is then arranged along with the other letters. The practice set's INDOOROOPILLY and WOOLLOONGABBA questions use both moves, and "not next to each other" is counted as all arrangements minus those with the pair glued together.

Common mistakes

- **Ordering a subset.** $6 \cdot 5 \cdot 4 = 120$ is the number of *ordered* selections of 3 from 6. Each 3-element subset is counted $3! = 6$ times in it, and the number of subsets is $\binom{6}{3} = 20$.
- **Dividing by the wrong thing.** The divisor for a subset is $r!$, the number of orders of the r chosen objects. It is not r, and not 2.
- **Swapping n and r in n^r.** The exponent is the number of choices made: 26^8 eight-letter passwords, not 8^{26}.
- **"Exactly one" without choosing which one.** Exactly one even number in a 7-element subset of $\{1, \ldots, 21\}$ is $\binom{11}{6}\binom{10}{1} = 4620$, not $\binom{11}{6} = 462$. Leaving out the $\binom{10}{1}$ gives 115 488 for "at least two evens" in place of the correct 111 330.
- **Counting "at least one" by fixing one.** It counts selections with several of the wanted objects several times. The complement avoids this.
- **A position that cannot be used.** A block of two inside four positions has 3 starting places, not 4.

- **Numbers of different lengths.** To count the integers from 0 to 9999 digit by digit, write every one with four digits, so 7 is 0007. The added zeros never contain a 5, so the count is unchanged, and now every position has 10 choices.
- **Treating repeated letters as different.** 7! for BARBARA counts each word $2!\,3!\,2! = 24$ times.
- **Using $n^r/r!$ for unordered selections with repeats.** It fails because a selection with a repeat has fewer than $r!$ orderings.

See also

- counting-principles[90] — the multiplication, addition and difference rules, and permutations, which every formula here is built from
- sets-and-set-notation[91] — subsets, which are what $\binom{n}{r}$ counts
- binomial-coefficients[92] — Pascal's formula, the Binomial Theorem, and other identities for $\binom{n}{r}$, with their combinatorial proofs
- [probability] — probabilities of equally likely outcomes, worked out with these counts
- one-to-one-and-onto-functions[93] — a one-to-one function from an r-element set to an n-element set is an ordered selection of images without repeats, so there are $\frac{n!}{(n-r)!}$ of them
- 2026-10-13-counting-selections[94] — Lecture 30 · 2026-10-12-introduction-to-counting[95] — Lecture 29
- practice-problems[96] — §38, with full worked solutions

The Examination Formula Page

The *MATH1061/MATH7861 Examination Formula Page* is **provided in both exams**, which are otherwise closed book with no written materials permitted (see math1061[97]). Knowing what is on it — and what is not — is what decides whether a fact needs memorising.

It has **seven blocks**.

[90] courses/math1061/counting-principles.pdf
[91] courses/math1061/sets-and-set-notation.pdf
[92] courses/math1061/binomial-coefficients.pdf
[93] courses/math1061/one-to-one-and-onto-functions.pdf
[94] courses/math1061/2026-10-13-counting-selections.pdf
[95] courses/math1061/2026-10-12-introduction-to-counting.pdf
[96] courses/math1061/practice-problems.pdf
[97] courses/math1061/math1061.pdf

1. Logical equivalences

Eleven named laws, given any statement variables p, q, r, a tautology $\mathbf{t}$ and a contradiction $\mathbf{c}$. Reproduced in full in logical-equivalence-laws[98].

Commutative · Associative · Distributive · Identity · Negation · Double negative · Idempotent · Universal bound · De Morgan's · Absorption · Negations of $\mathbf{t}$ and $\mathbf{c}$.

2. Valid argument forms

Nine forms. Reproduced in full in valid-argument-forms[99].

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

3. Set identities

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

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

[98] courses/math1061/logical-equivalence-laws.pdf
[99] courses/math1061/valid-argument-forms.pdf

Reproduced with worked proofs in proving-set-properties[100].

Note the one-to-one correspondence with the logical equivalences in block 1 — laws 1–11 are those same eleven laws in the same order, plus set difference at 12. The names are not quite identical: *negation* becomes **complement** (5), *double negative* becomes **double complement** (6), and *negations of* **t** *and* **c** becomes **complement of U and $\emptyset$** (11). That correspondence is not a coincidence: $\cup$ behaves as $\vee$, $\cap$ as $\wedge$, and complement as $\sim$. Law 12 is the one with no counterpart in block 1.

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

4. The Quotient-Remainder Theorem

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

See modular-arithmetic[101]. The uniqueness clause and the range $0 \leq r < d$ are what let you read a remainder off a rearranged expression.

5. Unique Factorisation Theorem

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

See divisibility-and-factorisation[102]. The second half is the "unique" part, and it is the half students leave out when asked to state the theorem.

[100] courses/math1061/proving-set-properties.pdf
[101] courses/math1061/modular-arithmetic.pdf
[102] courses/math1061/divisibility-and-factorisation.pdf

6. Schröder-Bernstein Theorem

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

See cardinality[103]. In use it means two injections, one each way, in place of one bijection, and the two must point in opposite directions between the same two sets.

7. Binomial Theorem

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

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

Belongs to the counting material (L30–L31). The coefficient $\binom{n}{k}$ is "n choose k", the number of k-element subsets of an n-element set (counting-selections[104]). The theorem, with its proof by counting a, b-sequences and the method for picking one coefficient out of an expansion, is in binomial-coefficients[105].

What this means for revision

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

Block 3 works the same way: the set identities are given, so the assessed skill is choosing and **citing by number**, not reciting the twelve laws — see proving-set-properties[106] for both worked methods that use them.

Blocks 4 and 5 are covered by modular-arithmetic[107] and divisibility-and-factorisation[108]. Block 6 is covered by cardinality[109]. Block 7 is covered by binomial-coefficients[110], and its $\binom{n}{k}$ by counting-selections[111].

Nothing else is provided. In particular the whole of set theory apart from block 3 — the definitions of $\subseteq$, $\subset$, $\mathcal{P}(A)$, $A \times B$, partition, function, image and preimage — is **not** on

[103] courses/math1061/cardinality.pdf
[104] courses/math1061/counting-selections.pdf
[105] courses/math1061/binomial-coefficients.pdf
[106] courses/math1061/proving-set-properties.pdf
[107] courses/math1061/modular-arithmetic.pdf
[108] courses/math1061/divisibility-and-factorisation.pdf
[109] courses/math1061/cardinality.pdf
[110] courses/math1061/binomial-coefficients.pdf
[111] courses/math1061/counting-selections.pdf

the page, and neither is any proof technique, nor anything about sequences, induction and recursion. Nor is anything about relations, groups or fields: the definitions of reflexive, symmetric, transitive and antisymmetric, of an equivalence relation (equivalence-relations[112]) and a partial order (partial-order-relations[113]), the four group properties (groups[114]), the subgroup checks (subgroups-and-cyclic-groups[115]) and the conditions for a field (fields[116]). Nor are the counting rules and selection formulas of counting-principles[117] and counting-selections[118], Pascal's formula, inclusion/exclusion (inclusion-exclusion[119]), the pigeonhole principle (pigeonhole-principle[120]) or the Handshake Theorem ([graphs]). Nor is any of the rest of the graph theory: the definitions of walk, trail, circuit and connected (walks-trails-and-circuits[121]), the Euler circuit and trail theorem (euler-circuits-and-trails[122]), adjacency and incidence matrices (adjacency-matrices[123], incidence-matrices[124]), or the theorem that a tree with n vertices has $n-1$ edges (trees[125]). All of that has to come from memory.

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[126]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[127]. What comes after builds on these: getting around a graph (walks-trails-and-circuits[128]), using every edge exactly once (euler-circuits-and-trails[129]), writing a graph as a matrix (adjacency-matrices[130], incidence-matrices[131]), and the connected graphs

[112] courses/math1061/equivalence-relations.pdf
[113] courses/math1061/partial-order-relations.pdf
[114] courses/math1061/groups.pdf
[115] courses/math1061/subgroups-and-cyclic-groups.pdf
[116] courses/math1061/fields.pdf
[117] courses/math1061/counting-principles.pdf
[118] courses/math1061/counting-selections.pdf
[119] courses/math1061/inclusion-exclusion.pdf
[120] courses/math1061/pigeonhole-principle.pdf
[121] courses/math1061/walks-trails-and-circuits.pdf
[122] courses/math1061/euler-circuits-and-trails.pdf
[123] courses/math1061/adjacency-matrices.pdf
[124] courses/math1061/incidence-matrices.pdf
[125] courses/math1061/trees.pdf
[126] courses/math1061/pigeonhole-principle.pdf
[127] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[128] courses/math1061/walks-trails-and-circuits.pdf
[129] courses/math1061/euler-circuits-and-trails.pdf
[130] courses/math1061/adjacency-matrices.pdf
[131] courses/math1061/incidence-matrices.pdf

with no circuits (trees[132]).

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, $e_1, e_2, \ldots$.

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.

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.

[132] courses/math1061/trees.pdf

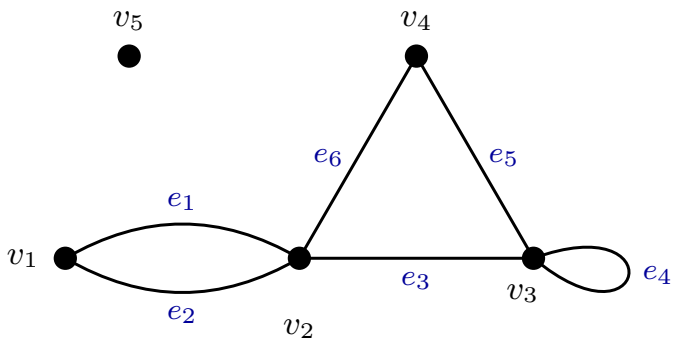


Figure 35: A graph with vertices v_1 to v_5 and edges e_1 to e_6. The edges e_1 and e_2 have the same endpoints, v_1 and v_2, so they are multiple edges. The edge e_4 has the single endpoint v_3, so it is a loop. v_5 is an isolated vertex: no edge has it as an endpoint, but it is still part of the graph. 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.

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[133]).

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.

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

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
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.

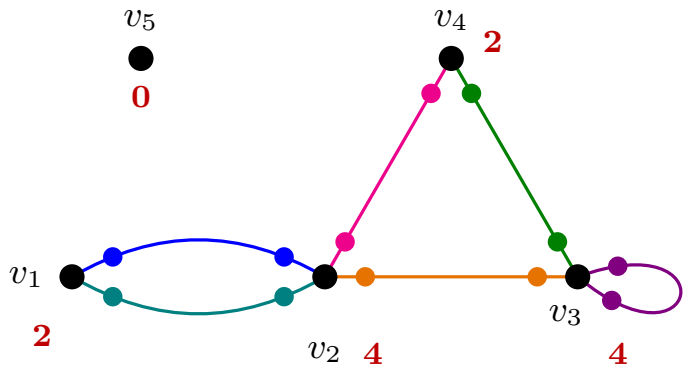


Figure 36: The proof of the Handshake Theorem, on the graph above. Every edge is drawn in its own colour, with a dot of that colour at each of its two ends. The loop e_4 has both of its dots at v_3. The degree of a vertex is the number of dots at it, so adding up the degrees counts every dot once. Each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

- **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.

Odd-degree vertices come in pairs

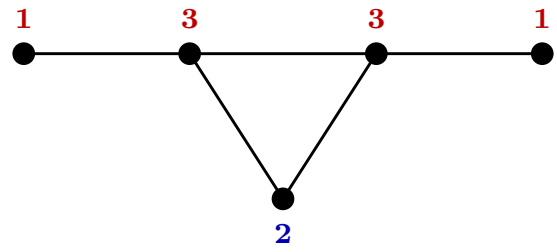
Corollary. Every graph has an even number of vertices of odd degree.

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. □



$$\underbrace{2}_{\text{even}} + \underbrace{(3+3)+(1+1)}_{\text{odd degrees, in pairs}} = 10 = 2 \cdot 5 \text{ edges}$$

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.

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[134].

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:

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

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 $3, 3, 3, 1$.

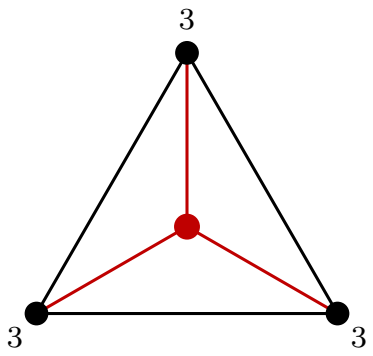


Figure 38: Why no simple graph has degree sequence 3, 3, 3, 1. In a simple graph on 4 vertices, a vertex of degree 3 is joined to every other vertex. The three vertices that need degree 3, black, must each be joined to the fourth vertex, red, which is then forced to have degree 3 as well. The list passes 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[135]).

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

Worked: which lists are degree sequences

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

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[136]. 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[137]). 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.

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

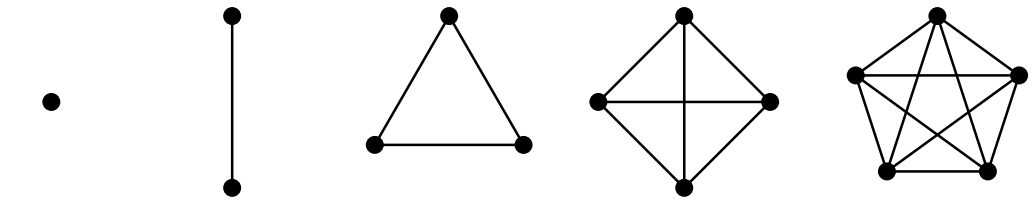


Figure 39: The complete graphs K_1 to K_5, each with every pair of vertices joined. Each vertex of K_n has degree $n-1$, so the degrees add to $n(n-1)$ and there are $\frac{n(n-1)}{2}$ edges: 0, 1, 3, 6 and 10. In K_4 and K_5 some lines cross where there is no vertex. Only the dots are vertices.

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[138] — every simple graph with at least two vertices has two vertices of equal degree
- counting-selections[139] — $\binom{n}{2}$, the number of edges of K_n
- 2026-07-27-welcome-and-intro-problems[140] — the bridges of Königsberg as a graph
- walks-trails-and-circuits[141] — walks, trails, circuits and connected graphs

[138] courses/math1061/pigeonhole-principle.pdf
[139] courses/math1061/counting-selections.pdf
[140] courses/math1061/2026-07-27-welcome-and-intro-problems.pdf
[141] courses/math1061/walks-trails-and-circuits.pdf

- euler-circuits-and-trails[142] — when a graph can be traced using every edge exactly once
- adjacency-matrices[143] · incidence-matrices[144] — a graph written as a matrix
- trees[145] — connected graphs with no circuits
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[146] — Lecture 33
- 2026-10-26-walks-trails-and-circuits[147] — Lecture 34, which recaps these definitions
- practice-problems[148] — §43, with full worked solutions

Inclusion/Exclusion

How to count a union of finite sets that overlap. The addition rule adds the sizes of sets only when they are disjoint; when an element can be in more than one set, adding the sizes counts it more than once. **Inclusion/exclusion** corrects this by subtracting the sizes of the pairwise intersections, adding back the triple intersections, and so on with alternating signs. This note covers the rule for two and three sets, why it counts every element exactly once, a proof of the three-set rule from the two-set rule, the general rule for n sets, counting "none of them" through the complement, counting multiples with the floor function, and the same rule for probabilities. The addition and difference rules it extends are in counting-principles[149]. First met in 2026-10-20-inclusion-exclusion[150].

Two sets

Inclusion/exclusion for two sets. For finite sets A and B,

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Why. Split $A \cup B$ into three disjoint pieces: $A - B$, $A \cap B$ and $B - A$. Then $|A|$ counts the first two pieces and $|B|$ counts the last two, so $|A| + |B|$ counts $A \cap B$ twice and the other two pieces once each. Subtracting $|A \cap B|$ once leaves every element of the union counted once.

	$A - B$	$A \cap B$	$B - A$
counted by $\lvert A\rvert$	1	1	0
counted by $\lvert B\rvert$	0	1	1
removed by $-\lvert A \cap B\rvert$	0	-1	0

[142] courses/math1061/euler-circuits-and-trails.pdf
[143] courses/math1061/adjacency-matrices.pdf
[144] courses/math1061/incidence-matrices.pdf
[145] courses/math1061/trees.pdf
[146] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[147] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[148] courses/math1061/practice-problems.pdf
[149] courses/math1061/counting-principles.pdf
[150] courses/math1061/2026-10-20-inclusion-exclusion.pdf

	$A-B$	$A\cap B$	$B-A$
total	**1**	**1**	**1**

If $A\cap B=\emptyset$, the correction is 0 and the rule is the addition rule, $|A\cup B|=|A|+|B|$ (counting-principles[151]). The three-piece split is also the quickest check on any two-set answer: once $|A\cap B|$ is known, $|A-B|=|A|-|A\cap B|$ and $|B-A|=|B|-|A\cap B|$, and the pieces together with the outside must add to the size of the universe.

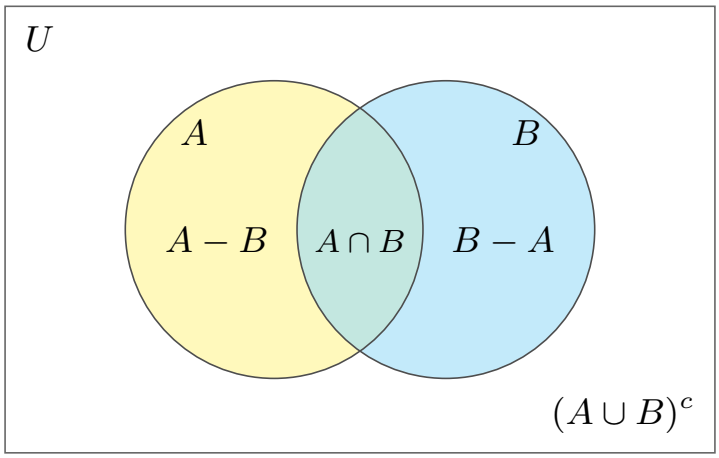


Figure 40: A universe U split by two sets into four disjoint regions. The circle A is the regions $A-B$ and $A\cap B$, and the circle B is $A\cap B$ and $B-A$, so the overlap is the one region inside both circles and is counted by both $|A|$ and $|B|$. Everything outside both circles is the complement $(A\cup B)^c$, the elements in neither set.

Three sets

Inclusion/exclusion for three sets. For finite sets A, B and C,

$$|A\cup B\cup C|=|A|+|B|+|C|-|A\cap B|-|A\cap C|-|B\cap C|+|A\cap B\cap C|.$$

Three groups of terms, with alternating signs: the three single sets added, the three pairwise intersections subtracted, the one triple intersection added.

[151] courses/math1061/counting-principles.pdf

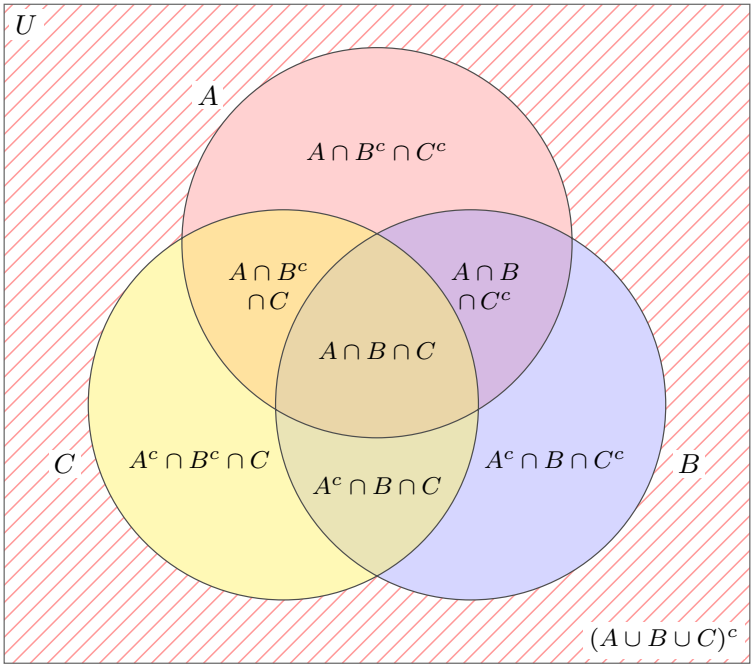


Figure 41: The eight disjoint regions into which three sets cut a universe U, each named by which of A, B and C it lies inside and which outside. Every term of the formula is a union of some of these regions: $|A|$ covers the four regions inside A, $|A \cap B|$ the two inside both A and B, and $|A \cap B \cap C|$ the centre alone. The hatched region outside all three circles is $(A \cup B \cup C)^c = A^c \cap B^c \cap C^c$, the elements in none of the sets.

Every region counted once

Three overlapping circles make seven regions inside the union. Each region is described by *how many* of the three sets it lies in, and that number decides how the formula counts it.

- **In exactly one set**, say A only. Counted once by $|A|$, and in none of the intersections. Net: 1.
- **In exactly two sets**, say A and B but not C. Counted by $|A|$ and $|B|$, so twice, and removed once, by $|A \cap B|$. It is not in $A \cap C$ or $B \cap C$, because those need C. Net: $2 - 1 = 1$.
- **In all three.** Counted three times by the singles, removed three times by the pairs, since it is in $A \cap B$, $A \cap C$ and $B \cap C$, and added once by the triple. Net: $3 - 3 + 1 = 1$.

This is why the triple intersection is added back **once**. After the pairs are subtracted, the centre has been counted $3 - 3 = 0$ times, one short of the 1 it needs. Adding $|A \cap B \cap C|$ twice would leave it counted twice.

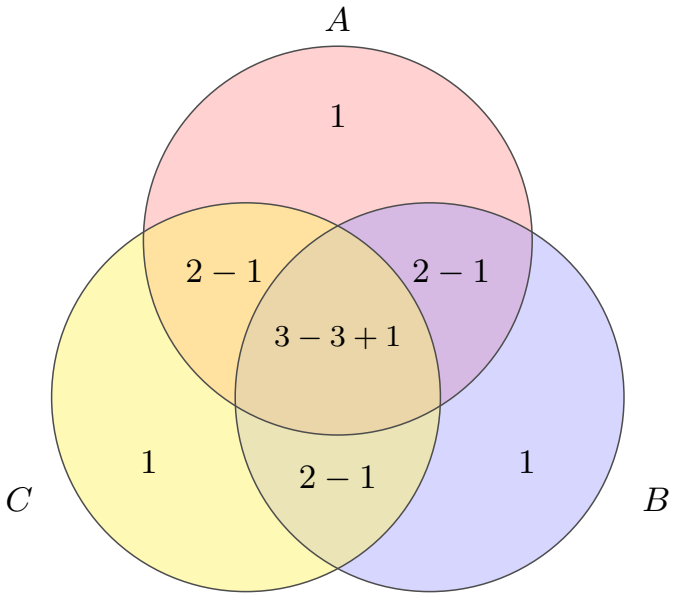


Figure 42: Each region of a three-set Venn diagram labelled with how the formula counts it: the number of single sets containing it, minus the number of pairwise intersections containing it, plus the triple intersection if it is in all three. A region in one set is counted 1; a region in two sets $2 - 1$; the centre $3 - 3 + 1$. Every region comes to exactly 1.

Proving the three-set rule from the two-set rule

The three-set rule is three applications of the two-set rule, $|X \cup Y| = |X| + |Y| - |X \cap Y|$, together with the set identities (formula-sheet[152]).

$$\begin{aligned}
|A \cup B \cup C| &= |A \cup (B \cup C)| && \text{associative law (2a)} \\
&= |A| + |B \cup C| - |A \cap (B \cup C)| && X = A,\ Y = B \cup C \\
&= |A| + |B| + |C| - |B \cap C| - |A \cap (B \cup C)| && X = B,\ Y = C \\
&= |A| + |B| + |C| - |B \cap C| - |(A \cap B) \cup (A \cap C)| && \text{distributive law (3b)} \\
&= |A| + |B| + |C| - |B \cap C| - (|A \cap B| + |A \cap C| - |A \cap B \cap C|) && X = A \cap B,\ Y = A \cap C \\
&= |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|.
\end{aligned}$$

The fifth line uses $(A \cap B) \cap (A \cap C) = A \cap B \cap C$, which is the commutative and associative laws (1b, 2b) to bring the two A's together and the idempotent law (7b), $A \cap A = A$. The triple term is subtracted inside a bracket that is itself subtracted, which is where its $+$ sign comes from. Each step is drawn in 2026-10-20-inclusion-exclusion[153].

The same move, splitting off the last set and applying the two-set rule, proves the rule for four sets from the rule for three, and so on: it is an induction on n (mathematical-induction[154]).

The general rule

Inclusion/exclusion for n sets. For finite sets $A_1, A_2, \dots, A_n$,

$$|A_1 \cup \cdots \cup A_n| = \sum_{1 \le i \le n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \sum_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|.$$

Add the singles, subtract the pairs, add the triples, subtract the four-way intersections, and keep alternating up to the intersection of all n, whose sign is $+$ when n is odd and $-$ when n is even. There are $\binom{n}{k}$ intersections of k sets, so the formula has $2^n - 1$ terms in all: 3 for two sets, 7 for three, 15 for four.

Written as a single sum over the non-empty sets S of indices, with $\bigcap_{t \in S} A_t$ the intersection of the A_t for $t \in S$ (for $S = \{2, 3, 6\}$, that is $A_2 \cap A_3 \cap A_6$):

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_{\emptyset \ne S \subseteq \{1, \dots, n\}} (-1)^{|S|+1} \left| \bigcap_{t \in S} A_t \right|.$$

[152] courses/math1061/formula-sheet.pdf
[153] courses/math1061/2026-10-20-inclusion-exclusion.pdf
[154] courses/math1061/mathematical-induction.pdf

Why each element is counted once. Take an element x of the union, and say it lies in exactly $m \geq 1$ of the sets. A term $|\bigcap_{t\in S} A_t|$ counts x exactly when every set in S contains x, that is, when S is a non-empty subset of the m indices of sets containing x. There are $\binom{m}{k}$ such S of size k, so x is counted

$$\binom{m}{1} - \binom{m}{2} + \binom{m}{3} - \cdots + (-1)^{m+1}\binom{m}{m} = 1 - (1-1)^m = 1$$

times. The middle step is the binomial theorem applied to $(1-1)^m = \sum_{k=0}^{m}\binom{m}{k}(-1)^k$, which is 0 because $m \geq 1$ (binomial-coefficients[155]). For $m = 1, 2, 3, 4$ the counts are 1, $2-1$, $3-3+1$ and $4-6+4-1$.

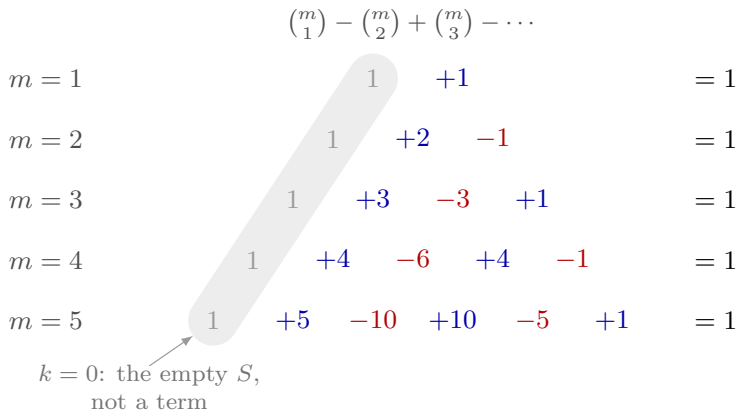


Figure 43: How the general formula counts an element lying in exactly m of the sets, for $m = 1$ to 5. Row m lists $\binom{m}{k}$, the number of intersections of k of those m sets, each carrying the sign of its group: $+$ for odd k and $-$ for even k. The grey entry is $\binom{m}{0} = 1$, which would belong to the empty set of indices and is not a term. Flipping the sign of every coloured entry and adding the grey 1 gives the expansion of $(1-1)^m = 0$, so the coloured entries themselves sum to $1-(1-1)^m = 1$ in every row.

None of them: the complement

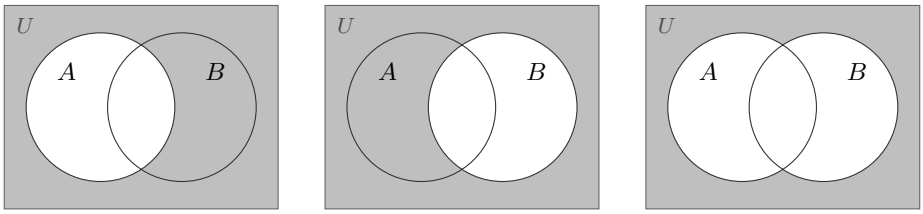
Inclusion/exclusion counts the elements in **at least one** of the sets. The elements in **none** of them are everything else, so inside a universe U,

$$|(A \cup B)^c| = |U| - |A \cup B| = |U| - |A| - |B| + |A \cap B|,$$

[155] courses/math1061/binomial-coefficients.pdf

$$|(A \cup B \cup C)^c| = |U| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|.$$

This is the difference rule (counting-principles[156]) applied to the union. By De Morgan's law (9a), $(A \cup B)^c = A^c \cap B^c$: "in neither A nor B" and "outside the union" are the same set. Questions phrased as "neither … nor", "none of", or "not divisible by any of" are complements of a union.



A^c B^c $A^c \cap B^c = (A \cup B)^c$

Figure 44: The elements in neither A nor B. The part of U outside A and the part outside B overlap in exactly the region outside both circles, which is the complement of the union: $A^c \cap B^c = (A \cup B)^c$. Counting that region is $|U| - |A \cup B|$, and inclusion/exclusion supplies $|A \cup B|$.

Running it backwards. The two-set rule links four numbers, $|A|$, $|B|$, $|A \cap B|$ and $|A \cup B|$, and any three determine the fourth. A question that gives the sizes of A, B and the "neither" region, and asks for "both", finds the union from the complement first and then solves for the intersection:

$$|A \cap B| = |A| + |B| - |A \cup B| = |A| + |B| - \big(|U| - |(A \cup B)^c|\big).$$

Counting multiples

The commonest use of inclusion/exclusion is counting integers with divisibility conditions. Two facts do all the work.

- **The multiples of d in $\{1, 2, \dots, N\}$** are $d, 2d, \dots, kd$ for the largest k with $kd \le N$, that is, $k \le N/d$. So there are $\lfloor N/d \rfloor$ of them. When d divides N the floor is not needed: $105/3 = 35$.
- **Being divisible by both a and b is being divisible by** $\operatorname{lcm}(a, b)$ (gcd-lcm-and-euclidean-algorithm[157]). When a and b have no common factor, $\operatorname{lcm}(a, b) = ab$, so the

[156] courses/math1061/counting-principles.pdf
[157] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf

multiples of both 3 and 5 are the multiples of 15. When they share a factor it is smaller than ab: the multiples of both 4 and 6 are the multiples of 12, not of 24.

The method, for "how many of $1, \dots, N$ are divisible by none of a, b, c":

1. Let A, B, C be the multiples of a, b, c in $\{1, \dots, N\}$.
2. Count each with $\lfloor N/d \rfloor$, using the lcm for each intersection.
3. Combine with inclusion/exclusion to get $|A \cup B \cup C|$.
4. Subtract from N.

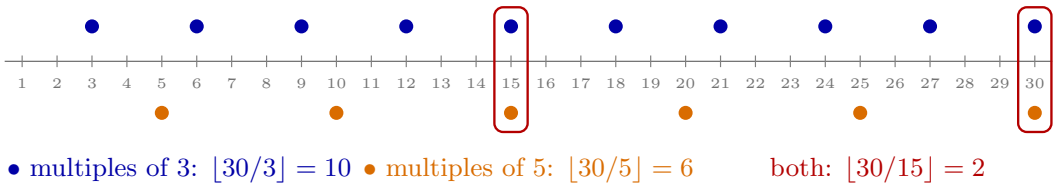


Figure 45: The integers 1 to 30, with the multiples of 3 marked above the line and the multiples of 5 below. There are $\lfloor 30/3 \rfloor = 10$ multiples of 3 and $\lfloor 30/5 \rfloor = 6$ of 5, but 15 and 30, the multiples of $\text{lcm}(3, 5) = 15$, are marked twice. So $10 + 6 - 2 = 14$ integers are divisible by 3 or 5, and the other 16 by neither.

With probabilities

When all outcomes in a finite sample space S are equally likely, $P(E) = |E|/|S|$ (probability[158]). Dividing the two-set rule through by $|S|$ gives

$$P(A \cup B) = P(A) + P(B) - P(A \cap B),$$

and the three-set and n-set rules divide through in the same way. The probability that *neither* happens is $1 - P(A \cup B)$. Either count first and divide at the end, or divide first and combine probabilities; the answer is the same.

Worked: divisible by 2, 3 or 5

How many of the integers $1, 2, \dots, 1000$ are divisible by none of 2, 3 and 5?

[158] courses/math1061/probability.pdf

Let A, B, C be the multiples of 2, 3 and 5 in $\{1, \dots, 1000\}$. The numbers are pairwise coprime, so each intersection is the multiples of the product. Not every division is exact this time.

$$|A| = \lfloor \tfrac{1000}{2} \rfloor = 500, \quad |B| = \lfloor \tfrac{1000}{3} \rfloor = 333, \quad |C| = \lfloor \tfrac{1000}{5} \rfloor = 200,$$

$$|A \cap B| = \lfloor \tfrac{1000}{6} \rfloor = 166, \quad |A \cap C| = \lfloor \tfrac{1000}{10} \rfloor = 100, \quad |B \cap C| = \lfloor \tfrac{1000}{15} \rfloor = 66, \quad |A \cap B \cap C| = \lfloor \tfrac{1000}{30} \rfloor = 33.$$

$$|A \cup B \cup C| = 500 + 333 + 200 - 166 - 100 - 66 + 33 = 734,$$

so $1000 - 734 = 266$ are divisible by none of 2, 3 and 5. A direct count over $1, \dots, 1000$ agrees.

Worked: the lcm, not the product

How many of the integers $1, 2, \dots, 100$ are divisible by 4 or by 6?

Let A be the multiples of 4 and B the multiples of 6. Then $|A| = \lfloor 100/4 \rfloor = 25$ and $|B| = \lfloor 100/6 \rfloor = 16$. A number divisible by both 4 and 6 is divisible by $\operatorname{lcm}(4, 6) = 12$, so $|A \cap B| = \lfloor 100/12 \rfloor = 8$. Hence

$$|A \cup B| = 25 + 16 - 8 = 33.$$

Using $4 \cdot 6 = 24$ for the intersection gives $\lfloor 100/24 \rfloor = 4$ and the wrong answer 37. The number 12 is divisible by both 4 and 6 but not by 24.

Worked: both, from neither

In a class of 60 students, 35 study French, 28 study German and 10 study neither. How many study both?

Let F and G be the students studying French and German. The students studying at least one are everyone except the 10, so $|F \cup G| = 60 - 10 = 50$. Then

$$|F \cap G| = |F| + |G| - |F \cup G| = 35 + 28 - 50 = 13.$$

Check: $35 - 13 = 22$ French only, $28 - 13 = 15$ German only, 13 both and 10 neither, and $22 + 15 + 13 + 10 = 60$.

Worked: at least one six

Two fair dice are rolled. What is the probability that at least one shows a six?

The 36 ordered pairs of results are equally likely. Let A be "the first die shows 6" and B "the second die shows 6". Each has 6 outcomes, and $A \cap B$ is the single outcome $(6, 6)$. So

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{6}{36} + \frac{6}{36} - \frac{1}{36} = \frac{11}{36}.$$

The answer $\frac{12}{36} = \frac{1}{3}$, from adding without the correction, counts the double six twice. The complement agrees: no six on either die has $5 \cdot 5 = 25$ outcomes, and $1 - \frac{25}{36} = \frac{11}{36}$.

Common mistakes

- **Adding overlapping sets.** $|A|+|B|$ is $|A \cup B|$ only when A and B are disjoint. Otherwise it counts every element of $A \cap B$ twice.
- **The wrong sign on the triple term.** $|A \cap B \cap C|$ is *added*. Subtracting it, as if every intersection were subtracted, leaves the centre counted $3 - 3 - 1 = -1$ times.
- **Leaving out the triple term.** Subtracting the three pairs and stopping counts the centre 0 times.
- **"Neither" as $|U| - |A| - |B|$.** That removes $A \cap B$ twice. The elements in neither are $|U| - |A \cup B| = |U| - |A| - |B| + |A \cap B|$.
- **The product instead of the lcm.** Divisible by 4 and 6 is divisible by 12, not 24. The product is right only when the numbers share no factor.
- **Forgetting the floor.** There are $\lfloor 1000/3 \rfloor = 333$ multiples of 3 up to 1000, not $333.\overline{3}$.
- **Including the empty set of indices.** In the sum over index sets S, S ranges over the non-empty subsets of $\{1, \ldots, n\}$. There is no intersection of no sets among the terms.
- **Reading the "neither" group wrongly.** "Came to class and scored below 60%" is outside both "did not come" and "scored at least 60%": it is $(A \cup B)^c$, not $A \cap B$ or A^c alone.

See also

- 2026-10-20-inclusion-exclusion[159] — Lecture 32, with every question worked in full
- counting-principles[160] — the addition rule for disjoint sets and the difference rule
- sets-and-set-notation[161] — unions, intersections and complements
- formula-sheet[162] — the numbered set identities used in the proof

[159] courses/math1061/2026-10-20-inclusion-exclusion.pdf
[160] courses/math1061/counting-principles.pdf
[161] courses/math1061/sets-and-set-notation.pdf
[162] courses/math1061/formula-sheet.pdf

- gcd-lcm-and-euclidean-algorithm[163] — the lcm, for intersections of sets of multiples
- binomial-coefficients[164] — $\binom{m}{k}$ and the binomial theorem behind the general rule
- [probability] — probability by counting equally likely outcomes
- practice-problems[165] — §41, 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[166] and counting-selections[167]. First met in 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[168].

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. □

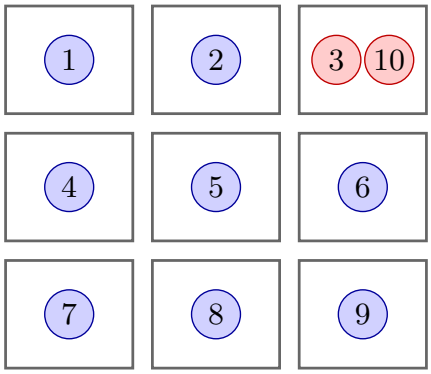
Three things about it:

- **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:

[163] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[164] courses/math1061/binomial-coefficients.pdf
[165] courses/math1061/practice-problems.pdf
[166] courses/math1061/counting-principles.pdf
[167] courses/math1061/counting-selections.pdf
[168] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf



10 pigeons, 9 holes: some hole holds 2

Figure 46: 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[169], and "one-to-one" is defined in one-to-one-and-onto-functions[170]. 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 $\lceil n/m \rceil \geq k+1$.

[169] courses/math1061/cardinality.pdf
[170] courses/math1061/one-to-one-and-onto-functions.pdf

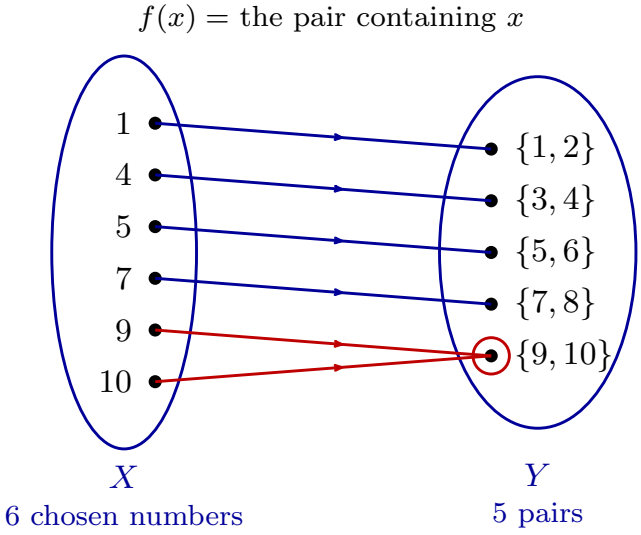
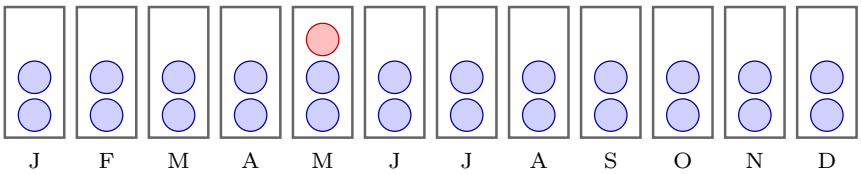


Figure 47: The function form on a small case: six numbers chosen from 1 to 10. X is the set of chosen numbers, the pigeons. Y is the set of five pairs of neighbours $1, 2, 3, 4, \ldots, 9, 10$, the holes. f sends each chosen number to the pair it lies in. Since $|X| = 6 > 5 = |Y|$, f cannot be one-to-one, 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 48: 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[171]).
- **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.

[171] 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[172].

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[173].

[172] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf
[173] 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[174], binomial-coefficients[175]).
- **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[176].

[174] courses/math1061/sets-and-set-notation.pdf
[175] courses/math1061/binomial-coefficients.pdf
[176] 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[177]). $n+1$ 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[178].

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.

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

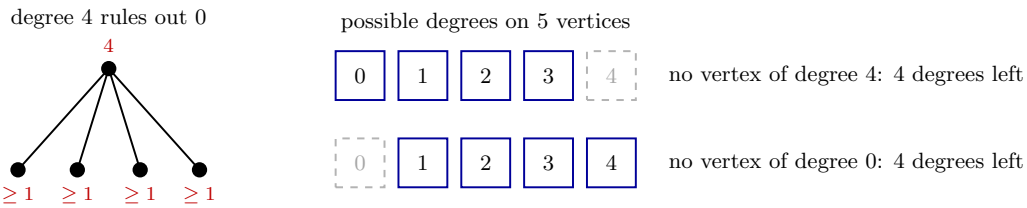


Figure 49: Why two vertices of a simple graph on 5 vertices have equal degree. The possible degrees are 0 to 4, five holes for five vertices, which forces nothing. But a vertex of degree 4 is joined to all four others, left, so each of them has degree at least 1 and none can have degree 0. So either 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[179] — 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[180] — what one-to-one means
- [graphs] — degree, used in equal degrees
- counting-selections[181] — counting the pigeons and the holes
- 2026-10-22-pigeonhole-principle-introduction-to-graph-theory[182] — Lecture 33

[179] courses/math1061/cardinality.pdf
[180] courses/math1061/one-to-one-and-onto-functions.pdf
[181] courses/math1061/counting-selections.pdf
[182] courses/math1061/2026-10-22-pigeonhole-principle-introduction-to-graph-theory.pdf

- 2026-10-26-walks-trails-and-circuits[183] — Lecture 34, which opens with equal degrees again
- practice-problems[184] — §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[185]). 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.

[183] courses/math1061/2026-10-26-walks-trails-and-circuits.pdf
[184] courses/math1061/practice-problems.pdf
[185] 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[186] 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[187]
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[188]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[189]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[190]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[191]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[192]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[193]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[194]

[186] courses/math1061/math1061.pdf
[187] courses/math1061/logical-connectives.pdf
[188] courses/math1061/logical-equivalence-laws.pdf
[189] courses/math1061/conditional-statements.pdf
[190] courses/math1061/valid-argument-forms.pdf
[191] courses/math1061/determining-argument-validity.pdf
[192] courses/math1061/quantified-statements.pdf
[193] courses/math1061/quantified-statements.pdf
[194] 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[195]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[196]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[197]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[198]
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[199]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[200]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[201]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[202]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[203]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[204]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[205]

[195] courses/math1061/proof-techniques.pdf
[196] courses/math1061/proof-techniques.pdf
[197] courses/math1061/proof-techniques.pdf
[198] courses/math1061/rational-and-irrational-numbers.pdf
[199] courses/math1061/divisibility-and-factorisation.pdf
[200] courses/math1061/modular-arithmetic.pdf
[201] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[202] courses/math1061/sequences-and-summations.pdf
[203] courses/math1061/mathematical-induction.pdf
[204] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[205] 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[206]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[207]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[208]
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[209]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[210]
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	

[206] courses/math1061/solving-recurrence-relations.pdf
[207] courses/math1061/sets-and-set-notation.pdf
[208] courses/math1061/sets-and-set-notation.pdf
[209] courses/math1061/proving-set-properties.pdf
[210] 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[211].

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

[211] 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[212].

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.

[212] 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[213].

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.

[213] 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[214].

[214] 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[215].

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

[215] 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[216].

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) $\forall m, n \in \mathbb{Z}^+,\ mn \geq m + n$.

[216] 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[217].

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.

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

Solutions

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

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

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

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

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

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

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

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

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

§8 — Statements with Multiple Quantifiers

Epp 4th ed. pp. 117–131 · 5th ed. (metric) pp. 131–146. Lecture 6 (week 2). Notes: quantified-statements[218].

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:

[218] 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[219].

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*

[219] 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[220].

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. □

[220] 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[221].

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.

[221] 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[222]*.*

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.

[222] 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[223].

[223] 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[224].

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 $58 \bmod 11$.

[224] 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[225].

[225] 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 $a = b$. $\square$

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 $a \mid b$. $\square$

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.

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

§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[226] — assessment weights and the full lecture schedule
- Logic: logical-connectives[227] · logical-equivalence-laws[228] · conditional-statements[229] · valid-argument-forms[230] · determining-argument-validity[231] · quantified-statements[232]
- Number theory and proof: proof-techniques[233] · rational-and-irrational-numbers[234] · divisibility-and-factorisation[235] · modular-arithmetic[236] · gcd-lcm-and-euclidean-algorithm[237]
- Graph theory (§43–§46): [graphs] · walks-trails-and-circuits[238] · euler-circuits-and-trails[239] · adjacency-matrices[240] · incidence-matrices[241] · trees[242]

Probability

When every outcome of a random process is equally likely, the probability of an event is a ratio of two counts: the number of outcomes in the event over the number of outcomes altogether. So probability problems of this kind are counting problems twice over, and every tool of counting-principles[243] and counting-selections[244] applies. This note sets up the language, sample spaces, events and equally likely outcomes, gives the formula, shows how the complement turns "at least one" and "not next to" into something easy, and works two examples through in full. Binomial coefficients, which most of the counts here use, have their own note in binomial-coefficients[245]. First met in 2026-10-19-probability-binomial-coefficients[246].

[226] courses/math1061/math1061.pdf
[227] courses/math1061/logical-connectives.pdf
[228] courses/math1061/logical-equivalence-laws.pdf
[229] courses/math1061/conditional-statements.pdf
[230] courses/math1061/valid-argument-forms.pdf
[231] courses/math1061/determining-argument-validity.pdf
[232] courses/math1061/quantified-statements.pdf
[233] courses/math1061/proof-techniques.pdf
[234] courses/math1061/rational-and-irrational-numbers.pdf
[235] courses/math1061/divisibility-and-factorisation.pdf
[236] courses/math1061/modular-arithmetic.pdf
[237] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[238] courses/math1061/walks-trails-and-circuits.pdf
[239] courses/math1061/euler-circuits-and-trails.pdf
[240] courses/math1061/adjacency-matrices.pdf
[241] courses/math1061/incidence-matrices.pdf
[242] courses/math1061/trees.pdf
[243] courses/math1061/counting-principles.pdf
[244] courses/math1061/counting-selections.pdf
[245] courses/math1061/binomial-coefficients.pdf
[246] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf

Sample spaces and events

- A **random process** (or experiment) is anything with an outcome that is not known in advance: rolling a die, choosing a committee by lot, shuffling a list of numbers.
- The **sample space** S is the set of all possible outcomes.
- An **event** E is a subset of the sample space, $E \subseteq S$. The event **happens** when the outcome is one of the elements of E.

Rolling one die: $S = \{1, 2, 3, 4, 5, 6\}$, and "the roll is even" is the event $E = \{2, 4, 6\}$. An event is a set, so the set operations apply. The **complement** $E^c = S - E$ is the event that E does not happen, here $\{1, 3, 5\}$, "the roll is odd".

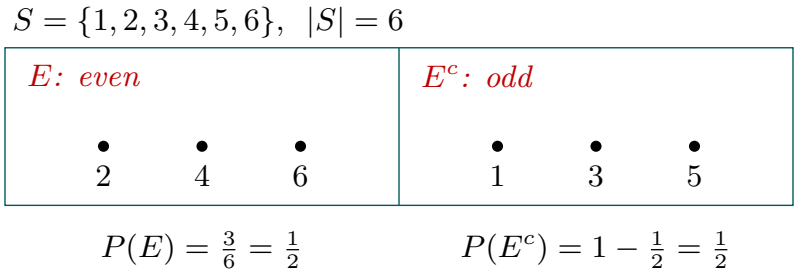


Figure 50: The sample space for one roll of a die, split into the event E, the roll is even, and its complement E^c, the roll is odd. Every outcome lies in exactly one of the two parts. With six equally likely outcomes, $P(E) = |E|/|S| = 3/6$, and since the two parts fill the whole sample space, $P(E^c) = 1 - P(E)$.

Equally likely outcomes

If S is a finite sample space in which every outcome is **equally likely**, the **probability** of an event $E \subseteq S$ is

$$P(E) = \frac{|E|}{|S|} = \frac{\text{number of outcomes in } E}{\text{total number of outcomes}}.$$

Wording such as "chosen at random", "a randomly chosen permutation", "a fair die" or "shuffled" signals equally likely outcomes. Some consequences come straight from the formula:

- $0 \leq P(E) \leq 1$, since $0 \leq |E| \leq |S|$.
- $P(\emptyset) = 0$ and $P(S) = 1$: an impossible event and a certain one.
- A probability is often quoted as a percentage: $\frac{7}{9} = 0.777\ldots \approx 77.8\%$.

The outcomes must really be equally likely. Roll two dice and ask for the probability that they add to 7. The sums $2, 3, \ldots, 12$ are eleven outcomes, but they are not equally likely, so $\frac{1}{11}$ is wrong. The equally likely outcomes are the 36 ordered pairs $(1,1), (1,2), \ldots, (6,6)$, of which 6 add to 7: $(1,6), (2,5), (3,4), (4,3), (5,2), (6,1)$. So the probability is $\frac{6}{36} = \frac{1}{6}$. Choosing a sample space whose outcomes are equally likely is the first step of every problem.

Probability by counting

1. **Decide what one outcome is**, and make sure all outcomes are equally likely. A committee is an unordered selection, a permutation is an ordered arrangement, a password is an ordered selection with repeats (counting-selections[247]).
2. **Count the sample space**, $|S|$.
3. **Count the event**, $|E|$, with the same kind of outcome. If S was counted as unordered selections, E must be too.
4. **Divide**, and simplify the fraction before turning it into a decimal.

Step 3 is where the counting tools come in: forcing part of the outcome, splitting into categories, gluing objects that must sit together, and the complement.

The complement

For any event E in a finite sample space S with equally likely outcomes,

$$P(E^c) = 1 - P(E), \qquad \text{equivalently} \qquad P(E) = 1 - P(E^c).$$

Why. E and E^c split S into two disjoint parts, so $|E^c| = |S| - |E|$ by the difference rule (counting-principles[248]). Dividing by $|S|$,

$$P(E^c) = \frac{|S| - |E|}{|S|} = 1 - \frac{|E|}{|S|} = 1 - P(E).$$

When to use it. When the event is easier to describe by what it rules out.

- **"At least one"** has opposite **"none"**, a single case. $P(\text{at least one}) = 1 - P(\text{none})$.
- **"Not next to each other"** has opposite **"next to each other"**, which is counted by gluing the two objects into one block. $P(\text{not adjacent}) = 1 - P(\text{adjacent})$.

[247] courses/math1061/counting-selections.pdf
[248] courses/math1061/counting-principles.pdf

Worked: a committee with at least one mathematician

> A committee of 5 is chosen at random from a group of 25 mathematicians and 25 physicists. What is the probability that at least one mathematician is chosen?

Outcomes. A committee is an unordered selection of 5 of the 50 people, and choosing at random makes every committee equally likely. So

$$|S| = \binom{50}{5} = \frac{50 \cdot 49 \cdot 48 \cdot 47 \cdot 46}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 2\,118\,760.$$

The complement. "At least one mathematician" means 1, 2, 3, 4 or 5 mathematicians, five cases. Its opposite, "no mathematicians", is one case: all 5 members are physicists, chosen from the 25 physicists, in

$$\binom{25}{5} = \frac{25 \cdot 24 \cdot 23 \cdot 22 \cdot 21}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 53\,130$$

ways. Writing $T = \binom{50}{5}$ for all committees and $N = \binom{25}{5}$ for those with no mathematicians,

$$\begin{aligned} P(\text{at least one mathematician}) &= \frac{\#(\text{committees with at least one mathematician})}{\#(\text{committees})} = \frac{T-N}{T} = 1 - \frac{N}{T} \\ &= 1 - \frac{\binom{25}{5}}{\binom{50}{5}} = 1 - \frac{53\,130}{2\,118\,760} = 1 - \frac{33}{1316} = \frac{1283}{1316} \\ &\approx 0.9749 \approx 97.5\%. \end{aligned}$$

A quicker route to $\frac{N}{T}$: the two 5!'s cancel, leaving $\frac{25 \cdot 24 \cdot 23 \cdot 22 \cdot 21}{50 \cdot 49 \cdot 48 \cdot 47 \cdot 46} = \frac{33}{1316} \approx 0.025$. An all-physicist committee happens about 2.5% of the time.

Worked: 5 not next to 6

> What is the probability that a randomly chosen permutation of $\{1, 2, \ldots, 9\}$ has 5 not next to 6?

Outcomes. A permutation is an ordering of all nine numbers: ordered, no repeats. There are $|S| = 9!$ of them, all equally likely.

The complement. "5 not next to 6" is awkward to count directly, because where 6 may go depends on where 5 is. Its opposite, "5 next to 6", is easy. If 5 and 6 are adjacent they appear as **56** or as **65**.

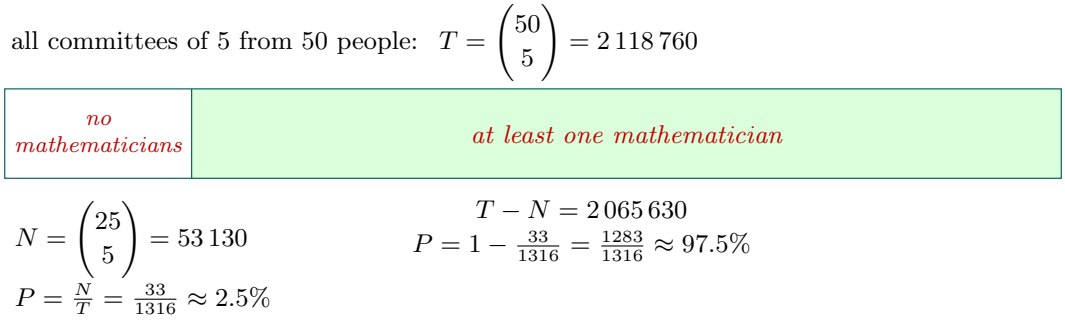


Figure 51: All $\binom{50}{5}$ committees of 5 drawn from 25 mathematicians and 25 physicists, split by whether they include a mathematician. The two parts are disjoint and fill the whole set, so the shaded event, at least one mathematician, has probability 1 minus the probability of the small part, an all-physicist committee. The widths are not to scale: the all-physicist committees are only about 2.5% of the total.

- **Permutations containing 56.** Glue 5 and 6 into a single tile **56**. Arranging the permutation is now arranging 8 objects, the tile and the other seven numbers, in a row: 8! ways. Each arrangement of the 8 objects gives exactly one permutation of $\{1, \dots, 9\}$ with 5 immediately before 6, and every such permutation arises once. (Writing it as $8 \cdot 7!$, with 8 places the tile can start and 7! orders for the rest, gives the same 8!.)
- **Permutations containing 65.** The same argument with the tile **65**: 8!.

No permutation contains both, so $2 \cdot 8!$ permutations have 5 next to 6. Then

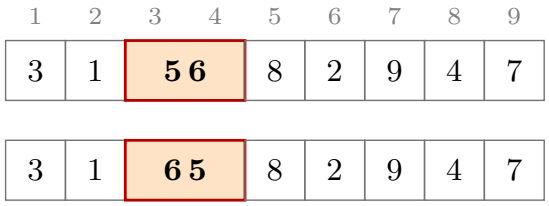
$$P(5 \text{ not next to } 6) = \frac{9! - 2 \cdot 8!}{9!} = 1 - \frac{2 \cdot 8!}{9 \cdot 8!} = 1 - \frac{2}{9}$$
$$= \frac{9-2}{9} = \frac{7}{9} = 0.777\ldots \approx 77.8\%.$$

In numbers, $9! = 362\,880$ and $2 \cdot 8! = 80\,640$, so 282 240 permutations have 5 and 6 apart.

A check by positions. Only the positions of 5 and 6 matter. As an unordered pair they are one of $\binom{9}{2} = 36$ equally likely pairs of positions, and 8 of those pairs are adjacent, $\{1,2\}, \{2,3\}, \dots, \{8,9\}$. So $P(\text{adjacent}) = \frac{8}{36} = \frac{2}{9}$, as before.

Common mistakes

- **Mixing kinds of outcome.** If the sample space counts committees as unordered selections, the event must too. Counting $|S|$ as $\binom{50}{5}$ and $|E|$ as ordered selections gives a "probability" up to $5! = 120$ times too large, and often bigger than 1.



5 next to 6: $2 \cdot 8! = 80\,640$ of $9! = 362\,880$

$$P(5 \text{ not next to } 6) = 1 - \frac{2 \cdot 8!}{9!} = 1 - \frac{2}{9} = \frac{7}{9}$$

Figure 52: Counting permutations of $1, \ldots, 9$ in which 5 and 6 are next to each other. Glue the pair into one tile. With the tile 56 there are 8 objects to arrange, the tile and the seven other numbers, in 8! ways, and each arrangement unglues to a permutation with 5 just before 6. The tile 65 gives another 8!, with 6 just before 5. So $2 \cdot 8!$ of the 9! permutations have 5 next to 6, and the probability that they are apart is $1 - \frac{2 \cdot 8!}{9!} = \frac{7}{9}$.

- **Outcomes that aren't equally likely.** The sum of two dice is not uniform on $2, \ldots, 12$; use the 36 ordered pairs.
- **Forgetting one of the orders when gluing.** "Next to" includes both 56 and 65. Counting only one gives $P(\text{adjacent}) = \frac{1}{9}$ and the wrong answer $\frac{8}{9}$.
- **Labelling the complement as the event.** $\frac{N}{T}$ is the probability of no mathematicians, about 2.5%; $1 - \frac{N}{T}$ is the probability of at least one, about 97.5%. Name each quantity before computing it.
- **Rounding too early.** Keep the exact fraction, here $\frac{1283}{1316}$ and $\frac{7}{9}$, and round only at the end.
- **A probability outside $[0, 1]$.** It always means a slip in one of the counts.

See also

- counting-selections[249] — the four kinds of selection, restrictions, gluing, and counting "at least" through the complement
- counting-principles[250] — the multiplication, addition and difference rules
- binomial-coefficients[251] — $\binom{n}{r}$, its symmetry and identities

[249] courses/math1061/counting-selections.pdf
[250] courses/math1061/counting-principles.pdf
[251] courses/math1061/binomial-coefficients.pdf

- inclusion-exclusion[252] — counting, and so finding the probability of, a union of events that overlap
- sets-and-set-notation[253] — events are subsets, and E^c is the set complement
- 2026-10-19-probability-binomial-coefficients[254] — Lecture 31
- practice-problems[255] — §39, with full worked solutions

Sets and Set Notation

The language the rest of mathematics is written in: what a set is, the difference between belonging to one and being contained in one, and the operations that build new sets from old. See proving-set-properties[256] for the proof methods that go with these definitions, and functions-on-general-sets[257] for what gets built on top of them.

Writing a set down

Two ways, both used constantly:

- **By listing the elements**, inside braces: $\{1, 2, 3\}$, $\{a\}$, $\{\emptyset, \{\emptyset\}\}$. An infinite list gets an ellipsis: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.
- **By a defining condition** — *set-builder* notation: $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$, read "the set of integers n such that $n \equiv 2 \bmod 8$".

Both a vertical bar and a colon are used as the "such that" separator, interchangeably. $\{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and $\{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$ take the bar; $f = \{(x, y) \in \mathbb{R} \times \mathbb{R} : y = 2x + 1\}$ and $f^{-1}(B) = \{x \in X : f(x) \in B\}$ take the colon. Read either as "such that"; nothing turns on which one is written.

Two conventions worth naming, because everything below relies on them: **sets take capital italic letters** (A, B, C, S, T, X, Y), with U reserved for the universal set, and **elements take lower case** (x, y, t, n). And $|A|$ denotes the **cardinality** of A — the number of elements it has (for infinite sets, where "number of elements" needs care, see cardinality[258]).

[252] courses/math1061/inclusion-exclusion.pdf
[253] courses/math1061/sets-and-set-notation.pdf
[254] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf
[255] courses/math1061/practice-problems.pdf
[256] courses/math1061/proving-set-properties.pdf
[257] courses/math1061/functions-on-general-sets.pdf
[258] courses/math1061/cardinality.pdf

"Is an element of" versus "is a subset of"

> **Warning.** Take care with the distinction between *is an element of* ($\in$) and *is a subset of* ($\subseteq$).

This is the single most common source of error in the whole topic, and it is worth being blunt about why: the two relate **different kinds of thing**.

	Reads	Left-hand side is	Right-hand side is
$x \in A$	x is an element of A	an **object**	a **set**
$A \subseteq B$	A is a subset of B	a **set**	a **set**

Is $\mathbb{Z} \in \mathbb{Q}$? False. The elements of $\mathbb{Q}$ are rational *numbers*, and $\mathbb{Z}$ is not a number — it is a set of numbers. The true statement in the neighbourhood is $\mathbb{Z} \subseteq \mathbb{Q}$.

The instinct behind the mistake ("but aren't all integers rational?") is right; it is the symbol that is wrong. "All integers are rational" is exactly the claim $\mathbb{Z} \subseteq \mathbb{Q}$.

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

Worked: true or false?

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

Each false line becomes true if you swap the symbol or the braces, which is the point of the exercise. In (c), $\{4\} \subseteq \{2, 3, 4\}$ **is** true.

The reliable technique: **write out the set's elements and ask whether the left-hand object is literally one of the things in the list.** For $\{\{4\}\}$ that list is a single item, the set $\{4\}$ — and 4 is not on it.

Subsets and proper subsets

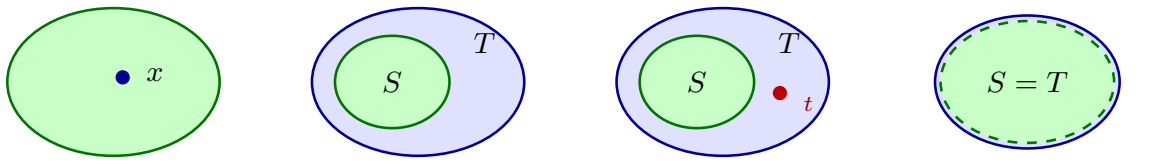
A set S is a **subset** of a set T, written $S \subseteq T$, if every element in S is also in T. Formally, $\forall x$, if $x \in S$ then $x \in T$.

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

So $\subset$ is $\subseteq$ plus "and they are not equal" — exactly parallel to $<$ against $\leq$ for numbers.

	Holds	Fails
$\subseteq$	$\mathbb{Z} \subseteq \mathbb{Q}$, and $\mathbb{Z} \subseteq \mathbb{Z}$	
$\subset$	$\mathbb{Z} \subset \mathbb{Q}$	$\mathbb{Z} \not\subset \mathbb{Z}$

A set is always a subset of itself and never a *proper* subset of itself — that single line is the whole difference between the two symbols.



A — $x \in A$ | $S \subseteq T$ | $S \subset T$ (some $t \in T$, $t \notin S$) | $S \subseteq T$ and $T \subseteq S$

Figure 53: The four situations the symbols distinguish. An element sits inside a set; a subset is a set inside a set; a proper subset leaves something over; and equality is containment holding both ways at once. The contained set is green and the containing set pale blue, with elements as small blue dots; the red dot is the element that keeps the containment proper.

Proving one set is a subset of another

To prove $S \subseteq T$, consider an **arbitrary** element of S and show it is also in T. That is: **suppose $x \in S$, and prove $x \in T$.**

This is the *element method*, and it is used so heavily that proving-set-properties[259] treats it in full. The word doing the work is "arbitrary" — you may assume nothing about x beyond membership of S, which is what makes the one argument cover every element at once.

[259] courses/math1061/proving-set-properties.pdf

Worked. Let $D = \{n \in \mathbb{Z} \mid n \equiv 2 \pmod 8\}$ and let E be the set of even integers, i.e. $E = \{n \in \mathbb{Z} \mid n \equiv 0 \pmod 2\}$. Prove $D \subseteq E$.

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

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

Since $4k + 1 \in \mathbb{Z}$, we have $x \equiv 0 \pmod 2$, and therefore $x \in E$. Thus $D \subseteq E$. ■

Rewriting $8k + 2$ as $2(4k + 1)$ is the entire proof — see modular-arithmetic[260] for the definition being applied.

Is $D \subset E$? Yes. We have $D \subseteq E$, and $4 \in E$ while $4 \notin D$ (since $4 \not\equiv 2 \bmod 8$), so the containment is proper. Note that upgrading $\subseteq$ to $\subset$ needs **one** witness, not a general argument.

When are two sets equal?

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

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

$$S = T \quad \text{is logically equivalent to} \quad (S \subseteq T) \wedge (T \subseteq S)$$

So **to prove two sets are equal, do two separate proofs**:

- Suppose $x \in S$, and prove $x \in T$. This shows $S \subseteq T$.
- Suppose $x \in T$, and prove $x \in S$. This shows $T \subseteq S$.

Together these give $S = T$. This is not a convention but a consequence — the double containment argument is just the biconditional law of logical-equivalence-laws[261] read through the definition of $\subseteq$, which is why "prove both directions" is never optional.

[260] courses/math1061/modular-arithmetic.pdf
[261] courses/math1061/logical-equivalence-laws.pdf

The empty set

$\emptyset = \{\ \}$ — the set with no elements.

Why is $\emptyset \subseteq A$ for every set A? Because "$\forall x$, if $x \in \emptyset$ then $x \in A$" is true for every set A. The hypothesis $x \in \emptyset$ is never satisfied, and a conditional with a false hypothesis is true — so the statement holds **vacuously**. See conditional-statements[262] for that truth-table row, which is doing all the work here.

Do not confuse this with $\emptyset \in A$. Some sets do contain the empty set as an element; many do not. $\emptyset \subseteq A$ is a theorem about every set; $\emptyset \in A$ is a claim about one particular set that usually fails.

Why is $A \subseteq A$ for every set A? Because "$\forall x$, if $x \in A$ then $x \in A$" is true for every set A — this one for the opposite reason, that the conclusion simply restates the hypothesis.

There is only one empty set

Lemma. There is only one empty set.

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

This is why we say *the* empty set and write a single symbol for it. The proof is a neat demonstration of the double-containment criterion doing real work: both containments come free from vacuous truth, and equality falls out.

Unions and intersections

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\} \qquad A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

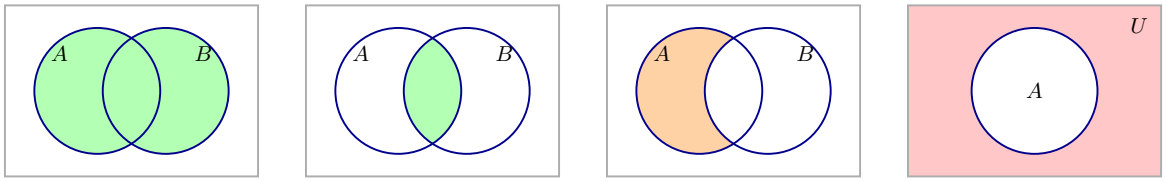
Worked. Let $A_1 = \{1, 2, 3\}$, $A_2 = \{1, 2, 4\}$ and $A_3 = \{3, 4, 5\}$.

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

Indexed over all three:

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

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



$A \cup B$ $A \cap B$ $A - B$ (also written $A \setminus B$) $A^c = U - A$

Figure 54: The four operations as shaded regions. Union takes everything in either circle, intersection only the overlap, difference removes B from A, and the complement is everything in the universe outside A — which is why a complement is only meaningful once the universe U is fixed. The enclosing rectangle is that universe.

Worth noticing: **the three sets intersect pairwise in a non-empty set every time, and yet the triple intersection is empty.** Pairwise overlap does not survive to the whole family, so an indexed intersection has to be computed, not inferred.

Indexed families

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{at least one } i \in I\} \qquad \bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ for } \textbf{every } i \in I\}$$

These extend to infinite index sets unchanged, which is where they earn their keep.

Worked, over $i = 0, 1, 2, ...$:

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

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

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

The intersection is the interesting one. The intervals **grow** as i increases, so the intersection is pinned by the *smallest* of them, the $i = 0$ term $[0, 0] = \{0\}$. Every larger interval contains 0, so nothing is lost, and nothing else survives.

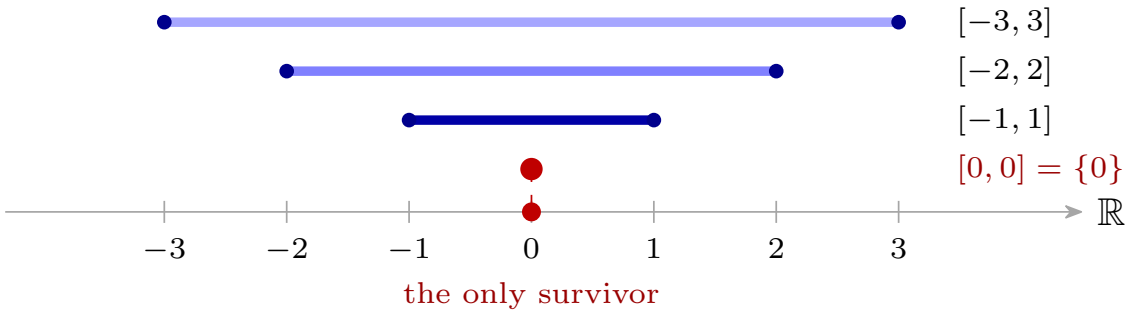


Figure 55: An intersection over an increasing family is decided by its smallest member. Each interval contains the one below it, so the only real number lying in all of them is the single point the innermost interval contains. The intervals sit above the number line, with a filled dot at each closed endpoint.

Set difference and complement

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

Both are drawn in Figure 54 above.

The backslash and the minus sign mean the same thing: $A - B$ can equally be written $A \setminus B$. Different textbooks pick different ones; there is no distinction to learn.

The **complement** A^c is the set difference from the universal set U under discussion: $A^c = U - A$. It is only meaningful once U is fixed, so a complement always sits inside a stated universe.

The power set

$\mathcal{P}(A)$ is the set of **all subsets** of A.

Worked. Let $S = \{1, 2, 3\}$. Then

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

Note that the elements of $\mathcal{P}(S)$ are **sets**, which resets the $\in$ / $\subseteq$ trap one level up:

Statement		Why
$\{1,2\} \in \mathcal{P}(S)$	**True**	$\{1,2\}$ is one of the eight things listed

Statement		Why
$\{1,2\} \subseteq \mathcal{P}(S)$	**False**	that would need 1 and 2 themselves to be elements of $\mathcal{P}(S)$, i.e. to be subsets of S — and they are numbers, not sets
$\{\{1,2\}\} \subseteq \mathcal{P}(S)$	**True**	the one element it has, $\{1,2\}$, is in $\mathcal{P}(S)$

Also worth recording as a standing fact: since $\emptyset \subseteq A$ for every set A, it follows that $\emptyset \in \mathcal{P}(A)$ for every set A. Every power set is non-empty, including $\mathcal{P}(\emptyset)$.

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

The finiteness matters — the count is meaningless otherwise. The 2^n comes from building a subset by making n independent in/out choices. Sorting the same subsets by size instead gives $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ (binomial-coefficients[263]).

Worked: is $\{1,3,-1\} \subset \mathcal{P}(\mathbb{Z})$?

False, and the reasoning is the $\in/\subseteq$ distinction again, run carefully:

- $1, 3, -1 \in \mathbb{Z}$, so $\{1,3,-1\} \subseteq \mathbb{Z}$.
- Therefore $\{1,3,-1\} \in \mathcal{P}(\mathbb{Z})$ — it is one of the subsets of $\mathbb{Z}$, hence an *element* of the power set.
- So $\{1,3,-1\} \notin \mathcal{P}(\mathbb{Z})$: for that, its **elements** 1, 3 and -1 would have to be elements of $\mathcal{P}(\mathbb{Z})$, i.e. subsets of $\mathbb{Z}$ — and they are integers, not sets.

The statement is off by exactly one level, which is the characteristic failure mode with power sets.

Worked: power sets of power sets

Building up from the empty set, with the 2^n fact as a running check:

	Value	$\lvert\cdot\rvert$ of the input	Check
$\mathcal{P}(\{a\})$	$\{\emptyset,\ \{a\}\}$	$\lvert\{a\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\emptyset)$	$\{\emptyset\}$	$\lvert\emptyset\rvert = 0$	$2^0 = 1$ ✓
$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$	$\{\emptyset,\ \{\emptyset\}\}$	$\lvert\{\emptyset\}\rvert = 1$	$2^1 = 2$ ✓

[263] courses/math1061/binomial-coefficients.pdf

	Value	$\lvert\cdot\rvert$ of the input	Check
$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset, \{\emptyset\}\})$	$\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset, \{\emptyset\}\}\}$	$\lvert\{\emptyset, \{\emptyset\}\}\rvert = 2$	$2^2 = 4$ ✓

$\mathcal{P}(\emptyset) = \{\emptyset\}$ is the line to get right: the empty set has exactly one subset — itself — so its power set has **one** element and is **not** empty. Counting the elements at each stage and checking against 2^n is the cheapest way to catch a dropped or duplicated brace.

Cartesian products

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

the set of **ordered pairs** with first coordinate from A and second from B.

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

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

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

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

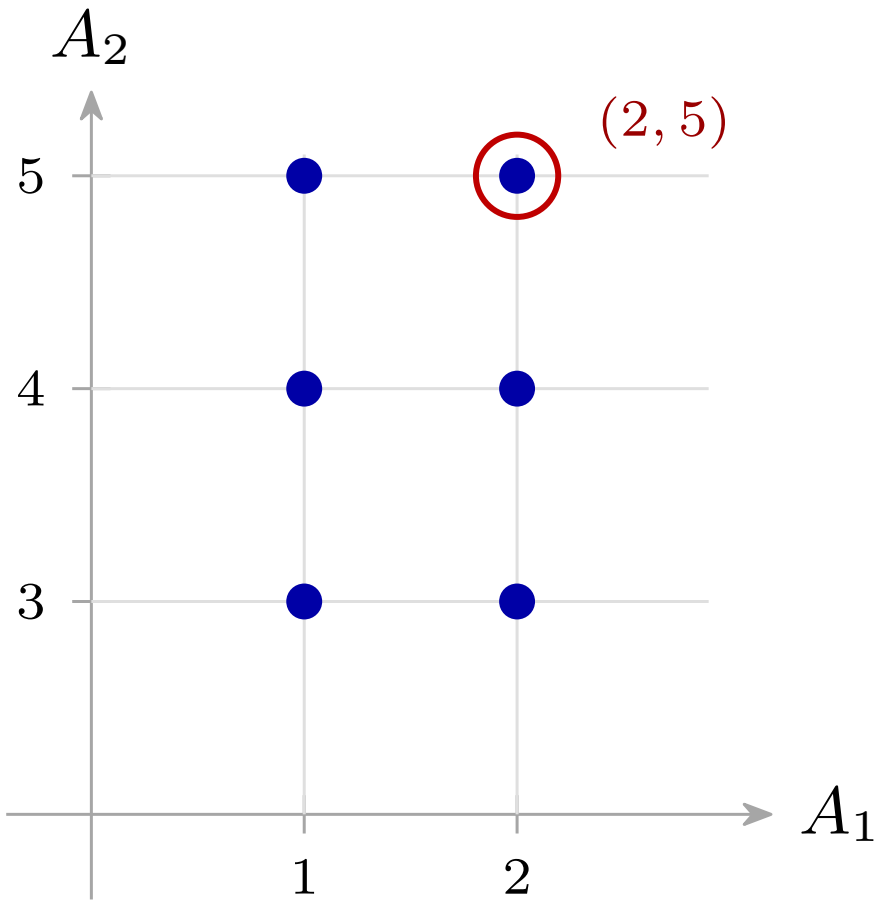
- $(d, c) \notin S \times T$, since $d \notin S$ — the **order matters**, and d is disqualified as a first coordinate.
- $(c, d) \in S \times T$, since $c \in S$ and $d \in T$.
- $S \times T$ contains $3 \times 2 = 6$ elements.

The familiar case is $\mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R} \text{ and } y \in \mathbb{R}\}$, usually written $\mathbb{R}^2$ — the plane is a Cartesian product, which is where the name comes from.

Two facts:

- If $A = \emptyset$ or $B = \emptyset$ then $A \times B = \emptyset$ — there is no way to choose a coordinate from an empty set.
- For finite sets, $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.

  Notation clash to be aware of. (a, b) can mean an **ordered pair**, and (a, b) can also mean an **open interval** — the real numbers x with $a < x < b$. Nothing in the symbols distinguishes them; only the context does.



$$|A_1 \times A_2| = |A_1| \cdot |A_2| = 2 \times 3 = 6$$

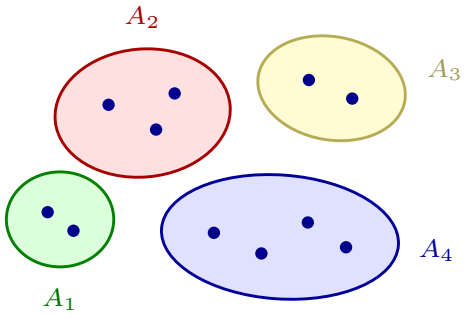
Figure 56: A Cartesian product laid out as a grid: one row per element of the first set, one column per element of the second, one ordered pair at every crossing. The rectangular shape is the counting fact — the number of pairs is the product of the two sizes.

Partitions

A finite or infinite collection of **non-empty** sets $\{A_1, A_2, A_3, \dots\}$ is a **partition** of a set A if and only if

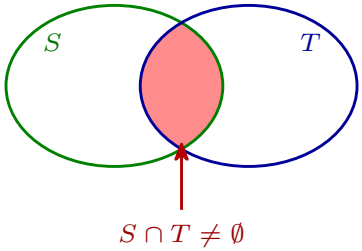
$$A = A_1 \cup A_2 \cup A_3 \cup \cdots \qquad \text{and} \qquad A_i \cap A_j = \emptyset \text{ for each } i, j \geq 1,\ i \neq j$$

Three conditions, all of which are checkable and all of which get tested: the pieces are **non-empty**, they **cover** A, and they are **pairwise disjoint**.



a partition of A

$A = A_1 \cup A_2 \cup A_3 \cup A_4$, pairwise disjoint



not a partition of R

$R = S \cup T$, but the pieces overlap

Figure 57: A partition cuts a set into non-empty pieces that cover it with no overlap — every element lands in exactly one piece. Failing any one of the three conditions is enough to disqualify a collection. On the left is a partition: separate closed curves, one per piece, each holding its elements as dots. On the right, two pieces share an element, so the collection is not a partition.

Examples over $\mathbb{Z}$:

- $\{E, O\}$, where E is the even integers and O the odd integers, is a partition of $\mathbb{Z}$.
- $\{\{0\},\ \mathbb{Z}^+,\ \mathbb{Z}^-\}$ is another partition of $\mathbb{Z}$ — a set can be partitioned in many ways.

Worked: a collection that fails

Let $S = \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\}$, let $T = \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 4\}$, and let $R = S \cup T$. **Is $\{S, T\}$ a partition of R?**

No. The covering condition holds by construction — $R = S \cup T$ is how R was defined. But disjointness fails:

$$10 = 3(3) + 1 \;\Rightarrow\; 10 \equiv 1 \pmod 3 \;\Rightarrow\; 10 \in S$$
$$10 = 4(2) + 2 \;\Rightarrow\; 10 \equiv 2 \pmod 4 \;\Rightarrow\; 10 \in T$$

so $10 \in S \cap T$ and $S \cap T \neq \emptyset$. Therefore $\{S, T\}$ is **not** a partition of R.

A single witness settles it — disjointness is a universal claim, so one counterexample is a complete disproof.

Worked: two partitions of $\mathbb{Z} \times \mathbb{Z}$

Any rule that sorts every pair into exactly one bucket works. Two independent ways:

By the sign of the first coordinate.

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

$\{N, P\}$ is a partition of $\mathbb{Z} \times \mathbb{Z}$ — every integer a is either ≥ 0 or < 0, never both.

By the parity of the second coordinate.

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

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

The recipe generalises: **take any property that every element either has or lacks, and the two resulting sets partition the whole** — provided neither comes out empty. That connection is made exact by equivalence relations: every partition is the set of classes of one, and the other way round (equivalence-classes-and-partitions[264]).

See also

- proving-set-properties[265] — the element method, the set identities, and proofs about these operations
- functions-on-general-sets[266] — functions defined as subsets of a Cartesian product
- equivalence-classes-and-partitions[267] — partitions as the classes of an equivalence relation
- modular-arithmetic[268] — the congruence sets used throughout the worked examples
- counting-principles[269] · counting-selections[270] — $|A \times B| = |A| \times |B|$ as the multiplication rule, and $\binom{n}{r}$, the number of r-element subsets of an n-element set

[264] courses/math1061/equivalence-classes-and-partitions.pdf
[265] courses/math1061/proving-set-properties.pdf
[266] courses/math1061/functions-on-general-sets.pdf
[267] courses/math1061/equivalence-classes-and-partitions.pdf
[268] courses/math1061/modular-arithmetic.pdf
[269] courses/math1061/counting-principles.pdf
[270] courses/math1061/counting-selections.pdf

- inclusion-exclusion[271] · [probability] — the size of a union of sets that overlap, with De Morgan's law for "neither", and events as subsets of a sample space
- pigeonhole-principle[272] — a partition as the set of pigeonholes
- conditional-statements[273] · logical-equivalence-laws[274] — vacuous truth, and the biconditional behind set equality
- 2026-09-03-set-theory-definitions[275] — Lecture 17
- practice-problems[276] — §21 Set Theory Definitions, with full worked solutions
- practice-problems[277] — §22 More Definitions and Examples of Sets

[271] courses/math1061/inclusion-exclusion.pdf
[272] courses/math1061/pigeonhole-principle.pdf
[273] courses/math1061/conditional-statements.pdf
[274] courses/math1061/logical-equivalence-laws.pdf
[275] courses/math1061/2026-09-03-set-theory-definitions.pdf
[276] courses/math1061/practice-problems.pdf
[277] courses/math1061/practice-problems.pdf