MATH1061 — Week 11 Notes

Table of contents

Lecture 29 — Introduction to Counting **1**

Goals . . . 1
Worked: arranging $1, 2, 3, 4, 5$ . . . 2
Worked: one odd and one even . . . 3
Choosing from $\{1, \ldots, 8\}$: prime, composite or neither . . . 4
Permutations . . . 5
Worked: what comes second . . . 8
Worked: permutations of $\{1, \ldots, 60\}$ . . . 9
Worked: number plates . . . 12
When to add and when to multiply . . . 13
See also . . . 15

Lecture 30 — Counting Selections **16**

Goals . . . 16
Finishing the number plates . . . 16
Four ways to select . . . 17
Which case is which . . . 19
The formulas . . . 19
Ordered and unordered: dividing by $r!$ . . . 21
Worked: 8-letter passwords . . . 22
Worked: passwords with a vowel . . . 23
Worked: integers containing a 5 . . . 23
Worked: 5 immediately followed by 6 . . . 24
Worked: 3-element subsets of a 6-element set . . . 26
Worked: three even and two odd . . . 26
Worked: at least two even numbers . . . 27
Worked: arranging BARBARA . . . 28
Worked: arranging BANANAS . . . 29
See also . . . 29

Reference material **30**
Cardinality 30
Counting Principles 36
Counting Selections 45
Practice Problems — the Semester-wide Set 55
Recursive Definitions 180
Sets and Set Notation 184
The Symmetric Group 196

Lecture 29 — Introduction to Counting

Counting the outcomes of a process without listing them. The multiplication rule handles a choice made in steps, the addition rule handles a count that splits into separate cases, and subtracting from the total handles "at least one". Together they count permutations, first of a whole set and then with conditions on the first few positions. Pre-work: Video 037 (Introduction to Counting). The rules, why they work and where they go wrong are collected in counting-principles[1], and choosing elements without regard to order carries on in 2026-10-13-counting-selections[2].

Goals

1. Learn how to solve simple counting problems.
2. Learn how to count permutations when restrictions are added.
3. Learn some counting techniques and understand why they work.

Two questions to keep in mind:

- **How do you count arrangements of only some of the elements, the r-permutations?** A four-symbol number plate with no repeated symbol is one, in the number plates, part (b). The general count is in counting-principles[3].
- **When do you add and when do you multiply?** Multiply across the steps of one choice, add across cases that cannot both happen. The summary at the end.

Worked: arranging $1, 2, 3, 4, 5$

How many permutations of $\{1, 2, 3, 4, 5\}$ are there? Explain your reasoning.

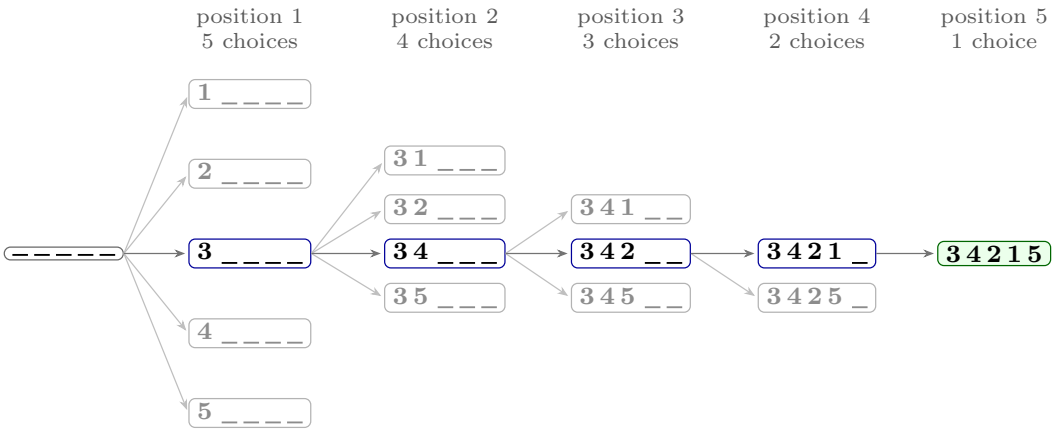
[1] courses/math1061/counting-principles.pdf
[2] courses/math1061/2026-10-13-counting-selections.pdf
[3] courses/math1061/counting-principles.pdf

Build the arrangement one position at a time. Any of the 5 numbers can go first. Whichever it was, 4 numbers are left for the second position, then 3 for the third and 2 for the fourth, and the last position takes the one number remaining. So there are

$$5 \times 4 \times 3 \times 2 \times 1 = 5! = 120$$

permutations.

Following one arrangement through shows what "4 left" means. Put 3 first. The second position can then take 1, 2, 4 or 5, which is 4 options. Put 4 there, and the third can take 1, 2 or 5. Put 2, and the fourth can take 1 or 5. Put 1, and the last must be 5. That builds 3 4 2 1 5. Starting with 1 instead of 3 leaves a different four for the second position, $\{2, 3, 4, 5\}$, but still four of them. **What the multiplication rule needs is that the number of options at each step is the same whatever was chosen before**, even though the options themselves change. As a possibility tree, the start has 5 branches, each of those has 4, each of those 3, and so on, so there are $5 \times 4 \times 3 \times 2 \times 1$ leaves, one per permutation.



$5 \times 4 \times 3 \times 2 \times 1 = 5! = 120$ leaves, one per permutation

Figure 1: Part of the possibility tree for arranging $1, 2, 3, 4, 5$, one position at a time. Only the path that builds $3, 4, 2, 1, 5$ is followed; every grey node branches in the same way. At each level every node has the same number of branches, 5, then 4, 3, 2 and 1, whichever numbers have been used, so the tree has $5 \times 4 \times 3 \times 2 \times 1 = 120$ leaves, one for each permutation.

The complete tree for three elements, small enough to draw in full, is in counting-principles[4].

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

Worked: one odd and one even

> How many ways are there to choose two of the numbers $1, 2, 3, 4, 5, 6, 7, 8, 9$ if one of the chosen numbers is odd and the other is even?

Sort the nine numbers by parity:

$$D = \{1, 3, 5, 7, 9\}, \qquad E = \{2, 4, 6, 8\}.$$

There are five odd numbers to choose from and four even ones. Every odd number goes with every even number, so the valid choices fill a grid with one row per odd number and one column per even number:

	2	4	6	8
1	1 and 2	1 and 4	1 and 6	1 and 8
3	3 and 2	3 and 4	3 and 6	3 and 8
5	5 and 2	5 and 4	5 and 6	5 and 8
7	7 and 2	7 and 4	7 and 6	7 and 8
9	9 and 2	9 and 4	9 and 6	9 and 8

For each of the 5 choices of odd number there are 4 choices of even number, so there are $5 \times 4 = 20$ ways. In set terms the grid is the Cartesian product $D \times E$, the ordered pairs (a, b) with a odd and b even, and

$$|D \times E| = |D| \times |E| = 5 \times 4 = 20$$

(sets-and-set-notation[5]).

The order of choosing does not matter. Choosing 1 and 2 is the same as choosing 2 and 1. Even so, the ordered pairs count the unordered choices exactly: every valid choice has exactly one odd member, so writing the odd one first turns each choice into exactly one pair $(a, b) \in D \times E$, and each pair comes from exactly one choice. That matching is a bijection, and matched finite sets have the same size (cardinality[6]). Each choice appears once in the grid, in the row of its odd number. Counting "first number picked, then second" instead gives $5 \times 4 + 4 \times 5 = 40$, which counts every pair twice.

[5] courses/math1061/sets-and-set-notation.pdf
[6] courses/math1061/cardinality.pdf

Choosing from $\{1, \ldots, 8\}$: prime, composite or neither

Let $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$, so $|X| = 8$. Every element of X is in exactly one of

$$P = \{2, 3, 5, 7\} \text{ (prime)}, \qquad C = \{4, 6, 8\} \text{ (composite)}, \qquad \{1\} \text{ (neither)}.$$

1 is neither prime nor composite, and both questions turn on it.

Worked: one prime and one composite

> How many ways are there to choose two numbers from X such that one is prime and the other is composite?
>
> A. 7 B. 12 C. 15 D. 24

B, 12. As with odd and even, a valid choice has exactly one prime member and one composite member, so it matches exactly one ordered pair in $P \times C$:

$$|P \times C| = |P| \times |C| = 4 \times 3 = 12.$$

The other options each make a recognisable mistake. 24 counts every pair twice, once in each order. 7 is $4 + 3$, adding where both choices are made and so the counts multiply. 15 is 5×3, which treats 1 as a prime.

Worked: prime or composite

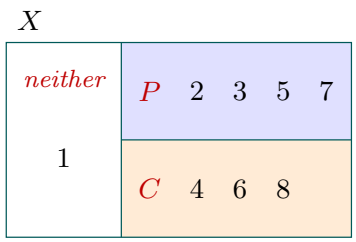
> How many ways are there to choose one number from X such that it is prime or composite?
>
> A. 3 B. 7 C. 8 D. 12

B, 7. Every element of X except 1 is prime or composite, so the count is

$$|X - \{1\}| = 8 - 1 = 7.$$

That counts by the complement: take everything and remove what is excluded. Counting the wanted numbers directly gives the same. No number is both prime and composite, so P and C are disjoint, and by the addition rule $|P \cup C| = |P| + |C| = 4 + 3 = 7$. Only one number is chosen, and it is a prime *or* a composite, so the counts add. 12 multiplies as if two numbers were chosen, 8 forgets to leave out 1, and 3 counts only the composites.

The two counts use the same sets and the same sizes, 4 and 3, and differ only in how many numbers are chosen. One number from either of two disjoint sets adds their sizes. One number from each of them multiplies.



one number, prime *or* composite:
$|P| + |C| = 4 + 3 = 7$

$P \times C$

	4	6	8
2	(2, 4)	(2, 6)	(2, 8)
3	(3, 4)	(3, 6)	(3, 8)
5	(5, 4)	(5, 6)	(5, 8)
7	(7, 4)	(7, 6)	(7, 8)

one prime *and* one composite:
$|P| \times |C| = 4 \times 3 = 12$

Figure 2: $X = 1, \ldots, 8$ split into the primes P, the composites C, and 1, which is neither. Left: one number that is prime or composite is a single choice from the shaded part of X. No number is in both P and C, so the shaded part has $4 + 3 = 7$ elements. Right: one prime and one composite is a choice from each part. Every prime can go with every composite, so the choices fill a grid with a row for each prime and a column for each composite, $4 \times 3 = 12$ cells, the pairs of $P \times C$. A choice from either part adds the sizes; a choice from each part multiplies them. 1 is in neither count.

Permutations

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

How many permutations of $\{1, 2, 3, 4\}$ are there? For each of the four choices for the first number, there are three ways to choose the second. Once the first two are chosen there are two ways to choose the third, and then the fourth is forced. So there are $4 \times 3 \times 2 \times 1 = 24$ permutations. Listed in dictionary order they fall into blocks, and the sizes of the blocks are the factors of the product.

The same reasoning works for any number of objects.

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

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

$n!$ is read "n factorial", or "n bang". As a product, $n! = \prod_{i=1}^{n} i$ for $n \in \mathbb{Z}^+$, and $0! = 1$ by definition (recursive-definitions[7]). The values grow very fast:

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

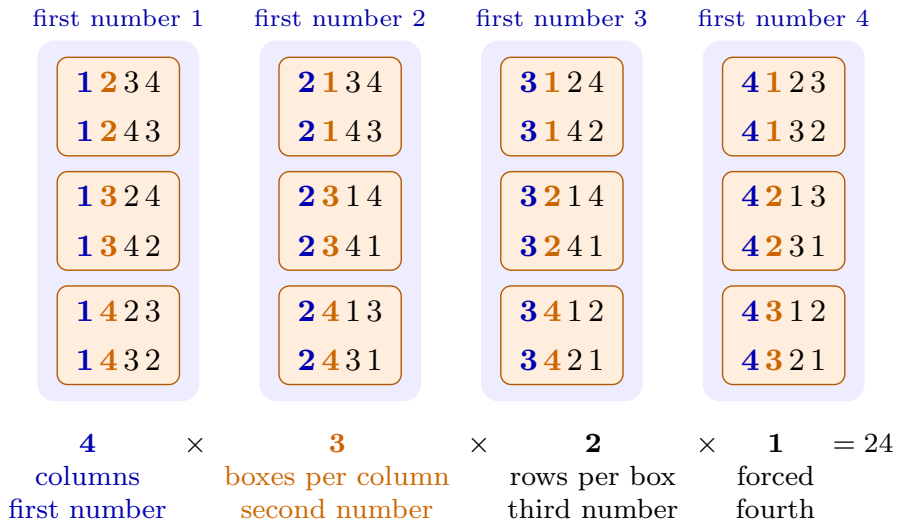


Figure 3: The 24 permutations of $1, 2, 3, 4$ in dictionary order, as nested blocks. The first number picks the column, 4 ways. Inside a column the second number picks one of 3 boxes, since one number is already used. Inside a box the third number picks one of 2 rows, and the fourth number is whatever is left. Each level splits every block into the same number of pieces, so the total is $4 \times 3 \times 2 \times 1 = 4! = 24$.

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

A bijection from $\{1, \dots, n\}$ to itself is fixed by listing $f(1), f(2), \dots, f(n)$, which is a permutation of $\{1, \dots, n\}$. So the symmetric group S_n has $n!$ elements, and S_3 has the six of symmetric-group[8].

Worked: starting with an even number

How many permutations of the numbers 1, 2, 3, 4, 5 start with an even number?

Fill the restricted position first. The first number must be 2 or 4, so there are 2 choices. Whichever it is, the other four numbers fill the remaining four positions in any order, in $4! = 24$ ways. So the answer is

$$2 \times 4! = 2 \times 24 = 48.$$

Position by position that is $2 \times 4 \times 3 \times 2 \times 1$. If 2 goes first, the second position can take any of 1, 3, 4, 5, and 4 is still among them: the even number not chosen is free to go anywhere else.

A check: each of the five numbers starts the same number of permutations, 4! each, and two of the five are even, so the answer is $\frac{2}{5}$ of the $5! = 120$ permutations, which is 48.

Worked: starting with a prime

How many permutations of $\{1, 2, 3, 4, 5, 6, 7\}$ start with a prime number?

A. $4 \times 6 = 24$ B. $4! \times 3! = 144$ C. $4 \times 6! = 2880$ D. $5 \times 6! = 3600$

C, 2880. Let $N = \{1, 2, 3, 4, 5, 6, 7\}$ and $P = \{2, 3, 5, 7\}$. The first position has $|P| = 4$ choices. Once it is filled, any of the $|N| - 1 = 6$ remaining numbers can go second, any of the $|N| - 2 = 5$ still remaining can go third, and so on down to 1 for the last position:

$$|P| \times (|N| - 1)! = 4 \times 6! = 4 \times 720 = 2880.$$

If 5 goes first, for instance, the other six positions are filled from $\{1, 2, 3, 4, 6, 7\}$. That includes the primes 2, 3 and 7. Only the first position is restricted, and the rest is an unrestricted arrangement of what is left.

Each wrong option is a different mistake:

[8] courses/math1061/symmetric-group.pdf

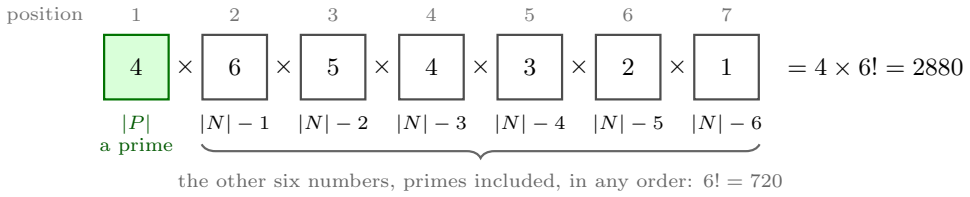


Figure 4: Counting the permutations of $1, \ldots, 7$ that start with a prime, one position at a time. The restricted position is filled first, from the 4 primes. Each later position has one fewer number available than the one before, whatever was placed earlier, so the last six positions are an arrangement of the six numbers left: 6! ways. The multiplication rule gives $4 \times 6! = 2880$.

- **A,** 4×6**,** fills the first two positions and forgets the other five.
- **B,** $4! \times 3!$**,** arranges the four primes among themselves and the three non-primes among themselves. That counts the permutations with *all four* primes at the front, a much stronger condition.
- **D,** $5 \times 6!$**,** counts 1 as a prime.

Worked: what comes second

(a) How many permutations of $\{1, 2, 3, 4, 5, 6, 7\}$ start with a prime number followed by a composite number?

(b) How many permutations of $\{1, 2, 3, 4, 5, 6, 7\}$ start with a prime number followed by an odd number?

The sets involved, inside $N = \{1, 2, 3, 4, 5, 6, 7\}$:

$$P = \{2, 3, 5, 7\}, \qquad C = \{4, 6\}, \qquad D = \{1, 3, 5, 7\} \text{ (odd)}.$$

(a) Position 1 is a prime, 4 choices. Position 2 is a composite, 2 choices, however position 1 was filled: no prime is composite, so the first choice never uses up a composite. Positions 3 to 7 hold the 5 numbers left, in any order. So

$$|P| \times |C| \times (|N| - 2)! = 4 \times 2 \times 5! = 8 \times 120 = 960.$$

(b) The same approach stalls at position 2. How many odd numbers are left depends on which prime went first. If it was 2, all four odd numbers are still available. If it was 3, 5 or 7, an odd number has been used and only three remain. The multiplication rule needs the count at each

step to be the same whatever came before, so **split into cases on the first number**, and within each case it is the same every time.

- **Case 1: the first number is even**, so it is 2. One choice for position 1, then $|D| = 4$ for position 2, then 5! for the rest: $1 \times 4 \times 5!$.
- **Case 2: the first number is odd**, so it is 3, 5 or 7. That is $|P| - 1 = 3$ choices for position 1, then $|D| - 1 = 3$ for position 2, since the first number used up an odd number, then 5! for the rest: $3 \times 3 \times 5!$.

Every qualifying permutation is in exactly one case, because its first number either is 2 or is not. So the addition rule adds them:

$$1 \times 4 \times 5! + 3 \times 3 \times 5! = (4 + 9) \times 5! = 13 \times 120 = 1560.$$

Multiplying straight through, $4 \times 4 \times 5! = 1920$, is wrong: it allows four odd numbers in position 2 after an odd prime, when only three are left.

Worked: permutations of $\{1, \dots, 60\}$

(a) How many permutations of $\{1, 2, \dots, 60\}$ start with an even number followed by a number that is divisible by 3?

(b) How many permutations of $\{1, 2, \dots, 60\}$ have at least one even number in the first two positions?

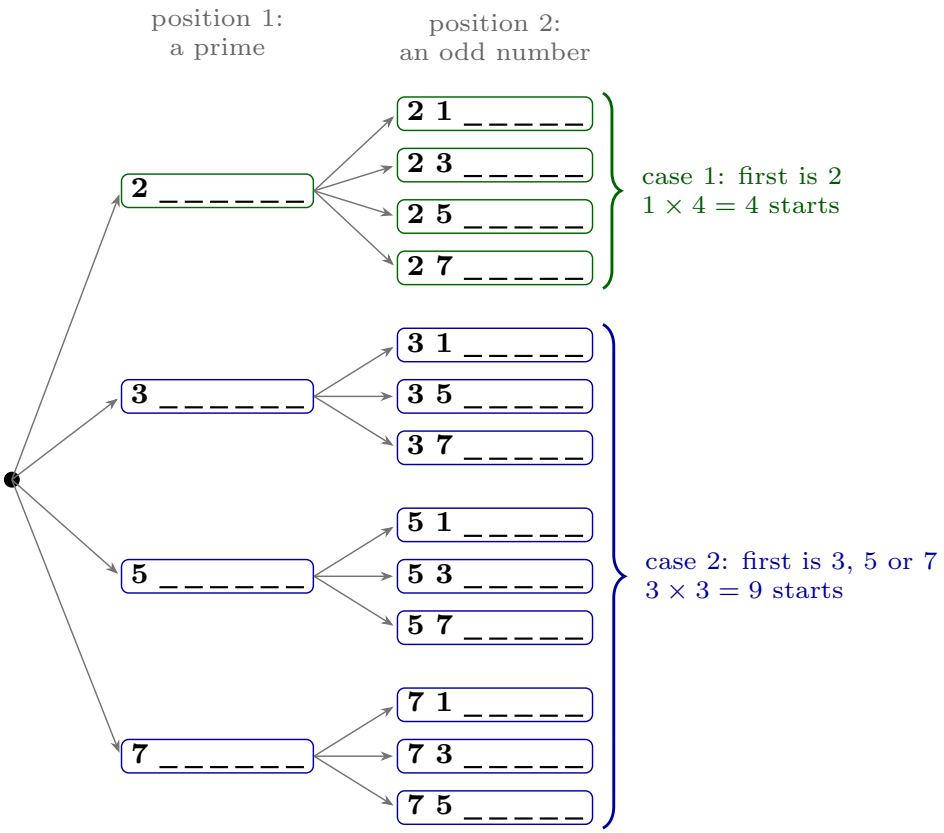
Let $N = \{1, 2, \dots, 60\}$, so $|N| = 60$, and

$$E = \{n \in N : n \text{ is even}\}, \qquad T = \{n \in N : 3 \mid n\}.$$

Then $|E| = 30$ and $|T| = 20$. The numbers in both are the multiples of 6, so $|E \cap T| = 10$, and $|E - T| = 30 - 10 = 20$.

(a) This is the difficulty of prime followed by odd again. An even first number that is also a multiple of 3 uses up one of the multiples of 3, and one that is not leaves all 20 of them. So split on whether the first number is divisible by 3.

- **Case 1: the first number is divisible by 3.** It is in $E \cap T$, 10 choices. Position 2 takes any of the other $|T| - 1 = 19$ multiples of 3. The remaining 58 numbers go in any order: $10 \times 19 \times 58!$.
- **Case 2: the first number is not divisible by 3.** It is in $E - T$, 20 choices. Position 2 takes any of the $|T| = 20$ multiples of 3. Then 58! for the rest: $20 \times 20 \times 58!$.



each start is finished in 5! ways: $(4 + 9) \times 5! = 1560$

Figure 5: The possibility tree for the first two positions of a permutation of $1, \ldots, 7$ that starts with a prime followed by an odd number. The tree is lopsided: after 2 there are four odd numbers to follow, but after 3, 5 or 7 there are only three, because the first number used one of them up. So the multiplication rule cannot be applied in one go. Splitting on the first number gives two cases that are each regular, 1×4 and 3×3 starts. They add to 13, and each start is completed by arranging the other five numbers.

$$\text{total} = 10 \times 19 \times 58! + 20 \times 20 \times 58! = (190 + 400) \times 58! = 590 \times 58!.$$

That is about 1.39×10^{81}, and the factorial form is the sensible way to leave it.

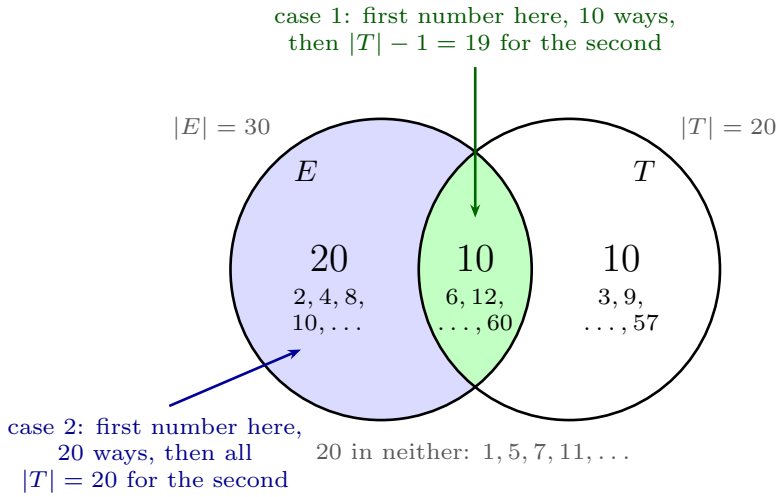


Figure 6: The even numbers E and the multiples of 3, T, in $1, \ldots, 60$, with the size of each region. The two cases of part (a) are the two parts of E. If the first number comes from the overlap, the multiples of 6, it is itself a multiple of 3 and leaves only 19 for the second position. If it comes from the rest of E, all 20 multiples of 3 are still available.

(b) "At least one even number in the first two positions" happens in three ways, writing E for even and O for odd: EE, EO and OE. Each is a regular count.

- **EE:** 30 even numbers for position 1, then 29 for position 2: $30 \times 29 \times 58!$.
- **EO:** 30 even, then 30 odd: $30 \times 30 \times 58!$.
- **OE:** 30 odd, then 30 even: $30 \times 30 \times 58!$.

$$(30 \times 29 + 30 \times 30 + 30 \times 30) \times 58! = (870 + 900 + 900) \times 58! = 2670 \times 58!.$$

Or count the complement. The only way to fail is OO, both odd. So

$$\#\text{permutations} = (\text{all permutations, no restriction}) - (\text{permutations starting odd, odd}) = 60! - 30 \times 29 \times 58!.$$

The two answers agree: $60! = 60 \times 59 \times 58! = 3540 \times 58!$, and $3540 - 870 = 2670$. The complement is one case to count instead of three, which is why it is the natural tool for "at least one".

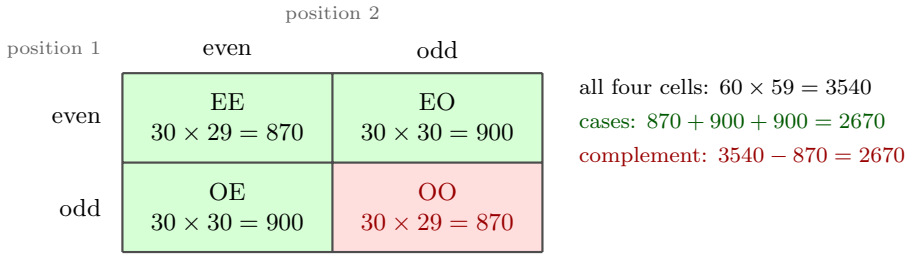


Figure 7: Every permutation of $1, \dots, 60$ falls in exactly one cell, according to the parity of its first two numbers; each count shown is then multiplied by 58! for the other positions. A diagonal cell is 30×29 because the second number has the same parity as the first and one of them is used up. The three shaded green cells are the permutations with at least one even number in the first two positions. They can be added cell by cell, or found as everything, $60 \times 59 = 3540$, minus the one red cell where both are odd. Both give $2670 \times 58!$.

Worked: number plates

In a certain state, number plates consist of four, five or six symbols chosen from the 26 letters of the alphabet together with the ten digits $0, 1, \dots, 9$.
(a) How many distinct number plates are possible if repetition of symbols is allowed?
(b) How many distinct number plates are possible if repetition of symbols is not allowed?
(c) How many distinct number plates contain at least one repeated symbol?
(d) How many distinct number plates contain exactly one digit?

The symbols form a set S of $|S| = 26 + 10 = 36$, adding because no symbol is both a letter and a digit. A plate is **ordered**: `AB12` and `21BA` are different plates. So a plate of length k is a sequence of k symbols. Every plate has exactly one length, so in each part the plates split into three cases, of length 4, 5 and 6, which add.

(a) Repetition allowed. Each position can be any of the 36 symbols, whatever is in the other positions. A four-symbol plate can be made in $36 \times 36 \times 36 \times 36 = 36^4$ ways, and in general a k-symbol plate in 36^k ways.

$$36^4 + 36^5 + 36^6 = 1\,679\,616 + 60\,466\,176 + 2\,176\,782\,336 = 2\,238\,928\,128.$$

(b) Repetition not allowed. Each symbol placed leaves one fewer for the positions after it. A four-symbol plate can be made in

$$36 \times 35 \times 34 \times 33 = \frac{36!}{32!} = \frac{36!}{(36-4)!}$$

ways. It is an ordered selection of 4 of the 36 symbols, a **4-permutation** of S (counting-principles[9]).

$$\begin{aligned} &36 \times 35 \times 34 \times 33 \\ &+ 36 \times 35 \times 34 \times 33 \times 32 \qquad = \; 1\,413\,720 + 45\,239\,040 + 1\,402\,410\,240 \;=\; 1\,449\,063\,000. \\ &+ 36 \times 35 \times 34 \times 33 \times 32 \times 31 \end{aligned}$$

(c) At least one repeated symbol. A plate has at least one repeated symbol exactly when it is not a plate with no repeats. The plates in (b) are among the plates in (a), with the same lengths, so subtract:

$$\text{part (a)} - \text{part (b)} = 2\,238\,928\,128 - 1\,449\,063\,000 = 789\,865\,128.$$

Counted directly, "at least one repeat" would need cases for which symbol repeats, where and how often. The complement avoids all of that.

(d) Exactly one digit. Repetition is allowed here, as in (a): the letters may repeat, and with only one digit the digit cannot. Write $D = \{0, 1, \ldots, 9\}$ and $L = \{\mathtt{A}, \mathtt{B}, \ldots, \mathtt{Z}\}$. For a four-symbol plate with its digit first, the positions hold a digit, a letter, a letter and a letter:

$$|D| \times |L| \times |L| \times |L| = 10 \times 26^3.$$

The digit can be in any of the 4 positions, and those are 4 disjoint cases of the same size, so a four-symbol plate with exactly one digit can be made in $4 \times 10 \times 26^3$ ways. Equivalently, choose the digit's position (4 ways), then the digit (10), then the three letters (26^3). Doing the same for each length and adding,

$$4 \times 10 \times 26^3 + 5 \times 10 \times 26^4 + 6 \times 10 \times 26^5 = 703\,040 + 22\,848\,800 + 712\,882\,560 = 736\,434\,400.$$

If repetition were not allowed, only the letters would change: $26 \times 25 \times 24$ in place of 26^3, and so on.

When to add and when to multiply

Every question above used one or more of three moves.

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

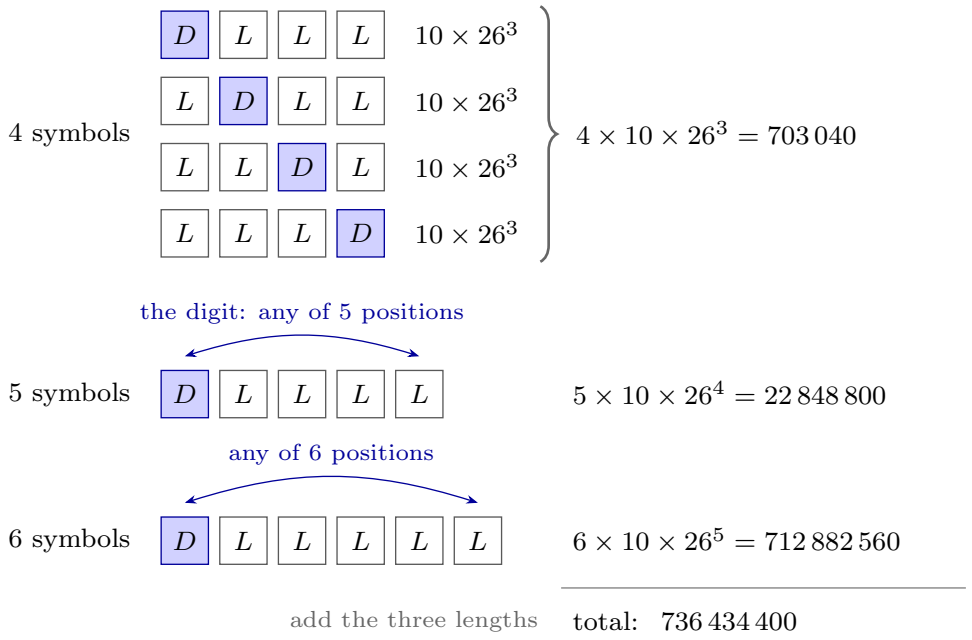


Figure 8: Plates with exactly one digit, D, and letters, L, everywhere else. A four-symbol plate has its digit in one of four positions, and each of those four disjoint cases is filled in 10×26^3 ways, so the four rows together give $4 \times 10 \times 26^3$. Five- and six-symbol plates work the same way, with 5 and 6 positions for the digit. Within a length the rule is multiply; across the three lengths, which no plate can share, it is add.

Move	When	Examples here
Multiply	One outcome is built in steps, and the number of options at each step is the same whatever was chosen before.	5! arrangements; one odd and one even, 5×4; prime then composite, $4 \times 2 \times 5!$
Add	The outcomes split into cases that cannot happen together, and every outcome is in one of them.	prime or composite, $4 + 3$; prime then odd, $(4 + 9) \times 5!$; plates of length 4, 5 or 6
Subtract	What is *not* wanted is easier to count than what is.	$\lvert X - \{1\}\rvert = 8 - 1$; $60! - 30 \times 29 \times 58!$; plates with a repeat, (a) − (b)

"Followed by" and "one from each" are steps, so they multiply. An "or" between alternatives that exclude each other is a case split, so it adds. When a step's count *does* depend on an earlier choice, split on that choice: inside each case the count is fixed, so the cases multiply out separately and then add. The rules, with the reasons and the common traps, are in counting-principles[10].

See also

- counting-principles[11] — the multiplication and addition rules, possibility trees, the complement, permutations and r-permutations
- counting-selections[12] — the four kinds of selection, ordered or not and with or without repeats; a number plate is an ordered one
- sets-and-set-notation[13] — $|A \times B| = |A| \times |B|$, the two-step multiplication rule
- recursive-definitions[14] — $n!$ defined recursively, with $0! = 1$
- symmetric-group[15] — the $n!$ bijections of $\{1, \ldots, n\}$ as a group
- 2026-10-08-definitions-and-examples-of-fields[16] — Lecture 28 · 2026-10-13-counting-selections[17] — Lecture 30
- practice-problems[18] — §37, with full worked solutions

[10] courses/math1061/counting-principles.pdf
[11] courses/math1061/counting-principles.pdf
[12] courses/math1061/counting-selections.pdf
[13] courses/math1061/sets-and-set-notation.pdf
[14] courses/math1061/recursive-definitions.pdf
[15] courses/math1061/symmetric-group.pdf
[16] courses/math1061/2026-10-08-definitions-and-examples-of-fields.pdf
[17] courses/math1061/2026-10-13-counting-selections.pdf
[18] courses/math1061/practice-problems.pdf

Lecture 30 — Counting Selections

Selecting r objects from n: the four cases that come from asking whether order matters and whether repeats are allowed, a formula for each, and counting problems where the selection is restricted. Pre-work: Video 038 (Counting Selections). The four cases and their formulas, the ways of handling restrictions, counting "at least" through the complement, and arrangements of words with repeated letters are all collected in counting-selections[19]. The multiplication, addition and difference rules and the permutations they rest on are in counting-principles[20]. The note starts by finishing the number-plate question from 2026-10-12-introduction-to-counting[21].

Goals

1. Understand the different cases for selections of r objects from n.
2. Learn how to count selections in each case, and when restrictions are added.
3. Gain confidence with solving counting problems.

Three questions to keep in mind:

- **How is n choose r calculated?** The formulas, and why it divides by $r!$.
- **How many distinct arrangements do the letters of BANANAS have?** After BARBARA, which is the same kind of problem.
- **How many ways are there to choose 7 candies from 4 colours?** The fourth case, which counts them as strings of X's and bars.

Finishing the number plates

> In a certain state, number plates consist of four, five or six symbols chosen from the 26 letters of the alphabet together with the ten digits $0, 1, \ldots, 9$.
> (a) How many distinct number plates are possible if repetition of symbols is allowed?
> (b) How many distinct number plates are possible if repetition of symbols is not allowed?
> (c) How many distinct number plates contain at least one repeated symbol?
> (d) How many distinct number plates contain exactly one digit?

The full working is in 2026-10-12-introduction-to-counting[22]. In short: there are $26 + 10 = 36$ symbols, a plate is an ordered selection of them, and each part is counted separately for 4, 5 and 6 symbols and then added.

[19] courses/math1061/counting-selections.pdf
[20] courses/math1061/counting-principles.pdf
[21] courses/math1061/2026-10-12-introduction-to-counting.pdf
[22] courses/math1061/2026-10-12-introduction-to-counting.pdf

	Count	Answer
(a) repeats allowed	$36^4 + 36^5 + 36^6$	2 238 928 128
(b) no repeats	$36 \cdot 35 \cdot 34 \cdot 33 \ + \ 36 \cdot 35 \cdots 32 \ + \ 36 \cdot 35 \cdots 31$	1 449 063 000
(c) at least one repeat	(a) − (b)	789 865 128
(d) exactly one digit	$4 \cdot 10 \cdot 26^3 + 5 \cdot 10 \cdot 26^4 + 6 \cdot 10 \cdot 26^5$	736 434 400

For (d), a k-symbol plate has k places the digit can go, 10 choices of digit, and 26 letters for each of the other $k-1$ places. For four symbols with the digit first that is $10 \cdot 26 \cdot 26 \cdot 26 = 10 \cdot 26^3$, and the digit can be in any of the 4 places, so $4 \cdot 10 \cdot 26^3 = 703\,040$. The five- and six-symbol plates add 22 848 800 and 712 882 560.

Two ideas from this question run through the rest of the note. The four-symbol term of (b) is

$$36 \cdot 35 \cdot 34 \cdot 33 = \frac{36!}{32!} = \frac{36!}{(36-4)!},$$

the first of the four formulas. And (c) counts "at least one" as everything minus "none", which is how the vowel, the digit 5 and two evens questions are done.

Four ways to select

Selecting 2 numbers from $\{1, 2, 3, 4\}$ gives four different answers, depending on two questions. Does the order matter, so that 12 and 21 are different selections? Can a number be chosen twice, as in 11? Write each selection as the two numbers in the order chosen.

	The selections	Count
(1) ordered, without repeats	12, 13, 14, 21, 23, 24, 31, 32, 34, 41, 42, 43	12
(2) ordered, with repeats	the twelve above, and 11, 22, 33, 44	16
(3) unordered, without repeats	12, 13, 14, 23, 24, 34	6
(4) unordered, with repeats	11, 12, 13, 14, 22, 23, 24, 33, 34, 44	10

In the unordered cases each selection is written with its smaller number first, since 21 is the same selection as 12.

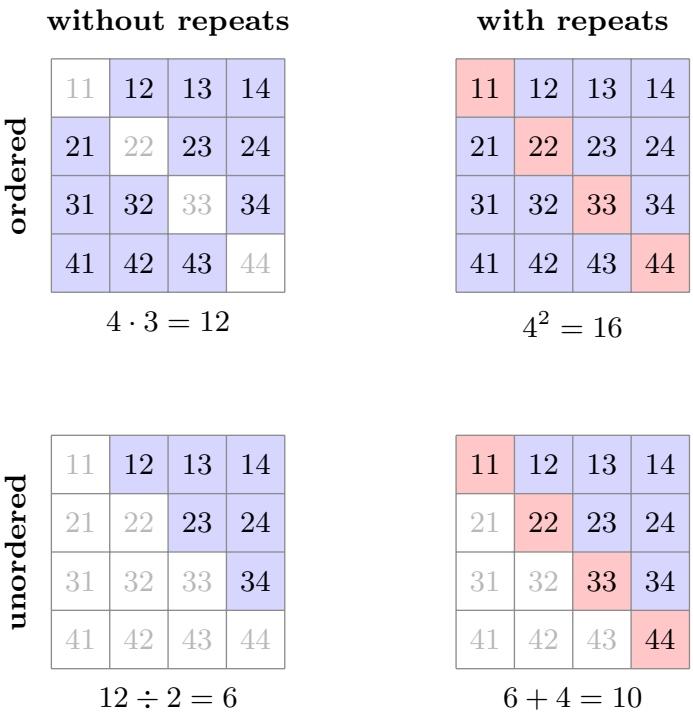


Figure 9: Every way of picking a first and a second number from $1, 2, 3, 4$ is a cell of a 4 by 4 grid, first number down the side and second along the top. Each case of selection keeps a different part of the grid. Ordered with repeats keeps all 16. Ordered without repeats drops the diagonal, the repeats 11, 22, 33, 44, leaving 12. Unordered selections keep one cell of each mirror pair, since 21 is the same selection as 12. Without repeats that is the 6 cells above the diagonal, half of the 12. With repeats the diagonal comes back, and there are $6 + 4 = 10$.

Which case is which

Four questions, one for each case:

- **How many different possibilities are there for first, second and third in a race of 10 people?** Ordered, since first and second are different prizes, and without repeats, since nobody finishes twice. Case (1).
- **How many 3-digit passwords are there?** Ordered, since 123 and 321 are different passwords, and with repeats, since 112 is allowed. Case (2).
- **How many 3-element subsets of $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ are there?** A set has no order and no repeated elements. Case (3).
- **How many ways are there to select 3 chocolate bars when there are 10 different kinds to choose from?** The bars end up in one pile, so there is no order, but two bars of the same kind are allowed. Case (4).

All four select $r = 3$ from $n = 10$. Their answers, 720, 1000, 120 and 220, come from the formulas below.

The formulas

With $n = 10$ and $r = 3$ in the right-hand column:

Case	Formula	Selecting 3 from 10
(1) ordered, without repeats	$\dfrac{n!}{(n-r)!} = \underbrace{n(n-1)\cdots(n-r+1)}_{r \text{ factors}}$	$10 \cdot 9 \cdot 8 = 720$
(2) ordered, with repeats	$n^r = \underbrace{n \cdot n \cdots n}_{r \text{ factors}}$	$10^3 = 10 \cdot 10 \cdot 10 = 1000$
(3) unordered, without repeats	$\dbinom{n}{r} = \dfrac{n!}{r!\,(n-r)!} = \dfrac{n(n-1)\cdots(n-r+1)}{r(r-1)\cdots 1}$	$\dfrac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$
(4) unordered, with repeats	$\dbinom{n+r-1}{r} = \dfrac{n(n+1)\cdots(n+r-1)}{r(r-1)\cdots 1}$	$\dfrac{10 \cdot 11 \cdot 12}{3 \cdot 2 \cdot 1} = 220$

Case (1) is the multiplication rule with one fewer option at each step. Case (2) is the

multiplication rule with all n options every time. Each formula is explained in counting-selections[23].

Case (4) is extension material. It is not assessable in MATH1061. It is Section 9.6 of Epp, and it is covered in MATH2302.

Calculating n choose r. $\binom{n}{r}$ is read "n choose r" and also written $C(n, r)$. It is the number of r-element subsets of an n-element set. To work it out, write r factors counting down from n over r factors counting down from r, and cancel:

$$\binom{10}{3} = \frac{10!}{3!\,7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = \frac{720}{6} = 120.$$

The 7! in 10! cancels against the 7! underneath, which is why only three factors are left on top. Case (4) is the same except that the top counts **up** from n.

Worked: choosing candies

> How many ways are there to choose 7 candies when there are 4 colours, red, blue, yellow and pink, any colour can be taken any number of times, and candies of the same colour are identical?

The candies are not ordered and colours can repeat, so this is case (4), with $n = 4$ colours and $r = 7$ candies.

A selection is settled by how many of each colour are taken. Write an X for each candy, the red ones first, then blue, yellow and pink, and put a bar | between one colour and the next. Two red, one blue, four yellow and no pink is

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

and two red, two blue, one yellow and two pink is

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

Each selection corresponds to an arrangement of 7 X's and 3 bars, and each such arrangement is one selection. An arrangement is fixed by choosing which 3 of the 10 positions hold the bars, so there are

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

$$\binom{10}{3} = \frac{10!}{3!\,7!} = \frac{10 \cdot 9 \cdot 8}{3 \cdot 2 \cdot 1} = 120$$

selections. The formula agrees: $\binom{n+r-1}{r} = \binom{4+7-1}{7} = \binom{10}{7} = \binom{10}{3} = 120$. The two selections are drawn in counting-selections[24].

Ordered and unordered: dividing by $r!$

Cases (1) and (3) are linked. Take the selections of 3 objects from $\{1, 2, 3, 4\}$ without repeats.

Ordered, there are $4 \cdot 3 \cdot 2 = 24$:

123	124	134	234
132	142	143	243
213	214	314	324
231	241	341	342
312	412	413	423
321	421	431	432

Unordered, there are 4: 123, 124, 134, 234.

Each column of the table holds the same three numbers in all $3 \cdot 2 \cdot 1 = 3! = 6$ possible orders, and forgetting the order collapses the whole column to one subset. So

$$\binom{4}{3} = \frac{24}{3!} = \frac{4 \cdot 3 \cdot 2}{3 \cdot 2 \cdot 1} = 4.$$

The same thing happens for any n and r. Every r-element subset turns up $r!$ times among the ordered selections, once in each order, so

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

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

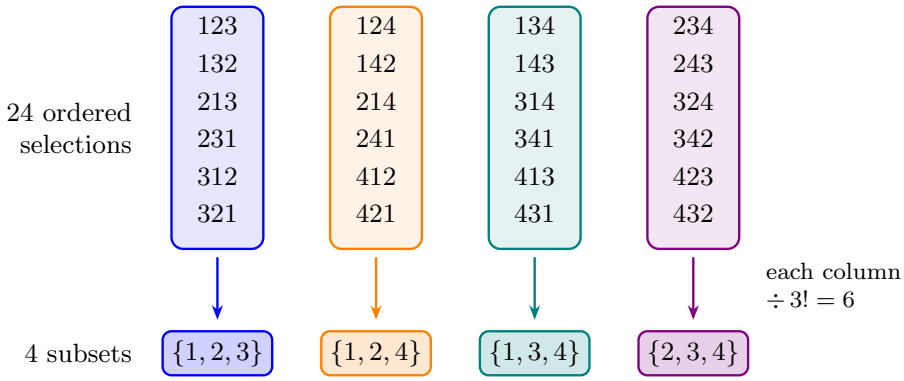


Figure 10: The 24 ordered selections of 3 objects from $1, 2, 3, 4$, sorted by which three numbers they use. Each column holds one set of three numbers in all $3! = 6$ of its orders. Ignoring order merges each column into a single subset, so there are $24 \div 3! = 4$ subsets. In general each r-element subset accounts for $r!$ of the ordered selections, which is why $\binom{n}{r}$ is the ordered count divided by $r!$.

Worked: 8-letter passwords

A certain website requires users to choose a password consisting of 8 lower-case letters of the 26-letter alphabet $a, b, c, d, \ldots, x, y, z$. How many different passwords are there?
A. $26!$
B. $8!$
C. $26 \times 25 \times 24 \times 23 \times 22 \times 21 \times 20 \times 19$
D. 8^{26}
E. 26^8

Answer: E, $26^8 = 208\,827\,064\,576$**.**

A password is **ordered**: *cat* and *cta* are different passwords. And it allows **repeats**: nothing stops a letter being used twice. So it is case (2) with $n = 26$ letters and $r = 8$ positions, and each of the 8 positions has 26 choices.

The other options:

- **A,** $26!$, counts the ways to put all 26 letters in a row, each used once.
- **B,** $8!$, counts the orders of 8 letters already chosen.
- **C,** $26 \cdot 25 \cdots 19$, counts 8-letter passwords with no letter repeated, which is case (1).
- **D,** 8^{26}, has n and r the wrong way round. It would count 26 positions with 8 choices each.

Worked: passwords with a vowel

> How many of the passwords from the question above contain a vowel? (There are 5 vowels: a, e, i, o, u.)

"Contain a vowel" means at least one vowel. It could be 1, 2, 3, up to 8 vowels. Counting those cases one by one is long. Their opposite, no vowel at all, is one product: each of the 8 positions is one of the $26 - 5 = 21$ consonants.

$$\#(\text{passwords with no vowel}) = 21^8.$$

Every password either contains a vowel or does not, so

$$\begin{aligned}\#(\text{passwords with at least one vowel}) &= \#(\text{all passwords}) - \#(\text{passwords with no vowel}) \\ &= 26^8 - 21^8 \\ &= 208\,827\,064\,576 - 37\,822\,859\,361 \\ &= 171\,004\,205\,215.\end{aligned}$$

Worked: integers containing a 5

> How many of the integers from 0 to 9999 contain the digit 5?

Make every number four digits long by writing leading zeros: 0 is 0000, 1 is 0001, 42 is 0042. The added zeros never contain a 5, so this does not change which numbers contain a 5. Now the integers from 0 to 9999 are exactly the strings of 4 digits, and each of the 4 positions has 10 choices:

$$\#(\text{integers from 0 to 9999}) = 10 \cdot 10 \cdot 10 \cdot 10 = 10^4.$$

A number with no 5 has 9 choices in each position, $\{0, 1, 2, 3, 4, 6, 7, 8, 9\}$:

$$\#(\text{those with no 5}) = 9^4 = 6561.$$

So

$$\#(\text{those containing at least one 5}) = 10^4 - 9^4 = 10\,000 - 6561 = 3439.$$

The long way, as a check. Count by the exact number of 5s and add. For exactly k fives, choose which k of the 4 positions hold them, $\binom{4}{k}$ ways, and fill each of the others with one of the 9 other digits:

$$\begin{aligned}&\#(\text{one 5}) + \#(\text{two 5s}) + \#(\text{three 5s}) + \#(\text{four 5s})\\ &= \binom{4}{1}9^3 + \binom{4}{2}9^2 + \binom{4}{3}9 + \binom{4}{4}\\ &= 2916 + 486 + 36 + 1 = 3439.\end{aligned}$$

Same answer, four terms instead of two.

Worked: 5 immediately followed by 6

(a) How many ordered selections without repetition of 4 elements are there from the set $\{1, 2, \ldots, 10\}$?

(b) How many ordered selections without repetition of 4 elements from the set $\{1, 2, \ldots, 10\}$ have 5 immediately followed by 6?

(a) Case (1) with $n = 10$ and $r = 4$:

$$\frac{n!}{(n-r)!} = \frac{10!}{(10-4)!} = 10 \cdot 9 \cdot 8 \cdot 7 = 5040.$$

Four positions, with 10, 9, 8 and 7 numbers left for them in turn.

(b) Place the restricted part first. "5 immediately followed by 6" is a block of two neighbouring positions, 5 then 6. In 4 positions the block can start at position 1, 2 or 3. It cannot start at position 4, because the 6 would have nowhere to go. Wherever the block is, the two positions it leaves are filled, in order, from the 8 numbers other than 5 and 6: 8 choices for the first and 7 for the second.

$$\#(\text{choices}) = 3\,(1 \cdot 1 \cdot 8 \cdot 7) = 3 \cdot 8 \cdot 7 = 21 \cdot 8 = 168.$$

The 1s are the positions of 5 and 6, which have no choice once the block is placed.

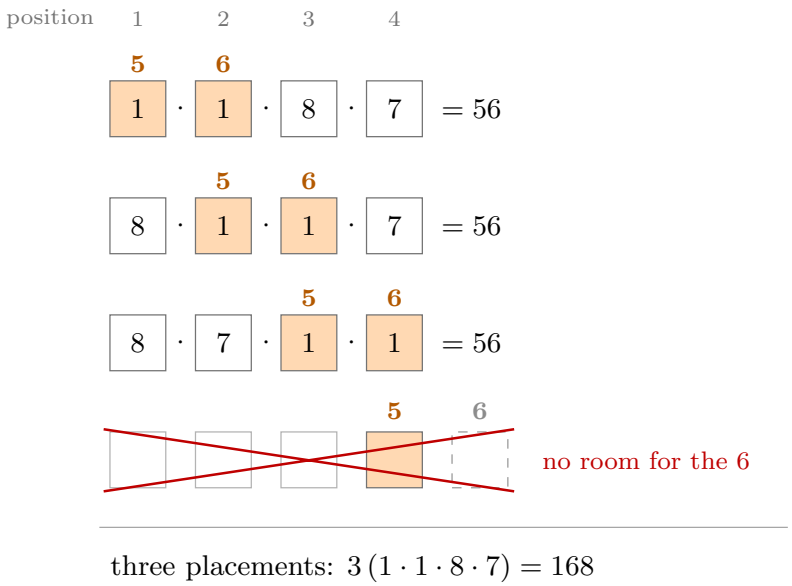


Figure 11: The ordered selections of 4 from $1, \ldots, 10$ with 5 immediately followed by 6, counted one position at a time. Each box holds the number of choices for its position. The block 5 then 6, shaded, takes two neighbouring positions, and once it is placed those positions have 1 choice each; the value forced into each is written above it. The block fits in three places. Wherever it goes, the two positions left over take two of the other 8 numbers in order, 8 choices and then 7. A fourth placement would put the 5 last, leaving no room for the 6. So there are $3, (1 \cdot 1 \cdot 8 \cdot 7) = 168$ selections.

Worked: 3-element subsets of a 6-element set

How many 3-element subsets of $\{1, 2, 3, 4, 5, 6\}$ are there?
A. 18
B. 20
C. 60
D. 120

Answer: B, 20.

A subset is unordered and has no repeated elements, so this is case (3):

$$\binom{6}{3} = \frac{6!}{3!\,3!} = \frac{6 \cdot 5 \cdot 4}{3 \cdot 2 \cdot 1} = 20.$$

The other options:

- **D, 120**, is $6 \cdot 5 \cdot 4$, the number of *ordered* selections. Each subset is counted $3! = 6$ times in it.
- **C, 60**, is $120 \div 2$. It divides by 2 where it should divide by $3! = 6$.
- **A, 18**, is $6 \cdot 3$, which doesn't count any kind of selection.

Worked: three even and two odd

How many 5-element subsets of $\{1, 2, \ldots, 11\}$ contain 3 even numbers and 2 odd numbers?

Split the set into its evens and its odds:

$$E = \{2, 4, 6, 8, 10\},\ |E| = 5, \qquad O = \{1, 3, 5, 7, 9, 11\},\ |O| = 6.$$

A subset of the required kind is a choice of 3 elements of E together with a choice of 2 elements of O. The two choices are independent, and every pair of them gives a different subset, so by the multiplication rule

$$\begin{aligned} \#(\text{subsets}) &= \#(\text{ways to choose 3 evens}) \cdot \#(\text{ways to choose 2 odds}) \\ &= \binom{5}{3}\binom{6}{2} = \frac{5!}{3!\,2!} \cdot \frac{6!}{2!\,4!} = \frac{5 \cdot 4}{2} \cdot \frac{6 \cdot 5}{2} = 10 \cdot 15 = 150. \end{aligned}$$

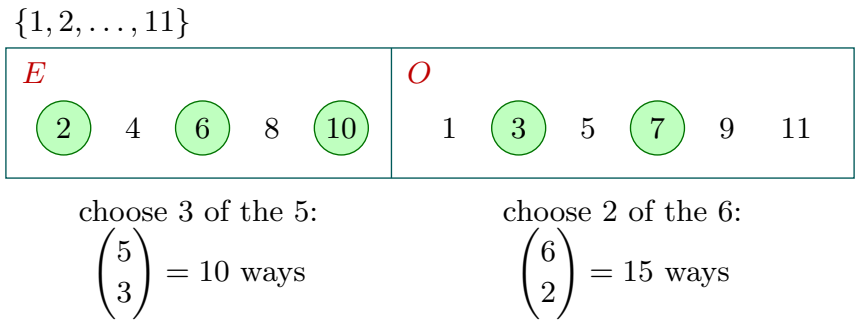


Figure 12: The 5-element subsets of $1, \dots, 11$ with 3 even and 2 odd numbers. The set splits into its evens E and its odds O, and a subset of this kind is 3 elements taken from E together with 2 taken from O. One of them, $2, 3, 6, 7, 10$, is shaded. The two choices are made separately, and whichever 3 evens are taken, any 2 odds can go with them, so the numbers of ways multiply: $\binom{5}{3}\binom{6}{2} = 10 \cdot 15 = 150$.

Worked: at least two even numbers

How many 7-element subsets of $\{1, 2, \dots, 21\}$ contain at least two even numbers?

Let $N = \{1, 2, \dots, 21\}$, so $|N| = 21$. Its evens are $E = \{2, 4, \dots, 20\}$ with $|E| = 10$, and its odds are $O = \{1, 3, \dots, 21\}$ with $|O| = 11$.

"At least two" could be 2, 3, 4, 5, 6 or 7 evens. Its opposite is "no evens" or "exactly one even", two cases instead of six. So

$$\#(\text{at least 2 evens}) = \#(\text{all}) - \#(\text{no evens}) - \#(\text{exactly 1 even}).$$

- **All.** Any 7 of the 21 numbers: $\binom{21}{7} = 116\,280$.
- **No evens.** All 7 come from the 11 odds: $\binom{11}{7} = \binom{11}{4} = 330$.
- **Exactly one even.** Choose the one even from 10 and the other six numbers from the 11 odds: $\binom{10}{1}\binom{11}{6} = 10 \cdot 462 = 4620$.

Therefore

$$\begin{aligned}\#(\text{subsets with at least 2 evens}) &= \binom{21}{7} - \binom{11}{7} - \binom{11}{6}\binom{10}{1} \\ &= \frac{21!}{14!\,7!} - \frac{11!}{7!\,4!} - \frac{11!}{6!\,5!} \cdot 10 \\ &= 116\,280 - 330 - 4620 \\ &= 111\,330.\end{aligned}$$

The factor of 10 is easy to drop. Without it the answer comes out at 115 488, which is wrong: there are 10 different evens that could be the one even. A direct count over 2 to 7 evens, $\sum_{k=2}^{7} \binom{10}{k}\binom{11}{7-k}$, gives $20\,790 + 39\,600 + 34\,650 + 13\,860 + 2310 + 120 = 111\,330$, the same answer.

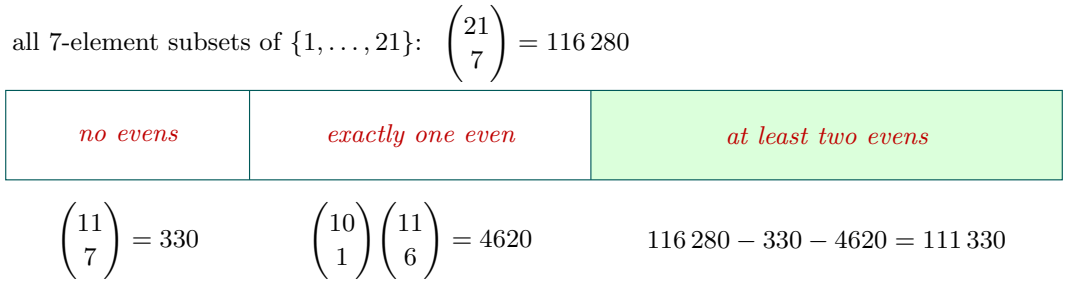


Figure 13: The 7-element subsets of $1, \ldots, 21$, split by how many even numbers they contain. Every subset has none, exactly one, or at least two, and no subset is in two of these parts. So the count wanted, shaded, is the total minus the other two parts. Exactly one even is a choice of the even, 10 ways, times a choice of six odds. The widths are not to scale.

Worked: arranging BARBARA

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

The letters are B, A and R: two B's, three A's and two R's, 7 letters in all. An arrangement puts one letter in each of 7 positions. It is ordered, since ARBAABR and BARBARA are different words, and it has no repeats, since each position gets exactly one letter. If the 7 letters were all different that would make 7! arrangements. They are not, so count it instead by **choosing positions** for one kind of letter at a time.

- **Place the two B's:** choose 2 of the 7 positions, $\binom{7}{2}$ ways. It is a choice, not an ordered selection: once the positions are chosen, the two B's look identical, so it doesn't matter which B goes in which of the chosen positions.

- **Place the three A's:** choose 3 of the 5 positions left, $\binom{5}{3}$ ways.
- **Place the two R's:** they go in the 2 positions left, $\binom{2}{2} = \frac{2!}{2!} = 1$ way.

For example, B's in positions 3 and 6, A's in 1, 4 and 5, and R's in 2 and 7 give ARBAABR. By the multiplication rule,

$$\begin{aligned}\#(\text{arrangements}) &= \binom{7}{2}\binom{5}{3}\binom{2}{2} = \frac{7!}{2!\,5!}\cdot\frac{5!}{3!\,2!}\cdot\frac{2!}{2!} \\ &= \frac{7\cdot 6}{2}\cdot\frac{5\cdot 4}{2}\cdot 1 = 7\cdot 6\cdot 5 = 210.\end{aligned}$$

The 5!s cancel, leaving $\frac{7!}{2!\,3!\,2!}$: the factorial of the length over the factorial of the number of copies of each letter. The stages are drawn, and the general formula derived, in counting-selections[25]. The same formula comes out a second way, by tagging the copies so that all seven letters differ and dividing out the orders of the copies, in 2026-10-19-probability-binomial-coefficients[26].

Worked: arranging BANANAS

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

BANANAS has 7 letters: one B, three A's, two N's and one S. Choosing positions as for BARBARA:

$$\binom{7}{1}\binom{6}{3}\binom{3}{2}\binom{1}{1} = 7\cdot 20\cdot 3\cdot 1 = 420,$$

placing the B, then the A's, then the N's, then the S. The factorial form gives the same:

$$\frac{7!}{1!\,3!\,2!\,1!} = \frac{5040}{6\cdot 2} = 420.$$

See also

- counting-selections[27] — the four cases and their formulas, restrictions, the complement, and words with repeated letters
- counting-principles[28] — the multiplication, addition and difference rules, and permutations

[25] courses/math1061/counting-selections.pdf
[26] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf
[27] courses/math1061/counting-selections.pdf
[28] courses/math1061/counting-principles.pdf

- 2026-10-12-introduction-to-counting[29] — Lecture 29 · 2026-10-19-probability-binomial-coefficients[30] — Lecture 31
- practice-problems[31] — §38, with full worked solutions

Reference material

Cardinality

What it means for two sets to be the same size, and how to compare the sizes of sets that are infinite. It all comes down to functions: **same size means there is a bijection**, and **no bigger means there is an injection**. The one-to-one, onto and bijection machinery is in one-to-one-and-onto-functions[32]. Which infinite sets can be listed, and which cannot, is in countable-and-uncountable-sets[33]. The lectures are 2026-09-14-cardinalities[34] and 2026-09-15-countable-and-uncountable-sets[35].

Same size means a bijection

> Any two sets have the same **cardinality** if and only if there is a bijection between them. If the sets A and B have the same cardinality, then we write $|A| = |B|$.

This is a **definition**, and it is the same idea as counting. Counting a finite set means pairing its elements off with $1, 2, \ldots, n$, so "A has n elements" says $|A| = |\{1, 2, \ldots, n\}|$. For finite sets the definition therefore agrees with counting:

> Any two **finite** sets have the same number of elements if and only if there is a bijection between them.

The definition drops only the requirement that the pairing stop. That is what makes it work for infinite sets, and also what makes it surprising there.

Because bijections can be inverted and composed (inverse-functions[36], composition-of-functions[37]), "same cardinality" behaves like equality. Every set has the same cardinality as itself (the identity). If $|A| = |B|$ then $|B| = |A|$ (the inverse). If $|A| = |B|$ and $|B| = |C|$ then $|A| = |C|$ (the composite). That is what lets results be chained, as in $|\mathbb{Z}^+| = |\mathbb{Z}| = |\mathbb{Q}|$.

[29] courses/math1061/2026-10-12-introduction-to-counting.pdf
[30] courses/math1061/2026-10-19-probability-binomial-coefficients.pdf
[31] courses/math1061/practice-problems.pdf
[32] courses/math1061/one-to-one-and-onto-functions.pdf
[33] courses/math1061/countable-and-uncountable-sets.pdf
[34] courses/math1061/2026-09-14-cardinalities.pdf
[35] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[36] courses/math1061/inverse-functions.pdf
[37] courses/math1061/composition-of-functions.pdf

Finite sets

For **finite** sets A and B:

1. If A has more elements than B, there is no one-to-one function $f : A \to B$.
2. If A has fewer elements than B, there is no onto function $f : A \to B$.
3. If A and B have the same number of elements, then any function $f : A \to B$ is one-to-one **if and only if** it is onto.
4. When A and B have the same number of elements there can still be functions from A to B that are neither.

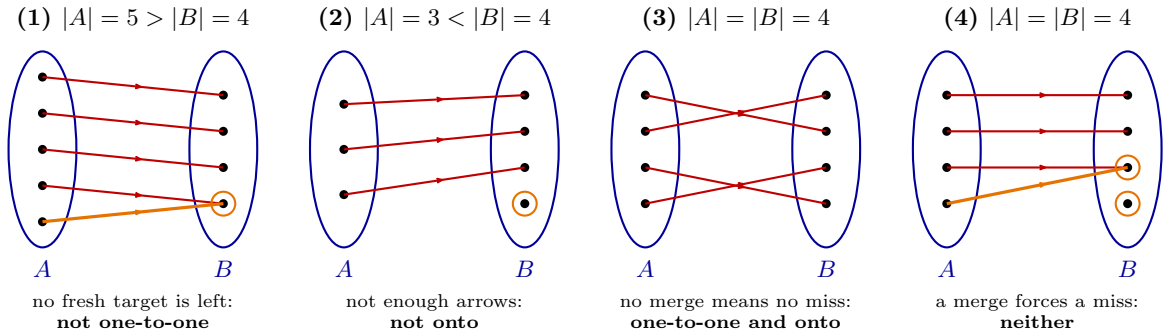


Figure 14: The four facts about finite sets, each with the counting reason. (1) With more elements in A than in B, the arrows run out of fresh targets: once every dot of B is used, the next arrow must share one. (2) With fewer elements in A, there are not enough arrows to reach every dot of B. (3) With equal numbers, merging two arrows is the same thing as missing a target, so one-to-one and onto stand or fall together. (4) Equal numbers do not force either property, only their agreement: this function merges two arrows and so misses one dot.

Fact 1 is the **pigeonhole principle** in function form, a name the course reaches later in the semester (pigeonhole-principle[38]). Fact 3 is the useful one in practice. Between two finite sets of the same size, checking **one** of one-to-one and onto is enough.

Fact 3 is false for infinite sets. On $\mathbb{Z}^+$:

- $f(n) = 2n$ is one-to-one but not onto (nothing maps to 1);
- $g(n) = \lceil n/2 \rceil$ is onto but not one-to-one ($g(1) = g(2) = 1$).

Both go from a set to itself, so the two sides certainly have the same cardinality. For infinite sets one-to-one and onto have to be checked separately, every time.

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

Infinite sets break the finite intuition

For finite sets a proper subset is always strictly smaller. For infinite sets it need not be:

Set	Proper subset	Bijection
$\mathbb{Z}^+$	$2\mathbb{Z}^+$ (even positive integers)	$n \mapsto 2n$
$\mathbb{Z}^+$	$\mathbb{Z}^+ - \{1\}$	$n \mapsto n+1$
$\mathbb{Z}$	$\{n \in \mathbb{Z} : n \bmod 3 = 1\}$	$n \mapsto 3n+1$

Sets that look very different in size can match up too. $\mathbb{Z}^+$ pairs off with all of $\mathbb{Z} \times \mathbb{Z}$ along a spiral (2026-09-14-cardinalities[39]), and the short interval $[0, 1]$ with the long interval $[6, 9]$ by projection (2026-09-15-countable-and-uncountable-sets[40]).

This is the point of **Hilbert's Hotel** (2026-09-14-cardinalities[41]). A full hotel with infinitely many rooms can take one more guest, or a busload, or infinitely many busloads, by moving everyone, because $\mathbb{Z}^+$ can be put in one-to-one correspondence with a proper part of itself.

"Clearly $|\mathbb{Q}| > |\mathbb{Z}| > |\mathbb{Z}^+|$" is the containment intuition applied where it no longer holds. Containment gives $\leq$ (the inclusion map is an injection, see below), never automatically $<$.

Beyond the course: this property characterises infinite sets. A set is infinite exactly when it has the same cardinality as some proper subset of itself.

Proving $|X| = |Y|$

The template, used in 2026-09-14-cardinalities[42]:

> **One way to show $|X| = |Y|$ for sets X and Y:**
>
> 1. Define a function $f : X \to Y$ and explain why it is a function (each element of X has a unique image in Y).
> 2. Show f is one-to-one (injective).
> 3. Show f is onto (surjective).

Step 1 is where most of the real checking happens. $f(x)$ has to land **in** Y, not merely somewhere. In step 3 the preimage you construct has to be **in** X. Both are range checks, and both use the definitions of X and Y.

[39] courses/math1061/2026-09-14-cardinalities.pdf
[40] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[41] courses/math1061/2026-09-14-cardinalities.pdf
[42] courses/math1061/2026-09-14-cardinalities.pdf

Worked: $|\mathbb{Z}^+| = |\mathbb{Z}|$

The listing $0, 1, -1, 2, -2, 3, -3, \ldots$ (drawn in countable-and-uncountable-sets[43]) as a formula:

$$f : \mathbb{Z}^+ \to \mathbb{Z}, \qquad f(n) = \begin{cases} \dfrac{n}{2} & n \text{ even}, \\ -\dfrac{n-1}{2} & n \text{ odd}. \end{cases}$$

It is a function into $\mathbb{Z}$. Every $n \in \mathbb{Z}^+$ is even or odd, not both, so exactly one case applies. If n is even, $\frac{n}{2} \in \mathbb{Z}$. If n is odd, $n-1$ is even and $-\frac{n-1}{2} \in \mathbb{Z}$.

One-to-one. Suppose $f(n_1) = f(n_2)$. The even case gives values ≥ 1, and the odd case gives values ≤ 0, so n_1 and n_2 fall in the same case. If both are even, $\frac{n_1}{2} = \frac{n_2}{2}$ gives $n_1 = n_2$. If both are odd, $-\frac{n_1-1}{2} = -\frac{n_2-1}{2}$ gives $n_1 = n_2$.

Onto. Let $m \in \mathbb{Z}$. If $m \geq 1$, take $n = 2m$, a positive even integer, and $f(2m) = m$. If $m \leq 0$, take $n = 1 - 2m$, a positive odd integer, and $f(1-2m) = -\frac{(1-2m)-1}{2} = m$.

So f is a bijection and $|\mathbb{Z}^+| = |\mathbb{Z}|$. $\square$

The case split in the one-to-one step is the part to notice. With a function defined by cases, first show the two inputs must be in the same case, here by comparing the *values* each case can produce. Then argue within the case.

Comparing sizes: injections and surjections

For any sets A and B:

$|A| \leq |B| \leftrightarrow \exists$ **injective** $f : A \to B$.

$|A| \geq |B| \leftrightarrow \exists$ **surjective** $f : A \to B$.

$|A| < |B| \leftrightarrow \exists$ injective $f : A \to B$ but $\nexists$ bijective $f : A \to B$.

$|A| > |B| \leftrightarrow \exists$ surjective $f : A \to B$ but $\nexists$ bijective $f : A \to B$.

Both definitions are the finite facts turned round. An injection **fits** A **inside** B without collisions, so B has at least as much room. A surjection **covers** B **using** A, so A has at least as much to spend. The functions witnessing $\leq$ and $\geq$ need not be the same function, and usually are not.

(The rightmost panel is drawn with finite sets only to show the shape of the argument. For finite sets an injection each way already forces equal sizes by counting. The theorem is needed, and is surprising, only for infinite sets.)

Two consequences used all the time:

[43] courses/math1061/countable-and-uncountable-sets.pdf

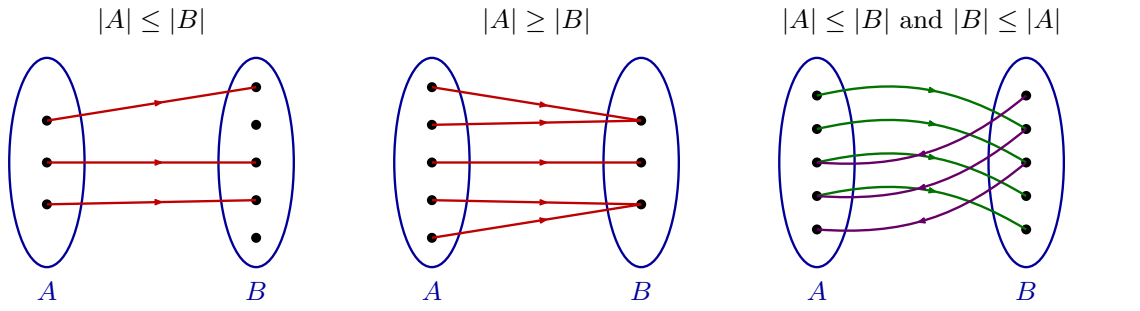


Figure 15: The three comparisons as functions. Left: an injection fits A inside B with no collisions, so $|A| \le |B|$; some of B may be left over. Middle: a surjection covers all of B using A, so $|A| \ge |B|$; arrows may double up. Right: an injection each way, $f : A \to B$ and a different $g : B \to A$. Neither need be onto, but by the Schröder–Bernstein Theorem together they guarantee that some bijection exists, so $|A| = |B|$.

- **A subset is never bigger.** If $A \subseteq B$ then $|A| \le |B|$, by the inclusion map $a \mapsto a$, which is injective. This is all that "$\mathbb{Z}^+ \subset \mathbb{Q}$" proves about sizes.
- **A list of things is never bigger than $\mathbb{Z}^+$.** If $x_1, x_2, x_3, \ldots$ is any sequence, then $i \mapsto x_i$ is onto the set $\{x_1, x_2, x_3, \ldots\}$, so that set has cardinality $\le |\mathbb{Z}^+|$. The set is countable, whether or not the sequence repeats (2026-09-15-countable-and-uncountable-sets[44]).

Beyond the course: the surjection definition of $\ge$ needs one exception. There is no function at all from a non-empty set to $\emptyset$, so $|A| \ge |\emptyset|$ has no surjection behind it, yet it is plainly true. Read the surjection definition as being about non-empty B.

The Schröder–Bernstein Theorem

> **The Schröder–Bernstein Theorem.** For all sets A and B, if $|A| \le |B|$ and $|A| \ge |B|$, then $|A| = |B|$.

It is on the formula sheet (formula-sheet[45]). In practice it is used in this form:

> To show $|A| = |B|$, instead of finding a bijection from A to B, you can find a function that shows $|A| \le |B|$ and a **different** function that shows $|B| \le |A|$.

[44] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[45] courses/math1061/formula-sheet.pdf

That is, **one injection each way**. The two injections do not have to fit together, and neither has to be onto. It is the right tool when a bijection would be fiddly, typically because of endpoints or because the sets are built differently.

Worked: $|[0,1)| = |[0,1]|$

A bijection between these two exists but has to do something awkward to make room for the extra endpoint. Two injections are easy:

- $f : [0,1) \to [0,1]$, $f(x) = x$. It lands in $[0,1]$ because $[0,1) \subseteq [0,1]$, and it is one-to-one because $f(x_1) = f(x_2)$ says $x_1 = x_2$. So $|[0,1)| \leq |[0,1]|$.
- $g : [0,1] \to [0,1)$, $g(x) = \frac{x}{2}$. If $0 \leq x \leq 1$ then $0 \leq \frac{x}{2} \leq \frac{1}{2} < 1$, so it lands in $[0,1)$. $\frac{x_1}{2} = \frac{x_2}{2}$ gives $x_1 = x_2$. So $|[0,1]| \leq |[0,1)|$.

By the Schröder–Bernstein Theorem, $|[0,1)| = |[0,1]|$. $\square$

Same shape as the proof that $|[0,1]| = |(6,9)|$ (2026-09-15-countable-and-uncountable-sets[46]), and as the proof that $\mathbb{Z}^+ \times \mathbb{Z}^+$ is countable, which uses the injections $(a,b) \mapsto 3^a 5^b$ and $n \mapsto (n,1)$.

The direction trap

Both inequalities must be **about the same pair in opposite directions**. The trap is in the directions:

- an injection $X \to Y$ **and** a surjection $X \to Y$ — gives $|X| \leq |Y|$ and $|X| \geq |Y|$, **sufficient**;
- an injection $X \to Y$ **and** a surjection $Y \to X$ — gives $|X| \leq |Y|$ and $|Y| \geq |X|$, the **same** fact twice, **not sufficient**.

Before invoking the theorem, write out the two inequalities the functions give and check that one is $\leq$ and the other is $\geq$ between the same two sets in the same order.

Common mistakes

- **Reading size off containment.** $A \subsetneq B$ proves $|A| \leq |B|$, never $|A| < |B|$, when the sets are infinite.
- **Skipping the range check.** A formula is not a function *into* Y until you have shown every value lies in Y — $3n + 1 \in S$, $6 \leq 3x + 6 \leq 9$.
- **Proving only one of one-to-one and onto.** Enough for finite sets of equal size (fact 3), never enough for infinite ones.

[46] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf

- **Using Schröder–Bernstein with the arrows the wrong way round.** See the direction trap above.
- **Proving a set is *not* the same size by failing to find a bijection.** Not finding one proves nothing. That $\mathbb{R}$ is not the size of $\mathbb{Z}^+$ takes an argument that *no* list can work, the diagonal argument in countable-and-uncountable-sets[47].

See also

- countable-and-uncountable-sets[48] — finite, countable and uncountable sets; listing arguments; the diagonal argument
- one-to-one-and-onto-functions[49] — the definitions and proof templates every argument here uses
- inverse-functions[50] · composition-of-functions[51] — why "same cardinality" chains like equality
- formula-sheet[52] — the Schröder–Bernstein Theorem as printed on the exam formula page
- counting-principles[53] — counting finite sets without listing them, by the multiplication and addition rules
- pigeonhole-principle[54] — fact 1 put to work: choosing the pigeons and the holes to prove that two chosen things must coincide
- 2026-09-14-cardinalities[55] — Lecture 21 · 2026-09-15-countable-and-uncountable-sets[56] — Lecture 22
- practice-problems[57] — §27, 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

[47] courses/math1061/countable-and-uncountable-sets.pdf
[48] courses/math1061/countable-and-uncountable-sets.pdf
[49] courses/math1061/one-to-one-and-onto-functions.pdf
[50] courses/math1061/inverse-functions.pdf
[51] courses/math1061/composition-of-functions.pdf
[52] courses/math1061/formula-sheet.pdf
[53] courses/math1061/counting-principles.pdf
[54] courses/math1061/pigeonhole-principle.pdf
[55] courses/math1061/2026-09-14-cardinalities.pdf
[56] courses/math1061/2026-09-15-countable-and-uncountable-sets.pdf
[57] courses/math1061/practice-problems.pdf

order does not matter, and the other kinds of selection, are in counting-selections[58]. First met in 2026-10-12-introduction-to-counting[59].

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[60]). 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[61]).

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.

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 doesn't, as for a permutation of $\{1, \ldots, 7\}$ 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[62]).

[58] courses/math1061/counting-selections.pdf
[59] courses/math1061/2026-10-12-introduction-to-counting.pdf
[60] courses/math1061/sets-and-set-notation.pdf
[61] courses/math1061/2026-10-12-introduction-to-counting.pdf
[62] courses/math1061/2026-10-12-introduction-to-counting.pdf

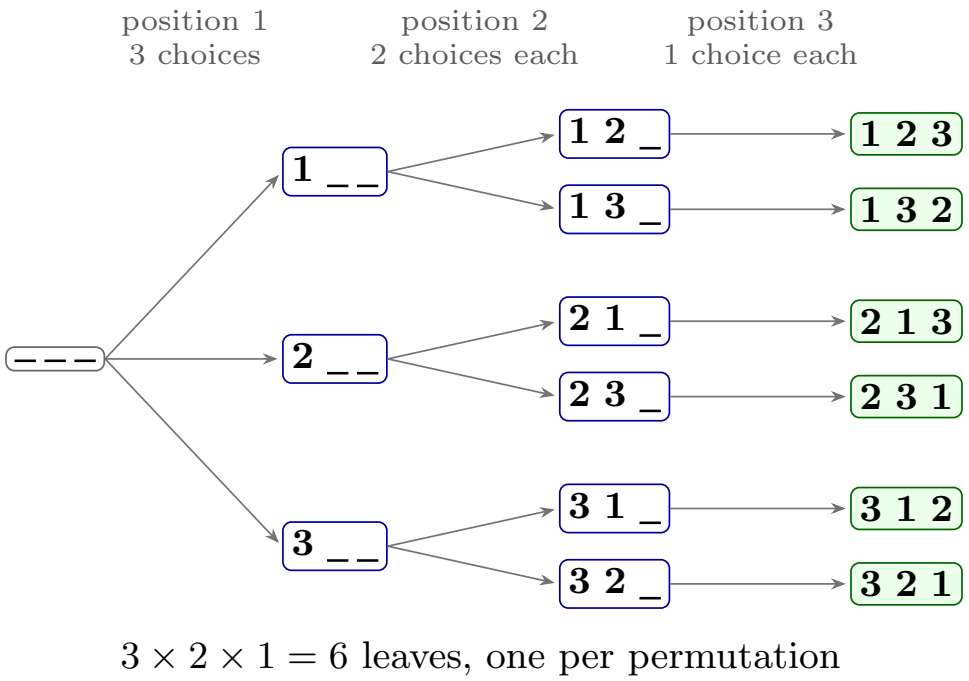


Figure 16: The possibility tree for arranging $1, 2, 3$, built one position at a time. Every node at the first level has 2 branches and every node at the second has 1, whichever numbers were used. Because each level splits evenly, the number of leaves is the product of the branch counts, $3 \times 2 \times 1 = 6$, one for each permutation. If the branch counts at a level differed, the leaves would have to be added up branch by branch.

Worked: casting two roles

From practice-problems[63], 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[64]): 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[65]).
- **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

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

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[66].

[63] courses/math1061/practice-problems.pdf
[64] courses/math1061/equivalence-classes-and-partitions.pdf
[65] courses/math1061/2026-10-12-introduction-to-counting.pdf
[66] courses/math1061/inclusion-exclusion.pdf

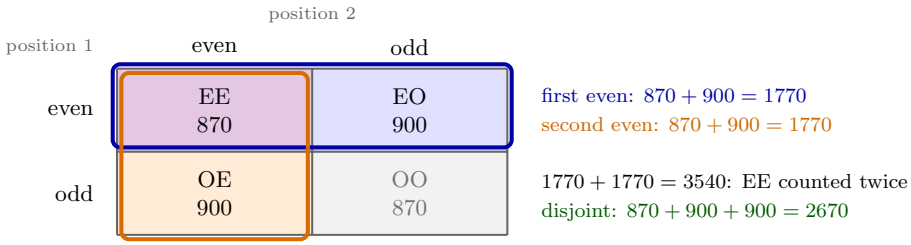


Figure 17: Why the addition rule needs disjoint cases. Each cell counts the permutations of $1, \dots, 60$ whose first two numbers have the given parities, as a multiple of 58!. The blue band, first number even, and the orange band, second number even, overlap in the cell EE. Adding the two bands counts 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 $1, \dots, 9$: $5 \times 4 = 20$	one number from $\{1, \dots, 8\}$ 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.

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[67]).

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.

- **Prime or composite from $\{1, \dots, 8\}$.** Only 1 is neither: $|X - \{1\}| = 8 - 1 = 7$.

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

- **At least one even number in the first two positions** of a permutation of $\{1, \dots, 60\}$. 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[68]). 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 $\{1, \dots, n\}$ to itself is the same thing as the arrangement $f(1), f(2), \dots, f(n)$, so the symmetric group S_n has $n!$ elements (symmetric-group[69]).

[68] courses/math1061/recursive-definitions.pdf
[69] 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[70]: $\{1,\dots,15\}$ 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.

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

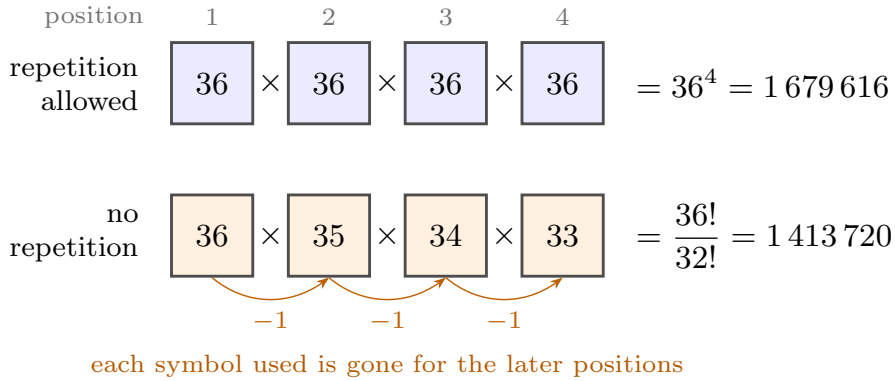


Figure 18: A four-symbol plate filled one position at a time, from 36 symbols. With repetition allowed, every position has all 36 symbols available, giving 36^4. Without repetition, each symbol placed is unavailable afterwards, so each position has one option fewer than the one before. That is a 4-permutation 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[71]). Unordered selections, where only *which* elements are chosen matters, are counted in counting-selections[72].

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.

[71] courses/math1061/2026-10-12-introduction-to-counting.pdf
[72] 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[73] — Lecture 29, with every question worked in full
- counting-selections[74] — ordered and unordered selections, with and without repeats, and more on restrictions
- inclusion-exclusion[75] — counting a union of sets that overlap, where the addition rule does not apply
- probability[76] — the difference rule divided through: $P(E) = 1 - P(E^c)$
- pigeonhole-principle[77] — counting pigeons and holes to prove that two must share a hole
- sets-and-set-notation[78] — $|A \times B| = |A| \times |B|$, the two-step multiplication rule
- equivalence-classes-and-partitions[79] — mutually disjoint sets, the condition in the addition rule
- cardinality[80] — finite sets matched by a bijection have the same size, which is what counting by correspondence relies on
- recursive-definitions[81] — $n!$ defined recursively, with $0! = 1$
- symmetric-group[82] — the $n!$ bijections of $\{1, \dots, n\}$
- practice-problems[83] — §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

[73] courses/math1061/2026-10-12-introduction-to-counting.pdf
[74] courses/math1061/counting-selections.pdf
[75] courses/math1061/inclusion-exclusion.pdf
[76] courses/math1061/probability.pdf
[77] courses/math1061/pigeonhole-principle.pdf
[78] courses/math1061/sets-and-set-notation.pdf
[79] courses/math1061/equivalence-classes-and-partitions.pdf
[80] courses/math1061/cardinality.pdf
[81] courses/math1061/recursive-definitions.pdf
[82] courses/math1061/symmetric-group.pdf
[83] 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[84]. First met in 2026-10-13-counting-selections[85].

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[86]) 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

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

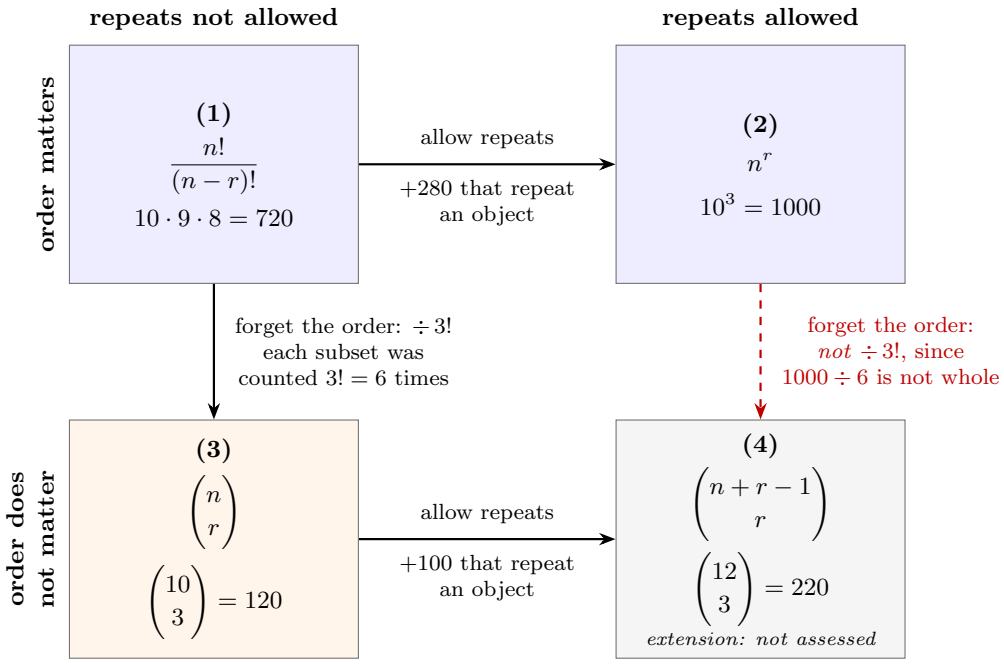


Figure 19: How the four cases are related, with the count for $n = 10$ and $r = 3$ in each. Moving right allows an object to be chosen again, which adds the selections that use some object more than once: $1000 - 720 = 280$ ordered ones and $220 - 120 = 100$ unordered ones. Moving down forgets the order. 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[87], 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[88].

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.

[87] courses/math1061/counting-principles.pdf
[88] 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[89], 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

[89] 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.

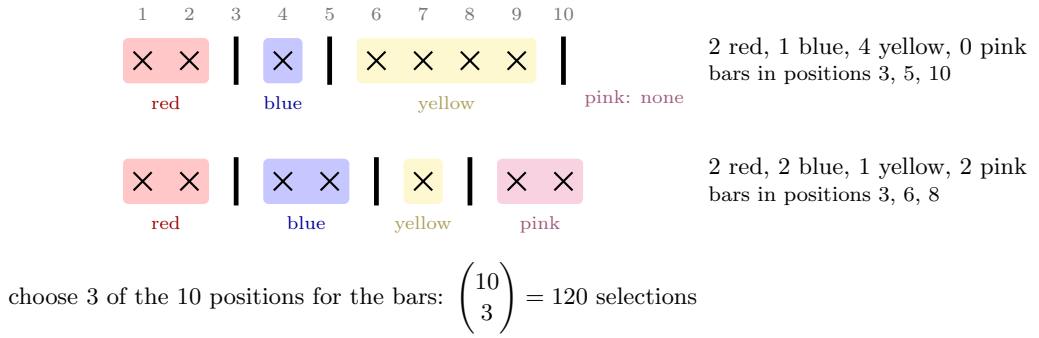


Figure 20: Choosing 7 candies from 4 colours, written as strings of 7 X's and 3 bars. The bars cut the string into four stretches, and the stretches, from left to right, are the red, blue, yellow and pink candies. Top: two red, one blue, four yellow and no pink, so the last stretch is empty. Bottom: 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[90]). 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[91]). The cases must not overlap.

[90] courses/math1061/2026-10-13-counting-selections.pdf
[91] 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[92].

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.

[92] 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.

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

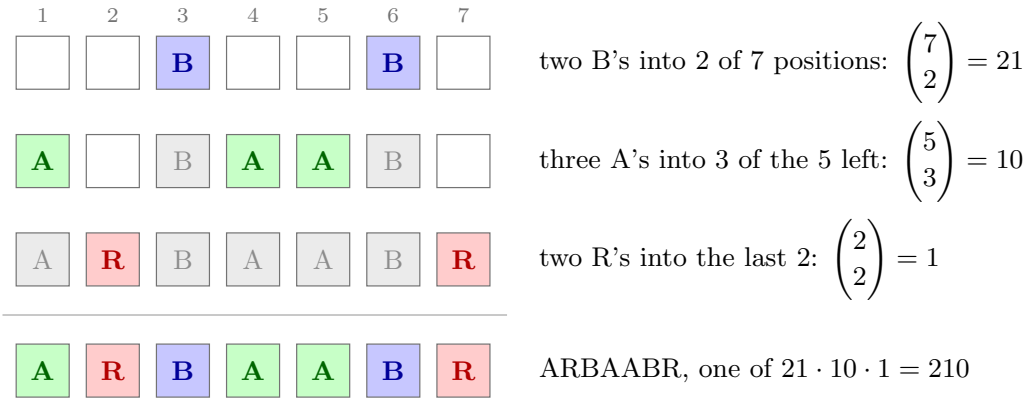


Figure 21: Building one arrangement of BARBARA by choosing positions. First the two B's take 2 of the 7 positions, here 3 and 6, in one of $\binom{7}{2} = 21$ ways. Then the three A's take 3 of the 5 positions still free, here 1, 4 and 5, in one of $\binom{5}{3} = 10$ ways. The two R's must take the 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[93] — the multiplication, addition and difference rules, and permutations, which every formula here is built from
- sets-and-set-notation[94] — subsets, which are what $\binom{n}{r}$ counts
- binomial-coefficients[95] — Pascal's formula, the Binomial Theorem, and other identities for $\binom{n}{r}$, with their combinatorial proofs
- probability[96] — probabilities of equally likely outcomes, worked out with these counts
- one-to-one-and-onto-functions[97] — 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[98] — Lecture 30 · 2026-10-12-introduction-to-counting[99] — Lecture 29
- practice-problems[100] — §38, 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[101]). Each week's class applies the *previous* week's lecture content, so the material a class covers runs roughly one week behind

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

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.

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[102] 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[103]

[102] courses/math1061/math1061.pdf
[103] courses/math1061/logical-connectives.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
2	Logical Equivalence	L2 (wk 1)	030–038	043–053	logical-equivalence-laws[104]
3	Conditional Statements	L3 (wk 1)	039–050	053–066	conditional-statements[105]
4	Valid and Invalid Arguments	L4 (wk 2)	051–063	066–079	valid-argument-forms[106]
5	Methods for Determining Validity	L5 (wk 2)	051–063	066–079	determining-argument-validity[107]
6	Quantified Statements	L5 (wk 2)	096–108	108–121	quantified-statements[108]
7	Negation of Quantified Statements	L6 (wk 2)	108–117	122–131	quantified-statements[109]
8	Statements with Multiple Quantifiers	L6 (wk 2)	117–131	131–146	quantified-statements[110]
9	Direct Proofs and Counterexamples	L7 (wk 3)	145–163	160–182	proof-techniques[111]
10	Proof by Contradiction	L8 (wk 3)	198–207	218–228	proof-techniques[112]
11	Proof by Contraposition	L9 (wk 3)	198–207	218–228	proof-techniques[113]
12	Rational Numbers	L9 (wk 3)	163–170	183–190	rational-and-irrational-numbers[114]

[104] courses/math1061/logical-equivalence-laws.pdf
[105] courses/math1061/conditional-statements.pdf
[106] courses/math1061/valid-argument-forms.pdf
[107] courses/math1061/determining-argument-validity.pdf
[108] courses/math1061/quantified-statements.pdf
[109] courses/math1061/quantified-statements.pdf
[110] courses/math1061/quantified-statements.pdf
[111] courses/math1061/proof-techniques.pdf
[112] courses/math1061/proof-techniques.pdf
[113] courses/math1061/proof-techniques.pdf
[114] courses/math1061/rational-and-irrational-numbers.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
13	Divisibility	L10 (wk 4)	170–179	190–199	divisibility-and-factorisation[115]
14	Modular Arithmetic	L11 (wk 4)	482–485	528–531	modular-arithmetic[116]
15	The Euclidean Algorithm	L12 (wk 4)	220–224	250–254	gcd-lcm-and-euclidean-algorithm[117]
16	Sequences	L13 (wk 5)	227–244	258–275	sequences-and-summations[118]
17	Mathematical Induction	L13 (wk 5)	244–268	275–301	mathematical-induction[119]
18	Strong Induction and the Well Ordering Principle	L14 (wk 5)	268–279	301–314	strong-induction-and-the-well-ordering-principle[120]
19	Recursive Definitions	L15 (wk 6)	290–304	325–340	recursive-definitions[121]
20	Solving Recurrence Relations	L16 (wk 6)	304–328	340–364	solving-recurrence-relations[122]
21	Set Theory Definitions	L17 (wk 6)	336–351	377–391	sets-and-set-notation[123]
22	More Definitions and Examples of Sets	L17 (wk 6)	336–351	377–391	sets-and-set-notation[124]

[115] courses/math1061/divisibility-and-factorisation.pdf
[116] courses/math1061/modular-arithmetic.pdf
[117] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[118] courses/math1061/sequences-and-summations.pdf
[119] courses/math1061/mathematical-induction.pdf
[120] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[121] courses/math1061/recursive-definitions.pdf
[122] courses/math1061/solving-recurrence-relations.pdf
[123] courses/math1061/sets-and-set-notation.pdf
[124] courses/math1061/sets-and-set-notation.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
23	Properties of Sets	L18 (wk 7)	352–366	391–407	proving-set-properties[125]
24	Functions Defined on General Sets	L18 (wk 7)	383–396	425–439	functions-on-general-sets[126]
25	one-to-one, Onto, and Inverse Functions	L19 (wk 7)	397–416	439–461	
26	Composition of Functions	L20 (wk 7)	416–427	461–472	
27	Cardinalities	L21 (wk 8)	428–441	473–486	
28	Countable and Uncountable Sets	L22 (wk 8)	428–441	473–486	
29	Relations on Sets	L23 (wk 8)	442–449	487–494	
30	Reflexivity, Symmetry, Transitivity	L23 (wk 8)	449–459	495–505	
31	Equivalence Relations	L24 (wk 9)	459–478	505–523	
32	Partial Order Relations	L25 (wk 9)	498–515	546–563	
33	Definitions and Examples of Groups	L26 (wk 9)	—	—	
34	Elementary Properties of Groups	L27 (wk 10)	—	—	
35	Group Isomorphisms	*not scheduled*	—	—	
36	Definitions and Examples of Fields	L28 (wk 10)	—	—	

[125] courses/math1061/proving-set-properties.pdf
[126] courses/math1061/functions-on-general-sets.pdf

§	Topic	Lecture (week)	4th ed.	5th ed.	Notes
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[127].

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?

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

3. Let p be the statement "DATAENDFLAG is off," q the statement "ERROR equals 0," and r the statement "SUM is less than 1,000." Express the following sentences in symbolic notation.

   (a) DATAENDFLAG is off, ERROR equals 0, and SUM is less than 1,000.

   (b) DATAENDFLAG is off but ERROR is not equal to 0.

   (c) DATAENDFLAG is off; however, ERROR is not 0 or SUM is greater than or equal to 1,000.

   (d) DATAENDFLAG is on and ERROR equals 0 but SUM is greater than or equal to 1,000.

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

Solutions

1. The truth table is

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

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

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

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

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

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

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

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

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

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

§2 — Logical Equivalence

Epp 4th ed. pp. 030–038 · 5th ed. (metric) pp. 043–053. Lecture 2 (week 1). Notes: logical-equivalence-laws[128].

Problems

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Solutions

1. (a) We have

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

(b) We have

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

2. (a) We have

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

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

(b) We have

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

Hence the statement is a **tautology**.

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

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

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

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

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

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

4. (a) We have

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

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

(b) We have

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

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

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

$(p \wedge r) \oplus (q \wedge r)$	
$\equiv ((p \wedge r) \vee (q \wedge r)) \wedge \sim ((p \wedge r) \wedge (q \wedge r))$	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[129].

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.

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

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

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

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

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

5. Negate the following two statements.

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

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

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

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

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

Solutions

1. We have

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

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

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

   while

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

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

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

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

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

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

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

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

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

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

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

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

Therefore the truth table for the statement is:

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

The statement is a **tautology**.

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

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

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

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

$$R \wedge \sim U,$$

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

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

$$H \wedge \sim B,$$

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

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

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

§4 — Valid and Invalid Arguments

Epp 4th ed. pp. 051–063 · 5th ed. (metric) pp. 066–079. Lecture 4 (week 2). Notes: valid-argument-forms[130].

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.

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

(a) **Elimination:**

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

(b) **Generalisation:**

1. $p \therefore p \vee q$

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

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

Solutions

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

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

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

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

3. (a)

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

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

   (b)

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

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

4. We compute the truth table:

p	q	r	$(p \wedge q) \rightarrow \sim r$	$p \vee \sim q$	$\sim q \rightarrow p$	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[131].

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.

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

(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

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

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

Solutions

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

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

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

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

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

Therefore the argument is valid.

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

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

2. The argument has the symbolic form:

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

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

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

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

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

We can write the argument as follows:

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

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

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

Application — Applications of Valid and Invalid Arguments

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

Application problems

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

   Consider the following predicates and domains:

   Predicates:

$F(x, y)$	disk x has more than y kilobytes of free space.
$S(m)$	mail message m can be saved.
$A(x)$	alert x is active.
$Q(m)$	message m is queued.
$T(m)$	message m is transmitted.

$D(s)$	the diagnostic monitor tracks the status of system s.

Domains:

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

Express the system specifications below using quantifiers and logical connectives:

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

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

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

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

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

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

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

Application solutions

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

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

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

2. (a) Define the following variables:

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

   Now we can express the specifications as follows:

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

   Solution Option 1. If these specifications are consistent, then we must be able to find truth values for each of the variables that makes all of the specifications true. Assume the specifications are consistent (so we assume each specification is true). For specification 5 to be true we know i **is false**. For specification 4 to be true, with i false, we know $\sim m$ is false so m **is true**. For premise 1 to be true, with m true, we have n **is true**. For specification 2 to be true, and since n is true, we have k **is true**. However, now $\sim k$ is false and i is false, which means specification 3 is false. This contradicts our assumption that all the specifications are true, and so it is impossible for the system to be consistent. Therefore, the system is **not consistent**.

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

1.	$m \leftrightarrow n$	specification
2.	$n \to k$	specification
3.	$\sim k \vee i$	specification
4.	$\sim m \to i$	specification
5.	$\sim i$	specification
6.	$\sim k$	from 3 and 5 by elimination (and double negative law)
7.	$\sim n$	from 2 and 6 by Modus Tollens

8.	$(m \to n) \wedge (n \to m)$	from 1 by definition of $\leftrightarrow$
9.	$m \to n$	from 8 by specialisation
10.	$\sim m$	from 9 and 7 by Modus Tollens
11.	i	from 4 and 10 by Modus Ponens

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

(b) Define the following variables:

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

Now we can express the specifications as follows:

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

Assume the specifications are consistent, so each specification is true. For specification 4 to be true, $\sim a$ is true, so a **is false**. For specification 1 to be true with a false we must have r **is false**. Now, since r is false and specification 3 is true, we have s **is false**. We double-check that specification 2 is true, which it is because a is false. Thus, we have found truth values of the statement variables that make all of the specifications true, so the system **is consistent**.

§6 — Quantified Statements

Epp 4th ed. pp. 096–108 · 5th ed. (metric) pp. 108–121. Lecture 5 (week 2). Notes: quantified-statements[132].

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

Problems

1. Rewrite each of the following in the form "$\forall$__, __." Here, let D be the set of all dinosaurs, and let L be the set of all logicians.

   (a) All dinosaurs are extinct.

   (b) Every real number is positive, negative, or zero.

   (c) No irrational numbers are integers.

   (d) No logicians are lazy.

   (e) The number 2,147,581,953 is not equal to the square of any integer.

   (f) The number -1 is not equal to the square of any real number.

2. Rewrite each of the following in the form "$\exists$__ such that __." Here, let X be the set of all exercises.

   (a) Some exercises have answers.

   (b) Some real numbers are rational.

3. Determine whether the following statements are true or false. Justify your reasoning.

   (a) $\forall x \in \mathbb{R},\ x \geq \frac{1}{x}$.

   (b) $\forall a \in \mathbb{Z},\ \frac{a-1}{a} \notin \mathbb{Z}$.

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

Solutions

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

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

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

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

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

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

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

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

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

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

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

§7 — Negation of Quantified Statements

Epp 4th ed. pp. 108–117 · 5th ed. (metric) pp. 122–131. Lecture 6 (week 2). Notes: quantified-statements[133].

Problems

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

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

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

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

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

   (a) All fire engines are red.

   (b) Some apples are ripe.

   (c) A triangle with equal sides exists.

Solutions

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

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

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

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

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

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

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

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

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

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

§8 — Statements with Multiple Quantifiers

Epp 4th ed. pp. 117–131 · 5th ed. (metric) pp. 131–146. Lecture 6 (week 2). Notes: quantified-statements[134].

Problems

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

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

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

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

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

2. For each of the following English sentences:

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

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

   do the following:

   i. Write the statement in symbolic form.

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

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

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

Solutions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

§9 — Direct Proofs and Counterexamples

Epp 4th ed. pp. 145–163 · 5th ed. (metric) pp. 160–182. Lecture 7 (week 3). Notes: proof-techniques[135].

Problems

1. For each of the following statements, either prove the statement or disprove it using a counterexample.

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

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

   (c) There is an even integer n such that $5n - 4$ is prime.

   (d) $\forall n \in \mathbb{Z}^+$, if $n \geq 4$ then $2n^2 - 5n + 2$ is composite.

   (e) $\forall x, y \in \mathbb{R}$, if $y^2 > x^2$ then $y > x$.

2. Find a counterexample that disproves the following statement:

   $$\text{For all } x \in \mathbb{R},\ \lfloor x^2 \rfloor = \lfloor x \rfloor^2.$$

   (Recall that $\lfloor \cdot \rfloor$ denotes the floor function.)

3. Find the errors in the following proofs and rewrite the proof correctly. Here is a list of common errors made when writing proofs:

   - Arguing from examples
   - Using the same variable to mean two different things
   - Jumping to the conclusion
   - Assuming what is to be proved
   - Confusion between what is known and what is to be shown
   - Use of the word *any* instead of *some*
   - Misuse of the word *if*

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

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

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

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

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

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

therefore the statement is true.

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

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

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

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

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

where

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

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

Solutions

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

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

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

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

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

Proof. Consider the positive integers $a = 3$, $b = 4$, $c = 5$. Then $a^2 + b^2 = 9 + 16 = 25 = c^2$. □

(c) **There is an even integer n such that $5n - 4$ is prime.** This statement is **false**. We prove the negation: $\forall n \in \mathbb{Z}^{\text{even}}$, $5n - 4$ is not prime.

Proof. Suppose that n is an even integer. Thus $n = 2k$ for some integer k. Hence

$$5n - 4 = 5(2k) - 4 = 10k - 4 = 2(5k - 2).$$

By definition, this means that $5n - 4$ is even. The only even prime is 2. If $2(5k - 2) = 2$, then $5k - 2 = 1$ and hence $k = \frac{3}{5}$ which is not an integer. Therefore $5n - 4$ is not a prime number. □

(d) $\forall n \in \mathbb{Z}^+$**, if** $n \geq 4$ **then** $2n^2 - 5n + 2$ **is composite.**

Proof. Suppose n is a positive integer and $n \geq 4$. Let us factor

$$2n^2 - 5n + 2 = (2n - 1)(n - 2).$$

Since $n \geq 4$, we have $2n - 1 \geq 7$ and $n - 2 \geq 2$, so both factors are integers > 1. Hence the expression is composite for all $n \geq 4$. □

(e) $\forall x, y \in \mathbb{R}$**, if** $y^2 > x^2$ **then** $y > x$**.** This statement is **false**. Take $x = 1$ and $y = -2$. Then $y^2 = 4 > x^2 = 1$, but $y = -2 \not> 1 = x$.

2. Take $x = \frac{3}{2}$. Then $\lfloor x^2 \rfloor = \lfloor \frac{9}{4} \rfloor = 2$, while $\lfloor x \rfloor^2 = \lfloor \frac{3}{2} \rfloor^2 = 1^2 = 1$. Hence $\lfloor x^2 \rfloor \neq \lfloor x \rfloor^2$, so the statement is false.

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

Proof. Let m be any odd integer, then $m = 2k + 1$ where $k \in \mathbb{Z}$ and let n be any even integer, so $n = 2k$ for any $k \in \mathbb{Z}$. [**Error: using** k **for both** m **and** n **means that the statement is only proved when** $m = n + 1$**.**] Then $m - n = 2k + 1 - 2k = 1$ and 1 is odd so the statement is true.

Correct proof. Let m be any odd integer and let n be any even integer. Then there exist $k, \ell \in \mathbb{Z}$ such that $m = 2k + 1$ and $n = 2\ell$. Hence

$$m - n = (2k + 1) - 2\ell = 2(k - \ell) + 1,$$

which is an odd integer by definition. □

(b) **Statement.** If a and b are even integers, then $4a + 2b$ is even. [**Error: the proof forgets to state its assumptions.**]

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

$$\begin{aligned} 4a + 2b &= 2\ell \quad \text{[Error: this line assumes what is to be proved.]} \\ 4(2k) + 2(2j) &= 2\ell \\ 8k + 4j &= 2\ell \\ 2(4k + 2j) &= 2\ell \end{aligned}$$

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	$p \vee q$	$\sim p \vee r$	$(p \vee q) \wedge (\sim p \vee r)$	$q \vee r$	$\big((p \vee q) \wedge (\sim p \vee r)\big) \rightarrow (q \vee r)$
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[136].

Problems

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

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

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

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

Solutions

1. **For integers a and b, if $6a + 3b$ is odd, then b is odd.**

   Proof. Suppose the statement is false, that is, suppose that there exist integers a and b for which $6a + 3b$ is odd and b is even.

   Since b is even, $b = 2k$ for some integer k. Thus

   $$6a + 3b = 6a + 3(2k) = 6a + 6k = 2(3a + 3k).$$

   Since $a, k \in \mathbb{Z}$, $3a + 3k \in \mathbb{Z}$ so $6a + 3b$ is even. This contradicts our assumption that $6a + 3b$ is odd, so our assumption was incorrect and hence the original statement is true. □

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

   Proof. Suppose, for contradiction, that x and y are positive integers satisfying $x^2 - y^2 = 1$. Now, by factoring, we have

   $$1 = x^2 - y^2 = (x - y)(x + y).$$

   Since x and y are positive integers, we must have $x - y = 1$ and $x + y = 1$. This means $2x = 2$, so $x = 1$. But then we must have $y = 0$ which is not a positive integer; this is a contradiction. Therefore the original statement is true. □

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

§11 — Proof by Contraposition

Epp 4th ed. pp. 198–207 · 5th ed. (metric) pp. 218–228. Lecture 9 (week 3). Notes: proof-techniques[137].

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.

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.

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

($\Leftarrow$) 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[138].

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

Problems

1. Prove the following statement:

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

2. Prove the following statement:

   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.

Solutions

1. **For real numbers m and n, if m is irrational and n is rational, then $m-n$ is irrational.**

   Proof. Let m and n be real numbers and suppose (for a contradiction) that m is an irrational number and n is rational, but $m-n$ is rational. Since n is rational, we have $n = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Since $m-n$ is rational, we have $m - n = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Notice that $m = (m-n) + n$. Hence

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

   Since $a, b, c, d \in \mathbb{Z}$ we have $bc + ad \in \mathbb{Z}$ and $bd \in \mathbb{Z}$. Further, since $b \neq 0$ and $d \neq 0$, we have $bd \neq 0$. Thus, by definition, m is rational. But this contradicts the assumption that m is irrational. $\square$

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

   Proof. We prove the contrapositive statement: for a real number r, if r is rational, then $2r^2 - 3r$ is rational.

   Let r be a real number and suppose $r \in \mathbb{Q}$. Then $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. So

   $$2r^2 - 3r = 2\left(\frac{a}{b}\right)^2 - 3\left(\frac{a}{b}\right) = \frac{2a^2 - 3ab}{b^2}.$$

   Since $a, b \in \mathbb{Z}$, we have $2a^2 - 3ab \in \mathbb{Z}$ and $b^2 \in \mathbb{Z}$. Further, $b^2 \neq 0$ because $b \neq 0$. This means $2r^2 - 3r$ is rational, by definition. □

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

   Proof. Suppose, for a contradiction, that the statement is false. Then there exist real numbers r, s and n such that r is an irrational number, s is rational, n is a positive integer, but $n(r - s)$ is rational. Since s is rational, $s = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ where $b \neq 0$. Since $n(r - s)$ is rational, we have $n(r - s) = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

   Now,

   $$\begin{aligned} r - s &= n(r - s)\left(\frac{1}{n}\right) \quad \text{noting that } n \neq 0 \\ r - s &= \frac{c}{d} \cdot \frac{1}{n} \\ r &= s + \frac{c}{d} \cdot \frac{1}{n} \\ &= \frac{a}{b} + \frac{c}{dn} \\ &= \frac{adn + bc}{bdn} \end{aligned}$$

   Since $a, b, c, d \in \mathbb{Z}$, we have $adn + bc \in \mathbb{Z}$ and $bdn \in \mathbb{Z}$. Further, since $b \neq 0$, $d \neq 0$ and $n \neq 0$, we have $bdn \neq 0$. This means r is rational, by definition, which is a contradiction. □

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

   (a) **Negation:** There exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$.

   (b)

   Proof. Suppose, for a contradiction, that the original statement is false. Then there exists $r \in \mathbb{Q}$ such that $r \neq 0$ and $r\sqrt{2} \in \mathbb{Q}$. Since r is rational, $r = \frac{a}{b}$ for some $a, b \in \mathbb{Z}$ with $b \neq 0$, and since $r \neq 0$, we have $a \neq 0$. Since we have assumed $r\sqrt{2}$ is rational, $r\sqrt{2} = \frac{c}{d}$ for some $c, d \in \mathbb{Z}$ where $d \neq 0$.

Now

$$\sqrt{2} = \frac{r\sqrt{2}}{r} = \left(r\sqrt{2}\right)\left(\frac{1}{r}\right) = \frac{c}{d} \cdot \frac{b}{a} = \frac{bc}{ad}.$$

Since $a, b, c, d \in \mathbb{Z}$, we know $bc \in \mathbb{Z}$ and $ad \in \mathbb{Z}$. Further, since $a \neq 0$ and $d \neq 0$, we have $ad \neq 0$. Thus, by definition, $\sqrt{2}$ is rational. However, this is a contradiction, as $\sqrt{2}$ is irrational. Thus, the original statement is true. □

§13 — Divisibility

Epp 4th ed. pp. 170–179 · 5th ed. (metric) pp. 190–199. Lecture 10 (week 4). Notes: divisibility-and-factorisation[139].

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:

   For all integers c, d and e, if $c \mid d$ and $c \nmid e$, 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.

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

Proof. Let m, n, and q be non-zero integers. Assume $m \mid n$ and $n \mid q$. Then, by definition, there exist integers a, b such that

$$n = ma \quad \text{and} \quad q = nb.$$

Then observe

$$nq = (ma)(nb) = ma \cdot (mab) = m^2(a^2b).$$

Since $a^2b \in \mathbb{Z}$, we conclude that $m^2 \mid nq$. □

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[140].

Problems

1. Prove the following statement:

   If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.

2. (a) Evaluate $58 \operatorname{div} 11$ and $58 \bmod 11$.

   (b) Find integers q and r, with $0 \leqslant r < d$ and $n = dq + r$, in the case that $n = -95$ and $d = 11$.

3. (a) An integer n, when divided by 7, leaves remainder 4. What is the remainder (between 0 and 6 inclusive) when $3n$ is divided by 7?

   (b) When the integer m is divided by 11, the remainder 9 is left. What remainder is left when $4m$ is divided by 22?

4. Prove or disprove the following statements.

   (a) For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

   (b) For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.

Solutions

1. **If y is any integer, then when y^2 is divided by 5, the remainder is always 0, 1 or 4, and never 2 or 3.**

   Proof. Fix $y \in \mathbb{Z}$. By the division algorithm, $y = 5m + r$ for some $m \in \mathbb{Z}$ and $r \in \{0, 1, 2, 3, 4\}$. Then

   $$y^2 = (5m + r)^2 = 25m^2 + 10mr + r^2 \equiv r^2 \pmod 5.$$

   Let us compute the possible values for $r^2 \bmod 5$:

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

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

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

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

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

(b) We want $-95 = 11q + r$ with $0 \le r < 11$. Taking $q = -9$ gives

$$11(-9) = -99 \quad \Rightarrow \quad -95 = -99 + 4 = 11(-9) + 4,$$

so $q = -9$ and $r = 4$.

3. (a) If n leaves remainder 4 upon division by 7, then $n = 7k + 4$ for some integer k. Hence

$$3n = 21k + 12 = 7(3k + 1) + 5,$$

so the remainder when $3n$ is divided by 7 is **5**. (The source PDF prints this step as $7(3k) + 5$, which equals $21k + 5$, not $21k + 12$ — the quotient is $3k + 1$, as above. The answer of 5 is unaffected.)

(b) If m leaves remainder 9 upon division by 11, then $m = 11k + 9$ for some integer k. Then

$$4m = 44k + 36 = 22(2k + 1) + 14,$$

so the remainder when $4m$ is divided by 22 is **14**.

4. (a) **For all real numbers x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.** The statement is **false**. For a counterexample, take $x = \frac{3}{2}$. Then

$$\lfloor x^2 \rfloor = \left\lfloor \frac{9}{4} \right\rfloor = 2 \quad \text{but} \quad \lfloor x \rfloor^2 = \left\lfloor \frac{3}{2} \right\rfloor^2 = 1^2 = 1.$$

(b) **For all odd integers n, $\left\lfloor \dfrac{n^2}{4} \right\rfloor = \left(\dfrac{n-1}{2}\right)\left(\dfrac{n+1}{2}\right)$.** 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[141].

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

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

Solutions

1. We apply the Euclidean Algorithm:

$$3003 = 14 \cdot 214 + 7, \qquad 14 = 7 \cdot 2 + 0.$$

Hence $\gcd(14, 3003) = 7$.

2. (a) We factor $12 = 2^2 \cdot 3$ and $18 = 2 \cdot 3^2$ so $\operatorname{lcm}(12, 18) = 2^2 \cdot 3^2 = 36$.

(b) Using the maximum exponents of each prime, we have

$$\operatorname{lcm}(2^2 \cdot 3 \cdot 5,\ 2^3 \cdot 3^2) = 2^3 \cdot 3^2 \cdot 5 = 360.$$

(c) We factor $2800 = 2^4 \cdot 5^2 \cdot 7$ and $6125 = 5^3 \cdot 7^2$. Thus

$$\operatorname{lcm}(2800, 6125) = 2^4 \cdot 5^3 \cdot 7^2 = 98000.$$

3. **For all positive integers a and b, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$.**

Proof. Let a and b be positive integers.

($\Longleftarrow$) It is clear that if $a = b$ then $\gcd(a, b) = \operatorname{lcm}(a, b)$.

($\Longrightarrow$) Assume $\gcd(a, b) = \operatorname{lcm}(a, b)$. Denoting $g = \gcd(a, b)$, we have $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$.

Now notice gm and gn have no common prime factors beyond those in g, so the least common multiple uses all primes from both m and n. Therefore

$$\operatorname{lcm}(a, b) = gmn.$$

Now, we have $g = gmn$. Therefore $mn = 1$, and so $m = n = 1$. This lets us conclude $a = b$. □

4. **For all positive integers a and b, $a \mid b$ if and only if $\operatorname{lcm}(a, b) = b$.**

Proof. Let us denote $g = \gcd(a, b)$ so that $a = gm$ and $b = gn$ for some positive integers m and n with $\gcd(m, n) = 1$. As explained in the previous question, we have

$$\operatorname{lcm}(a, b) = gmn.$$

($\Longrightarrow$) If $a \mid b$, then $gm \mid gn$, hence $m \mid n$. Since $\gcd(m, n) = 1$, we conclude $m = 1$. Therefore $\operatorname{lcm}(a, b) = gmn = gn = b$.

($\Longleftarrow$) If $\operatorname{lcm}(a, b) = b$, then $gmn = gn$ which means $m = 1$. Therefore $a = gm = g$ and so $a \mid b$. □

5. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 931 &= 301 \cdot 3 + 28 \\ 301 &= 28 \cdot 10 + 21 \\ 28 &= 21 \cdot 1 + 7 \\ 21 &= 7 \cdot 3 + 0. \end{aligned}$$

Hence $\gcd(931, 301) = 7$.

(b) Since $\gcd(931, 301) = 7$, we know $7 \mid 931$, and we have $931 = 7 \cdot 133$. The number 133 has prime factorisation $7 \cdot 19$. Therefore the unique prime factorisation of 931 is $7^2 \cdot 19$.

(c) We have $931 = 7^2 \cdot 19^1$ from part (b). Any divisor of 931 must have a prime factorisation of the form $7^a \cdot 19^b$ where $a \in \{0, 1, 2\}$ and $b \in \{0, 1\}$. Thus the number of positive divisors is

$$(2 + 1)(1 + 1) = 6.$$

(There are 3 choices for the exponent a and 2 choices for the exponent b.)

6. (a) Using the Euclidean Algorithm:

$$\begin{aligned} 116 &= 88 \cdot 1 + 28 \\ 88 &= 28 \cdot 3 + 4 \\ 28 &= 4 \cdot 7 + 0 \end{aligned}$$

Hence $\gcd(116, 88) = 4$.

(b) Using $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{Z}^+$,

$$\operatorname{lcm}(116, 88) = \frac{116 \cdot 88}{\gcd(116, 88)} = \frac{116 \cdot 88}{4} = 116 \cdot 22 = 2552.$$

Application — Trace Tables for Algorithms

Not assessable for MATH1061. For reference, see S. Epp, Discrete Mathematics with Applications, *Section 4.8 (4th edition) or Section 4.10 (5th edition), Brooks/Cole, Belmont, CA.*

The following pseudo-code describes the **Division Algorithm**, with annotations to explain what each step is doing.

Input: a (a non-negative integer), d (a positive integer). This algorithm will take two inputs, a and d, and will find the quotient $a \operatorname{div} d$ and the remainder $a \bmod d$.

Algorithm body:

```
r := a          -- defining our variables
q := 0
                -- starting with a, repeatedly subtract lots of d until we reach
                -- a number less than d; each round adds 1 to the quotient count
while r >= d,
    r := r - d
    q := q + 1
end while
```

Output: q, r. Once we have obtained a number less than d, we are finished. The output q is the quotient ($a \operatorname{div} d$) and the output r is the remainder ($a \bmod d$).

The following pseudo-code describes the **Euclidean Algorithm**, with annotations to explain what each step is doing.

Input: A, B (integers with $A > B \geq 0$).

Algorithm body:

```
a := A          -- defining our variables
b := B
r := B
                -- if b /= 0, compute a mod b (call the algorithm above for this
                -- step) and set r to be this value; replace a with b and b with r
                -- and repeat until b = 0
while b /= 0,
    r := a mod b
    a := b
    b := r
end while
gcd := a
```

Output: gcd (a positive integer).

A **trace table** keeps track of the value of each variable at each step of an algorithm. For example, the trace table for the Division Algorithm with input variables $a = 19$ and $d = 4$ is:

Variable / iteration	0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

Output: $q = 4$, $r = 3$.

Application problems

1. Construct a trace table to trace the action of the Division Algorithm for the following inputs.

   (i) $a = 26$, $d = 7$

   (ii) $a = 15$, $d = 6$

2. Construct a trace table to trace the action of the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$.

Application solutions

1. (i) Trace table for the Division Algorithm with $a = 26$, $d = 7$:

Variable / iteration	0	1	2	3
a	26			
d	7			
r	26	19	12	5
q	0	1	2	3

   Output: $q = 3$, $r = 5$.

   (ii) Trace table for the Division Algorithm with $a = 15$, $d = 6$:

Variable / iteration	0	1	2
a	15		
d	6		
r	15	9	3
q	0	1	2

Output: $q = 2$, $r = 3$.

2. Trace table for the Euclidean Algorithm with inputs $A = 1001$ and $B = 871$:

Variable / iteration	0	1	2	3	4	5
A	1001					
B	871					
a	1001	871	130	91	39	13
b	871	130	91	39	13	0
r	871	130	91	39	13	0
gcd						13

Output: gcd = 13.

§16 — Sequences

Epp 4th ed. pp. 227–244 · 5th ed. (metric) pp. 258–275. Lecture 13 (week 5).

Problems

1. Write down the first four terms in the sequence defined by $a_k = \dfrac{k}{10+k}$ for $k = 1, 2, \ldots$.
2. Consider the sequences $a_k = 2k + 1$ and $b_k = (k-1)^3 + k + 2$ where $k = 0, 1, 2, \ldots$. Show that the first three terms of these sequences are identical, but that their fourth terms differ.
3. (a) Find an explicit formula for a sequence c_n whose first six terms are $-1, 1, -1, 1, -1, 1$.

   (b) Find an explicit formula for a sequence d_n whose first six terms are $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$.
4. (a) Write $(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)$ in summation notation.

   (b) Evaluate $\displaystyle\prod_{i=1}^{5}(-1)^i \cdot i$.

   (c) Write $(y-1)(y^2-2)(y^3-3)(y^4-4)$ in product notation.

(d) Evaluate $\displaystyle\sum_{j=1}^{n}(-1)^j\frac{1}{2^j}$ when $n=5$.

Solutions

1. We have

$$a_1=\frac{1}{11},\qquad a_2=\frac{2}{12}=\frac{1}{6},\qquad a_3=\frac{3}{13},\qquad a_4=\frac{4}{14}=\frac{2}{7}.$$

2. We compute

$$a_0=1,\quad a_1=3,\quad a_2=5,\quad a_3=7;$$

$$b_0=(-1)^3+0+2=1,\quad b_1=0^3+1+2=3,\quad b_2=1^3+2+2=5,\quad b_3=2^3+3+2=13.$$

Hence the first three terms agree ($a_0=b_0$, $a_1=b_1$ and $a_2=b_2$), but the fourth terms differ ($a_3=7$ while $b_3=13$).

3. (a) One explicit formula is

$$c_n=(-1)^n\qquad n=1,2,3,...$$

(b) The denominators are square numbers, so an explicit formula is

$$d_n=\frac{n}{(n+1)^2}\qquad n=1,2,3,...$$

4. (a) We have

$$(x^2-1)+(2x^3-1)+(3x^4-1)+(4x^5-1)+(5x^6-1)=\sum_{k=1}^{5}\left(kx^{k+1}-1\right).$$

(b) We have

$$\prod_{i=1}^{5}(-1)^i\cdot i=\left(\prod_{i=1}^{5}(-1)^i\right)\left(\prod_{i=1}^{5}i\right)=(-1)^{1+2+3+4+5}\cdot 5!=(-1)^{15}\cdot 120=-120.$$

(c) We have

$$(y-1)(y^2-2)(y^3-3)(y^4-4) = \prod_{k=1}^{4} (y^k - k)\,.$$

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

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

Proof. Let $P(n)$ be the predicate

$$\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}.$$

Basis: consider $n = 1$. We have $\sum_{i=1}^{1} i^3 = 1^3 = 1$ and $\frac{1^2(1+1)^2}{4} = \frac{4}{4} = 1$ so $P(1)$ is true.

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

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(k)$ is true. That is,

$$\sum_{i=1}^{k} i^3 = \frac{k^2(k+1)^2}{4}.$$

Now consider $n = k + 1$.

$$\begin{aligned}
\sum_{i=1}^{k+1} i^3 &= \sum_{i=1}^{k} i^3 + (k+1)^3 && \text{(splitting off the last term)} \\
&= \frac{k^2(k+1)^2}{4} + (k+1)^3 && \text{by the inductive hypothesis} \\
&= \frac{k^2(k+1)^2}{4} + \frac{4(k+1)^3}{4} \\
&= \frac{(k+1)^2}{4}(k^2 + 4(k+1)) \\
&= \frac{(k+1)^2}{4}(k^2 + 4k + 4) \\
&= \frac{(k+1)^2}{4}(k+2)^2
\end{aligned}$$

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

Therefore, by the principle of mathematical induction, $\sum_{i=1}^{n} i^3 = \frac{n^2(n+1)^2}{4}$ for every integer $n \geq 1$. $\square$

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

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

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** $a_1, a_2, a_3, ...$ 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 $P(1), ..., P(k)$ 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 $P(0), P(1), ..., P(k)$ are all true then $P(k+1)$ is true.)

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(m)$ holds for all integers $m = 0, 1, \ldots, k$.

We now aim to show that $P(k+1)$ is true. Notice that

$$\begin{aligned} a_1 a_k &= \left(x + \frac{1}{x}\right)\left(x^k + \frac{1}{x^k}\right) \\ &= \left(x^{k+1} + \frac{1}{x^{k+1}}\right) + \left(x^{k-1} + \frac{1}{x^{k-1}}\right) = a_{k+1} + a_{k-1}. \end{aligned}$$

Therefore $a_{k+1} = a_1 a_k - a_{k-1}$. By the inductive hypothesis, a_k and a_{k-1} are integers, and a_1 is an integer, so a_{k+1} is an integer. Hence $P(k+1)$ holds.

Therefore, by the principle of strong mathematical induction, a_n is an integer for all $n \geq 0$. □

§19 — Recursive Definitions

Epp 4th ed. pp. 290–304 · 5th ed. (metric) pp. 325–340. Lecture 15 (week 6).

Problems

1. Define the sequence $b_1 = 2$, $b_2 = 6$ and

$$b_k = b_{k-1} + b_{k-2} + \gcd(b_{k-1}, b_{k-2})$$

for all $k \geq 3$. Use strong induction to prove b_n is even for all $n \geq 1$.

2. A sequence is defined by $a_1 = 2$ and

$$a_k = k(a_{k-1} + k - 1)$$

for all integers $k \geq 2$. Use mathematical induction to prove a_n is even for all $n \geq 1$.

3. Recursively define the set S of binary strings as follows.

   (a) *(Base rule)* $1 \in S$.

   (b) *(Recursion rule)* If $s \in S$ then $0s \in S$ and $1s \in S$ (e.g. if $s = 1$ then $0s = 01$).

   (c) *(Restriction rule)* No other strings lie in S besides those given by the rules above.

   What are the strings contained in S arising from the first three applications of the recursive rule?

Solutions

1. *Proof.* Let $P(n)$ be the predicate "b_n is even".

   Base case. The base cases are $n = 1, 2$. We have $b_1 = 2$ and $b_2 = 6$ so $P(1)$ and $P(2)$ are true.

   Inductive hypothesis. Assume $P(m)$ is true for all integers m with $1 \leq m \leq k$, where $k \geq 2$ is an integer. That is, we assume $b_1, b_2, \ldots, b_k$ are all even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. b_{k+1} is even. Using the recursive definition, we have

   $$b_{k+1} = b_k + b_{k-1} + \gcd(b_k, b_{k-1}).$$

   By the inductive hypothesis, b_k and b_{k-1} are even, so $2 \mid b_k$ and $2 \mid b_{k-1}$, hence $2 \mid \gcd(b_k, b_{k-1})$ as well. Therefore each term on the right-hand side is even, so their sum b_{k+1} is even. Thus $P(k+1)$ holds.

   Therefore, b_n is even for all integers $n \geq 1$. □

2. *Proof.* Let $P(n)$ be the predicate "a_n is even".

   Base case. The base case is $n = 1$. We have $a_1 = 2$, which is even, so $P(1)$ is true.

   Inductive hypothesis. Assume $P(k)$ is true for some integer $k \geq 1$. That is, assume a_k is even.

   Inductive step. We need to show that $P(k+1)$ is true, i.e. a_{k+1} is even. By the recursive definition, we have

   $$a_{k+1} = (k+1)(a_k + (k+1) - 1) = (k+1)(a_k + k).$$

   Note that a_k is even by the inductive hypothesis. We split into cases:

   - If k is even, then $a_k + k$ is even, hence a_{k+1} is even.
   - If k is odd, then $k+1$ is even, hence a_{k+1} is even.

   In all cases, a_{k+1} is even, so $P(k+1)$ is true.

   Therefore, a_n is even for all integers $n \geq 1$. □

3. By the base rule, we only know $1 \in S$.

   First application of the recursive rule:

   $$01 \in S, \qquad 11 \in S.$$

   Second application of the recursive rule:

$$001 \in S, \quad 101 \in S, \quad 011 \in S, \quad 111 \in S.$$

Third application of the recursive rule:

$$0001 \in S, \quad 1001 \in S, \quad 0101 \in S, \quad 1101 \in S,$$
$$0011 \in S, \quad 1011 \in S, \quad 0111 \in S, \quad 1111 \in S.$$

§20 — Solving Recurrence Relations

Epp 4th ed. pp. 304–328 · 5th ed. (metric) pp. 340–364. Lecture 16 (week 6).

Problems

1. Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that

$$a_n = 5a_{n-1} - 6a_{n-2}$$

for all integers $n \geq 2$.

2. Let $\{b_n\}_{n\geq 0}$ be the sequence defined by

$$b_0 = 2, \qquad b_1 = 5, \qquad \text{and} \qquad b_k = 2b_{k-1} - b_{k-2} \text{ for each integer } k \geq 2.$$

   (a) Write down the values of $b_0, b_1, b_2, b_3, b_4, b_5$.

   (b) Based on your answers for part (a), guess an explicit formula for this sequence.

   (c) Prove that your guess from part (b) is correct.

3. Let T_n be a sequence defined by $T_1 = 1$ and

$$T_{n+1} = 1 + (T_1 \times T_2 \times T_3 \times \cdots \times T_n)$$

for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.

4. Consider the Fibonacci sequence defined recursively by

$$\begin{aligned} a_0 &= 0 \\ a_1 &= 1 \\ a_n &= a_{n-2} + a_{n-1} \qquad \text{for all integers } n \geq 2. \end{aligned}$$

Use strong mathematical induction to prove the explicit formula

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}$$

for all integers $n \geq 0$, where $\phi = \frac{1+\sqrt{5}}{2}$ and $\psi = \frac{1-\sqrt{5}}{2}$. (You may use the fact that $\phi^2 = \phi + 1$ and $\psi^2 = \psi + 1$.)

Solutions

1. **Define a sequence $a_n = 2^n + 5 \cdot 3^n$ for all integers $n \geq 0$. Show that $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$.**

Proof. For $n \geq 2$, we have $n - 2 \geq 0$ so all three terms a_n, a_{n-1} and a_{n-2} are defined in the given formula. Then,

$$\begin{aligned} 5a_{n-1} - 6a_{n-2} &= 5\left(2^{n-1} + 5 \cdot 3^{n-1}\right) - 6\left(2^{n-2} + 5 \cdot 3^{n-2}\right) \\ &= \left(5 \cdot 2^{n-1} - 6 \cdot 2^{n-2}\right) + \left(25 \cdot 3^{n-1} - 30 \cdot 3^{n-2}\right) \\ &= (10 - 6)2^{n-2} + (75 - 30)3^{n-2} \\ &= 4 \cdot 2^{n-2} + 45 \cdot 3^{n-2} \\ &= 2^n + 5 \cdot 3^n \\ &= a_n. \end{aligned}$$

Hence $a_n = 5a_{n-1} - 6a_{n-2}$ for all integers $n \geq 2$. □

2. (a)

$$\begin{aligned} b_0 &= 2 \\ b_1 &= 5 \\ b_2 &= 2(5) - 2 = 8 \\ b_3 &= 2(8) - 5 = 11 \\ b_4 &= 2(11) - 8 = 14 \\ b_5 &= 2(14) - 11 = 17 \end{aligned}$$

(b) Guess that $b_n = 3n + 2$ for each integer $n \geq 0$.

(c)

Proof. The guess gives $b_0 = 3(0) + 2 = 2$ and $b_1 = 3(1) + 2 = 5$ so it gives the correct initial conditions. Now we substitute the guess into the recurrence relation. The LHS of the recurrence relation is $b_k = 3k + 2$. The RHS of the recurrence relation is

$$\begin{aligned} 2b_{k-1} - b_{k-2} &= 2(3(k-1)+2) - (3(k-2)+2) \\ &= 2(3k-1) - (3k-4) \\ &= 6k - 2 - 3k + 4 \\ &= 3k + 2 \end{aligned}$$

So the guess also satisfies the recurrence relation. Thus the guess is correct. □

Alternative proof (by strong induction). Let $P(n)$ be the predicate $b_n = 3n + 2$.

Basis: $b_0 = 2$ from the recursive definition and $3(0) + 2 = 2$ so $P(0)$ is true. $b_1 = 5$ from the recursive definition and $3(1) + 2 = 5$ so $P(1)$ is true.

Inductive hypothesis: suppose $k \geq 1$ is an integer and $P(0), P(1), \ldots, P(k)$ are true.

Now

$$\begin{aligned} b_{k+1} &= 2b_k - b_{k-1} && \text{by the rec. rel. since } k+1 \geq 2 \\ &= 2(3k+2) - (3(k-1)+2) && \text{since } P(k) \text{ and } P(k-1) \text{ are true} \\ &= 6k + 4 - (3k - 1) \\ &= 3k + 5 \\ &= 3(k+1) + 2 \end{aligned}$$

So $P(k+1)$ is true. Therefore, by the principle of (strong) mathematical induction, the guess is correct for this recursively defined sequence. □

3. **Let T_n be a sequence defined by $T_1 = 1$ and $T_{n+1} = 1 + (T_1 \times \cdots \times T_n)$ for all $n \geq 1$. Prove that $T_{n+1} = (T_n)^2 - T_n + 1$ for all $n \geq 2$.**

Proof. We can prove this simply by applying the recursive formula twice, once for T_{n+1} and once for T_n:

$$\begin{aligned} T_{n+1} &= 1 + (T_1 \cdot T_2 \cdot T_3 \cdots T_n) && \text{by the recursive definition} \\ &= 1 + T_n \cdot (T_1 \cdot T_2 \cdot T_3 \cdots T_{n-1}) \\ &= 1 + T_n \cdot (T_n - 1) && \text{since } T_n = 1 + (T_1 \cdots T_{n-1}) \text{ by rec. def.} \\ &= 1 + (T_n)^2 - T_n \\ &= (T_n)^2 - T_n + 1. \end{aligned}$$

Note that both applications of the recursive definition are valid, since $n-1 \geq 1$. $\square$

4. **Fibonacci explicit formula.**

Proof. Let $P(n)$ be the predicate

$$a_n = \frac{\phi^n - \psi^n}{\sqrt{5}}.$$

Basis. The base cases are $n = 0, 1$, which are true because

$$\frac{\phi^0 - \psi^0}{\sqrt{5}} = \frac{1-1}{\sqrt{5}} = 0 = a_0,$$

and

$$\frac{\phi - \psi}{\sqrt{5}} = \frac{\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}}{\sqrt{5}} = \frac{\sqrt{5}}{\sqrt{5}} = 1 = a_1.$$

Inductive hypothesis. Now suppose that for some integer $m \geq 1$, we have that $P(i)$ is true for all $0 \leq i \leq m$. In particular, $P(m)$ and $P(m-1)$ are true, that is,

$$a_m = \frac{\phi^m - \psi^m}{\sqrt{5}} \qquad \text{and} \qquad a_{m-1} = \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}}.$$

We need to show that $P(m+1)$ is true. That is, we aim to show

$$a_{m+1} = \frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}}.$$

Starting with the right-hand side of $P(m+1)$, we have

$$\begin{aligned}
\frac{\phi^{m+1} - \psi^{m+1}}{\sqrt{5}} &= \frac{\phi^2\phi^{m-1} - \psi^2\psi^{m-1}}{\sqrt{5}} \\
&= \frac{(\phi+1)\phi^{m-1} - (\psi+1)\psi^{m-1}}{\sqrt{5}} && \text{since } \phi^2 = \phi + 1 \text{ and } \psi^2 = \psi + 1 \\
&= \frac{(\phi^m + \phi^{m-1}) - (\psi^m + \psi^{m-1})}{\sqrt{5}} \\
&= \frac{\phi^m - \psi^m}{\sqrt{5}} + \frac{\phi^{m-1} - \psi^{m-1}}{\sqrt{5}} \\
&= a_m + a_{m-1} && \text{by the inductive hypothesis} \\
&= a_{m+1} && \text{by definition.}
\end{aligned}$$

Hence $P(m+1)$ is true. $\square$

§21 — Set Theory Definitions

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Define the sets

$$\begin{aligned} V &= \{x \in \mathbb{Z} \mid 2 \leqslant x \leqslant 11 \text{ and } x \text{ is odd}\}, \\ X &= \{x \in \mathbb{Z} \mid -1 \leqslant x \leqslant 4\}, \\ Y &= \{2, 3, 7, 9\}, \\ Z &= \{x \in \mathbb{Z} \mid x \neq 0\}. \end{aligned}$$

   Write down the following sets, listing their elements and using brackets as appropriate.

   (a) $V \cap X$. (b) $V \cup Y$. (c) $X \cap Z$.

   (b) $X \cap (Z - Y)$. (e) $(X \cup Y) \cap V$. (f) $X \cup (Y \cap V)$.

2. For each of the following sets, write down its elements and then state the size of the set; that is, find $|A|$, $|B|$, $|C|$ and $|D|$.

   (a) $A = \{x \in \mathbb{Z} \mid \exists\, i \in \mathbb{Z} \text{ such that } x = 1 + (-1)^i\}$.

   (b) $B = \{y \in \mathbb{Z} \mid -8 < y \leqslant -5\}$.

   (c) $C = \{s \in \mathbb{Z} \mid s^2 + 1 = 0\}$.

   (d) $D = \{t \in \mathbb{Z} \mid t^4 = 1\}$.

3. Define the sets $A = \{0, 1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ and $C = \{1, 2, 4, 5, 7\}$. List the elements of the set

$$R = ((A - B) \cap (A - C)) \cup (B \cap C \cap A).$$

4. Are the following statements true or false? Justify in one or two sentences.

   (a) $x \in \{x\}$ (b) $\{x\} \subseteq \{x\}$ (c) $\{\emptyset\} \in \{\{\emptyset\}\}$

   (b) $\emptyset \subseteq \{x\}$ (e) $\emptyset \in \{x\}$

Solutions

1. (a) $V \cap X = \{3\}$

   (b) $V \cup Y = \{2, 3, 5, 7, 9, 11\}$

   (c) $X \cap Z = \{-1, 1, 2, 3, 4\}$

   (d) $X \cap (Z - Y) = \{-1, 1, 4\}$

   (e) $(X \cup Y) \cap V = \{3, 7, 9\}$

   (f) $X \cup (Y \cap V) = \{-1, 0, 1, 2, 3, 4, 7, 9\}$

2. (a) Note that $(-1)^i$ is either $+1$ or -1 (according as i is even or odd). So x is either $1 + 1$ or $1 - 1$, that is, 2 or 0. So $A = \{2, 0\}$ and $|A| = 2$.

   (b) $B = \{-7, -6, -5\}$, so $|B| = 3$.

   (c) If $s^2 + 1 = 0$, we have $s^2 = -1$, and there are no such real numbers s, let alone integers! So $C = \emptyset$ and $|C| = 0$.

   (d) $D = \{-1, 1\}$, since $t^4 = 1$ with $t \in \mathbb{Z}$ implies $t = \pm 1$. Hence $|D| = 2$.

3. We have $A - B = \{0, 1, 2\}$ and $A - C = \{0, 3\}$, so $(A - B) \cap (A - C) = \{0\}$. Also $B \cap C \cap A = \{4\}$. Thus $R = \{0\} \cup \{4\} = \{0, 4\}$.

4. (a) **True:** $\{x\}$ is the set whose only element is x, so $x \in \{x\}$.

   (b) **True:** every set is a subset of itself, so $\{x\} \subseteq \{x\}$.

   (c) **True:** $\{\{\emptyset\}\}$ has the single element $\{\emptyset\}$, so $\{\emptyset\} \in \{\{\emptyset\}\}$.

   (d) **True:** $\emptyset \subseteq S$ for every set S, in particular $\emptyset \subseteq \{x\}$.

   (e) **False** (in general): $\emptyset \in \{x\}$ would require $\emptyset = x$.

Application — Computer Representations of Sets

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 134–138.*

There are various ways to represent sets using a computer. One such method involves the use of binary strings.

If we fix a finite universal set U with an arbitrary ordering, for example $U = \{a_1, a_2, \ldots, a_n\}$, we can represent subsets of U using binary strings of length n. A 1 in the ith position of the string indicates that element a_i is in the subset and a 0 indicates it is not.

For example if $U = \{1, 2, 3\}$ then the string 000 represents the empty set, 101 represents the subset $\{1, 3\}$ and 111 represents the entire set U.

The set operations union and intersection can be computed at the level of binary strings by utilising the bitwise OR and AND operations. The union of two sets corresponds to the bitwise OR operation on the strings and the intersection corresponds to bitwise AND.

Application problems

1. Define the universal set $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.

   (a) Express each of the following subsets of U using binary strings:

   i. $\{3, 4, 5\}$

   ii. $\{1, 3, 6, 10\}$

   iii. $\{a \in U \mid a \text{ is prime}\}$.

   (b) Using the same U, find the set represented by the following strings:

   i. 1111001111

   ii. 0101111000

   iii. 1000000001

   (c) Use binary strings to compute the following set operations.

   i. $\{1, 3, 4, 6, 10\} \cap \{2, 3, 6, 9, 10\}$

   ii. $\{2, 4, 6, 8\} \cup \{3, 4, 5\}$

Application solutions

1. (a) i. 0011100000

   ii. 1010010001

   iii. 0110101000 — the primes in U are $2, 3, 5, 7$. (The source PDF prints 1010111000 here, which decodes to $\{1, 3, 5, 6, 7\}$ and is not the set of primes; the string above is the correct one.)

   (b) i. $\{1, 2, 3, 4, 7, 8, 9, 10\}$

   ii. $\{2, 4, 5, 6, 7\}$

   iii. $\{1, 10\}$

   (c) i. 1011010001 AND 0110010011 = 0010010001, so the intersection is $\{3, 6, 10\}$.

   ii. 0101010100 OR 0011100000 = 0111110100, so the union is $\{2, 3, 4, 5, 6, 8\}$.

§22 — More Definitions and Examples of Sets

Epp 4th ed. pp. 336–351 · 5th ed. (metric) pp. 377–391. Lecture 17 (week 6).

Problems

1. Let $A = \{1, 2\}$, $B = \{2, 3\}$ and $C = \{3, 4\}$. List the elements of the following sets.
   (a) $A \cap C$
   (b) $(A \cup C) - B$
   (c) $(A \times B) \cap (A \times C)$
   (d) $\mathcal{P}(B \cap C)$
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\}$
2. Are the following statements true or false?
   (a) $\mathbb{Q} \in \mathbb{R}$.
   (b) $\{1, 2\} \subseteq \mathbb{Z}$.
   (c) $\{-3, 0\} \subseteq \mathcal{P}(\mathbb{Z})$.
   (d) $\{(1, 2), (0, 1)\} \in \mathbb{Z} \times \mathbb{Z}$.
3. Let $X = \mathcal{P}(\emptyset)$ and $Y = \mathcal{P}(\mathcal{P}(\emptyset))$. List the elements of each of the following sets.
   (a) X (b) Y (c) $X \cap Y$ (d) $X \cup Y$
4. Define sets $S = \{3, 5\}$ and $T = \{2, 3, 7\}$. Are the following statements true or false?
   (a) $S \subseteq T$
   (b) $\emptyset \in \mathcal{P}(S)$
   (c) $\emptyset \in T$
   (d) $(3, 3, 3) \in S \times T$

Solutions

1. (a) $A \cap C = \emptyset$.
   (b) $(A \cup C) - B = \{1, 4\}$.
   (c) $(A \times B) \cap (A \times C) = \{(1, 3), (2, 3)\}$.
   (d) $\mathcal{P}(B \cap C) = \{\emptyset, \{3\}\}$.
   (e) $\{x : (x \subseteq A) \wedge (x \in \mathcal{P}(B))\} = \{\emptyset, \{2\}\}$.
2. (a) **False.** ($\mathbb{Q}$ is a *subset* of $\mathbb{R}$, not an element of it.)
   (b) **True.**
   (c) **False.** (The elements of $\mathcal{P}(\mathbb{Z})$ are sets of integers; -3 and 0 are integers, not sets.)
   (d) **False.** (It is a *subset* of $\mathbb{Z} \times \mathbb{Z}$, not an element — the elements of $\mathbb{Z} \times \mathbb{Z}$ are ordered pairs.)
3. (a) $X = \mathcal{P}(\emptyset) = \{\emptyset\}$.
   (b) $Y = \mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.
   (c) $X \cap Y = \{\emptyset\}$.
   (d) $X \cup Y = \{\emptyset, \{\emptyset\}\}$.
4. (a) **False.** ($5 \in S$ but $5 \notin T$.)
   (b) **True.** (The empty set is an element of every power set.)
   (c) **False.** (T's elements are 2, 3 and 7.)
   (d) **False.** (The elements of $S \times T$ are ordered *pairs*, not triples.)

§23 — Properties of Sets

Epp 4th ed. pp. 352–366 · 5th ed. (metric) pp. 391–407. Lecture 18 (week 7).

Problems

1. (a) Use the element method to prove that for all sets A and B

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

   (b) Use the element method to prove that for all sets X, Y and Z,

$$(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset.$$

   (c) Use set identities to prove that for all sets A, B and C

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

2. Prove or disprove the following:

   (a) For all sets A and B, we have $\mathcal{P}(A \cup B) = \mathcal{P}(A) \cup \mathcal{P}(B)$.

   (b) For all sets A and B, we have $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$.

   (c) There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$.

   (d) Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$.

3. Let A, B and C be sets. Prove that

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

Solutions

1. (a) **For all sets A and B, $A \cup (B - A) = A \cup B$.**

   Proof. First we show that $A \cup (B - A) \subseteq A \cup B$.

   Consider an arbitrary element $x \in A \cup (B - A)$. Then we know $x \in A$ or $x \in B - A$. This means $x \in A$, or $x \in B$ and $x \notin A$. If $x \in A$, then $x \in A \cup B$. Similarly if $x \in B - A$, then it must be in B and so $x \in A \cup B$. In either case, we have $x \in A \cup B$, thus $A \cup (B - A) \subseteq A \cup B$.

   Now we show that $A \cup B \subseteq A \cup (B - A)$.

   Let $x \in A \cup B$, then $x \in A$ or $x \in B$ or it is in both A and B. If $x \in A$, then $x \in A \cup (B - A)$. If $x \notin A$ then $x \in B$ since $x \in A \cup B$. So we have that $x \in B$ and $x \notin A$, hence $x \in B - A$ and thus $x \in A \cup (B - A)$. This proves that $A \cup B \subseteq A \cup (B - A)$, and together this proves that $A \cup B = A \cup (B - A)$. $\square$

(b) **For all sets X, Y and Z, $(X - Z) \cap (Y - Z) \cap (X - Y) = \emptyset$.**

Proof. Assume that $(X - Z) \cap (Y - Z) \cap (X - Y) \neq \emptyset$.

So let $x \in (X - Z) \cap (Y - Z) \cap (X - Y)$. Then, in particular, $x \in Y - Z$ and $x \in X - Y$. The former implies $x \in Y$, but the latter implies $x \notin Y$. No such x exists. Therefore the set is empty. □

(c) **For all sets A, B and C, $(A - B) - C = A - (B \cup C)$.**

Proof. Using $A - B = A \cap B^c$, $(S - T) = S \cap T^c$, and De Morgan's law, we have

$$(A-B)-C = (A\cap B^c)\cap C^c = A\cap(B^c\cap C^c) = A\cap(B\cup C)^c = A-(B\cup C). \qquad \square$$

2. (a) **For all sets A and B, $\mathcal{P}(A\cup B) = \mathcal{P}(A)\cup\mathcal{P}(B)$. False.** Counterexample: $A = \{1\}$, $B = \{2\}$. Then

$$\mathcal{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \neq \{\emptyset, \{1\}\} \cup \{\emptyset, \{2\}\} = \{\emptyset, \{1\}, \{2\}\}.$$

(b) **For all sets A and B, $\mathcal{P}(A) = \mathcal{P}(B) \iff A = B$. True.**

($\Longleftarrow$) If $A = B$ then clearly $\mathcal{P}(A) = \mathcal{P}(B)$.

($\Longrightarrow$) We next show that if $\mathcal{P}(A) = \mathcal{P}(B)$, then $A = B$. Suppose (for a contradiction) that $\mathcal{P}(A) = \mathcal{P}(B)$ but $A \neq B$. Then (without loss of generality), there exists an element x in A that is not in B. Therefore, there is an element $\{x\}$ in $\mathcal{P}(A)$ that is not in $\mathcal{P}(B)$. Therefore $\mathcal{P}(A) \neq \mathcal{P}(B)$ — a contradiction. Thus, for all sets A and B, if $\mathcal{P}(A) = \mathcal{P}(B)$ then $A = B$. □

(c) **There exists a set A such that $\mathcal{P}(A) = \{\{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, \{a, b, c\}\}$. False.**

No such set exists. The power set of any set must contain the empty set — that is, $\emptyset \in \mathcal{P}(A)$, where A is any set. Also, the power set of any set of size n has cardinality 2^n. The power set above contains 7 elements, and there does not exist any integer n such that $2^n = 7$.

(d) **Let A, B and C be sets. If $B \subseteq C$ then $A \times B \subseteq A \times C$. True.**

First note that if $A = \emptyset$ then $A \times B = A \times C = \emptyset$ and the statement is true. Also, if $B = \emptyset$ then $A \times B = \emptyset$ and $\emptyset \subseteq A \times C$ for any C, so the statement is true.

Suppose A, B and C are non-empty sets with $B \subseteq C$. Thus if $b \in B$, then $b \in C$. Consider any element $(a, b) \in A \times B$, where $a \in A$ and $b \in B$. Since

$b \in B$, $b \in C$. As such, $a \in A$ and $b \in C$ for all a or b, so $(a, b) \in A \times C$. Therefore $A \times B \subseteq A \times C$. □

3. **For all sets A, B and C, $A - (B \cup C) = (A - B) - C$.**

   Proof Option 1. For any x, we have

   $$x \in A - (B \cup C) \iff x \in A \wedge x \notin (B \cup C) \iff x \in A \wedge (x \notin B) \wedge (x \notin C).$$

   Also, we have

   $$x \in (A - B) - C \iff x \in (A - B) \wedge x \notin C \iff (x \in A \wedge x \notin B) \wedge x \notin C.$$

   The statements on the right-hand side are equivalent. Hence $A - (B \cup C) = (A - B) - C$. □

   Proof Option 2.

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

§24 — Functions Defined on General Sets

Epp 4th ed. pp. 383–396 · 5th ed. (metric) pp. 425–439. Lecture 18 (week 7).

Problems

1. Consider the function $f : \mathbb{R} \to \mathbb{R}$ defined by $f(x) = x^2 - 1$.
   (a) What is the domain, codomain and range of f?
   (b) What is the image of $\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}$ under f?
   (c) What is the preimage of $\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}$ under f?
2. Let $X = \{1, 3, 5\}$ and $Y = \{s, t, u, v\}$ be sets. Define $f : X \to Y$ by the arrow diagram

   $$1 \mapsto v, \qquad 3 \mapsto s, \qquad 5 \mapsto v$$

   (the elements t and u of Y receive no arrows).

(a) Write the domain of f and the co-domain of f.

(b) Determine $f(1)$, $f(3)$, and $f(5)$.

(c) Determine the range of f.

(d) Is 3 an inverse image of s? Is 1 an inverse image of u?

(e) What is the inverse image of s? of u? of v?

(f) Represent f as a set of ordered pairs.

3. Let D be the set of all finite subsets of $\mathbb{Z}^+$. Consider the function $T : \mathbb{Z}^+ \to D$ defined by $T(n) := \{d \mid d \in \mathbb{Z}^+ \text{ and } d \text{ divides } n\}$. Find the following:

(a) $T(1)$ (b) $T(15)$ (c) $T(17)$ (d) $T(5)$ (e) $T(18)$ (f) $T(21)$

4. Let S be the set of all strings of a's and b's.

(a) Define the function $f : S \to \mathbb{Z}$ by

$$f(s) = \begin{cases} \text{the number of } b\text{'s to the left of the left-most } a \text{ in } s, & \text{if } s \text{ contains an } a, \\ 0, & \text{if } s \text{ contains no } a\text{'s.} \end{cases}$$

Find $f(aba)$, $f(bbab)$, and $f(b)$. What is the range of f?

(b) Define the function $g : S \to S$ by

$$g(s) = \text{the string obtained by writing the characters of } s \text{ in reverse order.}$$

Find $g(aba)$, $g(bbab)$, and $g(b)$. What is the range of g?

Solutions

1. (a) The domain is $\mathbb{R}$, the codomain is $\mathbb{R}$, and the range is $[-1, \infty)$.

(b) $f(\{x \in \mathbb{R} \mid -1 \leq x \leq 2\}) = [-1, 3]$.

(c) $f^{-1}(\{y \in \mathbb{R} \mid 0 \leq y \leq 3\}) = \{x \in \mathbb{R} \mid 1 \leq x^2 \leq 4\} = [-2, -1] \cup [1, 2]$.

2. (a) The domain is $X = \{1, 3, 5\}$ and the codomain is $Y = \{s, t, u, v\}$.

(b) $f(1) = v$, $f(3) = s$, $f(5) = v$.

(c) $\text{range}(f) = \{s, v\}$.

(d) **Yes**, 3 is an inverse image of s. **No**, 1 is not an inverse image of u.

(e) $f^{-1}(s) = \{3\}$, $f^{-1}(u) = \emptyset$, $f^{-1}(v) = \{1, 5\}$.

(f) $f = \{(1, v), (3, s), (5, v)\}$.

3. (a) $T(1) = \{1\}$.

(b) $T(15) = \{1, 3, 5, 15\}$.

(c) $T(17) = \{1, 17\}$.

(d) $T(5) = \{1, 5\}$.

(e) $T(18) = \{1, 2, 3, 6, 9, 18\}$.

(f) $T(21) = \{1, 3, 7, 21\}$.

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

(b) $g(aba) = aba$, $g(bbab) = babb$, $g(b) = b$, $\text{range}(g) = S$.

§25 — one-to-one, Onto, and Inverse Functions

Epp 4th ed. pp. 397–416 · 5th ed. (metric) pp. 439–461. Lecture 19 (week 7).

Problems

1. Consider the function $f : \mathbb{Z} \to \mathbb{Z}$ defined by $f(n) = \left\lfloor \dfrac{1 - 6n}{3} \right\rfloor$.

(a) Is f one-to-one?

(b) Is f onto?

(c) Is f bijective?

(d) Prove or disprove that for all $m, n \in \mathbb{Z}$, we have $f(mn) = f(m)f(n)$.

2. Define the set $A = \{0, 1, 2, 3, 4\}$ and the functions $f : A \to A$ and $g : A \to A$ by

$$f(a) = (a + 4)^2 \pmod 5, \qquad g(a) = (a^2 + 3a + 1) \pmod 5.$$

Is $f = g$?

3. Consider the function $f : \mathbb{Z}^+ \times \mathbb{Z}^+ \to \mathbb{Z}^+$ defined by $f((m, n)) = 2^m 3^n$.

(a) Determine $f((3, 1))$.

(b) Determine the pre-image of $\{36\}$.

(c) Prove f is one-to-one.

4. Consider the function $f : \mathbb{R} \to \mathbb{Z}$ defined by $f(x) = \lfloor x^2 \rfloor$.

   (a) What is the image $f([-1, 1])$?

   (b) What is the preimage $f^{-1}(\{1\})$?

   (c) Is f one-to-one?

   (d) Is f onto?

   (e) Is f bijective?

Solutions

1. First, we note that, for $n \in \mathbb{Z}$,

$$f(n) = \left\lfloor \frac{1-6n}{3} \right\rfloor = \left\lfloor -2n + \frac{1}{3} \right\rfloor = -2n$$

   since $-2n \in \mathbb{Z}$ and $\frac{1}{3} \in [0, 1)$.

   (a) **Yes.** If $f(m) = f(n)$ then $-2m = -2n$, hence $m = n$. Therefore f is one-to-one.

   (b) **No.** Since $f(n) = -2n$ we see that f never maps to any odd integer; for example, there is no integer w with $f(w) = 1$. Therefore f is not onto.

   (c) **No**, f is not a bijection. (It is injective but not surjective.)

   (d) This is **false**; take $m = n = 1$. Then $f(mn) = -2$ but $f(m)f(n) = 4$.

2. **Yes.** First note f and g have the same domain and codomain. This means we just need to show $f(a) = g(a)$ for all $a \in A$. Notice that we have

$$(a+4)^2 = a^2 + 8a + 16 \equiv a^2 + 3a + 1 \pmod 5,$$

   so $f(a) = g(a)$ for all $a \in A$, and hence $f = g$.

3. (a) $f((3, 1)) = 2^3 3^1 = 24$.

   (b) $36 = 2^2 3^2$, so $f((m, n)) = 36$ if and only if $(m, n) = (2, 2)$. Hence $f^{-1}(\{36\}) = \{(2, 2)\}$.

   (c) If $f((m, n)) = f((m', n'))$, then $2^m 3^n = 2^{m'} 3^{n'}$, so $2^{m-m'} = 3^{n'-n}$. By unique prime factorisation, this forces $m - m' = 0$ and $n' - n = 0$. That is, $m = m'$ and $n = n'$, and hence $(m, n) = (m', n')$. So f is one-to-one.

4. (a) Note that if $x \in [-1, 1]$ then $x^2 \in [0, 1]$. This means we have $\lfloor x^2 \rfloor \in \{0, 1\}$. Both values occur because $\lfloor 0^2 \rfloor = 0$ and $\lfloor 1^2 \rfloor = 1$. Thus $f([-1, 1]) = \{0, 1\}$.

(b) $f^{-1}(\{1\}) = \{x \in \mathbb{R} : 1 \leq x^2 < 2\} = (-\sqrt{2}, -1] \cup [1, \sqrt{2})$.

(c) **No**, f is not one-to-one. For example, $f\left(\frac{1}{2}\right) = 0 = f\left(-\frac{1}{2}\right)$ but $\frac{1}{2} \neq -\frac{1}{2}$.

(d) **No**, f is not onto since $f(x) = \lfloor x^2 \rfloor \geq 0$ for all x. This means, for instance, that -1 is not in the image of f.

(e) **No**, f is not bijective.

§26 — Composition of Functions

Epp 4th ed. pp. 416–427 · 5th ed. (metric) pp. 461–472. Lecture 20 (week 7).

Problems

1. Let $f, g : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = x^3 - 1$ and $g(x) = x + 5$.

   (a) Determine the functions $(g \circ f)(x)$ and $(f \circ g)(x)$.

   (b) Is $g \circ f$ a bijection?

2. Define $f : \mathbb{Q} \to \mathbb{Z}$ by $f(x) = 2\lfloor x + 1 \rfloor$.

   (a) What is the range of f?

   (b) Is f one-to-one?

   (c) Is f onto?

   (d) Define $g : \mathbb{Z} \to \mathbb{Z}$ by $g(x) = 2x - 1$. Determine the composition $(g \circ f)(x)$.

   (e) Calculate $(g \circ f)\left(-\frac{3}{4}\right)$.

   (f) What is the range of $g \circ f$?

3. Let f and g be functions. Prove or disprove the following statements:

   (a) If f and $f \circ g$ are one-to-one, then g is one-to-one.

   (b) If f and $f \circ g$ are onto, then g is onto.

Solutions

1. (a) We have

$$(g \circ f)(x) = g(x^3 - 1) = x^3 + 4$$

and

$$(f \circ g)(x) = f(x + 5) = (x + 5)^3 - 1 = x^3 + 15x^2 + 75x + 124.$$

(b) **No**, $g \circ f$ is not a bijection. The map $x \mapsto x^3 + 4$ is one-to-one on $\mathbb{Z}$, but it is not onto (e.g. 0 is not in its image since $x^3 = -4$ has no integer solution).

2. (a) The range is a subset of the even integers because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. If $2m$ is an even integer then $f(m - 1) = 2\lfloor m - 1 + 1 \rfloor = 2m$, so the range is the set of all even integers.

(b) **No**, f is not one-to-one. For example,

$$f(0) = 2\lfloor 0 + 1 \rfloor = 2\lfloor 1 \rfloor = 2 \times 1 = 2, \quad \text{and}$$
$$f\left(\tfrac{1}{2}\right) = 2\left\lfloor \tfrac{1}{2} + 1 \right\rfloor = 2\left\lfloor \tfrac{3}{2} \right\rfloor = 2 \times 1 = 2,$$

but $0 \neq \frac{1}{2}$.

(c) **No**, f is not onto since $\text{range}(f) \neq \mathbb{Z}$ (e.g. there is no $x \in \mathbb{Q}$ such that $f(x) = 1$ because 1 is odd).

(d) We have

$$(g \circ f)(x) = g(f(x)) = 2(2\lfloor x + 1 \rfloor) - 1 = 4\lfloor x + 1 \rfloor - 1.$$

(e) We have

$$(g \circ f)\left(-\frac{3}{4}\right) = 4 \cdot 0 - 1 = -1.$$

(f) The range is a subset of $\{4n - 1 \mid n \in \mathbb{Z}\}$ because $\lfloor x + 1 \rfloor \in \mathbb{Z}$. This *is* the range because, given an integer $4n - 1$, we have $f(n - 1) = 4\lfloor n - 1 + 1 \rfloor - 1 = 4n - 1$. Note that you can also write the range as $\{n \in \mathbb{Z} \mid n \equiv -1 \pmod 4\}$ which is the same as $\{n \in \mathbb{Z} \mid n \equiv 3 \pmod 4\}$.

3. (a) The statement is **true**.

Proof. Suppose that f and $f \circ g$ are one-to-one functions. Suppose for a contradiction that g is not one-to-one. Thus there exist two distinct elements in the domain of g, say x_1 and x_2, for which $g(x_1) = g(x_2)$. Let $g(x_1) = y = g(x_2)$. Thus $f(g(x_1)) = f(y) = f(g(x_2))$, but $x_1 \neq x_2$, which contradicts the fact that $f \circ g$ is one-to-one. Therefore g must be one-to-one. □

(b) The statement is **false**.

Counterexample. Consider the functions $g : \{1\} \to \{2, 3\}$ defined by $g(1) = 2$, and $f : \{2, 3\} \to \{4\}$ defined by $f(2) = 4$ and $f(3) = 4$. Then f is onto, and $f \circ g$ is onto (since $f \circ g : \{1\} \to \{4\}$ and $f(g(1)) = 4$). However, g is not onto. □

§27 — Cardinalities

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 21 (week 8).

Problems

1. Let $A = \{-2, -1, 0, 1\}$ and $B = \{3, 4, 5, 6\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.
2. Prove that $|\{1, 2, 3\}| \leq |\mathbb{Z}|$ by providing an appropriate injective (one-to-one) function.
3. Consider the intervals

$$[6, 12] = \{x \in \mathbb{R} \mid 6 \leq x \leq 12\} \quad \text{and} \quad (6, 12) = \{x \in \mathbb{R} \mid 6 < x < 12\}.$$

   Prove that $|[6, 12]| \leq |(6, 12)|$ by providing an appropriate injective (one-to-one) function.
4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$. Prove that $|A| = |B|$ by providing a bijection between A and B.

Solutions

1. Define the function $f : A \to B$ by

$$f(-2) = 3, \qquad f(-1) = 4, \qquad f(0) = 5, \qquad f(1) = 6.$$

   Then f is bijective, hence $|A| = |B|$.
2. Define the function $g : \{1, 2, 3\} \to \mathbb{Z}$ by $g(1) = 1$, $g(2) = 2$, and $g(3) = 3$. Then g is injective (one-to-one), so $|\{1, 2, 3\}| \leq |\mathbb{Z}|$.

3. Define $h : [6, 12] \to (6, 12)$ by

$$h(x) = \frac{x}{2} + 4.$$

For each $x \in [6, 12]$ we have

$$\begin{aligned} \frac{6}{2} + 4 \leq h(x) &\leq \frac{12}{2} + 4 \\ 7 \leq h(x) &\leq 10. \end{aligned}$$

Thus h is indeed a function from $[6, 12]$ to $(6, 12)$, and h has range $[7, 10] \subseteq (6, 12)$.

Suppose $x, y \in [6, 12]$ and $h(x) = h(y)$. Then $\frac{x}{2} + 4 = \frac{y}{2} + 4$, so $x = y$. Therefore h is injective (one-to-one).

Thus $|[6, 12]| \leq |(6, 12)|$.

4. Let $A = \{x \in \mathbb{R} \mid -1 \leq x \leq 1\}$ and $B = \{x \in \mathbb{R} \mid 3 \leq x \leq 7\}$.

Consider the function $f : A \to B$ where $f(x) = 2x + 5$. Since $x \geq -1$, $f(x) = 2x + 5 \geq 2(-1) + 5 = 3$, and since $x \leq 1$, $f(x) = 2x + 5 \leq 2(1) + 5 = 7$. Also each value of x gives a unique value of $2x + 5$. Thus f is a function with the correct domain and codomain.

We now prove that f is one-to-one. Suppose that $x_1, x_2 \in A$ and $f(x_1) = f(x_2)$. Thus $2x_1 + 5 = 2x_2 + 5$, and so $x_1 = x_2$. Thus f is one-to-one.

We now prove that f is onto. Suppose $y \in [3, 7]$. Let $x = \frac{y-5}{2}$. Since $y \leq 7$, we have $x \leq 1$ and since $y \geq 3$, we have $x \geq -1$. So $x \in [-1, 1]$. Furthermore $f(x) = f\left(\frac{y-5}{2}\right) = 2\left(\frac{y-5}{2}\right) + 5 = y - 5 + 5 = y$. Thus f is onto.

Hence f is a bijection and so $|A| = |B|$.

§28 — Countable and Uncountable Sets

Epp 4th ed. pp. 428–441 · 5th ed. (metric) pp. 473–486. Lecture 22 (week 8).

Note that this content will not be assessed in MATH1061.

Problems

1. Determine whether each of the following sets is countable or uncountable.
   (a) $\{1, 2, \ldots, n\}$.
   (b) $\mathbb{Z} \times \mathbb{Z}$.
   (c) $\mathbb{Q} \times \mathbb{Q}$.
   (d) $\mathbb{Z} \times \mathbb{Z} \times \cdots$ (infinitely many copies of $\mathbb{Z}$).
2. (a) Is $|\mathbb{Z}| = |\mathbb{Q}|$?
   (b) Is $|\mathbb{Z}| = |\mathbb{Z} \times \mathbb{Z}|$?
   (c) Is $|\mathbb{R}| = |\mathbb{Q} \times \mathbb{Q}|$?
3. (a) Show that the union of a countable number of countable sets is countable.
   (b) Show that the set of all finite binary strings is countable.
   (c) Use (a) to show that the set of all irrational numbers is uncountable.

Solutions

1. (a) The set is **countable** because the function $f : \{1, 2, \ldots, n\} \to \mathbb{N}$ defined by $f(i) = i$ is injective.
   (b) The set $\mathbb{Z} \times \mathbb{Z}$ is **countable**. Define the function $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{N}$ by

$$f(a,b) = \begin{cases} 2^a 3^b, & a > 0,\ b > 0, \\ 5^{-a} 7^{-b}, & a < 0,\ b < 0, \\ 11^a 13^{-b}, & a > 0,\ b < 0, \\ 17^{-a} 19^b, & a < 0,\ b > 0, \\ 23^b, & a = 0,\ b > 0, \\ 29^a, & a > 0,\ b = 0, \\ 31^{-b}, & a = 0,\ b < 0, \\ 37^{-a}, & a < 0,\ b = 0, \\ 1, & (a,b) = (0,0). \end{cases}$$

   We claim f is injective. Suppose $f(a,b) = f(c,d)$. By unique prime factorisation, the set of primes dividing $f(a,b)$ and the set of primes dividing $f(c,d)$ must be equal. Hence (a,b) and (c,d) lie in the same case. Again, by unique prime factorisation, the corresponding exponents must agree, so $a = c$ and $b = d$. Therefore f is injective.

(c) The set $\mathbb{Q} \times \mathbb{Q}$ is **countable**. First define an injection $e : \mathbb{Z} \to \mathbb{N}$ by

$$e(z) = \begin{cases} 2z, & z \geq 0, \\ -2z - 1, & z < 0. \end{cases}$$

Next define an injection $c : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ by

$$c(m, n) = 2^m 3^n.$$

Write each rational in lowest terms with positive denominator: $x = \frac{p}{q}$, $y = \frac{r}{s}$ with $p, r \in \mathbb{Z}$ and $q, s \in \mathbb{N}$. Define $F : \mathbb{Q} \times \mathbb{Q} \to \mathbb{N}$ by

$$F\left(\frac{p}{q}, \frac{r}{s}\right) = 2^{\,c(e(p),\, q)}\, 3^{\,c(e(r),\, s)}.$$

If $F\left(\frac{p}{q}, \frac{r}{s}\right) = F\left(\frac{p'}{q'}, \frac{r'}{s'}\right)$, then by unique prime factorisation we get $c(e(p), q) = c(e(p'), q')$ and $c(e(r), s) = c(e(r'), s')$. Since c is injective, we have $e(p) = e(p')$, $q = q'$, $e(r) = e(r')$, $s = s'$. Moreover, since e is injective, we have $p = p'$ and $r = r'$. Therefore $\frac{p}{q} = \frac{p'}{q'}$ and $\frac{r}{s} = \frac{r'}{s'}$, so F is injective.

(d) The set $\mathbb{Z} \times \mathbb{Z} \times ...$ is **not countable**. We will prove this by giving an injection $\mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$.

For each $x \in \mathbb{R}$, write $x = n + r$ with $n = \lfloor x \rfloor \in \mathbb{Z}$ and $r \in [0, 1)$. Choose the unique decimal expansion of r that does not end with an infinite tail of 9's. Write this decimal expansion as

$$r = 0.d_1 d_2 d_3 \cdots, \qquad d_k \in \{0, 1, \ldots, 9\}.$$

Then define the function $\iota : \mathbb{R} \to \mathbb{Z} \times \mathbb{Z} \times \cdots$ by

$$\iota(x) = (n, d_1, d_2, d_3, \ldots) \in \mathbb{Z} \times \mathbb{Z} \times \cdots.$$

This is injective; if $\iota(x) = \iota(y)$ then the decimals of x and y are equal, so $x = y$.

2. (a) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Q}$ are countable and infinite.

   (b) **Yes.** Both $\mathbb{Z}$ and $\mathbb{Z} \times \mathbb{Z}$ are countable and infinite.

   (c) **No.** $\mathbb{Q} \times \mathbb{Q}$ is countable, while $\mathbb{R}$ is uncountable.

3. (a) Let $A_1, A_2, A_3, ...$ be countable. Then for each n we can list A_n as

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

Now list the union by going along diagonals:

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

Every element of every A_n appears somewhere in this list, so $\bigcup_{n=1}^{\infty} A_n$ can be listed in a sequence. Hence $\bigcup_{n=1}^{\infty} A_n$ is countable.

(b) Let B_n be the set of all binary strings of length n. Each B_n is finite (there are 2^n such strings), hence countable. Every finite binary string has some length, so

$$B = \{\text{all finite binary strings}\} = \bigcup_{n=0}^{\infty} B_n.$$

By (a), a countable union of countable sets is countable, so B is countable.

(c) Suppose, for contradiction, that the set of irrationals $\mathbb{R} \setminus \mathbb{Q}$ were countable. We already know $\mathbb{Q}$ is countable. Then by part (a),

$$\mathbb{R} = \mathbb{Q} \cup (\mathbb{R} \setminus \mathbb{Q})$$

would be a union of two countable sets, hence countable. But $\mathbb{R}$ is uncountable. This contradiction shows that $\mathbb{R} \setminus \mathbb{Q}$ is uncountable.

Application — Computability of Functions

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 170–177.*

An important application of the topic of countability to computer science is examining the **computability** of functions. In computer science, a function is **computable** if there is a computer program in some programming language that can find the values of the function. If there is no such program, we say the function is **uncomputable**.

Application problems

1. (a) Show the set of all computer programs in any given computer language is countable.

   Hint: a computer program written in a programming language can be thought of as a string of symbols from a finite alphabet.

   (b) Let T be the set of all functions from $\mathbb{Z}^+$ to the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Show that T is uncountable.

   Hint: start by finding an injection between the interval $(0, 1)$ *and a subset of* T*.*

   (c) Hence show that there are uncomputable functions.

Application solutions

1. (a) Given a computer language with a finite alphabet A, we let P be the set of all computer programs in the language. If P is finite, then it is countable and we are done, so assume P is infinite.

   Now we use the fact that we can think of each computer program as a series of strings made using the alphabet A. Consider all strings of length m made from alphabet A, and denote this set by A_m. It is easy to show that there are $|A|^m$ distinct strings of this type, and since A is finite, $|A|^m$ is also finite. Now P is a subset of $\bigcup_{i=1}^{\infty} A_m$. Since the union of a countable number of countable sets is also countable (see Question 3(a) from earlier in this section) it follows that $\bigcup_{i=1}^{\infty} A_m$ is countable and hence P is countable.

   (b) We use the hint and start by defining a function from $(0, 1)$ to T as follows. Recall that every real number in the interval $(0, 1)$ can be written in decimal notation as $0.a_1a_2a_3 \ldots a_n \ldots$ where each a_i is an integer from 0 to 9. Also recall that T is the set of all functions from $\mathbb{Z}^+$ to $\{0, 1, \ldots, 9\}$. Let $f : (0, 1) \to T$ be the function defined as

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

   where g is the function in T such that $g(n) = a_n$ for all $n \in \mathbb{Z}^+$.

   So for example, if $f(0.457013) = g$ then g is the function where $g(1) = 4$, $g(2) = 5$, $g(3) = 7$, $g(4) = 0$, $g(5) = 1$, $g(6) = 3$ and $g(n) = 0$ for all $n \geq 7$.

   Now we will prove that this function is one-to-one. Suppose that $f(x_1) = f(x_2)$ for $x_1, x_2 \in (0, 1)$. Then for these functions to be equal, they map every integer to the same value. For this to happen, every decimal digit of x_1 must be equal to the same decimal digit of x_2 and so we must have $x_1 = x_2$.

   Now denote the set of all outputs of f as S. Hence $S \subseteq T$. Now if we set the codomain of f to be S, which is the range of f, we have made this function surjective and hence a

bijection. This means that the subset $S \subseteq T$ is in bijection with the interval $(0, 1)$. Since the interval $(0, 1)$ is uncountable, we must have that S is also uncountable and since $S \subseteq T$, T must also be uncountable.

(c) Part (a) showed us that the set of all computer programs in a given language is countable. This means that there are a countable number of computable functions. However part (b) showed us that there is an uncountable number of functions in the set T, so we must have that some functions are uncomputable.

§29 — Relations on Sets

Epp 4th ed. pp. 442–449 · 5th ed. (metric) pp. 487–494. Lecture 23 (week 8).

Problems

1. Define a relation P on $\mathbb{Z}$ as follows: for every ordered pair $(m, n) \in \mathbb{Z} \times \mathbb{Z}$,

$$m \; P \; n \iff m \text{ and } n \text{ have a common prime factor.}$$

   (a) Is $15 \; P \; 25$?

   (b) Is $22 \; P \; 27$?

   (c) Is $0 \; P \; 5$?

   (d) Is $8 \; P \; 8$?

2. Let $X = \{a, b, c\}$. Define a relation S on the power set $\mathcal{P}(X)$ as follows: for all sets A and B in $\mathcal{P}(X)$,

$$A \; S \; B \iff A \text{ has the same number of elements as } B.$$

   (a) Is $\{a, b\} \; S \; \{b, c\}$?

   (b) Is $\{a\} \; S \; \{a, b\}$?

   (c) Is $\{c\} \; S \; \{b\}$?

3. Let $A = \{3, 4, 5\}$ and $B = \{4, 5, 6\}$ be sets. Let R be the 'divides' relation. That is, for every ordered pair (a, b) in $A \times B$, we have $a \; R \; b$ if and only if $a \mid b$. Draw an arrow diagram (i.e. the directed graph) of this relation.

Solutions

1. (a) **Yes**, since $15 = 3 \cdot 5$ and $25 = 5 \cdot 5$ share the prime factor 5.

   (b) **No**, since $22 = 2 \cdot 11$ and $27 = 3^3$ share no common prime factor.

   (c) **Yes**, since 0 is divisible by every prime; in particular $5 \mid 0$ and $5 \mid 5$, so 0 and 5 have a common prime factor.

   (d) **Yes**, since $8 = 2^3$ and 2 is a prime factor of 8 (so they share the prime factor 2).

2. (a) **Yes**, since $|\{a, b\}| = 2 = |\{b, c\}|$.

   (b) **No**, since $|\{a\}| = 1 \neq 2 = |\{a, b\}|$.

   (c) **Yes**, since $|\{c\}| = 1 = |\{b\}|$.

3. We have $A \times B = \{(3,4), (3,5), (3,6), (4,4), (4,5), (4,6), (5,4), (5,5), (5,6)\}$. The pairs (a, b) satisfying $a \mid b$ are

$$\{(3,6),\ (4,4),\ (5,5)\} \subseteq A \times B.$$

   So the directed graph has an arrow from 3 (in A) to 6 (in B), an arrow from 4 to 4, and an arrow from 5 to 5 — and no other arrows.

§30 — Reflexivity, Symmetry, Transitivity

Epp 4th ed. pp. 449–459 · 5th ed. (metric) pp. 495–505. Lecture 23 (week 8).

Problems

1. Let $X = \{1, 2, 3, 4, 5\}$ and consider the subset $R \subseteq X \times X$ given by

$$R = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,3), (3,4), (4,5), (5,1)\}.$$

   (a) Draw an arrow diagram for the binary relation R.

   (b) Draw an arrow diagram for the binary relation R^{-1}.

   (c) Draw an arrow diagram for the binary relation $R \cup R^{-1}$.

   (d) Is R symmetric? Is R^{-1} symmetric? Is $R \cup R^{-1}$ symmetric?

   (e) Is R transitive? Is R^{-1} transitive? Is $R \cup R^{-1}$ transitive?

2. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

- $(1, 2) \in R$
- $(2, 3) \in R$
- R is reflexive
- R is transitive

What is the minimum number of arrows required in an arrow diagram for a relation R that satisfies these criteria?

Solutions

1. (a) The arrow diagram for R has the five vertices $1, 2, 3, 4, 5$ drawn around a circle, with a **loop at every vertex** (from the pairs $(1, 1), \ldots, (5, 5)$) together with the directed 5-cycle

$$1 \to 2 \to 3 \to 4 \to 5 \to 1.$$

(b) The arrow diagram for R^{-1} is the same picture with every non-loop arrow reversed: a loop at every vertex, together with the directed 5-cycle

$$1 \to 5 \to 4 \to 3 \to 2 \to 1,$$

that is, $R^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (3, 2), (4, 3), (5, 4), (1, 5)\}$.

(c) The arrow diagram for $R \cup R^{-1}$ has a loop at every vertex and a **double-headed arrow** between each consecutive pair around the cycle — that is, both $(i, i + 1)$ and $(i + 1, i)$ for the cycle $1, 2, 3, 4, 5, 1$.

(d) R is **not** symmetric because $(1, 2) \in R$ but $(2, 1) \notin R$.

R^{-1} is **not** symmetric because $(2, 1) \in R^{-1}$ but $(1, 2) \notin R^{-1}$.

$R \cup R^{-1}$ **is** symmetric. If $(a, b) \in R \cup R^{-1}$ then $(a, b) \in R$ or $(a, b) \in R^{-1}$, which means $(b, a) \in R^{-1}$ or $(b, a) \in R$, and thus, in either case, $(b, a) \in R \cup R^{-1}$.

(e) R is **not** transitive because $(1, 2), (2, 3) \in R$ but $(1, 3) \notin R$.

R^{-1} is **not** transitive because $(3, 2), (2, 1) \in R^{-1}$ but $(3, 1) \notin R^{-1}$.

$R \cup R^{-1}$ is **not** transitive because $(1, 2), (2, 3) \in R \cup R^{-1}$ but $(1, 3) \notin R \cup R^{-1}$.

2. R is reflexive, so $(1,1),(2,2),(3,3) \in R$ — a loop on each point of the arrow diagram. We are also given $(1,2),(2,3) \in R$, and R is transitive, so $(1,3) \in R$. R is *not* required to be symmetric, so no further arrows are forced.

$$R = \{(1,1),(2,2),(3,3),(1,2),(2,3),(1,3)\}$$

So the **minimum number of arrows required is 6**.

§31 — Equivalence Relations

Epp 4th ed. pp. 459–478 · 5th ed. (metric) pp. 505–523. Lecture 24 (week 9).

Problems

1. Define the binary relations α, β and γ on $\mathbb{Z}$ as follows:

$$\begin{aligned} x\ \alpha\ y &\iff x+y \text{ is an even integer,} \\ x\ \beta\ y &\iff x \text{ is a multiple of } y, \\ x\ \gamma\ y &\iff 3 \text{ is a factor of } x^2-y^2. \end{aligned}$$

   (a) Fill in the table with 'Yes'/'No' to indicate the properties satisfied by each relation.

	α	β	γ
Reflexive			
Symmetric			
Transitive			
Equivalence relation			

   (b) For each equivalence relation, state its equivalence classes.

2. Let $A = \{a,b,c,d,e\}$ be a set and ρ be a binary relation defined by

$$\rho = \{(a,a),(a,b),(a,d),(b,b),(c,c),(d,d),(b,a),(d,a),(b,d),(d,b),(c,e),(e,c),(e,e)\}.$$

   For instance, $(a,b) \in \rho$ means $a\ \rho\ b$.

   (a) Draw the directed graph representing ρ.

   (b) Is ρ reflexive? Is ρ symmetric? Is ρ transitive?

(c) Is ρ an equivalence relation on A? If so, give its equivalence classes.

(d) What is the smallest subset τ of ρ which forms an equivalence relation on A?

(e) Give the equivalence classes for τ.

3. Consider a positive integer n and any set of strings S. Define a relation R_n on S by the condition $s\ R_n\ t$ if and only if $s = t$ or both s and t have at least n characters and the first n characters are the same. Show that R_n is an equivalence relation.

Solutions

1. (a)

	α	β	γ
Reflexive	Yes	Yes	Yes
Symmetric	Yes	No	Yes
Transitive	Yes	Yes	Yes
Equivalence relation	Yes	No	Yes

(b) The equivalence relations are α and γ.

For α, notice $x\ \alpha\ y \iff x + y$ is even $\iff x$ and y have the same parity. This means the equivalence classes are $\mathbb{Z}^{\text{even}}$ and $\mathbb{Z}^{\text{odd}}$.

For γ, notice $x\ \gamma\ y \iff 3 \mid (x^2 - y^2) \iff x^2 \equiv y^2 \pmod 3$. But modulo 3 the only possible square residues are

$$0^2 \equiv 0, \qquad 1^2 \equiv 1, \qquad 2^2 \equiv 1 \pmod 3.$$

Hence $x^2 \equiv 0 \pmod 3$ exactly when $3 \mid x$, and $x^2 \equiv 1 \pmod 3$ exactly when $3 \nmid x$. Therefore $x\ \gamma\ y$ iff either both x and y are multiples of 3, or neither is. So the equivalence classes are $\{n \in \mathbb{Z} : 3 \mid n\}$ and $\{n \in \mathbb{Z} : 3 \nmid n\}$. Note that another way to write the equivalence classes is $\{3n \mid n \in \mathbb{Z}\}$ and $\{3n + 1,\ 3n + 2 \mid n \in \mathbb{Z}\}$.

2. (a) A digraph for ρ (vertex set $A = \{a, b, c, d, e\}$) has a **loop at every vertex**, double-headed arrows between each pair of $\{a, b, d\}$ — that is between a and b, between a and d, and between b and d — and a double-headed arrow between c and e. There are no arrows between $\{a, b, d\}$ and $\{c, e\}$.

(b) ρ is **reflexive**: we have $(x, x) \in \rho$ for all $x \in A$ (loops on all vertices).

ρ is **symmetric**: whenever $(x, y) \in \rho$, we have $(y, x) \in \rho$ (no single-direction arrow between any two distinct vertices).

ρ is **transitive**: within $\{a, b, d\}$ all relations occur, within $\{c, e\}$ all relations occur, and there are no relations between $\{a, b, d\}$ and $\{c, e\}$. That is, whenever (x, y) and (y, z) are in ρ, then (x, z) is also in ρ (and $x = z$ is possible).

(c) **Yes**, ρ is an equivalence relation. Its equivalence classes are

$$[a] = [b] = [d] = \{a, b, d\}, \qquad [c] = [e] = \{c, e\}.$$

(d) An equivalence relation $\tau \subseteq \rho$ must be reflexive, so $(x, x) \in \tau$ for all $x \in A$. But notice if τ is the relation

$$\tau = \{(a, a), (b, b), (c, c), (d, d), (e, e)\}$$

then τ is an equivalence relation. Therefore this is the smallest relation which is an equivalence relation.

(e) The equivalence classes for τ are the singletons:

$$[a] = \{a\},\ [b] = \{b\},\ [c] = \{c\},\ [d] = \{d\},\ [e] = \{e\}.$$

3. Let S be any set of strings and fix $n \in \mathbb{Z}^+$.

   R_n **is reflexive:** for any $s \in S$, since $s = s$, by definition $s\ R_n\ s$.

   R_n **is symmetric:** let $s, t \in S$, and assume $s\ R_n\ t$. If $s = t$ then $t\ R_n\ s$; otherwise both s and t must have at least n characters and, since $s\ R_n\ t$, they must have the same first n characters, so $t\ R_n\ s$.

   R_n **is transitive:** let $s, t, u \in S$ and assume $s\ R_n\ t$ and $t\ R_n\ u$. Since $s\ R_n\ t$ we either have $s = t$, or s and t both have at least n characters and have the same first n characters. Similarly, since $t\ R_n\ u$, either $t = u$, or t and u both have at least n characters and have the same first n characters. Thus either $s = t = u$, or s and u both have at least n characters and they both share the first n characters with t (and hence each other). Thus $s\ R_n\ u$ and so R_n is transitive.

   Since R_n is reflexive, symmetric and transitive it is an equivalence relation. □

Application — Identifiers

Not assessable for MATH1061. Taken from K. Rosen, Discrete Mathematics and its Applications, *7th edition, 1991, pages 608–618.*

In the C programming language, an **identifier** is the name of a variable, a function or another type of entity.

Each identifier is a nonempty string of characters where each character is a lowercase or uppercase English letter, a digit, or an underscore.

There is no limit on the number of characters used in the identifier; however, for some compilers for some versions of C, there is a limit on the number of characters checked when two names are compared.

For example, Standard C compilers consider two identifiers the same when they agree in their first 31 characters. We see that two identifiers will be considered the same if and only if they are related under the relation R_n when $n = 31$ (defined in a previous question).

Application problems

1. Using R_{31} on the set of all possible identifiers, determine the equivalence classes of each of the following identifiers:

   (a) `file_1`

   (b) `Number_of_tropical_storms`

   (c) `Number_of_named_tropical_storms`

   (d) `Number_of_named_tropical_storms_in_the_Atlantic_in_2005`

Application solutions

1. Let I be the set of all possible identifiers (strings over letters, digits and underscores).

   (a) Since `file_1` has length $6 < 31$, its equivalence class is just

   $$[\texttt{file_1}]_{R_{31}} = \{\texttt{file_1}\}.$$

   (b) Since `Number_of_tropical_storms` has length $25 < 31$, its equivalence class is

   $$[\texttt{Number_of_tropical_storms}]_{R_{31}} = \{\texttt{Number_of_tropical_storms}\}.$$

(c) The identifier `Number_of_named_tropical_storms` has length exactly 31, so two identifiers are R_{31}-equivalent to it iff they have at least 31 characters and their first 31 characters equal this string. Hence

$$[\texttt{Number_of_named_tropical_storms}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 31 characters of} \\ t \text{ are } \texttt{Number_of_named_tropical_storms} \end{array} \right\}.$$

(d) The identifier `Number_of_named_tropical_storms_in_the_Atlantic_in_2005` begins with the same first 31 characters `Number_of_named_tropical_storms`, so it has the same R_{31}-equivalence class as in (c):

$$[\texttt{Number_of_named_tropical_storms_in_the_Atlantic_in_2005}]_{R_{31}} = \left\{ t \in I : \begin{array}{l} |t| \geq 31 \text{ and the first 3} \\ t \text{ are } \texttt{Number_of_name} \end{array} \right.$$

§32 — Partial Order Relations

Epp 4th ed. pp. 498–515 · 5th ed. (metric) pp. 546–563. Lecture 25 (week 9).

Problems

1. Let ρ be a relation on $\mathbb{Z}$ defined by $x \rho y$ if and only if $x^3 - 1 < y^3$.

   (a) Prove ρ is a partial order relation.

   (b) Is ρ a total order?

2. Let S be the set of binary strings of length 6. Define the **weight** of a binary string as the number of ones it contains. (For example, weight(110110) = 4.) Define a relation ρ on S by

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

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

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

3. Suppose R is a binary relation on the set $\{1, 2, 3\}$ such that:

   - $(2, 3) \in R$
   - $(3, 2) \in R$
   - $(1, 1) \notin R$

- R is transitive
- R is not symmetric
- R is not antisymmetric.

Draw an arrow diagram for the relation R.

Solutions

1. (a) To show that ρ is a partial order, we need to show that ρ is reflexive, antisymmetric and transitive.

   Reflexive: let $x \in \mathbb{Z}$. Then $x^3 - 1 < x^3$ and so $x \rho x$, so ρ is reflexive.

   Antisymmetric: suppose $x \rho y$ where $x \neq y$. (We must show that then $y \not\rho x$.) Now $x \rho y$ means that $x^3 - 1 < y^3$. And since $x \neq y$ we must have $x^3 < y^3$ and so $x^3 \leqslant y^3 - 1$. Hence $y^3 - 1 \not< x^3$ and so we do not have $y \rho x$. Therefore ρ is antisymmetric.

   Transitive: suppose that $x \rho y$ and $y \rho z$. Then we know that $x^3 - 1 < y^3$ and $y^3 - 1 < z^3$. So $x^3 - 1 \leqslant y^3 - 1 < z^3$, that is, $x^3 - 1 < z^3$ so that $x \rho z$, which means that ρ is transitive.

   Hence ρ is a partial order. □

   (b) To check whether ρ is a total order, let x and y be any two distinct integers. Then $x^3 \neq y^3$ and so either $x^3 < y^3$ or else $y^3 < x^3$.

   If $x^3 < y^3$ then $x^3 - 1 < y^3$ and so $x \rho y$.

   If $y^3 < x^3$ then $y^3 - 1 < x^3$ and so $y \rho x$.

   So for any integers $x \neq y$, we have either $x \rho y$ or else $y \rho x$. So any two integers are comparable under ρ. Hence ρ **is** a total order.

2. (a) It is **not an equivalence relation** because it is not symmetric. For instance, let $s = 000000$ and $t = 111111$. Then $\text{weight}(s) = 0 \leq 6 = \text{weight}(t)$, so $(s, t) \in \rho$, but $(t, s) \notin \rho$.

   (b) It is **not a partial order** because it is not antisymmetric. For instance, let $s = 100000$ and $t = 010000$. Then $\text{weight}(s) = \text{weight}(t) = 1$, so $s \rho t$ and $t \rho s$, but $s \neq t$.

3. One relation on $\{1, 2, 3\}$ satisfying all conditions is

$$R = \{(1, 2), (1, 3), (2, 2), (3, 3), (2, 3), (3, 2)\}.$$

(It contains $(2,3)$ and $(3,2)$; it is transitive; it is not symmetric since $(1,2) \in R$ but $(2,1) \notin R$; it is not antisymmetric since $2 \neq 3$ and $(2,3),(3,2) \in R$; and $(1,1) \notin R$.)

An arrow diagram for this R has vertices $1,2,3$ with: arrows $1 \to 2$ and $1 \to 3$; loops at 2 and at 3; and a double-headed arrow between 2 and 3. There is no loop at vertex 1.

§33 — Definitions and Examples of Groups

No relevant textbook pages. Lecture 26 (week 9).

Problems

1. Show $\mathbb{Z}_9 - \{0\} = \{1,2,3,\ldots,7,8\}$ is not a group under multiplication modulo 9.
2. Let G be the set of all odd integers. Define the binary operation $\star$ on G by

$$x \star y = x + y - 1.$$

   Show that $(G, \star)$ is an abelian group.
3. Show $\mathbb{Z}_9 - \{0,3,6\} = \{1,2,4,5,7,8\}$ is a group under multiplication modulo 9. Is the group abelian?
4. Define the group $H = \mathbb{Z}_5 - \{0\} = \{1,2,3,4\}$ under multiplication modulo 5. Write the Cayley table for H.
5. Define the group $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ under component-wise addition modulo 2. That is,

$$(a,b) + (c,d) = (a + c \bmod 2,\ b + d \bmod 2).$$

   Write the Cayley table for G.

Solutions

1. It is not a group under multiplication mod 9 because, for example, it is **not closed** ($3 \cdot 3 = 0 \notin \mathbb{Z}_9 - \{0\}$).

2. **Closure:** if x and y are odd, then $x+y$ is even, so $x+y-1$ is odd. Hence $x \star y \in G$.

   Associativity: for $x, y, z \in G$,

$$(x \star y) \star z = (x+y-1)+z-1 = x+y+z-2 = x+(y+z-1)-1 = x \star (y \star z).$$

   Commutativity: for $x, y \in G$,

$$x \star y = x+y-1 = y+x-1 = y \star x.$$

   Identity: we seek $e \in G$ such that $x \star e = x = e \star x$ for all x. Now the requirement $x \star e = x+e-1 = x$ implies that $e = 1$. Note 1 lies in G. Moreover, commutativity implies that $e \star x = x$ as well. Thus the identity is 1.

   Inverses: given $x \in G$, we want $y \in G$ with $x \star y = 1$. This means $x+y-1 = 1$, so $y = 2-x$. Since x is odd, $2-x$ is odd, hence $2-x \in G$. Thus the inverse of x is $x^{-1} = 2-x$.

   Therefore $(G, \star)$ is an abelian group. $\square$

3. **Closure:** if $a, b \in \{1,2,4,5,7,8\}$, then $3 \nmid a$ and $3 \nmid b$, hence $3 \nmid ab$, so $ab \not\equiv 0, 3, 6 \pmod 9$; thus $\{1,2,4,5,7,8\}$ is closed under multiplication modulo 9.

   Associativity and commutativity: normal multiplication between integers is associative and commutative, so multiplication modulo 9 in the set $\{1,2,4,5,7,8\}$ is also associative and commutative. This means the group **is abelian**.

   Identity: $1 \in G$ is the identity because $1 \cdot x \equiv x \pmod 9$.

   Inverse: every element has an inverse. We explicitly calculate the inverses:

$$\begin{aligned}
1^{-1} &= 1 \quad \text{because } 1 \cdot 1 \equiv 1 \pmod 9,\\
2^{-1} &= 5 \quad \text{because } 2 \cdot 5 = 10 \equiv 1 \pmod 9,\\
4^{-1} &= 7 \quad \text{because } 4 \cdot 7 = 28 \equiv 1 \pmod 9,\\
5^{-1} &= 2 \quad \text{because } 5 \cdot 2 = 10 \equiv 1 \pmod 9,\\
7^{-1} &= 4 \quad \text{because } 7 \cdot 4 = 28 \equiv 1 \pmod 9,\\
8^{-1} &= 8 \quad \text{because } 8 \cdot 8 = 64 \equiv 1 \pmod 9.
\end{aligned}$$

4. For $H = \mathbb{Z}_5 \setminus \{0\} = \{1,2,3,4\}$ under multiplication mod 5, the Cayley table is:

$\cdot$	1	2	3	4
1	1	2	3	4

$\cdot$	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

5. For $G = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0),(0,1),(1,0),(1,1)\}$ under componentwise addition mod 2, the Cayley table is:

$+$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(\mathbf{1},\mathbf{0})$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(\mathbf{1},\mathbf{1})$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

§34 — Elementary Properties of Groups

No relevant textbook pages. Lecture 27 (week 10).

Problems

1. Let $H = \{3n \mid n \in \mathbb{Z}\}$ be the set of multiples of 3. Prove H is a subgroup of $(\mathbb{Z}, +)$.
2. Fix elements g and h in a group G where e is the group identity. Prove the following statements:
   (a) If $g^{-1} = h$ then $h^{-1} = g$.
   (b) $(g^{-1})^{-1} = g$.
   (c) $(gh)^{-1} = h^{-1}g^{-1}$.
3. Prove $K = \{(0,0),(0,1),(2,0),(2,1)\}$ is a subgroup of $(\mathbb{Z}_4 \times \mathbb{Z}_2, +)$ where the group operation is componentwise addition:

$$(a,b) + (c,d) = (a + c \pmod 4,\ b + d \pmod 2).$$

4. Consider the group $(\mathbb{Z}_{11} - \{0\}, \cdot)$. Show that this group is cyclic.
   Hint: express every element of $\mathbb{Z}_{11} - \{0\}$ as a power of 2.

Solutions

1. First we note that $H \subseteq \mathbb{Z}$, and $H \neq \emptyset$.

   Closure: if $x, y \in H$ then $x = 3a$ and $y = 3b$ for some $a, b \in \mathbb{Z}$. Therefore $x + y = 3a + 3b = 3(a + b) \in H$.

   Identity: the identity of $(\mathbb{Z}, +)$ is 0, and since $0 = 3 \cdot 0$, we have $0 \in H$.

   Inverse: in $\mathbb{Z}$, the inverse of x is $-x$. In H, if $x \in H$ then $x = 3a$ for some $a \in \mathbb{Z}$. This means $-x = -3a = 3 \cdot (-a)$, and so $-x \in H$ also.

   Note that we do not need to check associativity for subgroups, since this property is automatically inherited from the parent group $(\mathbb{Z}, +)$. □

2. (a) Suppose $g^{-1} = h$. Now $gh = gg^{-1} = e$ and $hg = g^{-1}g = e$. Thus $h^{-1} = g$.

   (b) By definition, $gg^{-1} = e = g^{-1}g$, so $(g^{-1})^{-1} = g$.

   (c) Notice we have

   $$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = e$$

   and

   $$(h^{-1}g^{-1})(gh) = h^{-1}g^{-1}gh = e.$$

   This means $(gh)^{-1} = h^{-1}g^{-1}$.

3. We draw the Cayley table of $K = \{(0,0), (0,1), (2,0), (2,1)\}$ under componentwise addition in $\mathbb{Z}_4 \times \mathbb{Z}_2$:

$+$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{0})$	$(0,0)$	$(0,1)$	$(2,0)$	$(2,1)$
$(\mathbf{0},\mathbf{1})$	$(0,1)$	$(0,0)$	$(2,1)$	$(2,0)$
$(\mathbf{2},\mathbf{0})$	$(2,0)$	$(2,1)$	$(0,0)$	$(0,1)$
$(\mathbf{2},\mathbf{1})$	$(2,1)$	$(2,0)$	$(0,1)$	$(0,0)$

   Notice the operation is closed in K and every element of K has an inverse in K. Therefore K is a subgroup. □

4. Note that 2 is a generator of $(\mathbb{Z}_{11} - \{0\}, \cdot)$, so it is cyclic:

   $$1 = 2^0,\ 2 = 2^1,\ 4 = 2^2,\ 8 = 2^3,\ 5 = 2^4,\ 10 = 2^5,\ 9 = 2^6,\ 7 = 2^7,\ 3 = 2^8,\ 6 = 2^9.$$

§35 — Group Isomorphisms

No relevant textbook pages. No lecture in the published schedule — the Week 10 row jumps from L27 (V34) to L28 (V36).

This content is optional and will not be assessed. The source document carries no practice problems or solutions for this section.

§36 — Definitions and Examples of Fields

No relevant textbook pages. Lecture 28 (week 10).

Problems

1. (a) Solve $3x + 4 = 2$ in the field $(\mathbb{Z}_5, +, \cdot)$.
   (b) Solve $8x - 9 = 6$ in the field $(\mathbb{Z}_{11}, +, \cdot)$.
   (c) Solve $4(1 - x) = 10$ in the field $(\mathbb{Z}_{13}, +, \cdot)$.
   (d) Solve $16(x - 6) = 15$ in the field $(\mathbb{Z}_{19}, +, \cdot)$.
2. Prove $\mathbb{Z}_{12}$ with addition modulo 12 and multiplication modulo 12 is not a field.
3. Define addition and multiplication on $\mathbb{Q} \times \mathbb{Q}$ by

$$(a, b) + (c, d) = (a + c,\ b + d)$$

   and

$$(a, b) \cdot (c, d) = (ac + 3bd,\ ad + bc)$$

   for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$. Prove that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field.

Solutions

1. (a)

$$\begin{aligned} 3x + 4 &= 2 \\ \rightarrow 3x &= -2 \end{aligned}$$

Now, since $3 \times 2 = 6 \equiv 1 \pmod 5$, 2 is the multiplicative inverse of 3, and so we multiply both sides by 2 and obtain $x = -4$. That is, $x = 1$.

Check: $3 \cdot 1 + 4 = 7 \equiv 2 \pmod 5$.

(b)

$$\begin{aligned} 8x - 9 &= 6 \\ \rightarrow 8x &= 15 = 4 \end{aligned}$$

Now, since $8 \times 7 = 56 \equiv 1 \pmod{11}$, 7 is the multiplicative inverse of 8, and so we multiply both sides by 7 and obtain $x = 28$. That is, $x = 6$.

Check: $8 \cdot 6 - 9 = 39 \equiv 6 \pmod{11}$.

(c) Since $4 \times 10 = 40 \equiv 1 \pmod{13}$, 10 is the multiplicative inverse of 4, and so we multiply both sides by 10 and obtain $1 - x = 100 = 9$. That is, $x = 1 - 9 = 14 - 9 = 5$.

Check: $4(1 - 5) = -16 \equiv 10 \pmod{13}$.

(d) Since $16 \times 6 = 96 \equiv 1 \pmod{19}$, 6 is the multiplicative inverse of 16, and so we multiply both sides by 6 and obtain $x - 6 = 90 = 14$. That is, $x = 20 = 1$.

Check: $16(1 - 6) = -80 \equiv 15 \pmod{19}$.

2. $\mathbb{Z}_{12}$ is not a field because 2 has no multiplicative inverse modulo 12. Indeed $2 \cdot k \equiv 1 \pmod{12}$ has no solution since $2k$ is always even.

3. We show that $(\mathbb{Q} \times \mathbb{Q}, +, \cdot)$ is a field in three steps.

Step 1 — $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Closure: for all $(a, b), (c, d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a, b) + (c, d) = (a + c, b + d) \in \mathbb{Q} \times \mathbb{Q}$.

Associative: for all $(a, b), (c, d), (e, f) \in \mathbb{Q} \times \mathbb{Q}$ we have $\big((a, b) + (c, d)\big) + (e, f) = (a + c, b + d) + (e, f) = (a + c + e, b + d + f) = (a, b) + (c + e, d + f) = (a, b) + \big((c, d) + (e, f)\big)$.

Identity: for all $(a, b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a, b) + (0, 0) = (a + 0, b + 0) = (a, b) = (0 + a, 0 + b) = (0, 0) + (a, b)$.

Inverses: for all $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ we have $(a,b) + (-a,-b) = (a-a, b-b) = (0,0)$ and $(-a,-b) + (a,b) = (-a+a, -b+b) = (0,0)$. So $(-a,-b)$ is the inverse of (a,b).

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have $(a,b) + (c,d) = (a+c, b+d) = (c+a, d+b) = (c,d) + (a,b)$.

Thus $(\mathbb{Q} \times \mathbb{Q}, +)$ is an abelian group.

Step 2 — $((\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\},\ \cdot)$ is an abelian group.

Closure: for all $(a,b),(c,d) \in (\mathbb{Q}\times\mathbb{Q}) - \{(0,0)\}$, we have $(a,b)\cdot(c,d) = (ac+3bd, ad+bc) \in \mathbb{Q} \times \mathbb{Q}$. So we only need to show that $(ac+3bd, ad+bc) \neq (0,0)$. For a contradiction, suppose $(ac+3bd, ad+bc) = (0,0)$. That is, $ac+3bd = 0$ and $ad+bc = 0$. Multiplying the first equation by d and the second by c we obtain $acd + 3bd^2 = 0$ and $acd + bc^2 = 0$, from which it follows that $3bd^2 = bc^2$.

Now, if $b = 0$, then $ac = 0$, $ad = 0$ and $a \neq 0$, and so $c = d = 0$; a contradiction. Thus $b \neq 0$ and we have $3d^2 = c^2$. This is a contradiction because if $d = 0$, then $c \neq 0$ and the equation does not hold, and if $d \neq 0$, then we have $3 = \frac{c^2}{d^2}$, which implies $\sqrt{3} = \frac{c}{d}$ is rational. Thus $(ac+3bd, ad+bc) \neq (0,0)$ and we have closure.

Associative: for all $(a,b),(c,d),(e,f) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have

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

and

$$\begin{aligned}\big((a,b)\cdot(c,d)\big)\cdot(e,f) &= (ac+3bd,\ ad+bc)\cdot(e,f)\\ &= \big((ac+3bd)e+3(ad+bc)f,\ (ac+3bd)f+(ad+bc)e\big)\\ &= (ace+3bde+3adf+3bcf,\ acf+3bdf+ade+bce)\\ &= (ace+3adf+3bcf+3bde,\ acf+ade+bce+3bdf).\end{aligned}$$

Identity: for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$ we have $(a,b)\cdot(1,0) = (a,b)$ and $(1,0)\cdot(a,b) = (a,b)$, so $(1,0)$ is a multiplicative identity.

Commutativity: for all $(a,b),(c,d) \in \mathbb{Q} \times \mathbb{Q}$, we have

$$(a,b)\cdot(c,d) = (ac+3bd,\ ad+bc) = (ca+3db,\ cb+da) = (c,d)\cdot(a,b).$$

Inverses: we check that for all $(a,b) \in (\mathbb{Q} \times \mathbb{Q}) - \{(0,0)\}$,

$$(a,b)^{-1} = \left(\frac{a}{a^2-3b^2},\ \frac{-b}{a^2-3b^2}\right).$$

First, note that $a^2-3b^2 \neq 0$, because $a^2-3b^2=0$ implies either $(a,b)=(0,0)$ or $\sqrt{3}=\frac{a}{b}$, both of which are contradictions (the second because $\sqrt{3}$ is not rational). Thus $(a,b)^{-1} \in (\mathbb{Q}\times\mathbb{Q})-\{(0,0)\}$, and notice

$$\begin{aligned}(a,b)\cdot\left(\frac{a}{a^2-3b^2},\frac{-b}{a^2-3b^2}\right) &= \left(a\cdot\frac{a}{a^2-3b^2}+3b\cdot\frac{-b}{a^2-3b^2},\ a\cdot\frac{-b}{a^2-3b^2}+b\cdot\frac{a}{a^2-3b^2}\right)\\ &= \left(\frac{a^2-3b^2}{a^2-3b^2},\ \frac{-ab+ab}{a^2-3b^2}\right)\\ &= (1,0).\end{aligned}$$

So every nonzero element has an inverse. Thus $((\mathbb{Q}\times\mathbb{Q})-\{(0,0)\},\cdot)$ is an abelian group.

Step 3 — the distributive laws. For all $(a,b),(c,d),(e,f)\in\mathbb{Q}\times\mathbb{Q}$ we have

$$\begin{aligned}(a,b)\cdot((c,d)+(e,f)) &= (a,b)\cdot(c+e,\ d+f)\\ &= (a(c+e)+3b(d+f),\ a(d+f)+b(c+e))\\ &= ((ac+3bd)+(ae+3bf),\ (ad+bc)+(af+be))\\ &= (ac+3bd,\ ad+bc)+(ae+3bf,\ af+be)\\ &= (a,b)\cdot(c,d)+(a,b)\cdot(e,f)\end{aligned}$$

and (since we have already shown that multiplication and addition are commutative)

$$\begin{aligned}((a,b)+(c,d))\cdot(e,f) &= (e,f)\cdot((a,b)+(c,d))\\ &= (e,f)\cdot(a,b)+(e,f)\cdot(c,d) \quad \text{(by the first distributive law)}\\ &= (a,b)\cdot(e,f)+(c,d)\cdot(e,f).\end{aligned}$$

Thus $(\mathbb{Q}\times\mathbb{Q},+,\cdot)$ is a field. □

§37 — Introduction to Counting

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 29 (week 11).

Problems

1. The UQ drama club is auditioning for its annual production of *Romeo and Juliet*. Six people are auditioning for the role of Romeo, and eight other people are auditioning for the role of Juliet. In how many ways can the director cast the lead couple?
2. There are eleven questions on the final exam, but you decide — based on your successful grade for your in-semester exam — that you will only do five of them. How many combinations of questions are there which you could complete?
3. (a) How many permutations of $\{1, 2, \dots, 15\}$ start with an odd number?

   (b) How many 5-element subsets of $\{1, 2, \dots, 15\}$ contain exactly two numbers from $\{1, 2, 3, 4\}$?

Solutions

1. There are 6 choices for Romeo and 8 choices for Juliet, so $6 \cdot 8 = 48$ ways.
2. Since the order in which you do the 5 questions does not matter, there are $\binom{11}{5} = 462$ combinations of questions.
3. (a) There are 8 odd numbers in the set $\{1, \dots, 15\}$. Choose the first entry in 8 ways, then permute the remaining 14 numbers, so $8 \cdot 14!$ permutations.

   (b) We choose exactly 2 numbers from the set $\{1, 2, 3, 4\}$ and exactly 3 numbers from the remaining 11 numbers, so the number of subsets is

$$\binom{4}{2}\binom{11}{3}.$$

Application — Runtime

Not assessable for MATH1061. Taken from S. Epp, Discrete Mathematics with Applications, *5th edition, pages 787–799.*

In many algorithms, the runtime is well approximated by counting how many times the basic instructions are executed.

For programs with nested `for`-loops and no early exits, the total number of executions of the inner loop body equals the number of choices of the outer-loop index multiplied by the number of choices of the inner-loop index.

Concretely, if i runs through M values and, for each fixed i, the variable j runs through N values, then the inner loop body is executed exactly MN times.

Application problems

1. The following algorithms are written in pseudo-code and contain nested loops. For each algorithm, count the total number of iterations of the inner loop that the algorithm will run.

   (a)

```
for i := 1 to 30
    for j := 1 to 15
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (b)

```
for i := 5 to 50
    for j := 10 to 20
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

   (c) (Fix integers $a, b, c, d \in \mathbb{Z}^+$ with $a \leq b$ and $c \leq d$.)

```
for i := a to b
    for j := c to d
        [Statements in body of inner loop. None contain
         branching statements that lead outside the loop.]
    next j
next i
```

Application solutions

1. (a) $i = 1, \ldots, 30$ gives 30 iterations and $j = 1, \ldots, 15$ gives 15 iterations, so the inner loop runs $30 \cdot 15 = 450$ times.

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

   (c) $i = a, \ldots, b$ gives $b - a + 1$ iterations and $j = c, \ldots, d$ gives $d - c + 1$ iterations, so the inner loop runs $(b - a + 1)(d - c + 1)$ times.

§38 — Counting Selections

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 30 (week 11).

Problems

1. (a) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY?

   (b) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with R and end with P?

   (c) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that begin with I and end with Y?

   (d) How many distinct arrangements can be made from the letters of the word INDOOROOPILLY that have all four Os next to each other?

2. (a) How many distinct arrangements can be made of the letters of the word WOOLLOONGABBA?

   (b) How many distinct arrangements are there of the letters of the word WOOLLOONGABBA such that **exactly one** of the following is true?

   - The two As are not next to each other.
   - The two Bs are not next to each other.
   - The two Ls are not next to each other.

3. (a) How many one-to-one (injective) functions are there from $\{a, b, c\}$ to $\{1, 2, 3, 4, 5\}$?

   (b) How many onto (surjective) functions are there from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$?

Solutions

1. (a) There are 13 letters in INDOOROOPILLY, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!} = 64\,864\,800.$$

   (b) Fix R in the first position and P in the last position. There are 11 letters remaining, with four O's, two I's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!\,2!} = 415\,800.$$

(c) Fix I in the first position and Y in the last position. There are 11 letters remaining, with four O's, two L's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{11!}{4!\,2!} = 831\,600.$$

(d) Treat the four O's as one 'letter'. There are 10 'letters' with two I's, two L's, and the remaining 'letters' appearing once each. Therefore the number of distinct arrangements is

$$\frac{10!}{2!\,2!} = 907\,200.$$

2. (a) There are 13 letters in WOOLLOONGABBA, with four O's, two L's, two A's, two B's, and the remaining letters appearing once each. Therefore the number of distinct arrangements is

$$\frac{13!}{4!\,2!\,2!\,2!} = 32\,432\,400.$$

(b) We want exactly one of the pairs AA, BB, LL to be non-adjacent. That is, there are three cases to consider:

- **Case 1:** the two A's are not adjacent but BB and LL are adjacent.
- **Case 2:** the two B's are not adjacent but AA and LL are adjacent.
- **Case 3:** the two L's are not adjacent but AA and BB are adjacent.

Note that the number of ways Case 1 can occur is exactly the same as the number of ways Case 2 can occur (and similarly for Case 3).

To count the number of ways Case 1 can occur, we first count arrangements with BB adjacent and LL adjacent. Treat BB as one 'letter' and LL as one 'letter'. Then there are 11 'letters' (W, O, O, LL, O, O, N, G, A, BB, A) to arrange, with four O's, two A's, and the remaining 'letters' appearing once each. Therefore the number of such arrangements is

$$\frac{11!}{4!\,2!}.$$

In order to determine the number of these for which the two A's are not adjacent, we take this total and subtract those where AA is also adjacent. For this, treat AA, BB, and LL as 'letters'. Then there are 10 'letters' to arrange, with four O's and the remaining 'letters' appearing once each. Therefore the number of arrangements with AA adjacent and BB adjacent and LL adjacent is

$$\frac{10!}{4!}.$$

Hence, the number of ways that Case 1 can occur is

$$\frac{11!}{4!\,2!} - \frac{10!}{4!}.$$

Case 2 and Case 3 have exactly the same number of occurrences as Case 1. Also note that the three cases are mutually exclusive (you cannot have both Case 1 and Case 2 occurring at the same time, for example).

So the number of arrangements of the word WOOLLOONGABBA for which exactly one of the three cases occurs is

$$3\left(\frac{11!}{4!\,2!} - \frac{10!}{4!}\right).$$

3. (a) An injective function $f : \{a, b, c\} \to \{1, 2, 3, 4, 5\}$ is determined by choosing distinct images for a, b, c. The number of choices is

$$5 \cdot 4 \cdot 3 = {}^5P_3 = 60.$$

(b) The number of surjective functions $f : \{1, 2, 3, 4, 5\} \to \{a, b, c\}$ is the total number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ minus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ which are not surjective. The former number is 3^5. A function which is not surjective must have image of size 1 or 2.

- In the first case, there are 3 such functions (one for each of the three choices for the image).
- In the latter case, first choose which 2 elements of $\{a, b, c\}$ will be in the image. There are $\binom{3}{2}$ such choices. For this fixed two-element image, the number of functions with this image is

$$2^5 - 2,$$

since there are 2^5 total functions from a 5-element set to a 2-element set, and we subtract the 2 constant ones (which fall into the first case, having image of size 1). Thus the number of functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ with an image of size 2 is

$$\binom{3}{2}(2^5 - 2) = 3 \cdot 30 = 90.$$

This means there are 93 functions which are not surjective, so the number of surjective functions from $\{1, 2, 3, 4, 5\}$ to $\{a, b, c\}$ is

$$3^5 - 93 = 150.$$

§39 — Introduction to Probability

Epp 4th ed. pp. 516–553 · 5th ed. (metric) pp. 564–604. Lecture 31 (week 11).

Problems

1. To form a committee, five people are to be chosen from a group of ten people.
   (a) How many different committees of five can be chosen?
   (b) Amongst the ten people, we have Alice, Bob, Eve and Oscar. Alice and Bob are extremely talkative during meetings, and so at most one of these two can be chosen. Eve and Oscar are inseparable, and so a committee must either contain both of them or neither of them. With these constraints, how many different five-person committees can be formed?
   (c) What is the probability that none of Alice, Bob, Eve and Oscar are on a committee, given that a random committee of five is chosen subject to the constraints in part (b)?
2. (a) How many positive two-digit integers are multiples of 3?
   (b) What is the probability that a randomly chosen positive two-digit integer is a multiple of 3?
   (c) What is the probability that a randomly chosen positive two-digit integer is a multiple of 4?

Solutions

1. (a) Number of different committees of five is

$$\binom{10}{5} = \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{5 \cdot 4 \cdot 3 \cdot 2} = 252.$$

(b) Let A, B be Alice and Bob, and let E, O be Eve and Oscar. There are 6 other people. We split into cases.

Case 1: the committee contains both E and O. Then we choose 3 more people from the remaining 8 with the restriction that we cannot choose both A and B. There are $\binom{8}{3}$ ways to choose 3 more people from the remaining 8 to be on the committee; of these, there are $\binom{6}{1}$ ways in which both A and B are chosen (such a committee must have E, O, A, B so there is only one more person to choose from the remaining 6 people). Thus the number of committees for this case is

$$\binom{8}{3} - \binom{6}{1} = 56 - 6 = 50.$$

Case 2: the committee contains neither E nor O. Then we choose 5 people from the remaining 8, again not allowing both A and B. There are $\binom{8}{5}$ ways to choose 5 people from the remaining 8 people to be on the committee; of these, there are $\binom{6}{3}$ ways in which both A and B are chosen. Thus the number of committees for this case is

$$\binom{8}{5} - \binom{6}{3} = 56 - 20 = 36.$$

Hence the total number is $50 + 36 = 86$.

(c) To have none of Alice, Bob, Eve, or Oscar on the committee, we must choose all 5 members from the other 6 people, which can be done in $\binom{6}{5} = 6$ ways. Therefore the probability is

$$\frac{6}{86} = 0.069767\ldots$$

2. (a) The positive two-digit multiples of 3 occur as every third number from 12 to 99, so there are

$$\frac{99 - 12}{3} + 1 = 30$$

such numbers.

(b) There are 90 positive two-digit integers (9 choices for the first digit and 10 choices for the second digit). Thus, by part (a), the probability that a randomly selected positive two-digit number is a multiple of 3 is

$$\frac{30}{90} = \frac{1}{3}.$$

(c) The positive two-digit multiples of 4 occur as every fourth number from 12 to 96, so there are

$$\frac{96-12}{4} + 1 = 22$$

such numbers. Hence the probability that a randomly selected positive two-digit number is a multiple of 4 is

$$\frac{22}{90} = \frac{11}{45}.$$

§40 — Binomial Coefficients

Epp 4th ed. pp. 565–591 · 5th ed. (metric) pp. 617–641. Lecture 31 (week 11).

Problems

1. What is the coefficient of x^4 in $(2+3x)^7$?
2. (a) What is the coefficient of x^{12} in $(3-x^3)^6$?
   (b) What is the coefficient of x^8 in $(3-x^3)^6$?
3. What is the coefficient of x^2 in the expansion of $(3-x)^6$?
4. What is the coefficient of x^5 in the expansion of $(2x+1)^{20}$?
5. What is the coefficient of x^5 in the expansion of $\left(3x^2 - \dfrac{2}{x}\right)^7$?

Solutions

1. By the binomial theorem,

$$(2+3x)^7 = \sum_{k=0}^{7} \binom{7}{k} 2^{7-k}(3x)^k.$$

The term x^4 appears only when $k=4$. This term is $\binom{7}{4}2^3(3x)^4$. Therefore the coefficient of x^4 is

$$\binom{7}{4}2^3 3^4 = 35 \times 8 \times 81 = 22\,680.$$

2. By the binomial theorem,

$$(3-x^3)^6 = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-x^3)^k = \sum_{k=0}^{6} \binom{6}{k} 3^{6-k}(-1)^k x^{3k}.$$

(a) The term involving x^{12} is $\binom{6}{4}3^2(-1)^4 x^{3\cdot 4}$, so the coefficient of x^{12} is

$$15 \times 9 \times (-1)^4 = 135.$$

(b) Every power of x that appears is a multiple of 3. Since 8 is not a multiple of 3, there is no x^8 term, so the coefficient of x^8 is $\mathbf{0}$.

3. By the binomial theorem,

$$(3-x)^6 = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-x)^i = \sum_{i=0}^{6} \binom{6}{i} 3^{6-i}(-1)^i x^i.$$

The term x^2 appears only when $i=2$, so the coefficient of x^2 is

$$\binom{6}{2}3^{6-2}(-1)^2 = \binom{6}{2}3^4 = 1215.$$

4. By the binomial theorem,

$$(2x+1)^{20} = \sum_{k=0}^{20} \binom{20}{k} (2x)^{20-k}(1)^k.$$

The term x^5 appears only when $k = 15$, where the term is $\binom{20}{15}(2x)^5$, so the coefficient of x^5 is

$$\binom{20}{5} 2^5 = 496\,128.$$

5. By the binomial theorem,

$$\left(3x^2 - \frac{2}{x}\right)^7 = \sum_{i=0}^{7} \binom{7}{i} (3x^2)^{7-i} \left(-\frac{2}{x}\right)^i = \sum_{i=0}^{7} \binom{7}{i} 3^{7-i}(-2)^i x^{14-3i}.$$

The term x^5 appears only when $14 - 3i = 5$, i.e. $i = 3$. Therefore the coefficient of x^5 is

$$\binom{7}{3} 3^4(-2)^3 = -22\,680.$$

§41 — Inclusion Exclusion

Epp 4th ed. pp. 545–549 · 5th ed. (metric) pp. 595–599. Lecture 32 (week 12).

Problems

1. Out of 100 people surveyed, 40 people like apples, 50 like bananas and 40 like cherries. 15 like apples and bananas, 16 like bananas and cherries, 17 like cherries and apples and 10 people like all three. How many people do not like any of the three fruits?
2. How many integers between 1 and 600 inclusive are coprime with 15? That is, how many integers n satisfy $1 \leq n \leq 600$ and $\gcd(n, 15) = 1$?
3. Seven friends, named Alice, Bob, Charlie, Delia, Edward, Fred and George, stand in a line for a photograph. How many different arrangements are there of the seven friends standing in a line such that Alice is not next to Charlie and Bob is not next to Delia?

Solutions

1. Let A be the set of people who like apples, B the set of people who like bananas, and C the set of people who like cherries. We are given

$$|A| = 40,\ |B| = 50,\ |C| = 40, \quad |A \cap B| = 15,\ |B \cap C| = 16,\ |C \cap A| = 17, \quad |A \cap B \cap C| = 10.$$

   By inclusion–exclusion,

$$\begin{aligned} |A \cup B \cup C| &= |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \\ &= 40 + 50 + 40 - 15 - 17 - 16 + 10 \\ &= 92. \end{aligned}$$

   Hence the number of people who do not like any of the three fruits is

$$100 - |A \cup B \cup C| = 100 - 92 = 8.$$

2. Let $U = \{1, 2, \ldots, 600\}$. Define

$$A = \{n \in U : 3 \mid n\}, \qquad B = \{n \in U : 5 \mid n\}.$$

   Then n is not coprime to 15 if and only if $n \in A \cup B$. We have

$$|A| = \frac{600}{3} = 200, \qquad |B| = \frac{600}{5} = 120, \qquad |A \cap B| = \frac{600}{15} = 40.$$

   By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 200 + 120 - 40 = 280.$$

   Therefore the number of n with $\gcd(n, 15) = 1$ is

$$|U| - |A \cup B| = 600 - 280 = 320.$$

3. Let U be the set of all linear arrangements of the 7 friends, so $|U| = 7!$. Define

$$A = \{\text{arrangements in which Alice is next to Charlie}\},$$
$$B = \{\text{arrangements in which Bob is next to Delia}\}.$$

We want to count the number of arrangements in U which are neither in A nor in B. The required number is $|U \setminus (A \cup B)| = |U| - |A \cup B|$.

To count $|A|$, treat {Alice, Charlie} as a single block. There are 6! ways to arrange the 6 "objects", and for each of these there are 2 ways to order Alice and Charlie within their block (either Alice or Charlie to the left). Hence

$$|A| = 2 \cdot 6!.$$

Similarly, $|B| = 2 \cdot 6!$.

To count $|A \cap B|$, treat both pairs {Alice, Charlie} and {Bob, Delia} as two single blocks. There are 5! ways to arrange the 5 objects (two blocks plus the other three people), and for each of these there are $2 \cdot 2$ internal orders of the two blocks. Hence

$$|A \cap B| = 4 \cdot 5!.$$

By inclusion–exclusion,

$$|A \cup B| = |A| + |B| - |A \cap B| = 2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!.$$

Therefore

$$|U \setminus (A \cup B)| = 7! - (2 \cdot 6! + 2 \cdot 6! - 4 \cdot 5!) = 2640.$$

§42 — The Pigeonhole Principle

Epp 4th ed. pp. 554–565 · 5th ed. (metric) pp. 604–616. Lecture 33 (week 12).

Problems

1. (a) Explain why, in a group of 50 people, at least five people were born in the same month.

   (b) How many people do you need to ensure that at least seven people were born in the same month?

2. Show that, if we select six distinct integers from the set $\{1, 2, \ldots, 10\}$, two of these must add to give 11.

3. A computer network consists of six computers. Each computer is directly connected to zero or more of the other computers. Show that there are at least two computers in the network that are directly connected to the same number of other computers.

4. During a month with 30 days, a baseball team plays at least one game a day, but no more than 45 games. Show that there must be a period of some number of consecutive days during which the team must play exactly 14 games.

5. Let $S = \{1, 2, \ldots, 100\}$. What is the minimum number of integers you must pick from S to be sure that at least one pair has a difference which is divisible by 3?

Solutions

1. (a) There are 12 months (pigeonholes) and 50 people (pigeons). If each month had at most 4 birthdays, then there would be at most $12 \cdot 4 = 48$ people. Since $50 > 48$, by the pigeonhole principle some month must contain at least 5 people.

   (b) To guarantee at least 7 people are born in the same month, note that if each month had at most 6 birthdays, then there could be at most $12 \cdot 6 = 72$ people. Therefore with **73** people, by the pigeonhole principle some month has at least 7 people. Moreover, 72 people is not enough (take 6 born in each month), so the minimum is 73.

2. Partition $A = \{1, 2, \ldots, 10\}$ into the 5 pairs

$$\{1, 10\},\ \{2, 9\},\ \{3, 8\},\ \{4, 7\},\ \{5, 6\},$$

   each summing to 11. In order for a selection of distinct integers from the set A to **not** have two that add to give 11, at most one integer can be chosen from each of the subsets. Choosing 6 distinct integers from A forces us to select two numbers from the same pair (there are 5 pairs but 6 choices), by the pigeonhole principle. Those two numbers then add to 11.

3. For each computer, let its **degree** be the number of other computers it is directly connected to. With 6 computers, each degree is an integer in $\{0, 1, 2, 3, 4, 5\}$. It is impossible to have both a computer of degree 0 and a computer of degree 5 (if one is connected to everyone, then none has degree 0). Hence the degrees must all lie in one of the two 5-element sets

$$\{0, 1, 2, 3, 4\} \quad \text{or} \quad \{1, 2, 3, 4, 5\}.$$

So, in either case, there are only 5 possible degree values available for 6 computers. By the pigeonhole principle, at least two computers have the same degree, i.e. are connected to the same number of other computers.

4. Let g_i be the total number of games played in the first i days, for $i = 1, 2, \ldots, 30$. Then

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

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

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

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

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

all lying in the set $\{1, 2, \ldots, 59\}$ of size 59. By the pigeonhole principle, two of these 60 integers are equal. Since the g_i are strictly increasing, no equality can occur among the g_i themselves, and likewise no equality can occur among the $g_i + 14$ themselves. Therefore we must have

$$g_j = g_i + 14$$

for some $i, j \in \{1, \ldots, 30\}$. Then the number of games played from day $i + 1$ through day j is

$$g_j - g_i = 14,$$

so there is a period of consecutive days during which exactly 14 games are played.

5. First, we note that two integers have a difference that is divisible by 3 if and only if they are congruent modulo 3 (have the same remainder when divided by 3). Now, the set S can be partitioned into three sets based on their congruence class modulo 3. By the pigeonhole principle, if we select **4** numbers from S, at least two of them must belong to the same congruence class. These two will have difference that is divisible by 3. Note that 4 is the minimum number of selections that guarantees this, since it is possible to select 3 numbers where no two of them have difference divisible by 3 (select one from each congruence class).

§43 — Introduction to Graph Theory

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 33 (week 12).

Problems

1. For each of the following, state whether or not there exists a simple graph with the stated number of vertices and degrees. Draw the graph, or explain why one does not exist.
   (a) Five vertices with degrees 3, 3, 2, 2, 2.
   (b) Seven vertices with degrees 4, 2, 3, 1, 1, 1, 1.
   (c) Five vertices with degrees 5, 4, 3, 1, 1.
2. A graph has 10 edges and 6 vertices. Five of the vertices have degree 3. What is the degree of the remaining vertex?
3. Let n be a positive integer and let K_n be the complete graph with n vertices. How many edges does K_n have?
4. A graph has 27 edges and every vertex has degree 2, 3 or 4. If there are 7 vertices that have degree 4 and 4 vertices that have degree 3, then how many vertices of degree 2 are there?

Solutions

1. (a) **Yes**, such a simple graph exists. One drawing has vertices a, b, c, d, e and the six edges

$$ab, \quad ac, \quad ad, \quad bc, \quad be, \quad de,$$

giving $\deg(a) = 3$, $\deg(b) = 3$, $\deg(c) = 2$, $\deg(d) = 2$, $\deg(e) = 2$ as required.

   (b) **No** such graph exists. If the degrees are 4, 2, 3, 1, 1, 1, 1, then the sum of degrees is

$$4 + 2 + 3 + 1 + 1 + 1 + 1 = 13,$$

which is odd. Remember (by the Handshake Theorem) that the sum of the degrees in any graph equals twice the number of edges, and so is always even. So such a graph cannot exist.

(c) **No** such graph exists. In a simple graph on 5 vertices, the largest possible degree is 4, but the sequence contains a vertex of degree 5, which is impossible. So there is no such simple graph.

2. Since the graph has 10 edges, the sum of all the degrees is $2 \cdot 10 = 20$. If five vertices have degree 3, the sum of their degrees is $5 \cdot 3 = 15$, so the remaining vertex has degree

$$20 - 15 = 5.$$

3. In K_n, an edge is determined by choosing 2 distinct vertices, so the number of edges is

$$\binom{n}{2} = \frac{n(n-1)}{2}.$$

4. Let x be the number of vertices of degree 2. Since the graph has 27 edges, the sum of degrees is $2 \cdot 27 = 54$. Given that there are seven vertices of degree 4 and four vertices of degree 3, and all other vertices have degree 2, we have

$$2x + 4 \cdot 7 + 3 \cdot 4 = 54.$$

This means $x = 7$.

§44 — Walks, Trails and Circuits

Epp 4th ed. pp. 625–660 · 5th ed. (metric) pp. 677–697. Lecture 34 (week 12).

Problems

1. Let G and H be the graphs below.

   G has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is drawn with a **loop at** v_2, a **loop at** v_5, and **two parallel edges between** v_1 **and** v_2. Its degree sequence is

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   so G is connected with 10 edges.

   H has vertex set $\{v_1, v_2, v_3, v_4, v_5\}$ and is a simple connected graph drawn as the 4-cycle $v_1v_2v_3v_4v_1$ with a single pendant edge v_3v_5, giving degrees

   $$\deg(v_1) = 2, \quad \deg(v_2) = 2, \quad \deg(v_3) = 3, \quad \deg(v_4) = 2, \quad \deg(v_5) = 1.$$

   For each of the following statements, explain why it is true or false.

   (a) G is a simple graph.

   (b) The sum of the degrees of the vertices of G is 18.

   (c) G contains an Euler circuit.

   (d) H contains an Euler trail.

2. Does the following graph contain an Euler circuit? (The graph shown is connected and has exactly two vertices of degree 3.)

3. Let G be a simple, connected, Eulerian graph with eight vertices and let e be the number of edges in G. Prove that $8 \leq e \leq 24$.

Solutions

1. (a) This statement is **false**. The graph G has loops (at v_2 and v_5) and it also has multiple edges between v_1 and v_2, so G is not simple.

   (b) This statement is **false**. A loop contributes 2 to the degree, so we have

   $$\deg(v_1) = 4, \quad \deg(v_2) = 6, \quad \deg(v_3) = 4, \quad \deg(v_4) = 2, \quad \deg(v_5) = 4,$$

   and thus the sum of the degrees is $4 + 6 + 4 + 2 + 4 = 20 \neq 18$.

   (c) This statement is **true**. The graph G is connected and every vertex has even degree (as computed above), so G contains an Euler circuit.

(d) This statement is **true**. In H, the degrees are

$$\deg(v_1) = 2,\ \deg(v_2) = 2,\ \deg(v_4) = 2,\ \deg(v_3) = 3,\ \deg(v_5) = 1,$$

so exactly two vertices have odd degree (namely v_3 and v_5). Therefore H has an Euler trail (starting at one of v_3, v_5 and ending at the other).

2. **No.** The graph is connected, but has two vertices of degree 3, so not all vertices have even degree. Hence there is no Euler circuit.

3. Since G is connected and Eulerian, every vertex has even degree, and (because G is simple and connected with 8 vertices) each vertex has degree at least 2. Hence

$$2e = \sum_{v} \deg(v) \geq 8 \cdot 2 = 16,$$

so $e \geq 8$. Moreover, in a simple graph on 8 vertices we have $\deg(v) \leq 7$, and because G is Eulerian all degrees are even, so in fact $\deg(v) \leq 6$ for every vertex. Therefore

$$2e = \sum_{v} \deg(v) \leq 8 \cdot 6 = 48,$$

so $e \leq 24$. Hence $8 \leq e \leq 24$. □

§45 — Matrix Representations of Graphs

Epp 4th ed. pp. 661–675 · 5th ed. (metric) pp. 698–712. Lecture 35 (week 13).

Problems

1. Let G be the graph with vertex set $\{v_1, v_2, v_3, v_4\}$ and edge set $\{a, b, c, d, e, f\}$, where the edges are

edge	endpoints
a	$v_1 v_2$
b	$v_2 v_3$
c	$v_2 v_3$ (parallel to b)
d	$v_3 v_4$
e	$v_2 v_4$
f	loop at v_4

(a) Write down an adjacency matrix for G. Make sure you clearly label the rows and columns of your matrix.

(b) Write down an incidence matrix for G. Make sure you clearly label the rows and columns of your matrix.

(c) Does G have an Euler circuit? If yes, write it out as a sequence of vertices and edges. If not, determine the fewest number of edges that would need to be added to G to create a new graph that does have an Euler circuit.

2. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 3 \\ 1 & 0 & 2 & 0 & 0 \\ 0 & 2 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 3 & 0 & 1 & 1 & 0 \end{pmatrix}$$

(a) Draw the graph G.

(b) Explain whether or not G has an Euler circuit or an Euler trail.

3. Let G be the graph with the following adjacency matrix.

$$\begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Explain whether or not G is Eulerian.

Solutions

1. (a) The labelled adjacency matrix for G is

	v_1	v_2	v_3	v_4
$\mathbf{v_1}$	0	1	0	0
$\mathbf{v_2}$	1	0	2	1
$\mathbf{v_3}$	0	2	0	1
$\mathbf{v_4}$	0	1	1	1

(where the entry 1 on the diagonal at v_4 records the single loop at v_4).

(b) The labelled incidence matrix for G is

	a	b	c	d	e	f
$\mathbf{v_1}$	1	0	0	0	0	0
$\mathbf{v_2}$	1	1	1	0	1	0
$\mathbf{v_3}$	0	1	1	1	0	0
$\mathbf{v_4}$	0	0	0	1	1	2

(where the entry 2 in the bottom right indicates the loop that is incident twice with v_4).

(c) The degrees are

$$\deg(v_1) = 1, \quad \deg(v_2) = 4, \quad \deg(v_3) = 3, \quad \deg(v_4) = 4,$$

so G does **not** have an Euler circuit (since v_1 and v_3 have odd degree).

The fewest edges to add to make all degrees even is **1**; for example, adding an edge g between vertices v_1 and v_3 creates a new connected graph in which all of the vertices have even degree.

An example of an Euler circuit in the new graph is

$$v_1,\ a,\ v_2,\ b,\ v_3,\ d,\ v_4,\ f,\ v_4,\ e,\ v_2,\ c,\ v_3,\ g,\ v_1.$$

2. (a) Reading the matrix off (with vertices $v_1, \ldots, v_5$ in matrix order), G has the edges

- v_1v_2 — a single edge,
- v_1v_5 — **three** parallel edges,
- v_2v_3 — **two** parallel edges,
- v_3v_4 — a single edge,
- v_3v_5 — a single edge,
- v_4v_5 — a single edge.

(b) The degrees are

$$\deg(v_1) = 4,\ \deg(v_2) = 3,\ \deg(v_3) = 4,\ \deg(v_4) = 2,\ \deg(v_5) = 5,$$

so there is **no Euler circuit** (since v_2 and v_5 have odd degree), but there **is an Euler trail** (exactly two odd-degree vertices) from v_2 to v_5.

3. Let the vertices be $v_1, v_2, v_3, v_4, v_5, v_6$ in the order of the matrix. Reading the matrix off, G has edges

$$v_1v_2, \quad v_1v_4, \quad v_2v_4, \quad v_3v_5, \quad v_3v_6, \quad v_5v_6,$$

that is, two disjoint triangles: one on $\{v_1, v_2, v_4\}$ and one on $\{v_3, v_5, v_6\}$.

The graph is **not connected** (e.g. there is no walk from vertex v_1 to vertex v_3). Hence G is not Eulerian.

(Errata note: the source document's solution to 1(b) was corrected on 11 August 2026 — the note in brackets had previously copied the note from 1(a). The corrected note is the one given above.)

§46 — Trees

Epp 4th ed. pp. 683–701 · 5th ed. (metric) pp. 720–742. Lecture 36 (week 13).

Problems

1. A tree has 11 vertices, of which exactly four vertices have degree 1 and exactly one vertex has degree 4. Determine the degrees of the remaining six vertices.
2. Let T be a tree with p vertices, where $p \geq 11$. Suppose T has precisely six vertices of degree 1 and precisely four vertices of degree 3. Determine the degree of each of the remaining $p - 10$ vertices of T.
3. Let T be a tree on 12 vertices. Suppose T has exactly three vertices of degree 3 and each of the remaining vertices has degree 1 or 5. Using theorems that were given in lectures, determine the number of vertices of degree 5.
4. Two trees with the same vertex set $\{1, 2, \ldots, n\}$ are **distinct** if their edge sets are not equal. Use mathematical induction to prove that for each integer $n \geq 2$, the number of distinct trees with vertex set $\{1, 2, \ldots, n\}$ is at least $(n-1)!$.

Solutions

1. A tree with 11 vertices has $e = 10$ edges, so by the Handshake Theorem, the sum of degrees is $2e = 20$. We are given that exactly four vertices have degree 1 and exactly one vertex has degree 4. Let $v_1, v_2, \ldots, v_6$ be the remaining vertices whose degrees are to be determined. We have

$$\sum_{i=1}^{6} \deg(v_i) + 4 \cdot 1 + 1 \cdot 4 = 20$$

$$\sum_{i=1}^{6} \deg(v_i) = 12.$$

None of these six vertices $v_1, v_2, \ldots, v_6$ can have degree 1 (since there are exactly four vertices of degree 1, already accounted for). Hence each has degree at least 2. Because six vertices of degree at least 2 have total degree 12, each must have degree exactly 2.

Thus the remaining six vertices all have **degree 2**.

2. T is a tree with p vertices and so must have $p-1$ edges. Now by the Handshake Theorem we know

$$2(p-1) = \sum_{i=1}^{p} \deg(v_i).$$

Using the known degrees we can write this as

$$\begin{aligned} 2(p-1) &= 6 \cdot 1 + 4 \cdot 3 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-1) &= 18 + \sum_{i=1}^{p-10} \deg(v_i) \\ 2p - 2 - 18 &= \sum_{i=1}^{p-10} \deg(v_i) \\ 2(p-10) &= \sum_{i=1}^{p-10} \deg(v_i). \end{aligned}$$

Rewriting the final line as

$$\frac{\sum_{i=1}^{p-10} \deg(v_i)}{p-10} = 2, \qquad \text{i.e.} \qquad \frac{\deg(v_1) + \deg(v_2) + \cdots + \deg(v_{p-10})}{p-10} = 2,$$

we see that the average degree of the remaining $p-10$ vertices is 2. However, we know that there are no more vertices of degree 1. Thus each of the remaining $p-10$ vertices must have **degree exactly 2**.

3. Let x be the number of vertices of degree 5 and y the number of vertices of degree 1. Then, because the tree has 12 vertices, we have

$$x + y + 3 = 12.$$

This simplifies to give $x + y = 9$.

Now, since T is a tree on 12 vertices, it must have $e = 11$ edges. By the Handshake Theorem, the sum of degrees is $2e = 22$, so

$$3 \cdot 3 + 5x + 1 \cdot y = 22.$$

This simplifies to give $5x + y = 13$.

Subtracting $x + y = 9$ from $5x + y = 13$ gives $4x = 4$, hence $x = 1$. Therefore there is exactly **one** vertex of degree 5.

4. We prove by induction that the number of distinct trees with vertex set $\{1, 2, \dots, n\}$ is at least $(n-1)!$.

Basis: let $n = 2$. Here $(n-1)! = (2-1)! = 1$. There is exactly one tree on $\{1, 2\}$, namely the single edge $\{1, 2\}$. So the base case is true.

Inductive hypothesis. Suppose $k \geq 2$ is an integer and there are at least $(k-1)!$ distinct trees on $\{1, 2, \dots, k\}$.

Now consider $n = k + 1$. We aim to show that there are at least $k!$ distinct trees on vertex set $\{1, 2, \dots, k, k+1\}$.

Let T be a tree on vertex set $\{1, 2, \dots, k\}$. For any choice of $m \in \{1, 2, \dots, k\}$, we form a graph T_m on vertex set $\{1, 2, \dots, k, k+1\}$ as follows: start with tree T, add a new vertex $k+1$, and the edge $\{k+1, m\}$.

Note that T_m is connected (since $k+1$ is joined to m, and T was connected). Also, T_m has no circuit because T is a tree and adding a new leaf does not create a circuit. Thus T_m is a tree. Moreover, different choices of m give rise to distinct trees T_m, because their edge sets are different.

By the inductive hypothesis, there are at least $(k-1)!$ choices for the tree T. Since there are k choices for the vertex m, there are at least $k \cdot (k-1)! = k!$ trees T_m on vertex set $\{1, 2, \dots, k+1\}$.

By the principle of mathematical induction, this completes the proof. $\square$

See also

- math1061[142] — assessment weights and the full lecture schedule
- Logic: logical-connectives[143] · logical-equivalence-laws[144] · conditional-statements[145] · valid-argument-forms[146] · determining-argument-validity[147] · quantified-statements[148]
- Number theory and proof: proof-techniques[149] · rational-and-irrational-numbers[150] · divisibility-and-factorisation[151] · modular-arithmetic[152] · gcd-lcm-and-euclidean-algorithm[153]
- Graph theory (§43–§46): graphs[154] · walks-trails-and-circuits[155] · euler-circuits-and-trails[156] · adjacency-matrices[157] · incidence-matrices[158] · trees[159]

Recursive Definitions

Defining a sequence, or a set, by saying how to build its members out of members you already have. See sequences-and-summations[160] for the other ways to define a sequence, and strong-induction-and-the-well-ordering-principle[161] for the proof method that recursive definitions almost always call for.

Recursively defined sequences

To define a sequence recursively, two things are needed:

1. **Initial conditions** — the values of some number of initial terms of the sequence.
2. **A recurrence relation** — a formula specifying how to calculate the value of a term of the sequence from the values of one or more previous terms.

[142] courses/math1061/math1061.pdf
[143] courses/math1061/logical-connectives.pdf
[144] courses/math1061/logical-equivalence-laws.pdf
[145] courses/math1061/conditional-statements.pdf
[146] courses/math1061/valid-argument-forms.pdf
[147] courses/math1061/determining-argument-validity.pdf
[148] courses/math1061/quantified-statements.pdf
[149] courses/math1061/proof-techniques.pdf
[150] courses/math1061/rational-and-irrational-numbers.pdf
[151] courses/math1061/divisibility-and-factorisation.pdf
[152] courses/math1061/modular-arithmetic.pdf
[153] courses/math1061/gcd-lcm-and-euclidean-algorithm.pdf
[154] courses/math1061/graphs.pdf
[155] courses/math1061/walks-trails-and-circuits.pdf
[156] courses/math1061/euler-circuits-and-trails.pdf
[157] courses/math1061/adjacency-matrices.pdf
[158] courses/math1061/incidence-matrices.pdf
[159] courses/math1061/trees.pdf
[160] courses/math1061/sequences-and-summations.pdf
[161] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

Neither half is optional, and **the same recurrence relation with different initial conditions can give a completely different sequence**:

Definition	Sequence
$a_1 = 2$ and $a_k = 3a_{k-1}$ for each integer $k \geq 2$	$2, 6, 18, 54, ...$
$b_1 = 7$ and $b_k = 3b_{k-1}$ for each integer $k \geq 2$	$7, 21, 63, 189, ...$

The recurrence is identical; only the seed differs, and the two sequences share no terms.

Checking that a sequence satisfies a recurrence

Given an explicit formula and a candidate recurrence, the check is a one-step calculation: **assume the formula at $k-1$, substitute it into the recurrence, and see whether what comes out is the formula at k.**

For $b_n = 4n + 3$ and the candidate $b_k = 4 + b_{k-1}$:

$$b_k = 4 + b_{k-1} = 4 + \big(4(k-1) + 3\big) = 4k + 3 \quad \checkmark$$

For the candidate $b_k = 4b_{k-1}$, the same substitution gives

$$b_k = 4b_{k-1} = 4\big(4(k-1) + 3\big) = 16k - 16 + 3 = 16k - 13 \quad \times$$

which is not $4k + 3$, so that recurrence is not satisfied.

Reading a recursive definition off an explicit formula

> This section goes explicit → recursive. The reverse trip — recursive → explicit, which is the harder and more useful one — is solving-recurrence-relations[162].

Going the other way — from an explicit formula to a recursive definition — means computing the first few terms, spotting what is done to each term to get the next, then proving the guess.

Factorial. For $n \in \mathbb{Z}^+$, $n! = n(n-1)\cdots(2)(1)$, and $0! = 1$ **by definition**. Worth memorising: the $0! = 1$ convention is what makes formulas involving $n!$ work at $n = 0$ without a special case.

Example: $a_n = \dfrac{(-1)^n}{n!}$ **for each integer** $n \geq 0$**.**

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

The first five terms, and the factor taking each to the next:

$$\underbrace{1}_{a_0} \xrightarrow{\times -1} \underbrace{-1}_{a_1} \xrightarrow{\times -\frac{1}{2}} \underbrace{\frac{1}{2}}_{a_2} \xrightarrow{\times -\frac{1}{3}} \underbrace{-\frac{1}{6}}_{a_3} \xrightarrow{\times -\frac{1}{4}} \underbrace{\frac{1}{24}}_{a_4}$$

The multiplier at step n is $-\frac{1}{n}$, suggesting $a_n = -\frac{1}{n}a_{n-1}$. Verifying it against the explicit formula:

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

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

So the recursive definition is

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

Note how the recurrence relation's range starts one past the last initial condition — that is the general rule, and it is what makes the definition cover every term exactly once.

Recursively defined sets

To define a set recursively, **three** things are needed:

1. **Base** — a statement that certain (usually small) objects belong to the set.
2. **Recursion** — rules on how to build new set objects from those objects already known to be in the set.
3. **Restriction** — a statement saying that all objects in the set come from the Base and the Recursion.

The Restriction is the part that is easy to forget and easy to underrate. Without it the Base and Recursion only say what *must* be in the set; the Restriction is what says nothing *else* is, and it is what licenses arguing that a given object is **not** a member.

The set of all binary strings

A **binary string** is a sequence of 0's and 1's. The set B of all binary strings is defined recursively:

- **Base**: the empty string ε is in B.
- **Recursion**: if $s \in B$, then $s0 \in B$ and $s1 \in B$.
- **Restriction**: nothing is in B other than objects defined by the Base and the Recursion.

Every string therefore has a build history from ε, one character at a time — the string 011 is built up as $\varepsilon \to 0 \to 01 \to 011$. Applying the two rules repeatedly generates a binary tree of strings, and a build history is just a path down it from the root:

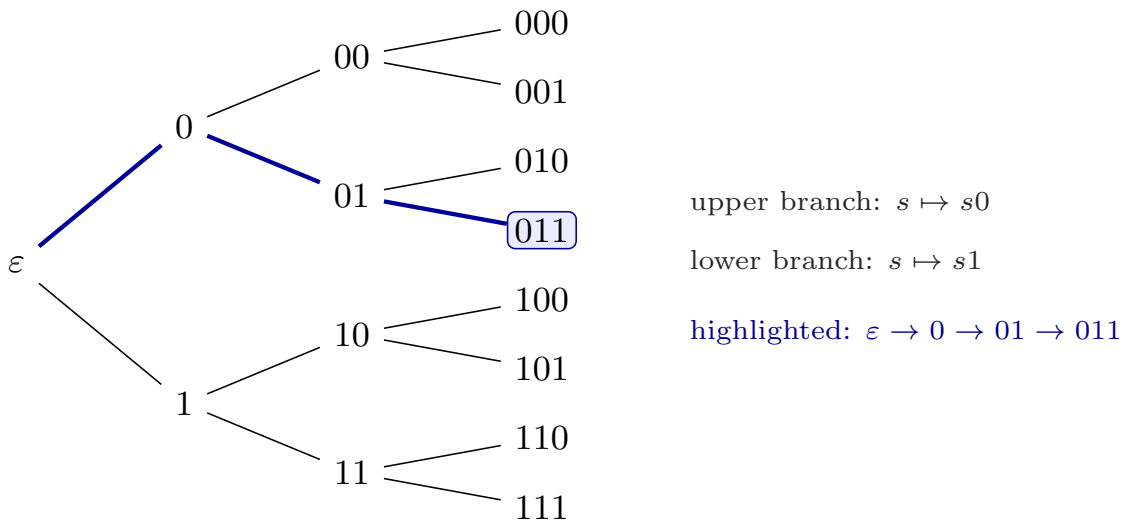


Figure 22: The Recursion applied three times over, drawn the way the lecture drew it: the Base object ε at the root on the left, the two rules fanning rightwards as plain segments with no arrowheads, and each node labelled with the string it is. The upper branch appends a 0 and the lower a 1, so the level a string sits at is its length. **The highlighted path is added here** — the lecture wrote the build history of 011 out as a separate chain rather than marking it on the tree; drawn on the tree it shows what a build history actually is, a route from the Base to the object.

Two things the picture makes plain that the rules alone do not. Every binary string appears **exactly once** in this tree, at depth equal to its length — so for B a build history is unique, and there is no ambiguity about how a given string was made. And the tree only ever grows: neither rule shortens a string, so a property that holds at the root and survives both rules holds everywhere below. That is the shape of argument the Restriction licenses, and it is what the next section turns into a method.

Arguing about membership

For a recursively defined set, the two directions of argument look quite different:

- **To show an object is in the set**, exhibit a build history — a chain from the Base to the object, with each step naming the rule used.
- **To show an object is not in the set**, find a property that the Base has and that every Recursion rule preserves, and observe the object lacks it. This is an induction over the structure of the set, and it works only because of the Restriction.

See also

- solving-recurrence-relations[163] — the other direction: recursive definition to explicit formula, and proving it
- sequences-and-summations[164] · strong-induction-and-the-well-ordering-principle[165] · mathematical-induction[166]
- counting-principles[167] — $n!$ as the number of arrangements of n objects
- 2026-08-31-recursive-definitions[168] — Lecture 15
- practice-problems[169] — §19 Recursive Definitions, 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[170] for the proof methods that go with these definitions, and functions-on-general-sets[171] 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: $\{\dots, -2, -1, 0, 1, 2, \dots\}$.

[163] courses/math1061/solving-recurrence-relations.pdf
[164] courses/math1061/sequences-and-summations.pdf
[165] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[166] courses/math1061/mathematical-induction.pdf
[167] courses/math1061/counting-principles.pdf
[168] courses/math1061/2026-08-31-recursive-definitions.pdf
[169] courses/math1061/practice-problems.pdf
[170] courses/math1061/proving-set-properties.pdf
[171] courses/math1061/functions-on-general-sets.pdf

- **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]).

"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

	Statement		Why
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.

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 $x \in T$.**

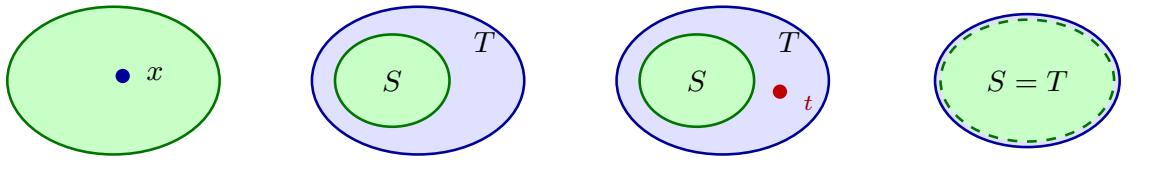


Figure 23: The four situations the symbols distinguish. An element sits inside a set; a subset is a set inside a set; a proper subset leaves something over; and equality is containment holding both ways at once. The contained set is green and the containing set pale blue, with elements as small blue dots; the red dot is the element that keeps the containment proper.

This is the *element method*, and it is used so heavily that proving-set-properties[172] treats it in full. The word doing the work is "arbitrary" — you may assume nothing about x beyond membership of S, which is what makes the one argument cover every element at once.

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

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

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

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

Rewriting $8k + 2$ as $2(4k + 1)$ is the entire proof — see modular-arithmetic[173] 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** $x \in T$.

[172] courses/math1061/proving-set-properties.pdf
[173] courses/math1061/modular-arithmetic.pdf

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[174] read through the definition of $\subseteq$, which is why "prove both directions" is never optional.

The empty set

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

Why is $\emptyset \subseteq A$ for every set A? Because "$\forall x$, if $x \in \emptyset$ then $x \in A$" is true for every set A. The hypothesis $x \in \emptyset$ is never satisfied, and a conditional with a false hypothesis is true — so the statement holds **vacuously**. See conditional-statements[175] 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.

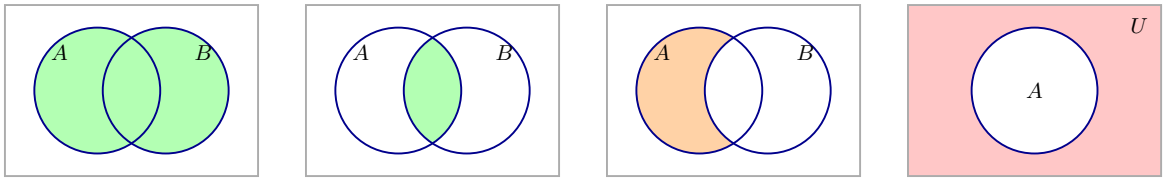
Proof (by contradiction). Suppose $\emptyset_1$ and $\emptyset_2$ are distinct sets each having no elements, so $\emptyset_1 \neq \emptyset_2$. Since $\emptyset_1$ has no elements, it is a subset of $\emptyset_2$; that is, $\emptyset_1 \subseteq \emptyset_2$. Also, since $\emptyset_2$ has no elements, $\emptyset_2 \subseteq \emptyset_1$. 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.

[174] courses/math1061/logical-equivalence-laws.pdf
[175] courses/math1061/conditional-statements.pdf

Unions and intersections

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



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

Figure 24: The four operations as shaded regions. Union takes everything in either circle, intersection only the overlap, difference removes B from A, and the complement is everything in the universe outside A — which is why a complement is only meaningful once the universe U is fixed. The enclosing rectangle is that universe.

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

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

Indexed over all three:

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

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

Indexed families

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

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

Worked, over $i = 0, 1, 2, \ldots$:

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

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

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

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

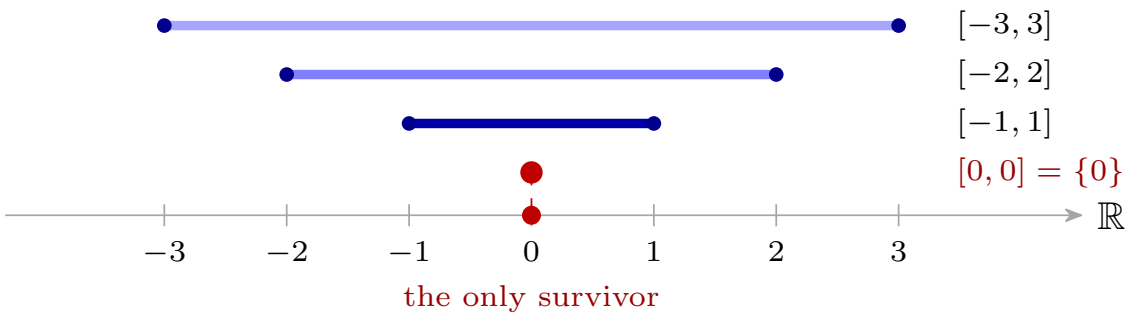


Figure 25: An intersection over an increasing family is decided by its smallest member. Each interval contains the one below it, so the only real number lying in all of them is the single point the innermost interval contains. The intervals sit above the number line, with a filled dot at each closed endpoint.

Set difference and complement

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

Both are drawn in Figure 24 above.

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

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

The power set

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

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

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

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

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

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

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

The finiteness matters — the count is meaningless otherwise. The 2^n comes from building a subset by making n independent in/out choices. Sorting the same subsets by size instead gives $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$ (binomial-coefficients[176]).

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

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

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

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

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

Worked: power sets of power sets

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

	Value	$\lvert\cdot\rvert$ of the input	Check
$\mathcal{P}(\{a\})$	$\{\emptyset,\ \{a\}\}$	$\lvert\{a\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\emptyset)$	$\{\emptyset\}$	$\lvert\emptyset\rvert = 0$	$2^0 = 1$ ✓
$\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$	$\{\emptyset,\ \{\emptyset\}\}$	$\lvert\{\emptyset\}\rvert = 1$	$2^1 = 2$ ✓
$\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))) = \mathcal{P}(\{\emptyset,\{\emptyset\}\})$	$\{\emptyset,\ \{\emptyset\},\ \{\{\emptyset\}\},\ \{\emptyset,\{\emptyset\}\}\}$	$\lvert\{\emptyset,\{\emptyset\}\}\rvert = 2$	$2^2 = 4$ ✓

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

Cartesian products

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

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

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

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

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

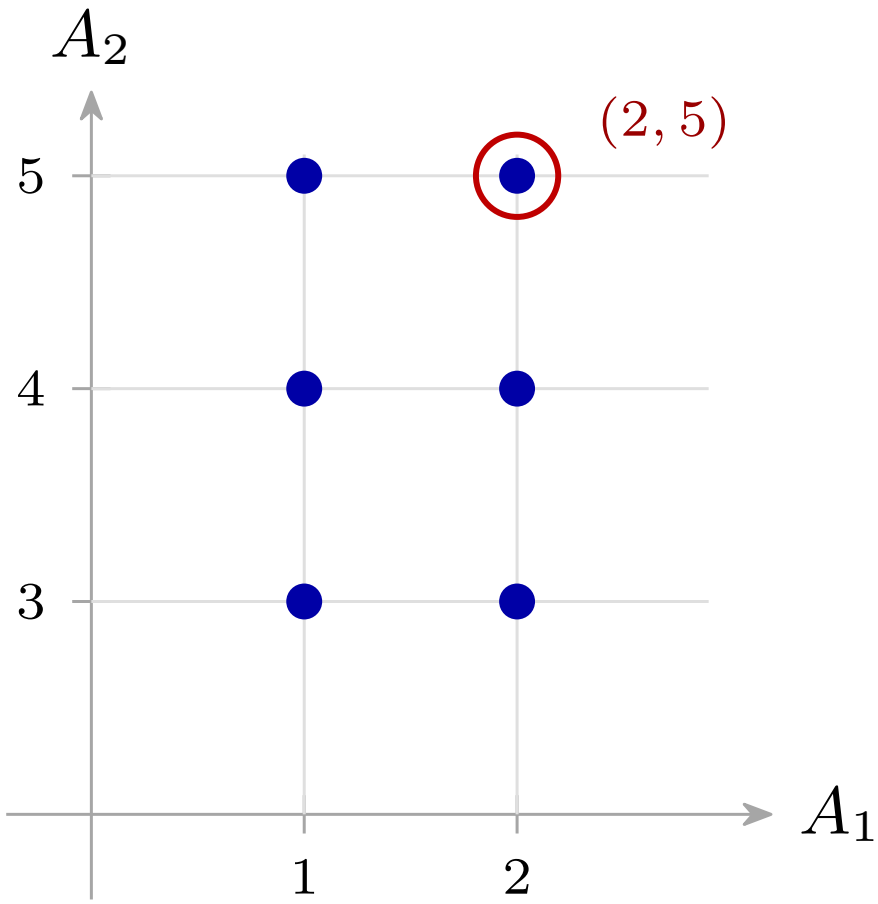
Worked. Let $S = \{a, b, c\}$ and $T = \{c, d\}$.

- $(d, c) \notin S \times T$, 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, $|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|$.



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

Figure 26: 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.

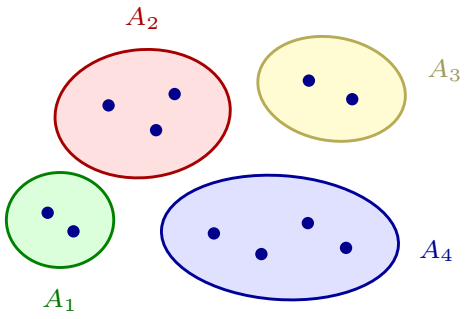
Notation clash to be aware of. (a, b) can mean an **ordered pair**, and (a, b) can also mean an **open interval** — the real numbers x with $a < x < b$. Nothing in the symbols distinguishes them; only the context does.

Partitions

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

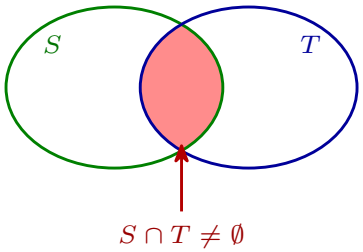
$$A = A_1 \cup A_2 \cup A_3 \cup \cdots \qquad \text{and} \qquad A_i \cap A_j = \emptyset \text{ for each } i, j \geq 1,\ i \neq j$$

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



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 27: 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[177]).

See also

- proving-set-properties[178] — the element method, the set identities, and proofs about these operations
- functions-on-general-sets[179] — functions defined as subsets of a Cartesian product
- equivalence-classes-and-partitions[180] — partitions as the classes of an equivalence relation
- modular-arithmetic[181] — the congruence sets used throughout the worked examples
- counting-principles[182] · counting-selections[183] — $|A \times B| = |A| \times |B|$ as the multiplication

[177] courses/math1061/equivalence-classes-and-partitions.pdf
[178] courses/math1061/proving-set-properties.pdf
[179] courses/math1061/functions-on-general-sets.pdf
[180] courses/math1061/equivalence-classes-and-partitions.pdf
[181] courses/math1061/modular-arithmetic.pdf
[182] courses/math1061/counting-principles.pdf
[183] courses/math1061/counting-selections.pdf

rule, and $\binom{n}{r}$, the number of r-element subsets of an n-element set
- inclusion-exclusion[184] · probability[185] — 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[186] — a partition as the set of pigeonholes
- conditional-statements[187] · logical-equivalence-laws[188] — vacuous truth, and the biconditional behind set equality
- 2026-09-03-set-theory-definitions[189] — Lecture 17
- practice-problems[190] — §21 Set Theory Definitions, with full worked solutions
- practice-problems[191] — §22 More Definitions and Examples of Sets

The Symmetric Group

S_n is the group whose elements are the bijections from $\{1, 2, \dots, n\}$ to itself, and whose operation is composition. Its elements are functions, not numbers, and it is the course's first group in which the order of a product matters. The definition of a group is in groups[192], and the two ingredients are one-to-one-and-onto-functions[193] and composition-of-functions[194]. First met in 2026-09-24-definitions-and-examples-of-groups[195].

The definition

> S_n is the group consisting of the set of all bijections from $\{1, 2, \cdots, n\}$ to $\{1, 2, \cdots, n\}$ together with the binary operation $\circ$ denoting composition of functions.

An element of S_n is a way of sending each of $1, \dots, n$ to one of $1, \dots, n$, so that no two go to the same place and every place is used. To combine two elements, do one and then the other.

How many elements. A bijection in S_3 can send 1 to any of three places. That leaves two places for 2, and then one for 3, so S_3 has $3 \cdot 2 \cdot 1 = 6$ elements. In general S_n has $n!$ elements, one for each arrangement of $1, \dots, n$ (counting-principles[196]).

[184] courses/math1061/inclusion-exclusion.pdf
[185] courses/math1061/probability.pdf
[186] courses/math1061/pigeonhole-principle.pdf
[187] courses/math1061/conditional-statements.pdf
[188] courses/math1061/logical-equivalence-laws.pdf
[189] courses/math1061/2026-09-03-set-theory-definitions.pdf
[190] courses/math1061/practice-problems.pdf
[191] courses/math1061/practice-problems.pdf
[192] courses/math1061/groups.pdf
[193] courses/math1061/one-to-one-and-onto-functions.pdf
[194] courses/math1061/composition-of-functions.pdf
[195] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[196] courses/math1061/counting-principles.pdf

The six elements of S_3

They are named f_1 to f_6 here, and each can be drawn as an arrow diagram (2026-09-24-definitions-and-examples-of-groups[197]). Each can also be written as a set of pairs or as a list of values.

	As a set of pairs	$1 \mapsto$	$2 \mapsto$	$3 \mapsto$	What it does
f_1	$\{(1,1),(2,2),(3,3)\}$	1	2	3	nothing
f_2	$\{(1,2),(2,1),(3,3)\}$	2	1	3	swaps 1 and 2
f_3	$\{(1,3),(2,2),(3,1)\}$	3	2	1	swaps 1 and 3
f_4	$\{(1,1),(2,3),(3,2)\}$	1	3	2	swaps 2 and 3
f_5	$\{(1,2),(2,3),(3,1)\}$	2	3	1	moves all three
f_6	$\{(1,3),(2,1),(3,2)\}$	3	1	2	moves all three, the other way

The pair form is the definition of a function as a set of pairs (functions-on-general-sets[198]). The names $f_1, \ldots, f_6$ are just labels, and other sources number the six differently.

Composing

$$(f \circ g)(x) = f(g(x))$$

The function on the right acts first. To work out $f \circ g$, take each of 1, 2, 3 in turn, apply g, then apply f to the result.

$f_2 \circ f_3$: f_3 first, then f_2.

x	$f_3(x)$	$f_2(f_3(x))$
1	3	3
2	2	1
3	1	2

[197] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[198] courses/math1061/functions-on-general-sets.pdf

So $f_2 \circ f_3$ sends $1 \mapsto 3$, $2 \mapsto 1$, $3 \mapsto 2$, which is f_6.

$f_3 \circ f_2$: f_2 first, then f_3.

x	$f_2(x)$	$f_3(f_2(x))$
1	2	2
2	1	3
3	3	1

So $f_3 \circ f_2$ sends $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$, which is f_5.

The same two functions in the two orders give different answers. $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$.

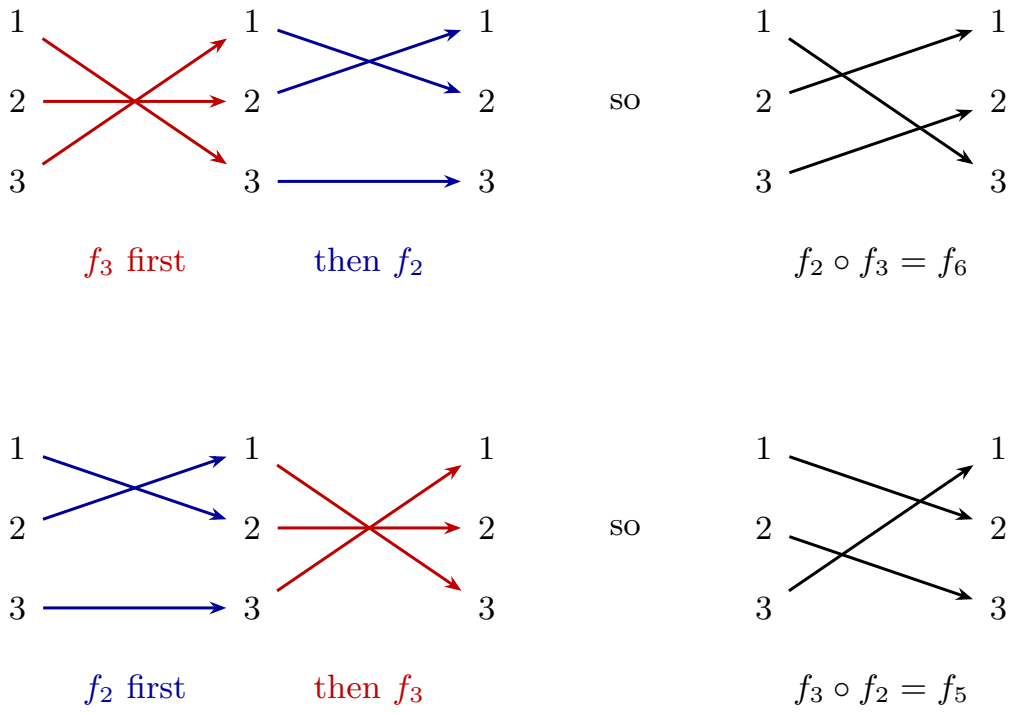


Figure 28: The same two elements of S_3 composed in both orders. Top: f_3 first and then f_2, which is $f_2 \circ f_3$. Following each number through both steps gives $1 \to 3$, $2 \to 1$, $3 \to 2$, the element f_6. Bottom: f_2 first and then f_3, which is $f_3 \circ f_2$. Now the result is $1 \to 2$, $2 \to 3$, $3 \to 1$, the element f_5. In each row the picture runs left to right in the order things happen, and the formula names the functions right to left.

Why it is a group

For S_3 the properties can be checked from its table, with associativity by a general argument (2026-09-24-definitions-and-examples-of-groups[199]). Each one also follows, for every n, from facts about functions:

- **Closure.** The composition of two bijections is a bijection (composition-of-functions[200]).
- **Associativity.** For any three functions, $f \circ (g \circ h)$ and $(f \circ g) \circ h$ both send x to $f(g(h(x)))$.
- **Identity.** The function that sends every number to itself, f_1 in S_3. Composing with it on either side changes nothing.
- **Inverses.** A bijection has an inverse function (inverse-functions[201]), which is again a bijection, and composing the two in either order gives the identity (composition-of-functions[202]).

So the inverse of f in the group S_n is the inverse function f^{-1}, and the two uses of the notation agree. In an arrow diagram the inverse is found by **reversing every arrow**.

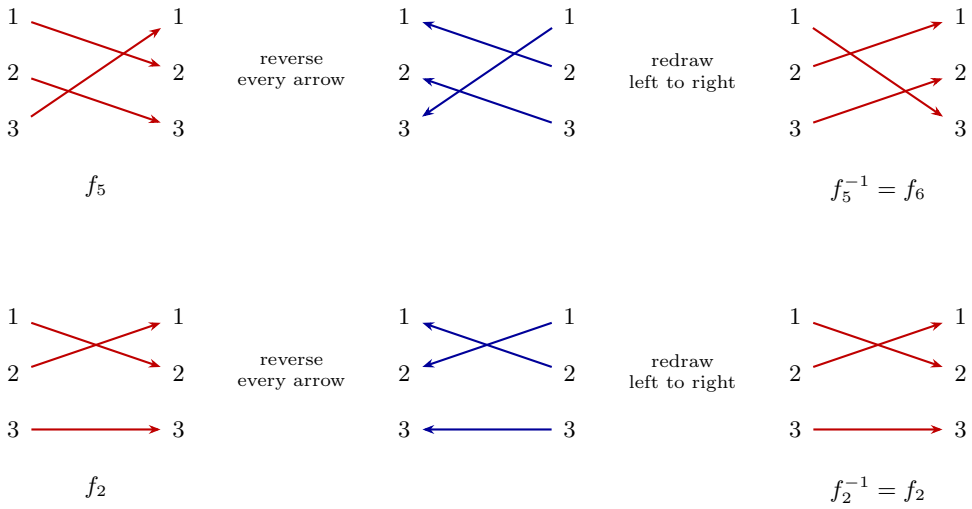


Figure 29: Inverses in S_3 by reversing arrows. Top: f_5 sends $1 \to 2$, $2 \to 3$, $3 \to 1$. Turning each arrow round gives $2 \to 1$, $3 \to 2$, $1 \to 3$, and reading that as a function of 1, 2, 3 gives $1 \to 3$, $2 \to 1$, $3 \to 2$, which is f_6. So $f_5^{-1} = f_6$. Bottom: f_2 swaps 1 and 2. Turning its arrows round gives the same diagram, so f_2 is its own inverse. The same holds for f_3 and f_4, the other two swaps.

[199] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[200] courses/math1061/composition-of-functions.pdf
[201] courses/math1061/inverse-functions.pdf
[202] courses/math1061/composition-of-functions.pdf

The Cayley table of S_3

The entry in the row of f and the column of g is $f \circ g$ (cayley-tables[203]).

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
$\mathbf{f_1}$	f_1	f_2	f_3	f_4	f_5	f_6
$\mathbf{f_2}$	f_2	f_1	f_6	f_5	f_4	f_3
$\mathbf{f_3}$	f_3	f_5	f_1	f_6	f_2	f_4
$\mathbf{f_4}$	f_4	f_6	f_5	f_1	f_3	f_2
$\mathbf{f_5}$	f_5	f_3	f_4	f_2	f_6	f_1
$\mathbf{f_6}$	f_6	f_4	f_2	f_3	f_1	f_5

Read off it:

- **Identity:** f_1.
- **Inverses:** $f_1^{-1} = f_1$, $f_2^{-1} = f_2$, $f_3^{-1} = f_3$, $f_4^{-1} = f_4$, $f_5^{-1} = f_6$, $f_6^{-1} = f_5$.
- **Not abelian:** $f_2 \circ f_3 = f_6$ but $f_3 \circ f_2 = f_5$.

The three swaps are their own inverses: doing a swap twice puts everything back. f_5 and f_6 undo each other. The table also shows $f_5 \circ f_5 = f_6$ and $f_6 \circ f_5 = f_1$, so doing f_5 three times returns everything to where it started.

Non-abelian does not mean nothing commutes. $f_5 \circ f_6 = f_6 \circ f_5 = f_1$, and f_1 commutes with everything. A group is non-abelian as soon as **one** pair fails to commute.

Powers and cyclic subgroups of S_3

Powers are defined in any group (subgroups-and-cyclic-groups[204]). In S_3 a power is a repeated composition, $f^2 = f \circ f$, and $f^0 = f_1$. Read from the table:

- f_5**.** $f_5^1 = f_5$, $f_5^2 = f_5 \circ f_5 = f_6$, $f_5^3 = f_5^2 \circ f_5 = f_6 \circ f_5 = f_1$. This is "doing f_5 three times returns everything to where it started": f_5 moves $1 \to 2 \to 3 \to 1$, and three moves bring each number home. So $\langle f_5 \rangle = \{f_5, f_6, f_1\}$.
- f_6**.** $f_6 = f_5^{-1}$, so $\langle f_6 \rangle = \langle f_5 \rangle$. Directly: $f_6^2 = f_6 \circ f_6 = f_5$ and $f_6^3 = f_5 \circ f_6 = f_1$.
- **The swaps.** $f_2^2 = f_2 \circ f_2 = f_1$, since swapping twice changes nothing. So $\langle f_2 \rangle = \{f_2, f_1\}$, and likewise $\langle f_3 \rangle = \{f_3, f_1\}$ and $\langle f_4 \rangle = \{f_4, f_1\}$.
- **The identity.** $\langle f_1 \rangle = \{f_1\}$.

[203] courses/math1061/cayley-tables.pdf
[204] courses/math1061/subgroups-and-cyclic-groups.pdf

a	Powers of a until f_1	$\langle a \rangle$
f_1	f_1	$\{f_1\}$
f_2	f_2, f_1	$\{f_1, f_2\}$
f_3	f_3, f_1	$\{f_1, f_3\}$
f_4	f_4, f_1	$\{f_1, f_4\}$
f_5	f_5, f_6, f_1	$\{f_1, f_5, f_6\}$
f_6	f_6, f_5, f_1	$\{f_1, f_5, f_6\}$

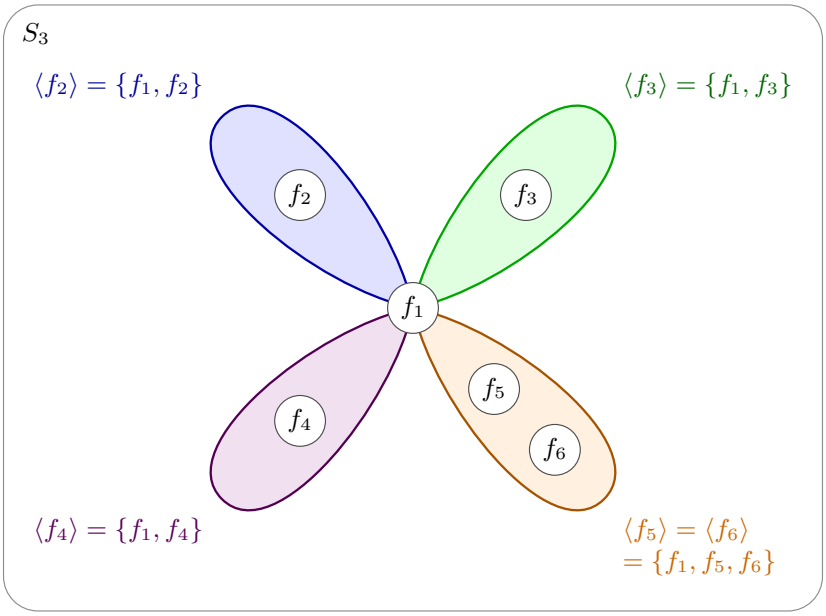


Figure 30: The cyclic subgroups of S_3, drawn inside it. Each petal is the set of powers of one element. The identity f_1, where the petals meet, is in every one, and it is the only element any two of them share. The three swaps f_2, f_3, f_4 each generate a subgroup of two elements, because a swap done twice changes nothing. f_5 and f_6 move all three numbers round and are each other's inverses, so they generate the same subgroup f_1, f_5, f_6. No petal is the whole of S_3, so no element generates it and S_3 is not cyclic.

None of the six is all of S_3, so S_3 **is not cyclic**. It could not have been: every cyclic group is abelian, and S_3 is not (subgroups-and-cyclic-groups[205]). $\{f_1, f_5, f_6\}$ also shows up as a block of the table when its elements are listed first (cayley-tables[206]).

[205] courses/math1061/subgroups-and-cyclic-groups.pdf
[206] courses/math1061/cayley-tables.pdf

Common mistakes

- **Composing in the wrong order.** $f \circ g$ means g first. Reading it left to right gives the other product, which in S_3 is usually a different element.
- **Reading the table as column $\circ$ row.**
- **Thinking S_3 has three elements.** It has six. The 3 is the size of the set being rearranged.
- **Treating the elements as numbers.** f_2 is a function. $f_2 \circ f_3$ is a composition, not a multiplication of 2 and 3.
- **Reading f^{-1} as $\frac{1}{f}$.** It is the inverse function.
- **Concluding from "non-abelian" that no two elements commute.**

See also

- groups[207] — the definition, and abelian against non-abelian
- cayley-tables[208] — reading a table, and why its rows and columns have no repeats
- composition-of-functions[209] — the operation of S_n, and why it is done right to left
- one-to-one-and-onto-functions[210] · inverse-functions[211] — bijections and their inverses, the elements of S_n and their group inverses
- functions-on-general-sets[212] — a function as a set of pairs
- subgroups-and-cyclic-groups[213] — powers, cyclic subgroups, and why a non-abelian group cannot be cyclic
- 2026-09-24-definitions-and-examples-of-groups[214] — Lecture 26 · 2026-10-06-elementary-properties-of-groups[215] — Lecture 27
- practice-problems[216] — §33, with full worked solutions

[207] courses/math1061/groups.pdf
[208] courses/math1061/cayley-tables.pdf
[209] courses/math1061/composition-of-functions.pdf
[210] courses/math1061/one-to-one-and-onto-functions.pdf
[211] courses/math1061/inverse-functions.pdf
[212] courses/math1061/functions-on-general-sets.pdf
[213] courses/math1061/subgroups-and-cyclic-groups.pdf
[214] courses/math1061/2026-09-24-definitions-and-examples-of-groups.pdf
[215] courses/math1061/2026-10-06-elementary-properties-of-groups.pdf
[216] courses/math1061/practice-problems.pdf