Discrete Mathematics and Graphs

This is a script for the lecture Discrete Mathematics and Graphs given in the winter semester 2023/24 at FEE CTU, Prague. It is not a textbook, all explanations are made very briefly. The purpose of this text is solely to list the stuff we made on the lecture. Therefore, I recommend either attending the lectures or reading some better written textbook. See references below.

References

[DP] N. Donaldson, A. Pantano: An Introduction to Abstract Mathematics Lecture notes available online

[De] M. Demlová: Discrete Mathematics and Graphs. Lecture notes for an earlier version of this course.

[C] L. N. Childs: A Concrete Introduction to Higher Algebra

[J] R. Johnsonbaugh: Discrete Mathematics

1 Logic and sets

1.1 Propositional logic

. . . is about *propositions* and how to combine them using *logical connectives*.

1.1.1 Informal definition. A **proposition** is a sentence, which is either true or false. That is, every proposition P has assigned its **truth value**, which is either **true** or **false** denoted T and F or 1 and 0, respectively.

1.1.2 Definition. Let P and Q be propositions. We define propositions

- "P and Q" denoted $P \wedge Q$,
- "P or Q" denoted $P \vee Q$,
- "if P, then Q" denoted $P \Rightarrow Q$,
- "P if and only if Q" denoted $P \Leftrightarrow Q$,

Their truth values are determined according to the following table

P	Q	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$
F	F	F	F	T	T
F	T	F	T	T	F
T	F	F	T	F	F
T	T	T	T	T	T

For a proposition P, we also define the proposition "not P" denoted by $\neg P$, whose truth value is the opposite of the truth value of P.

The connectives $\Rightarrow$ and $\Leftrightarrow$ represent logical consequence and equivalence, which is important for reasoning. In natural languages, they are translated in a several different ways.

The sentence "$P \Rightarrow Q$" can be read as

- If P, then Q.
- Q if P.
- P implies Q.
- P only if Q.
- P is sufficient for Q.
- Q is necessary for P.

The sentence "$P \Leftrightarrow Q$" can be read as

- P if and only if Q. (The "if and only if" is often shortened as "iff".)
- P is (logically) equivalent to Q.
- P is necessary and sufficient for Q.

1.1.3 Remark. The implication $\Rightarrow$ means *logical, not causal* consequence. For instance, take:

$$P = \text{I'll go for a walk tomorrow.}$$
$$Q = \text{There is no rain tomorrow.}$$

Then $P \Rightarrow Q$ seems like a nonsense if you translate it by "if P, then Q". But it is only because we intuitively assume speaking about a causal consequence. Logically it is perfectly fine as becomes obvious if you phrase the sentence as "Tomorrow, I'll go for a walk only if there is no rain." Makes perfect sense, right? And if I say that and you see me tomorrow walking around, you can make a logical conclusion that there must be no rain, because otherwise I wouldn't go for a walk.

All this language we built is based on the *informal definition* of a proposition in a beginning. It is not easy to make a formal definition of this notion since a *proposition* is not a mathematical object. It is a sentence *about* mathematical objects. But notice that all the stuff we were talking about afterwards do not really depend on what a *proposition* really is. The only important thing is that propositions are either true or false. So, if we wanted to formalize the logical connectives, we can do a slight workaround using *logical variables*.

1.1.4 Definition. Let A be a non-empty set whose elements will be called **logical variables**. We define **propositional formulas** as follows:

- Any logical variable is a propositional formula.
- If α and β are propositional formulas, then $(\neg\alpha)$, $(\alpha \wedge \beta)$, $(\alpha \vee \beta)$, $(\alpha \Rightarrow \beta)$, $(\alpha \Leftrightarrow \beta)$ are propositional formulas as well.

A **truth valuation** is a function $u\colon A \to \{0, 1\}$. We extend this function to all propositional formulas based on the truth tables above.

1.1.5 Definition. A propositional formula α is said to be a **tautology** if $u(\alpha) = 1$ for every truth valuation u. We denote it by $\models \alpha$. In contrast, if $u(\alpha) = 0$ for every

u, then α is called a **contradiction**. Finally, α is called **satisfiable** if there exists a truth valuation u such that $u(\alpha) = 1$.

1.1.6 Example. Consider a pair of logical variables a, b. Then $a \wedge b$ is satisfiable. Indeed, it is true if both a and b are true. But it is not a tautology (it can also happen that it is not true, for instance, if a is false).

The formula $a \vee (\neg a)$ is a tautology since it is true regardless of whether a is true or not. On the other hand $a \wedge (\neg a)$ is a contradiction as it is always false.

1.1.7 Definition. Propositional formulas α and β are **tautologically equivalent** if $\alpha \Leftrightarrow \beta$ is a tautology. We denote it by $\alpha \models\!\models \beta$.

1.1.8 Remark. Equivalently we may say that $\alpha \models\!\models \beta$ if $u(\alpha) = u(\beta)$ for any truth valuation u. That is, writing down the truth table, both α and β have the same entries in every row.

1.1.9 Theorem (De Morgan's laws). For any propositional formulas α and β, we have

$$\neg(\alpha \wedge \beta) \models\!\models \neg\alpha \vee \neg\beta,$$
$$\neg(\alpha \vee \beta) \models\!\models \neg\alpha \wedge \neg\beta.$$

Proof. We prove the first law, the second is by exercise. The proof is done by writing the truth table.

α	β	$\neg(\alpha \wedge \beta)$	$\neg\alpha \vee \neg\beta$
0	0	1	1
0	1	1	1
1	0	1	1
1	1	0	0

□

1.1.10 Definition. A propositional formula β is said to be a **tautological consequence** of a propositional formula α, denoted by $\alpha \models \beta$, if $\alpha \Rightarrow \beta$ is a tautology.

As an exercise, prove the following statements.

1.1.11 Theorem. $((\alpha \Rightarrow \beta) \wedge (\beta \Rightarrow \gamma)) \models (\alpha \Rightarrow \gamma)$ for any prop. formulas α, β, γ.

1.1.12 Theorem. $(\alpha \Rightarrow \beta) \models\!\models (\neg\beta \Rightarrow \alpha)$ for any prop. formulas α, β.

1.1.13 Theorem. $\neg(\alpha \Rightarrow \beta) \models\!\models (\alpha \wedge \neg\beta)$ for any prop. formulas α, β.

1.2 Theorems and proving methods

1.2.1 Informal definition. A **theorem** is a true statement of the form $P \Rightarrow Q$. Here, the proposition P is called the **hypothesis** and Q is called the **conclusion**. The truth of a theorem should be justified by a *proof*.

We usually distinguish three kinds of proves. The idea behind the three proving strategies is based on the tautological consequences 1.1.11–1.1.13. We can prove $P \Rightarrow Q$ by:

Direct proof: Assume P and deduce Q by a chain of implications.

Proof by contrapositive: Assume $\neg Q$ and deduce $\neg P$.

Proof by contradiction: Assume P and $\neg Q$ and deduce a false statement.

Let us illustrate this on a simple example:

1.2.2 Theorem. Suppose x is an integer. If $x+5$ is even, then x is odd.

Let me first remind that in order to manipulate with mathematical statements, it is essential to have clear definitions. So, let me first recall the things we need here:

1.2.3 Definition. A number $n \in \mathbb{Z}$ is said to be **even** if there is a number $k \in \mathbb{Z}$ such that $n = 2k$. It is said to be **odd** if there is a number $k \in \mathbb{Z}$ such that $n = 2k+1$.

1.2.4 Fact. Every number $n \in \mathbb{Z}$ is either even or odd.

(The fact above is itself a theorem. As an exercise, you can think about, how would you prove it. We will actually formulate a more general version of it later.)

Direct proof of Thm. 1.2.2. The hypothesis means that $x+5 = 2k$ for some $k \in \mathbb{Z}$. This implies that $x = 2k-5$. This implies that $x = 2(k-3)+1$. This by definition means that x is odd. □

Proof by contrapositiove of Thm. 1.2.2. We are supposed to assume that x is not odd. From Fact 1.2.4 it follows that x is even, that is, $x = 2k$ for some $k \in \mathbb{Z}$. Hence $x+5 = 2k+5 = 2(k+2)+1$, which means that $x+5$ is odd, so by Fact 1.2.4 $x+5$ is not even, which is what we needed to show. □

Proof by contradiction of Thm. 1.2.2. We are supposed to assume that $x+5$ is even, but x is not odd. The first assumption means that $x+5 = 2k$ for some $k \in \mathbb{Z}$, while the second means that x is even, so $x = 2l$ for some $l \in \mathbb{Z}$ (we already used the letter k, so we need to use another one this time). Substituting the second assumption to the first, we have that $2k = 2l+5 = 2(l+2)+1$. On the left hand side, there is an even number, while on the right hand side, there is an odd number. The equality means that a single number is both even and odd, which contradicts the Fact 1.2.4. □

This time the direct proof was easy and the other method made it just more complicated. But in general, it can be the other way around.

1.3 Sets

We present the *naïve set theory* based on the following informal definition of what a set is. This is connected with certain paradoxes (see e.g. Russel's paradox). There is a way to axiomatize set theory formally. That would, however, be unnecessarily complicated for our purposes.

1.3.1 Informal definition. A **set** is a collection of objects. That is, a set A, it is defined by specifying its **elements**. We write

- $x \in A$ to denote that x is an element of A,
- $x \notin A$ to denote that x is not an element of A.

We say that sets A and B are **equal**, denoted by $A = B$, if

$$x \in A \Leftrightarrow x \in B \qquad \text{for every } x.$$

1.3.2 Notation. In order to specify a set, we use braces $\{, \}$. If the set is finite, we can specify its elements directly like

$$S = \{1, 3, a, \{2\}, \{\}\}.$$

If it is clear, what we mean, we may describe even infinite sets like that:

$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}.$$

Often, we will use the notation $\{x \mid P(x)\}$, where $P(x)$ is some propositional function (a proposition that depends on a variable x. This means the set of all x such that $P(x)$ is true. For instance, the set of all positive even numbers can be described in a several different ways as follows:

$$\begin{aligned} E &= \{2, 4, 6, 8, 10, \ldots\} \\ &= \{x \mid x \in \mathbb{N},\ x \text{ is even}\} \\ &= \{x \in \mathbb{N} \mid x \text{ is even}\} \\ &= \{x \in \mathbb{N} \mid x = 2k \text{ for some } k \in \mathbb{N}\} \\ &= \{2k \mid k \in \mathbb{N}\}. \end{aligned}$$

1.3.3 Definition. The set containing no elements is called the **empty set** and we denote it by $\emptyset = \{\}$. A set is called **finite** if it has finitely many elements, **infinite** if it has infinitely many elements. If S is a finite set, we denote by $|S|$ or $\#S$ the number of its elements.

1.3.4 Notation. We define the following sets

- $\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}$ the set of all **natural numbers**,
- $\mathbb{N}_0 = \{0, 1, 2, 3, 4, 5, \ldots\}$ the set of all natural numbers including zero,
- $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ the set of all **integers**,
- $\mathbb{Q} = \{m/n \mid m \in \mathbb{Z}, n \in \mathbb{N}\}$ the set of all **rational numbers**,
- $\mathbb{R}$ the set of all **real numbers**,
- $\mathbb{C}$ the set of all **complex numbers**.

1.3.5 Definition. Let A, B be sets. We say that A is a **subset** of B, denoted by $A \subseteq B$ if $x \in B$ for every $x \in A$.

1.3.6 Definition. Consider two sets A, B. We define a new set $A \cap B$ called the **intersection** of A and B by

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

1.3.7 Definition. The **union** of two sets A and B is defined to be the following set

$$A \cup B = \{x \mid x \in A \vee x \in B\}.$$

1.3.8 Definition. The **complement** of a set A relative to set B is defined to be the following set

$$B \setminus A = \{x \in B \mid x \notin A\}.$$

1.3.9 Remark. Sometimes we consider all sets to be a subset of some *universe* U. Then we define the *complement* $A^{\mathbb{C}}$ (or $\bar{A}$) of A as a complement relative to U, i.e. $A^{\mathbb{C}} = U \setminus A$.

1.4 Quantifiers

Again, we will be slightly informal here. For a more formal introduction, see [[De]].

A **propositional function** is a proposition depending on some variable.

We introduce the symbol $\forall$ meaning *for all* and call it the **universal quantifier** and the symbol $\exists$ meaning *there exists* called the **existential quantifier**.

If we equip a propositional function $P(x)$ with a quantifier $\forall$ or $\exists$, we get a **quantified proposition** $\forall x\, P(x)$ or $\exists x\, P(x)$.

1.4.1 Example. We can define the following propositional functions:

$$P(x) = x \text{ is an even number},$$
$$Q(x) = x \text{ has a brain}$$

Now, we can form the following quantified propositions:

$\forall x\, P(x)$	Every number is even.
$\exists x\, \neg Q(x)$	Somebody has no brain.

Actually, there is something missing in the formulas on the left. We are silently assuming some domain for x. The formula $\forall x\, P(x)$ actually says that *every x is even*. But this makes sense only if x is an integer. If it is a real number or a set or a person, then the notion *even* is not defined. So, if we really want to say that *every integer is even* or *some person has no brain*, we should write

$$\forall x\ x \in \mathbb{Z} \Rightarrow P(x)$$
$$\exists x\ x \text{ is a human} \wedge \neg Q(x)$$

which is usually shortened as

$$(\forall x \in \mathbb{Z})(P(x))$$
$$(\exists x \text{ a human})(\neg Q(x))$$

An important question: How to negate quantified statements?

1.4.2 Fact. For any propositional function $P(x)$, we have

$$\begin{aligned} \neg(\forall x\ P(x)) &\quad \text{is equivalent to} \quad \exists x\ \neg P(x), \\ \neg(\exists x\ P(x)) &\quad \text{is equivalent to} \quad \forall x\ \neg P(x). \end{aligned}$$

1.4.3 Exercise. Show that a similar rule holds also if you use domains for your quantifiers. That is, for any set S, we have:

$$\begin{aligned} \neg((\forall x \in S)(P(x))) &\quad \text{is equivalent to} \quad (\exists x \in S)(\neg P(x)), \\ \neg((\exists x \in S)(P(x))) &\quad \text{is equivalent to} \quad (\forall x \in S)(\neg P(x)). \end{aligned}$$

Finally, let us have a look on how to prove quantified statements.

1.4.4 Example. Consider the statement

$$P: \quad (\forall x \in \mathbb{R})(\exists y \in \mathbb{R})(xy = 3).$$

Do you think it is true? A good idea might be trying to formulate its negation

$$\neg P: \quad (\exists x \in \mathbb{R})(\forall y \in \mathbb{R})(xy \neq 3).$$

Now $\neg P$ is easy to prove. Just take $x = 0$ and you see that for every $y \in \mathbb{R}$, we have $xy = 0 \neq 3$. Consequently, the original statement P was false. What we did was disproving P by constructing a *counterexample*.

In general, proving or disproving a quantified statement requires the following

	Prove	Disprove
$\forall x\ P(x)$	Needs abstract argumentation	Counterexample is enough
$\exists x\ P(x)$	Example is enough	Needs abstract argumentation

1.4.5 Exercise. In analysis you will learn (or maybe you already did) that a function $f\colon \mathbb{R} \to \mathbb{R}$ is said to be *continuous* in a point $a \in \mathbb{R}$ if

$$(\forall \varepsilon > 0)(\forall \delta > 0)(|x - a| < \delta \Rightarrow |f(x) - f(a)| < \varepsilon).$$

Your task is to characterize the situation when f is *not* continuous in a. That is, negate the quantified formula above.

1.5 Proof by induction

This is one last proof technique that we are going to learn. It is used in the cases when we need to prove something *for every* $n \in \mathbb{N}$ (in general for all elements of some totally ordered set).

1.5.1 Problem. What is the largest possible number of pieces you can divide a convex pizza into by making n straight cuts?

Solution. For $n \in \mathbb{N}_0$, denote by a_n the maximal number of pieces you can get after n cuts. Clearly $a_0 = 1$ as we have exactly one piece at the beginning. After one cut, we have surely two pieces, so $a_1 = 2$. Then $a_2 = 4$. If all cuts went through the middle, we would have six pieces after the third cut. But tha maximal number of pieces is obtained if no cut hits the already present intersection points. In that case $a_3 = 7$. In general, we can construct the n-th cut always in such a way that we hit all the previous $n-1$ cuts and hence we cut through n regions of the pizza. This adds new n regions. So, after the n-th cut, we have $a_n = a_{n-1} + n$. Now the question is, what a_n actually equals to?

Well, as a programmer, you would probably just open python and write

```
def pizza(n):
    if n==0:
        return(1)
    else:
        return(pizza(n-1)+n)
```

This very short programme would give you answer for any n. But can you also give a formula?

1.5.2 Claim. $a_n = \frac{1}{2}(n^2 + n + 2)$.

Proof. The proof goes exactly the same way as the computer code. First, check the starting point. For $n = 0$, we know that $a_0 = 1$. That's also what the formula says since $\frac{1}{2}(0^2 + 0 + 2) = 2/2 = 1$. So, the formula works.

Now, take any n. Suppose that the formula works for $n-1$. That is, suppose

$$a_{n-1} = \frac{1}{2}((n-1)^2 + (n-1) + 2) = \frac{1}{2}(n^2 - n + 2).$$

Then this means

$$a_n = a_{n-1} + n = \frac{1}{2}(n^2 - n + 2) + n = \frac{1}{2}(n^2 + n + 2),$$

which is what we wanted to show.

But remember there was this assumption that the formula works for $n-1$. But since we checked the formula for $n = 0$, the assumption works for $n = 1$ and hence we have the formula proven for $n = 1$. But then this means that the assumption works for $n = 2$ as well, so have it proven for $n = 2$. And so on and so forth. □

The general strategy for proof by induction is following. Suppose we have a propositional formula $P(n)$ and we need to prove that it is true for every $n \in \mathbb{N}$. Then we proceed as follows

1. Prove $P(1)$ (**base case**)
2. Assuming $P(n-1)$ (**induction hypothesis**), prove $P(n)$ (**induction step**).

1.5.3 Remark.

- If we need to prove something for all $n \in \mathbb{N}_0$. Then the base case is $n = 0$, not $n = 1$. In general, proof by induction works for any totally ordered set. We will not define that formally, but you probably know what I mean.
- Often the induction step does not work right from the beginning, but maybe from $n = 2$. Then we have to prove more than one base case.
- Sometimes it is useful to assume not only that $P(n-1)$ is true as the induction hypothesis, but that all $P(1), P(2), \ldots, P(n-1)$ are true. This is called the **complete induction**.

1.5.4 Exercise. Prove that

$$2 + 5 + 8 + \cdots + (3n - 1) = \frac{1}{2}n(3n + 1).$$

2 Number theory

2.1 Divisibility

2.1.1 Definition. Consider $n, m \in \mathbb{Z}$. We say that n is a **multiple of** m or that n is **divisible by** m or that m **divides** n and denote it by $m \mid n$ if there exists $k \in \mathbb{Z}$ such that $n = km$.

2.1.2 Remark. Observe that $m \mid n$ implies $m \leq n$.

2.1.3 Theorem (Division). Consider $n \in \mathbb{Z}$, $m \in \mathbb{N}$. Then there exists a unique $k \in \mathbb{Z}$, $r \in \{0, 1, \ldots, m-1\}$ such that $n = km + r$.

The process of finding the two unique numbers k and r is called the **division**. The number k is called the **quotient** and the number r is called the **remainder**.

Proof. First, we need to prove that there *exists* numbers k and r. Then we will prove that these numbers are *unique*.

So, take any $n \in \mathbb{Z}$ and $m \in \mathbb{N}$ and let us find the appropriate k and r. Taking arbitrary $k \in \mathbb{Z}$, we can put $r := n - km$ and we have a pair of numbers satisfying $n = km + r$. The thing that makes it complicated is the condition that $0 \leq r < m$.

So, take the set of all such possible remainders $R := \{n - jm \mid j \in \mathbb{Z}\}$ and choose the smallest non-negative one $r := \min\{z \in R \mid z \geq 0\}$. Obviously, $r \geq 0$. We claim that the condition $r < m$ is satisfied as well.

Since r is the smallest, we must have that $r - m = n - (k+1) < 0$, because this number is also an element of R. Therefore, $r < m$.

It remains to prove the uniqueness. Suppose we have two solutions (k_1, r_1) and (k_2, r_2). First, we will prove that $k_1 = k_2$ by contradiction. So, assume that $k_1 \neq k_2$. Then $r_1 - r_2 = m(k_2 - k_1)$. On the left-hand-side, we have a number which is in absolute value surely smaller than m, while on the right-hand-side, we have a non-zero multiple of m. This is a contradiction. Now if $k_1 = k_2$, then also $r_1 = n - k_1 = n - k_2 = r_2$, which is what we wanted to show. □

2.1.4 Exercise. Prove Fact 1.2.4 using this theorem.

2.1.5 Definition. Suppose $a, b \in \mathbb{Z} \setminus \{0\}$. A number $d \in \mathbb{N}$ is called the **greatest common divisor** of a and b if

- $d \mid a$ and $d \mid b$ (i.e. d is a their common divisor)
- For every $d' \in \mathbb{N}$ we have $(d' \mid a \wedge d' \mid b) \Rightarrow d' \mid d$ (i.e. it is the greatest one)

The greatest common divisor of any two numbers is obviously given uniquely. We will denote it by $\gcd(a, b)$. From our definition of the greatest common divisor, it is not obvious that it exists for any a, b. This will follow from Theorem 2.1.9.

2.1.6 Exercise. Assume that the greatest common divisor exists for a and b. Prove that we can replace $d' \mid d$ by $d' \leq d$ in the definition of gcd.

2.1.7 Problem. Find $\gcd(12, 18)$!

Solution. So far we do not have much tools to look for the gcd. We may just try all number ≤ 12 and just check, whether they divide both 12 and 18. Finally, we find out that $\gcd(12, 18) = 6$. Actually, we can make it a bit faster. After figuring out that 2 is a common divisor, it is enough to only go through even numbers. After figuring out that 6 is a common divisor, it is enough to only go through multiples of six. Why?

2.1.8 Problem. Find $\gcd(2^{16} + 1, 2^{32} + 1)$.

This seems impossible by hand. But we are going to develop a tool that makes computing the greatest common divisor very fast.

2.1.9 Theorem (Bézout). For any $a, b \in \mathbb{Z} \setminus \{0\}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$. (In particular, the greatest common divisor of a and b exists.)

Proof. Put $S_{a,b} := \{ax + by \mid x, y \in \mathbb{Z}\}$. Observe that

- $S_{a,b}$ is closed under addition,
- $S_{a,b}$ is closed under multiplying by any integer $k \in \mathbb{Z}$,
- $S_{a,b}$ contains a and b.

We need to show that it contains $\gcd(a, b)$.

Put $n := \min\{z \in S_{a,b} \mid z > 0\}$. The claim is that $n = \gcd(a, b)$. So let us check that it satisfies the definition of the greatest common divisor. Denote by $x_0, y_0 \in \mathbb{Z}$ the numbers satisfying $n = ax_0 + by_0$.

We need to prove that n is a divisor of a. By Division theorem (2.1.3), we have that $a = kn + r$ for some $0 \leq r < n$. Clearly $r \in S_{a,b}$. It follows that $r = 0$ since otherwise we would have a contradiction with n being minimal. The same way, we prove that n is a divisor of b.

Finally, suppose $d' \mid a$ and $d' \mid b$ for some d'. Then obviously $d' \mid ax_0 + by_0 = n$. □

We can use the proof of the theorem to derive a method for computing the greatest common divisor. Recall that $\gcd(a, b)$ is the minimal positive element of $S_{a,b}$. Now observe that $S_{a,b} = S_{a-b,b} = S_{a-kb,b}$ for any k. So, if $a > b > 0$ and $a = kb + r$, then $S_{a,b} = S_{r,b}$. Consequently $\gcd(a, b) = \gcd(r, b)$. We can repeat this taking $b = k_1 r + r_1$, then $\gcd(a, b) = \gcd(r, b) = \gcd(r, r_1) = \cdots$.

2.1.10 Algorithm (Euclid). Input: $a > b > 0$. Output: $\gcd(a, b)$.

Perform repeated integer division as follows:

$$\begin{aligned} a &= k_0 b + r_0 \\ b &= k_1 r_0 + r_1 \\ r_0 &= k_2 r_1 + r_2 \\ &\vdots \\ r_j &= k_{j+2} r_{j+1} + r_{j+2} \end{aligned}$$

After finitely many steps, we get $r_{j+2} = 0$. Then $\gcd(a, b) = r_{j+1}$.

2.1.11 Exercise. Try to rewrite the algorithm in pseudocode or some existing programming language. You can try to execute it on a computer and check how it works.

2.1.12 Example. Let us go back to computing $\gcd(2^{16} + 1, 2^{32} + 1)$:

$$\begin{aligned} 2^{32} + 1 &= (2^{16} - 1)(2^{16} + 1) + 2 \\ 2^{16} + 1 &= 2^{15} \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

So, $\gcd(2^{32} + 1, 2^{16} + 1) = \gcd(2^{16} + 1, 2) = \gcd(2, 1) = 2$.

2.1.13 Example. Compute $\gcd(432, 234)$!

$$\begin{aligned} 432 &= 1 \cdot 234 + 198 \\ 234 &= 1 \cdot 198 + 36 \\ 198 &= 5 \cdot 36 + 18 \\ 36 &= 2 \cdot 18 \end{aligned}$$

Hence, $\gcd(432, 234) = \gcd(36, 18) = 18$.

2.2 Linear Diophantine equations

Now, we might be interested to know, what the particular numbers x and y are.

2.2.1 Problem. Find all $x, y \in \mathbb{Z}$ such that $432x + 234y = 18$.

Solution. In order to do this, it is just enough to do the Euclid's algorithm backwards. In the example above, we found out that $198 = 5 \cdot 36 + 18$, so $18 = 198 - 5 \cdot 36$. Now, we can substitute for 36 from the equality above. Finally replace 198 using the first equality and we have the desired expression:

$$\begin{aligned} 18 = 198 - 5 \cdot 36 = 198 - 5 \cdot (234 - 198) &= 2 \cdot 198 - 5 \cdot 234 \\ &= 2 \cdot (432 - 234) - 5 \cdot 234 = 2 \cdot 432 - 7 \cdot 234. \end{aligned}$$

So, the numbers are (for instance) $x = 2$, $y = 7$.

This sounds interesting. Maybe we could try to study equations $ax + by = c$ in general. Note that they are *linear*. You will learn solving linear equations in linear algebra, but here we will consider the additional condition that the indeterminates x and y (as well as the coefficients a, b, c) are integers. While the original equation always has infinitely many solutions in $\mathbb{R}$, it is not clear, whether and how many solutions does it have in $\mathbb{Z}$.

Note that equations in the domain of integers are called *Diophantine equations*. Here, we will learn how to solve linear Diophantine equations with two variables. Having more equations or more variables is possible as well, but we will not do it here. Having non-linear Diophantine equations is of course more delicate.

2.2.2 Problem. Find all $x, y \in \mathbb{Z}$ such that $16x - 12y = 0$.

Solution. Well, the equation can clearly be simplified dividing by 4. We get $4x-3y = 0$. So, $y = \frac{4}{3}x$. Now the only point is to find all such $x \in \mathbb{Z}$ that $y = \frac{4}{3}x$ is integer as well. It is clear that if x is a multiple of 3, then y is an integer. Is it necessary that x is a multiple of 3? Try to think about it before reading further.

Well, we can divide the equation by x and get $\frac{y}{x} = \frac{4}{3}$. We have an equality of two fractions. Notice that the fraction $4/3$ is reduced to the lowest terms. So any other fraction y/x can be equal to $4/3$ only if $y = 4k$ and $x = 3k$, $k \in \mathbb{Z}$. And that's the solution we were looking for.

2.2.3 Theorem. Consider $a, b \in \mathbb{Z} \setminus \{0\}$. The equation $ax + by = 0$ has infinitely many solutions given by

$$x = k\frac{b}{\gcd(a,b)}, \quad y = -k\frac{a}{\gcd(a,b)}, \qquad k \in \mathbb{Z}.$$

These are all solutions of the given equation.

Proof. One of the solutions is clearly $x = y = 0$ (and if $x = 0$, then $y = 0$ and vice versa). So, suppose now that $x, y \neq 0$. In that case, the equation $ax + by = 0$ is equivalent to $y/x = -b/a$. We can reduce the fraction b/a to the lowest terms by cancelling the $\gcd(a, b)$, so we get

$$\frac{y}{x} = \frac{-b/\gcd(a,b)}{a/\gcd(a,b)}.$$

From this, it already follows that $y = -k\frac{b}{\gcd(a,b)}$, $x = k\frac{a}{\gcd(a,b)}$, $k \in \mathbb{Z}$. □

Now, let us get back to the linear equation with arbitrary right hand side $ax + by = c$. Here, the existence of a solution is not always guaranteed.

2.2.4 Theorem. Consider $a, b, c \in \mathbb{Z} \setminus \{0\}$. Then there exists $x, y \in \mathbb{Z}$ such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.

Proof. Suppose $ax + by = c$. Since $\gcd(a, b)$ divides both a and b, it must clearly divide c as well.

For the converse, suppose c is a multiple of $\gcd(a, b)$, so $c = k\gcd(a, b)$ for some $k \in \mathbb{Z}$. By Bézout's theorem (2.1.9), there are x_0, y_0 such that $ax_0 + by_0 = \gcd(a, b)$. Multiplying this equality by k, we get that $ax + by = c$ for $x = kx_0$, $y = ky_0$. □

2.2.5 Problem. Find all solutions of $24x + 105y = 33$.

Solution. First, we should figure out, whether the equation has a solution or not. So, let us find $\gcd(24, 105)$ by Euclid's algorithm.

$$\begin{aligned} 105 &= 4 \cdot 24 + 9 \\ 24 &= 2 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

We found out that $\gcd(24, 105) = 3$, which divides 33, so the original equation indeed has a solution. How do we find one? We can follow the proof of Theorem 2.2.4. First, let us find some solution of $24x + 105y = 3$. We know how to do that – by reversing the Euclid's algorithm:

$$3 = 9 - 6 = 3 \cdot 9 - 24 = 3 \cdot 105 - 13 \cdot 24.$$

Now, we can just multiply this equality by 11 and get

$$33 = 33 \cdot 105 - 143 \cdot 24.$$

So, we have one solution, namely $x = 33$, $y = 143$. But this may not be the only solution.

2.2.6 Theorem. Consider $a, b, c \in \mathbb{Z} \setminus \{0\}$ such that $\gcd(a, b) \mid c$. Suppose $x_1, y_1 \in \mathbb{Z}$ is some solution of the equation $ax + by = c$. Then all solutions $x, y \in \mathbb{Z}$ are of the form

$$x = x_1 + k\frac{b}{\gcd(a,b)}, \quad y = y_1 - k\frac{a}{\gcd(a,b)}, \qquad k \in \mathbb{Z}.$$

Proof. By assumption, we have $ax_1 + by_1 = c$. Suppose that $x, y \in \mathbb{Z}$ is another solution, so $ax+by = c$ as well. Subtracting these two, we get $a(x-x_1)+b(y-y_1) = 0$. By Theorem 2.2.3, all solutions of this equation are given by $x - x_1 = k\frac{b}{\gcd(a,b)}$, $y - y_1 = -k\frac{a}{\gcd(a,b)}$, $k \in \mathbb{Z}$, which is all we need. □

2.3 Positional number systems

2.3.1 Theorem. Consider $q \in \mathbb{N}$, $q \geq 2$. Then every number $n \in \mathbb{N}$ can be uniquely expressed as $n = \sum_{i=0}^{k} a_i q^i$, where $k \in \mathbb{N}_0$, $a_0, \ldots, a_k \in \{0, 1, \ldots, q-1\}$, $a_k \neq 0$.

The number q is called the **base**, the numbers $a_0, \ldots, a_k$ are the **digits**, so the number k represents the **number of digits**. We use the notation $n = (a_k a_{k-1} \cdots a_1 a_0)_q$.

2.3.2 Example. We usually represent numbers in base 10. Here, the digits are $0, 1, 2, \ldots, 9$. For instance, if we write 174, what we mean is *one hundred seventy four*, so more precisely, *one hundred, seven tens, and four ones*, so $174 = 1 \cdot 10^2 + 7 \cdot 10^1 + 4 \cdot 10^0$.

2.3.3 Problem. Write $n = 174$ in base 3.

Solution. First, we determine the number of digits. We do this by finding $k \in \mathbb{N}_0$ such that $3^k \leq n < 3^{k+1}$. Here, $3^1 = 3$, $3^2 = 9$, $3^3 = 27$, $3^4 = 81$, $3^5 = 273$. So, the appropriate k is four (hence we will have five digits). Secondly, we want to determine the actual digits. We go from the most significant (the leftmost) to the least (rightmost). Here, the most leftmost digit is a_4, which stands for the *eighty-ones*. So, we ask: How many eighty-ones fit into $n = 174$. The answer is two since $2 \cdot 81 = 162$ (but $3 \cdot 81 = 243$, which is too big already). So, the leftmost digit is two and we are left over with $174 - 162 = 12$, which we need to represent by the other digits. We essentially do the division with remainder. We continue in a similar manner:

$$\begin{aligned} 174 &= \underbrace{2}_{a_4} \cdot \underbrace{81}_{3^4} + 12 \\ 12 &= \underbrace{0}_{a_3} \cdot \underbrace{27}_{3^3} + 12 \\ 12 &= \underbrace{1}_{a_2} \cdot \underbrace{9}_{3^2} + 3 \\ 174 &= \underbrace{1}_{a_1} \cdot \underbrace{3}_{3^1} + \underbrace{0}_{a_0} \end{aligned}$$

So, we found out that $174 = (20110)_3$.

2.3.4 Algorithm. Input: Numbers $n, q \in \mathbb{N}$, $q > 2$. Output: Expressing n in base q.

1. **find** $k \in \mathbb{N}_0$: $q^k \leq n < q^{k+1}$
2. **for** $j = k, k-1, \ldots, 1, 0$ **do**
3. **find** $a_j \in \{0, \ldots, q-1\}$, $r \in \{0, \ldots, q^j - 1\}$: $n = a_j q^j + r$ (Euclid. division)
4. $n \leftarrow r$
5. **return** $(a_k, \ldots, a_0)$

2.3.5 Exercise. It is also possible to formulate an algorithm that would start with the least significant digit and proceed to the most significant one. Try to figure it out and formulate formally.

Proof of Theorem 2.3.1. Existence: Basically follows from the algorithm. As an exercise, try to formulate a formal proof using mathematical induction.

Uniqueness: For the sake of contradiction, suppose $n \in \mathbb{N}$ is the smallest number that has two different possible expressions in base q. So, $n = (a_k \cdots a_1 a_0)_q = (b_l \cdots b_1 b_0)_q$. We will study two cases – either $k \neq l$ or $k = l$. In both we are going to derive a contradiction.

So, assume $k = l$. Then $n - q^k$ would also have two different expressions, namely $((a_k - 1)a_{k-1} \cdots a_1 a_0)_q$ and $((b_k - 1)b_{k-1} \cdots b_1 b_0)$. This is a contradiction with the assumption that n is the smallest with non-unique expression.

Now, assume $k \neq l$. Without loss of generality, suppose $k > l$. Then using the first expression, we have

$$n = \sum_{i=0}^{k} a_i q^i \geq q^k,$$

but at the same time

$$n = \sum_{j=0}^{l} b_j q^j \leq \sum_{j=0}^{l} (q-1)q^j = (q-1)\frac{q^{l+1}-1}{q-1} = q^{l+1} - 1 < q^k.$$

This is obviously a contradiction. □

2.4 Congruence

2.4.1 Definition. Two numbers $a, b \in \mathbb{Z} \setminus \{0\}$ are called **relatively prime** if $\gcd(a, b) = 1$. We denote it by $a \perp b$.

2.4.2 Lemma (Euclid). Consider $a, b, c \in \mathbb{Z} \setminus \{0\}$ such that $a \perp b$. Then $a \mid bc$ implies that $a \mid c$.

Proof. The assumption $a \mid bc$ means by definition that $bc = ad$ for some $d \in \mathbb{Z}$. The assumption $a \perp b$ implies by Bézout's theorem that $ax + by = 1$ for some $x, y\mathbb{Z}$. Multiplying this equality by c, we get $c = acx + bcy = acx + ady = a(cx + dy)$, so c is indeed a multiple of a. □

2.4.3 Definition. Consider $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. We say that a is **congruent** to b **modulo** n if $n \mid (a - b)$. We denote it by $a \equiv b \pmod{n}$.

2.4.4 Theorem (Equivalent definitions of congruence). The following are equivalent.

1. $a \equiv b \pmod{n}$, i.e. $n \mid (a - b)$,
2. a and b have the same remainder when dividing by n,
3. $a = b + kn$ for some $k \in \mathbb{Z}$.

Proof. (1) ⇒ (2): Suppose that $n \mid (a - b)$, so $a - b = ln$ for some $l \in \mathbb{Z}$ and hence $b = a - ln$. Now, denote by r the remainder when dividing a by n, so $a = kn + r$ for some k. Then $b = a - ln = kn + r - ln = (k - l)n + r$, so r is also the remainder when dividing b by n.

(2) ⇒ (3): Suppose that $a = ln + r$ and $b = mn + r$. Then $a = ln + b - mn = b + (l - m)n = b + kn$, where $k = l - m \in \mathbb{Z}$.

(3) ⇒ (1): Suppose that $a = b + kn$. Then $a - b = kn$, which is what we wanted to show. □

2.4.5 Theorem (Properties of congruence). Consider arbitrary $a, b, c, d \in \mathbb{Z}$, $n, k \in \mathbb{N}$. Then:

1. $a \equiv a \pmod{n}$
2. $a \equiv b \pmod{n} \quad \Leftrightarrow \quad b \equiv a \pmod{n}$
3. $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \quad \Rightarrow \quad a \equiv c \pmod{n}$
4. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \quad \Rightarrow \quad a + c \equiv b + d \pmod{n}$
5. $a \equiv b \pmod{n} \quad \Rightarrow \quad a + c \equiv b + c \pmod{n}$
6. $a \equiv b \pmod{n} \wedge c \equiv d \pmod{n} \quad \Rightarrow \quad ac \equiv bd \pmod{n}$
7. $a \equiv b \pmod{n} \quad \Rightarrow \quad ac \equiv bc \pmod{n}$
8. $a \equiv b \pmod{n} \quad \Rightarrow \quad a^k \equiv b^k \pmod{n}$

9. $ac \equiv bc \pmod{n} \wedge c \perp n \quad \Rightarrow \quad a \equiv b \pmod{n}$
10. $a \equiv b \pmod{n} \quad \Leftrightarrow \quad ak \equiv bk \pmod{kn}$

Proof. Exercise! □

As an application we will study *divisibility criteria*. You might know the following one from high school:

2.4.6 Proposition. A number $n \in \mathbb{N}$ has the same remainder when dividing by 3 as the sum of its digits (in base 10). In particular, n is divisible by 3 if and only if its sum of digits is divisible by 3.

Proof. Suppose $n = (a_k a_{k-1} \cdots a_1 a_0)_{10} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0$. We claim that $n \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod{3}$.

Observe that 10 has remainder 1 when dividing by 3, so $10 \equiv 1 \pmod{3}$. Consequently, $10^i \equiv 1 \pmod{3}$ (using property (8) of congruence). Using property (7), we derive $a_i \cdot 10^i \equiv a_i \pmod{3}$. Finally, repeatedly using property (4), we have $n = \sum_{i=0}^{k} 10^i a_i \equiv \sum_{i=0}^{k} a_i \pmod{3}$, which is what we wanted to show. □

2.4.7 Problem. Derive the divisibility criterion for 11 in base 10.

Solution. All computations will be modulo 11. We have $10^0 = 1$, $10^1 \equiv -1$, $10^2 \equiv 1$ and so on. In general, $10^i = (-1)^i$ for any $n \in \mathbb{N}$. That is:

$$10^{2i} \equiv 1, \qquad 10^{2i+1} \equiv -1.$$

Hence, for any $n = (a_k \cdots a_0)_1 0 = \sum_{i=0}^{k} a_i \cdot 10^i$, we have

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots = \sum_{i=0}^{k} (-1)^i a_i.$$

So, a number n is divisible by 11 if and only if the sum of its digits with alternating $+/-$ signs is.

2.4.8 Problem. Derive the divisibility criterion for 13 in base 10.

Solution. All computations will be modulo 13. Take $n = (a_k \cdots a_0)_{10}$ Observe:

$$\begin{aligned} 10^0 &\equiv 1, \\ 10^1 &\equiv -3, \\ 10^2 &\equiv -4, \\ 10^3 &\equiv -1. \end{aligned}$$

Hence,

$$\begin{aligned} 10^{3i} &\equiv (-1)^i, \\ 10^{3i+1} 1 &\equiv (-1)^i (-3), \\ 10^{3i+2} &\equiv (-1)^i (-4). \end{aligned}$$

Consequently,

$$n \equiv a_0 - 3a_1 - 4a_2 - a_3 + 3a_4 + 4a_5 + 5a_6 - \cdots = \sum_{i \geq 0} (-1)^i (a_{3i} - 3a_{3i+1} - 4a_{3i+2}).$$

Finally, let us have a look on the problem of *solving congruences*. That is, the same as solving equations, but having the congruence $\equiv$ instead of equality $=$. We

will focus on the linear ones. That is, $ax+b \equiv cx+d \pmod n$. But this is equivalent to $(a-c)x \equiv d-b \pmod n$, so we can actually focus on congruences of the form

$$ax \equiv b \pmod n.$$

2.4.9 Problem. Find all $x \in \mathbb{Z}$ such that $21x \equiv 8 \pmod{39}$.

Solution. By equivalent definition of congruence, this means that $8 = 21x + 39k$ for some $k \in \mathbb{Z}$. That's a Diophantine equation, so we know how to solve it. First, compute $\gcd(21, 39) = 3$. But 8 is not a multiple of 3, so this equation actually has no solution.

2.4.10 Problem. Find all $x \in \mathbb{Z}$ such that $29x \equiv 1 \pmod{17}$.

We will show two ways how to solve this.

Solution using Euclid's algorithm. The congruence is equivalent to solving $1 = 29x+17k$. Now, let us solve this in the standard way. First, do the Euclid's algorithm.

$$\begin{aligned} 29 &= 1 \cdot 17 + 12 \\ 17 &= 1 \cdot 12 + 5 \\ 12 &= 2 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \end{aligned}$$

Then reversing it to get one solution:

$$1 = 5 - 2 \cdot 2 = -2 \cdot 12 + 5 \cdot 5 = 5 \cdot 17 - 7 \cdot 12 = -7 \cdot 29 + 12 \cdot 17.$$

So, one solution is $x = -7$ (and $k = 12$, but we are not interested in k now). All other solutions are given by $x = -7 + 17l$, $l \in \mathbb{Z}$ (where the corresponding k is given by $k = 12 - 29l$, but again, nobody asked for k).

Solution using simplification of the congruence. We can use the properties of congruence in a similar way as we use the properties of equality when solving equations. In the following derivation, each row is equivalent to the next one. Everything is computed modulo 17.

$$\begin{aligned} 29x &\equiv 1 && \text{//subtract } 17x \equiv 0 \\ 12x &\equiv 1 && \text{//add } 0 \equiv 17 \\ 12x &\equiv 18 && \text{//divide by 6} \\ 2x &\equiv 3 && \text{//add } 0 \equiv 18 \\ 2x &\equiv 20 && \text{//divide by 2} \\ x &\equiv 10 \end{aligned}$$

By equivalent definition of congruence, $x \equiv 10 \pmod{17}$ means that $x = 10+17k$ for some $k \in \mathbb{Z}$.

2.4.11 Theorem. Consider $n \in \mathbb{N}$, $a, b \in \mathbb{Z}$. Then the congruence $ax \equiv b \pmod n$ has some solution $x \in \mathbb{Z}$ if and only if $\gcd(a, n) \mid b$

Proof. The congruence $ax \equiv b \pmod n$ is equivalent to saying that $b = ax + kn$ for some $k \in \mathbb{Z}$. The latter equation has a solution if and only if $\gcd(a, n) \mid b$ by Theorem 2.2.4.

2.5 Primes

2.5.1 Definition. A **prime number** (or just a **prime**) is a number $p \in \mathbb{N}$, $p > 1$ that has exactly two positive divisors (namely 1 and p). A number $n \in \mathbb{N}$, $n > 1$ which is not a prime is called a **composite number**.

2.5.2 Theorem. Consider $p \in \mathbb{N}$, $p > 1$. Then p is a prime if and only if, for all $b, c \in \mathbb{N}$, we have that $p \mid bc$ implies $p \mid b$ or $p \mid c$.

Proof. ($\Rightarrow$): Suppose p is a prime and consider any $b, c \in \mathbb{N}$ such that $p \mid bc$. We want to prove that $p \mid b$ or $p \mid c$. If $p \nmid b$, then $p \perp b$ as p is a prime. By Euclid's lemma (2.4.2) we immediately get $p \mid c$.

($\Leftarrow$): Let's assume the implication and prove that p must be a prime. Suppose d_1 is some divisor of p, so $p = d_1 d_2$ for some $d_1, d_2 \in \mathbb{N}$. Clearly, we have $d_1, d_2 \leq p$. We want to prove that necessarily $d_1 = 1$ and $d_2 = p$ or vice versa. If $p = d_1 d_2$, then surely $p \mid d_1 d_2$. By assumption, $p \mid d_1$ or $p \mid d_2$. Suppose for instance the first happens, but then $p \leq d_1$. This actually means that $p = d_1$, which is what we wanted to show. □

2.5.3 Theorem (Fundamental theorem of arithmetics). Every $n \in \mathbb{N}$, $n > 1$ can be written as a product of primes. This **prime factorization** is unique up to the order of factors.

Proof. First, we prove the existence. If n is a prime, then it is clear, so it remains to prove it for the composites. We will do the proof by complete induction. We proved the existence for the primes, which serves as the base case. Now, take any composite n and assume that that the prime factorization exists for all numbers smaller than n. Since n is composite, we have $n = n_1 n_2$ for some $1 < n_1, n_2 < n$. By induction hypothesis both n_1 and n_2 have prime factorization, so their product n clearly has one too.

It remains to prove the uniqueness. We will do it by contradiction. Suppose n is the smallest[1] number, where the prime factorization is not unique. So,

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

for some primes $p_1, \ldots, p_k, q_1, \ldots, q_l$. From the first expression, we have that $p_1 \mid n$. Now, applying Theorem 2.5.2 to the second expression, we have that $p_1 \mid q_j$ for some j, so actually $p_1 = q_j$. But this means that the number $m := n/p_1 = n/q_j$ also has two different prime factorizations. □

2.5.4 Theorem. There is infinitely many primes

Proof. For the sake of contradiction, assume that $p_1, \ldots, p_k$ are the only primes that exist. Consider $n = p_1 p_2 \cdots p_k + 1$. Then no p_i is a divisor of n since the remainder when dividing by p_i is always equal to 1. But according to the fundamental theorem of mathematics, n has to have a prime factorization $n = q_1 \cdots q_l$. But these primes $q_1, \ldots, q_l$ are missing in our list! □

[1] This is a popular trick. It is essentially a hidden induction. As an exercise, you can try to reformulate the proof and instead of proving by contradiction, prove it directly by induction.

2.5.5 Theorem (Fermat's little theorem). Let p be a prime, $a \in \mathbb{N}$, $a \perp p$. Then $a^{p-1} \equiv 1 \pmod{p}$.

Proof. The proof is based on the identity $(x+y)^p \equiv x^p + y^p \pmod{p}$, which holds whenever p is a prime. Indeed, we know that $(x+y)^p = \sum_{j=0}^{p} \binom{p}{j} x^j y^{p-j}$. But all the binomial coefficients $\binom{p}{j} = \frac{p(p-1)\cdots(p-j+1)}{j!}$ are divisible by p unless $j = 0$ or $j = p$. Hence the corresponding summands are congruent to zero.

Now, we can use induction to prove that this holds for arbitrary sums: $(x_1 + x_2 + \cdots x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p$. The base case $n = 1$ is clear, $n = 2$ we proved above. Now, let us prove it for arbitrary n assuming it holds for $n-1$. But that is easy as $(x_1 + x_2 + \cdots + x_n)^p = ((x_1 + \cdots + x_{n-1}) + x_n)^p = (x_1 + \cdots + x_{n-1})^p + x_n^p = x_1^p + \cdots + x_{n-1}^p + x_n^p$.

Finally, write $a = 1 + 1 + \cdots + 1$. Then we must have

$$a^p = (1 + 1 + \cdots + 1)^p \equiv 1^p + 1^p + \cdots + 1^p = 1 + 1 + \cdots + 1 = a.$$

Dividing by a, we get the desired result $a^{p-1} \equiv 1 \pmod{p}$. □

2.5.6 Exercise. Did you read the proof carefully? How did we use the assumption that p is a prime? Where did we use the assumption $a \perp p$?

2.6 RSA cryptosystem

We describe the public key encryption algorithm by Rivest, Shamir, Adleman (1977).

Suppose Bob wants to send a secret message to Alice, but they did not have the opportunity to agree on some secret code beforehand. The solution is as follows:

Alice chooses randomly two very large prime numbers p and q and computes $n := pq$. Let us denote[2] $\phi(n) := (p-1)(q-1)$. Then Alice chooses some number $i \in \{2, 3, \ldots, \phi(n)-1\}$ such that i is coprime with $\phi(n)$. She can do that by choosing i randomly and then checking that $\gcd(i, \phi(n)) = 1$ by Euclid's algorithm. The Euclid's algorithm then produces a number j such that $ij - k\phi(n) = 1$ (in other words, $ij \equiv 1 \pmod{\phi(n)}$). This equation actually has infinitely many solutions, but we can choose one such that $j \in \{2, 3, \ldots, \phi(n) - 1\}$.

Now the pair (n, i) is called the **public key** and Alice can send it to Bob or put it on the Internet. She keeps the rest of the data (primes p and q and the number j) private. Note that in principle, it is possible to compute these data from the public key. (We just do the prime decomposition of n and then run the Euclid's algorithm.) Nevertheless, if the primes p and q are large enough, it is computationally practically impossible.[3]

Now, suppose Bob wants to send a message to Alice. In this setting a message is a number[4] x, $0 < x < n$. Before sending the message through a public channel he encrypts it as follows: He computes $y := x^i \bmod n$, that is, the remainder when

[2] This is actually the *Euler's totient function*. We will learn about it later in the course.

[3] In fact, this is still an open question, i.e. it is not proven yet, that there is no quick algorithm for prime decomposition. We just do not know any.

[4] Remember that all data in a computer is stored as numbers.

dividing x^i by n (based on the public key). Try to think about how to do such an exponentiation quickly!

Now Alice receives y. The claim is that the original message x can be recovered as $y^j \bmod n$, that is, as the remainder when dividing y^j by n.

Before proving this, let us have a look on an example.

2.6.1 Example. Suppose Alice chooses $p = 11$, $q = 13$, $n = pq = 143$, $\phi(n) = (p-1)(q-1) = 120$, $i = 17$. Let us compute j. This is easy in this case as $120 = 7 \cdot 17 + 1$. So, $1 = 120 - 7 \cdot 17 = -16 \cdot 120 + 113 \cdot 17$, so $j = 113$. Alice publishes the public key $n = 143$, $i = 17$.

Now, suppose Bob wants to send the number $x = 69$ to Alice. But he would feel somewhat embarrassed to send such a number publicly, so he wants to encrypt it. So, he needs to compute $69^{17} \bmod 143$. How to do this effectively? Using *exponentiation by squaring* (the following computation goes mod 143):

$$\begin{aligned} 69 &\equiv 69 \\ 69^2 &= 4761 \equiv 42 \\ 69^2 &\equiv 42^2 \equiv 48 \\ 69^8 &\equiv 48^2 \equiv 46 \\ 69^{16} &\equiv 16^2 \equiv 113 \end{aligned}$$

Finally, $69^{17} = 69^{16} \cdot 69 \equiv 113 \cdot 69 \equiv 75$. So, $y = 75$, which looks pretty innocent, so Bob can send this to Alice.

Now Alice is wondering, what is Bob sending to her, so she wants to decrypt the message. Therefor she needs to compute $y^{113} \bmod 143$. Try to do the computation yourself beforehand!

$$\begin{aligned} 75 &\equiv 75 \\ 75^2 &\equiv 48 \\ 75^4 &\equiv 48^2 \equiv 16 \\ 75^8 &\equiv 16^2 \equiv 113 \\ 75^{16} &\equiv 113^2 \equiv 42 \\ 75^{32} &\equiv 42^2 \equiv 48 \\ 75^{64} &\equiv 48^2 \equiv 46 \end{aligned}$$

Now, $113 = 64 + 32 + 16 + 1$ (in other words $113 = (1110001)_2$), so $75^{113} = 75^{64} \cdot 75^{32} \cdot 75^{16} \cdot 75 \equiv 46 \cdot 48 \cdot 42 \cdot 75 \equiv 69$.

So, it really works! Now, you may feel that doing the prime decomposition of 113 is actually fairly easy and, in particular, it is much easier than the rest of the stuff we did here. But now imagine that we double the primes. Then the prime factorization will take (about) twice as long, but the exponentiation or the Euclid's algorithm takes (about) just one more step. Double it again and the same happens. Once the primes p and q are large enough, the prime factorization becomes impossible, while the encryption/decryption process is still quite easy to handle.

Now, we prove that the algorithm works.

2.6.2 Theorem. Let p, q be prime numbers. Denote $n := pq$ and $\phi(n) := (p-1)(q-1)$. Let $i, j \in \mathbb{N}$ satisfy $ij \equiv 1 \pmod{\phi(n)}$. Then for every $x \in \mathbb{Z}$, we have $x^{ij} \equiv x \pmod{n}$.

Proof. First, recall that $ij \equiv 1 \pmod{\phi(n)}$ means that $ij = k\phi(n)+1 = k(p-1)(q-1)+1$ for some k. Secondly, note that $x^{ij} \equiv x \pmod{n}$ is equivalent to $x^{ij} \equiv x \pmod{p}$ and $x^{ij} \equiv x \pmod{q}$ (try to prove!). So, we will prove that $x^{ij} \equiv x \pmod{p}$ and the proof for q is then literally the same.

Suppose first that $x \perp p$. Then by the little Fermat's theorem, we have $x^{p-1} \equiv 1 \pmod{p}$. We can raise this to the power $k(q-1)$ and then multiply by x to obtain

$$\begin{aligned} x^{p-1} &\equiv 1 \pmod{p} \\ x^{k(p-1)(q-1)} &\equiv 1^{k(q-1)} = 1 \pmod{p} \\ x^{ij} = x^{k(p-1)(q-1)+1} &\equiv x \pmod{p} \end{aligned}$$

Now, suppose that $x \not\perp p$. This means that $x = ap$ for some a. But then $x \equiv 0 \pmod{p}$ as well as $x^{ij} \equiv 0 \pmod{p}$. □

3 Relations

3.1 Relations in general

The mathematical notion of a *relation* is used to describe a relations between in a set of objects. For example, *to be a grandfather* (on the set of all people), *to have the same length* (on the set of physical objects or on the set of all line segments or similar), *to be a subset* (on the class of all sets) and so on.

3.1.1 Definition. Let A, B be sets. We denote by $A \times B$ the **Cartesian product** of A and B, which is defined to be the set of all **ordered pairs** (a, b), $a \in A$, $b \in B$.

3.1.2 Definition. Let A, B be sets. A **(binary) relation** from A to B is a set of ordered pairs $R \subseteq A \times B$. If $B = A$, we say that R is a relation on A. If $(x, y) \in R$, we write xRy. If $(x, y) \notin R$, we write $x \not R\, y$.

3.1.3 Examples.

- Taking $A = B = \{1, 2, 3, 4, 5\}$, we can define

  $$R = \{(1, 3), (2, 2), (2, 3), (3, 2), (4, 1), (5, 2)\},$$

  which is a relation on A. As an exercise, check the following:

  $$2R2, \quad 1 \not R\, 1, \quad 1R3, \quad 3 \not R\, 1.$$

  Note that alternatively, we can also consider R to be a relation from $\{1, 2, 3, 4, 5\}$ to $\{1, 2, 3\}$. Also, we can consider R to be a relation on $\mathbb{N}$.

- Taking $A = B = \{\text{all people}\}$, we can define a relation R on A be saying
$$aRb \quad \Leftrightarrow \quad a \text{ is a parent of } b.$$
- Taking $A = B$ to be any set, we can define $R = \{(a, a) \mid a \in A\}$. This a special relation which is usually called the **equality** and denoted by $=$ instead of R.
- Take any set S and $A = B = \mathscr{P}(S) = \{T \mid T \subseteq S\}$. Then $\subseteq$ is a relation on $\mathscr{P}(S)$.
- Take $A = B = \mathbb{R}$ and define xRy if and only if $y = \sin x$. That is $R = \{(x, \sin x) \mid x \in \mathbb{R}\}$. In general, any *function* is a special kind of relation.
- Take $A = B = \mathbb{R}$ and define xRy if and only if $x^2 + y^2 = 1$. That is, $R = \{(x, y) \mid x^2 + y^2 = 1\}$. This is the circle in R^2, which is *not* a function. Why?

3.1.4 Definition. Let A, B be sets. A **function** from A to B is a relation $f \subseteq A \times B$ such that
$$(\forall a \in A)(\exists_1 b \in B)((a, b) \in f)$$
We write $f\colon A \to B$ instead of $f \subset A \times B$ and $f(a) = b$ instead of $(a, b) \in f$.

3.1.5 Exercise. Formulate a definition of a function being *injective*, *surjective*, *bijective*.

3.1.6 Definition. If $R \subseteq A \times B$ is a relation, we define its **inverse** $R^{-1} \subseteq B \times A$ by
$$R^{-1} = \{(y, x) \mid (x, y) \in R\}.$$

3.1.7 Exercise. Any function $f\colon A \to B$ can be taken as a relation, so it must have an inverse (as a relation). Prove that the inverse is again a function if and only if f is bijective.

3.2 Equivalence relations

3.2.1 Definition. A relation on a set A is called

- **reflexive** if $(\forall a \in A)(aRa)$,
- **symmetric** if $(\forall a, b \in A)(aRb \Rightarrow bRa)$,
- **transitive** if $(\forall a, b, c \in A)((aRb \wedge bRc) \Rightarrow aRc)$

3.2.2 Definition. A relation R on a set A is called an **equivalence** if it is reflexive, symmetric, and transitive.

3.2.3 Examples. The motivating example is the *equality*. But there are others. You may know *congruence* from Euclidean geometry, which is an equivalnce. Here, we studied the congruence of numbers modulo, which we proved to be an equivalence.

3.2.4 Definition. Let $\sim$ be an equivalence on a set A. For every $a \in A$, we define its **equivalence class**
$$[a]_\sim = \{x \in A \mid x \sim a\}.$$
The set of all equivalence classes is called the **quotient set** and denoted
$$A/\!\sim = \{[a] \mid a \in A\}.$$
Any element b of some equivalence class is called its **representative**.

3.2.5 Examples. What are the equivalence classes of the following relations?

- Take the relation of *congruence modulo* n on the set $\mathbb{Z}$ of all integers. For simplicity, take $n = 3$ first:

$$\begin{aligned}
[0] &= \{x \in \mathbb{Z} \mid x \equiv 0 \pmod 3\} = \{3k \mid k \in \mathbb{Z}\} \\
[1] &= \{x \in \mathbb{Z} \mid x \equiv 1 \pmod 3\} = \{3k+1 \mid k \in \mathbb{Z}\} \\
[2] &= \{x \in \mathbb{Z} \mid x \equiv 2 \pmod 3\} = \{3k+2 \mid k \in \mathbb{Z}\} \\
[3] &= \{x \in \mathbb{Z} \mid x \equiv 3 \equiv 0 \pmod 3\} = [0] \\
[4] &= \{x \in \mathbb{Z} \mid x \equiv 4 \equiv 1 \pmod 3\} = [1] \\
&\vdots
\end{aligned}$$

  So, there are just three equivalence classes of congruence modulo 3 – namely [0], [1], [2]. In general, congruence modulo n has n classes [0], [1],..., $[n-1]$. They are called the **residue classes** since

$$\begin{aligned}
[i] &= \{x \in \mathbb{Z} \mid x \equiv i \pmod n\} = \{nk+i \mid k \in \mathbb{Z}\} \\
&= \{\text{numbers with remainder } i \text{ when dividing by } n\}\,.
\end{aligned}$$

- Take $A = \{$all students, who passed DMG last year$\}$ and define $a \sim b$ if the student a got the same grade from the exam. There will be five equivalence classes corresponding to the five possible grades A, B, C, D, E they could get.
- Take again the set of all integers $\mathbb{Z}$ and define $x \sim y$ if and only if $x^2 \equiv y^2 \pmod 5$. Show that there are three equivalence classes [0], [1], [2].
- Take $A = \mathbb{R}^2$ and define $(x_1, y_1) \sim (x_2, y_2)$ if and only if $x_1^2 + y_1^2 = x_2^2 + y_2^2$. Then the equivalence class $[(x, y)]$ is the unique circle in $\mathbb{R}^2$ with the centre in $(0, 0)$ that goes through the point (x, y). The set of equivalence classes $A/\sim$ can be parametrized by a non-negative real number $r \geq 0$, which stands for the radius of the corresponding circle.

3.2.6 Definition. Let A be a set. A **partition** of A is a set $P \subseteq \mathscr{P}(A) = \{B \subseteq A\}$ of subsets of A that

1. are non-empty, i.e. $B \neq \emptyset$ for every $B \in P$,
2. are mutually disjoint, i.e. $B \cap C = \emptyset$ for every $B, C \in P$,
3. cover A, i.e. $\bigcup P = A$.

3.2.7 Theorem. Let A be a set. There is the following one-to-one correspondence between equivalence relations on A and partitions on A.

1. If $\sim$ is an equivalence on A, then $A/\sim$ is a partition of A.
2. If P is a partition of A, then we can define an equivalence on A by $x \sim y \Leftrightarrow (\exists B \in P)(x, y \in B)$

3.2.8 Example. Consider $A = \{1, 2, 3, 4, 5, 6\}$ and $R = \{(1, 2), (3, 2), (4, 5)\}$. Is R an equivalence? Certainly no! It is clearly neither reflexive, nor symmetric, nor transitive. Well, so try to figure out the smallest possible relation $\sim \subseteq A \times A$ which contains R and which is an equivalence. We can do this by first determining the

equivalence classes. You see that $1R2$ and $3R2$. If $\bar{R}$ is supposed to be an equivalence, then all the elements 1, 2, 3 must be mutually in relation. They will form one of the equivalence classes. Similarly, 4 and 5 are in a relation, so this will be the second equivalence class and 6 is not in a relation with anything, so it will have its own equivalence class.

So, we found out that $A/\sim = \{\{1,2,3\},\{4,5\},\{6\}\}$. The equivalence is then formally given by

$$\sim = \{(1,1),(2,2),(3,3),(1,2),(2,1),(1,3),(3,1),(2,3),(3,2),\\ (4,4),(5,5),(4,5),(5,4),(6,6)\}.$$

But if we wanted to be more practical and explain to somebody, how this relation works, we would just say that $1 \sim 2 \sim 3 \nsim 4 \sim 5 \nsim 6 \nsim 1$ and that it is an equivalence, from which the rest follows. Or it is just enough to specify the equivalence classes.

In order to prove the theorem, the following observation is crucial.

3.2.9 Lemma. Suppose $\sim$ is an equivalence on a set A. Then, for every $a, b \in A$,

a) $a \sim b \Rightarrow [a] = [b]$,
b) $a \nsim b \Rightarrow [a] \cap [b] = \emptyset$.

Proof. $[(a \sim b) \Rightarrow ([a] = [b])]$: Let us first prove that $[a] \subseteq [b]$. Take any $x \in [a]$. We are trying to prove that $x \in [b]$ as well. The fact $x \in [a]$ means that $x \sim a$. Since $a \sim b$, it follows by transitivity of $\sim$ that $x \sim b$. Hence, $x \in [b]$. The other inclusion works similar.

$[(a \nsim b) \Rightarrow ([a] \cap [b] = \emptyset)]$: Suppose there is $x \in [a] \cap [b]$. This means that $x \sim a$ and $x \sim b$. By symmetry of $\sim$, we have $a \sim x$ and by transitivity $a \sim b$. This is a contradiction. □

Proof of Theorem 3.2.7. The theorem has two parts, so let us prove them separately.

1. Take any equivalence $\sim$. We need to prove the defining properties of a partition. First, by reflexivity of $\sim$, all the equivalence classes are non-empty as $a \in [a]$. Second, the fact that the classes are mutually disjoint follows from Lemma 3.2.9. Finally, the fact that the classes cover A comes again from reflexivity as any $a \in A$ is an element of $[a]$.

2. Take any partition P. Proving that the given relation is an equivalence is straightforward. Do it as an exercise.

Finally, the reader may easily check that this is indeed a one-to-one correspondence: If you start with an equivalence $\sim$, construct the corresponding partition $P = A/\sim$ and then reconstruct the equivalence again, you must obtain the same thing you started with. The same work when starting with a partition P. □

3.3 Partial order

There are some other reasonable properties one might require from a relation. For instance, instead of being symmetric, one might require the following:

3.3.1 Definition. A relation R on a set A is called **antisymmetric** if $(\forall a, b \in A)(aRb \wedge bRa \Rightarrow a = b)$.

3.3.2 Definition. A relation R on a set A is called a **partial order** if it is reflexive, antisymmetric and transitive.

3.3.3 Examples.

- Take any set S and $A = \mathscr{P}(S)$. Then the relation $\subseteq$ is a partial order on A.
- For $A = \mathbb{R}$, we can consider the standard order $\leq$, which is a partial order. In this case, it is not only a partial order, but actually a *total* order as for any $x, y \in \mathbb{R}$, we have $x \leq y$ or $y \leq x$.
- For $A = \mathbb{N}$, the relation *divides* is a partial order.

3.3.4 Exercise. As you can easily check, the strict order $<$ on $\mathbb{R}$ is not a partial order. It is neither reflexive, nor antisymmetric. Try to modify these two axioms, so that $<$ would satisfy them. The modified axioms are known as being *irreflexive* and *asymmetric*.

4 Abstract algebra

4.1 Basic algebraic structures

4.1.1 Definition. Let S be a set. A **binary operation** on S is a mapping $S \times S \to S$.

The operation is usually denoted by some symbol such as $+, -, \cdot, \times, \circ, \bullet, *, \ldots$ So, we map for instance $(x, y) \mapsto x * y$.

4.1.2 Definition. An operation $\cdot\colon S \times S \to S$ is called

- **associative** if $(x \cdot y) \cdot z = x \cdot (y \cdot z)$,
- **commutative** if $x \cdot y = y \cdot x$.

4.1.3 Definition. A **semigroup** is a pair $(S, \cdot)$, where S is a set and $\cdot$ is a binary operation on S, which is associative.

4.1.4 Examples.

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{N}, +)$ are a semigroups.
- Subtraction $-$ is an operation on $\mathbb{R}$ as well as $\mathbb{Z}$. Nevertheless, it is not associative, so neither $(\mathbb{R}, -)$, nor $(\mathbb{Z}, -)$ is a semigroup. It does not restrict to $\mathbb{N}$ as for instance $2 - 3 \notin \mathbb{N}$, so $-$ is not a well-defined operation on $\mathbb{N}$ at all.
- $(\mathbb{R}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{N}, \cdot)$ are semigroups.
- $(M_n, +)$, $(M_n, \cdot)$ are semigroups, where M_n stands for the set of $n \times n$ matrices with entries in $\mathbb{R}$ (or any semigroup actually).
- For any set X, $(X^X, \circ)$ is a semigroup, where $X^X = \{f\colon X \to X\}$ and $\circ$ is the composition of functions.

4.1.5 Definition. Let S be a set, $\cdot$ a binary operation on S. An element $e \in S$ is called a **neutral element** (or an **identity**)[5] with respect to $\cdot$ if, for every $x \in S$, $x \cdot e = x = e \cdot x$.

4.1.6 Definition. A semigroup that contains an identity is called a **monoid**.

4.1.7 Examples.

- $(\mathbb{R}, +)$ is a monoid with $e = 0$. The same holds for $(\mathbb{Z}, +)$.
- $(\mathbb{R}, \cdot)$ is a monoid with $e = 1$. The same holds for $(\mathbb{Z}, \cdot)$.
- $(\mathbb{N}, +)$ is not a monoid, but $(\mathbb{N}, \cdot)$ is a monoid.
- $(M_n, +)$ is a monoid with $e = \mathbb{0}$, $(M_n, \cdot)$ is a monoid with $e = \mathbb{I}$.
- $(S_x, \circ)$ is a monoid with $e = \mathrm{id}$, where id is the identity function $\mathrm{id}(x) = x$.

4.1.8 Proposition. Let S be a set. For any operation $\cdot$ on S, there is at most one neutral element.

Proof. Suppose $e_1, e_2 \in S$ are both neutral elements. Then $e_1 = e_1 e_2 = e_2$. □

4.1.9 Definition. Let $(S, \cdot)$ be a monoid with identity e. We say that an element $x \in S$ has an **inverse** $y \in S$ if $x \cdot y = e = y \cdot x$.

4.1.10 Proposition. Let $(S, \cdot)$ be a monoid. If an element $x \in S$ has an inverse, then it is given uniquely.

Proof. Consider $x \in S$ and suppose $y_1, y_2 \in S$ are both its inverse. Then

$$y_1 = y_1 e = y_1(xy_2) = (y_1 x)y_2 = ey_2 = y_2.$$ □

4.1.11 Notation. Let $(S, \cdot)$ be a monoid. If $x \in S$ is *invertible* (has an inverse), we denote the inverse by x^{-1}. If the operation in the monoid is denoted by $+$, then the inverse of x is usually denoted by $-x$. Note that typically the sign $+$ is used to denote group operation only for abelian groups.

4.1.12 Proposition. Let $(S, \cdot)$ be a monoid with a unit e. Then

1. The unit is invertible with $e^{-1} = e$.
2. If $x \in S$ is invertible, then x^{-1} is invertible and $(x^{-1})^{-1} = x$.
3. If $x, y \in S$ are invertible, then $x \cdot y$ is invertible and $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

Proof. Follows from the following:

1. $e \cdot e = e$,
2. $x \cdot x^{-1} = e = x^{-1} \cdot x$,
3. $xy \cdot (y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e = \cdots = (y^{-1}x^{-1})xy$. □

4.1.13 Definition. A monoid where every element is invertible is called a **group**. A group is called **abelian** if the corresponding operation is commutative.

4.1.14 Examples.

[5] Actually *the* neutral element or *the* identity. See Prop. 4.1.8

- $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ are abelian groups.
- $(\mathbb{N}_0, +)$ is a monoid, but not a group.
- $(\mathbb{R}, \cdot)$ is not a group as $0 \in \mathbb{R}$ is not invertible.
- $(\mathbb{R} \setminus \{0\}, \cdot)$ is an abelian group. Also $(\mathbb{R}^+, \cdot)$ is an abelian group.
- $(\mathbb{Z}, \cdot)$ as well as $(\mathbb{N}, \cdot)$ is not a group.
- $(M_n, +)$ is an abelian group, while is $(M_n, \cdot)$ is not a group.
- $(\mathrm{GL}_n, \cdot)$ is a non-abelian group, where GL_n is the set of all invertible $n \times n$ matrices with entries in $\mathbb{R}$ (or any field).
- $(X^X, \circ)$ is not a group, but $(S_X, \circ)$ is a group, where S_X is the set of all bijections $X \to X$.

4.1.15 Theorem. Let $(S, \cdot)$ be a semigroup. Then $(S, \cdot)$ is a group if and only if $S \neq \emptyset$ and, for every $a, b \in S$, the equations $a \cdot x = b$ and $y \cdot a = b$ have a solution. If this is true, then the solution is unique.

Proof. $\Rightarrow$: Suppose $(S, \cdot)$ is a group. Then we can easily check that the solution is $x = a^{-1}b$ and $y = ba^{-1}$.

$\Leftarrow$: We need to check that $(S, \cdot)$ is a group. For that, we first need to find the unit. Take any $a \in S$ and $b := a$ and denote the solution of the first equation by e_a. So, $ae_a = a$. Now, take arbitrary $b \in S$. We find $y \in S$ such that $b = ya$, so $be_a = yae_a = ya = b$. So, $e := e_a$ is a *right unit*. By a similar procedure, we find a *left unit* e' satisfying $e'b = b$ for every $b \in S$. But now $e = e'e = e'$, so both must coincide and we have the unit. Finally, we must find the inverse for every $a \in S$. For that, solve equations $ax = e$ and $ya = e$. Then x is the *right inverse* of a and y is the *left inverse* of b. But these two must coincide by the proof of Proposition 4.1.10.

Finally, we prove the uniqueness. Suppose x_1, x_2 both satisfy the first equation. Then $x_1 = ex_1 = a^{-1}ax_1 = a^{-1}b = a^{-1}ax_2 = ex_2 = x_2$. Similarly for the second equation. □

4.2 Groups associated to $\mathbb{Z}_n$

4.2.1 Definition. Denoting $\equiv_n$ the relation of congruence modulo n for some $n \in \mathbb{N}$, we define

$$\mathbb{Z}_n = \mathbb{Z}/\equiv_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

where

$$[i]_n = \{x \in \mathbb{Z} \mid x \equiv i \pmod n\}.$$

If it is clear, which n, we take, we will usually omit the subscript n.[6]

We define the operations $+$ and $\cdot$ on $\mathbb{Z}_n$ as follows:

$$\begin{aligned} [i] + [j] &= [i + j], \\ [i] \cdot [j] &= [ij] \qquad \text{for any } i, j \in \mathbb{Z}. \end{aligned}$$

Before proceding further, we have to prove that this is a *good definition* – we have to prove that the result of these operations does not depend on the particular representatives of the equivalence classes we took.

[6] People are typically omitting the brackets as well and write just $i \in \mathbb{Z}_n$ instead of $[i] \in \mathbb{Z}_n$. I do not recommend doing that until you start feeling really familiar with $\mathbb{Z}_n$.

That is, for the addition $+$, we have to show that taking i', j' such that $[i'] = [i]$ and $[j'] = [j]$, we have $[i' + j'] = [i + j]$. Well, our assumption means that $i' \equiv i$ and $j' \equiv j$. Now, we can sum these two congruences and obtain $i' + j' \equiv i + j$. And this is exactly what we need.

For multiplication, it works the same.

4.2.2 Remark. By this, we just proved the fact that you we were intuitively using already when working with congruences. If we have any expression involving just addition and multiplication in a congruence modulo n, we can replace any number $x \in \mathbb{Z}$ by any other number $y \in \mathbb{Z}$ which is congruent to x.

4.2.3 Proposition. $(\mathbb{Z}_n, +)$ is an abelian group for any $n \in \mathbb{N}$.

Proof. Clearly, the operation $+$ is associative and commutative, because it has these properties on $\mathbb{Z}$. Clearly, $[0]$ is a neutral element. Finally, for any $[i] \in \mathbb{Z}_n$, we have the inverse $-[i] = [-i]$.

4.2.4 Example. Take $n = 3, 4$. We can write the *Cayley table* for $\mathbb{Z}_n$.

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

$+$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

Now, what about multiplication. Does it also form a group?

4.2.5 Proposition. $(\mathbb{Z}_n \cdot)$ is a commutative monoid for any $n \in \mathbb{N}$.

Proof. Exercise! □

4.2.6 Example. Again, write the Cayley table for $n = 3, 4$.

	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Now, we can see that $\mathbb{Z}_n$ is clearly never a group with respect to the multiplication simply because $[0] \cdot [i] = [0]$ for every i and hence $[0]$ is never invertible. We might try the idea of simply removing the $[0]$ and ask, whether $(\mathbb{Z}_n \setminus [0], \cdot)$ is a group. This looks that it might work for $n = 3$, but it will not work for $n = 4$ as you can see that $[2] \cdot [2] = [0]$. Let's try to understand the invertibility of elements in $(\mathbb{Z}_n, \cdot)$ better by computing some more complicated example.

4.2.7 Problem. Find the inverse of $[13]$ in $\mathbb{Z}_{36}$.

Solution. We look for $[j] \in \mathbb{Z}_{36}$ such that $[13][j] = [1]$. That is, we are trying to find $j \in \mathbb{Z}$ such that $13j \equiv 1 \pmod{36}$. We know how to do that! Just solve $1 = 13j + 36k$.

First, do the Euclid's algorithm:

$$36 = 2 \cdot 13 + 10$$
$$13 = 1 \cdot 10 + 3$$
$$10 = 3 \cdot 3 + 1$$

Now, express

$$1 = 10 - 3 \cdot 3 = -3 \cdot 13 + 4 \cdot 10 = 4 \cdot 36 - 11 \cdot 13,$$

so we found out that $[-11][13] = [1]$. That is $[13]^{-1} = [-11] = [25]$.

Will this computation work always? When does it fail?

4.2.8 Proposition. Consider $i, n \in \mathbb{N}$. Then $[i]$ is invertible in $\mathbb{Z}_n$ if and only if $i \perp n$.

Proof. By Theorem 2.4.11, there is $j \in \mathbb{Z}$ with $ij \equiv 1$ if and only if $i \perp n$.

4.2.9 Proposition. Let $(S, \cdot)$ be a monoid. Denote by G the set of all invertible elements in S. Then $(G, \cdot)$ is a group.

Proof. Follows from 4.1.12. □

4.2.10 Definition. For any $n \in \mathbb{N}$, we denote by $Z_n^\times$ the group of all invertible elements in $\mathbb{Z}_n$ with respect to the multiplication.

4.2.11 Proposition. If p is a prime, then all elements $[i] \in \mathbb{Z}_p$, $[i] \neq [0]$ are invertible. Therefore, $\mathbb{Z}_p \setminus \{[0]\} = \mathbb{Z}_p^\times$ is a group with respect to the multiplication.

Proof. For any i, $0 < i < p$, we clearly have $\gcd(i, p) = 1$. □

If n is not a prime, we have to kick out more elements than just $[0]$ from $\mathbb{Z}_n$ to obtain a group. So, it is not clear on the first sight, how many elements $\mathbb{Z}_n^\times$ should have.

4.2.12 Definition. We define the **Euler's totient function** $\phi\colon \mathbb{N} \to \mathbb{N}$ as

$$\phi(n) = \#\{k \in \mathbb{N} \mid k \leq n, k \perp n\} = |\mathbb{Z}_n^\times|.$$

4.2.13 Example. Let p, q be prime numbers. Try to prove that

$$\phi(p) = p - 1, \quad \phi(p^k) = p^k - p^{k-1}, \quad \phi(pq) = (p-1)(q-1).$$

4.2.14 Theorem. It holds that $\phi(nm) = \phi(n)\phi(m)$ if $n \perp m$.

We will not prove this theorem as it would require too much time. But in connection with Example 4.2.13 it gives us a practical way of computing the $\phi(n)$ for any n. For any n, consider its prime decomposition $n = p_1^{i_1} \cdots p_k^{i_k}$ such that all the primes $p_1, \ldots, p_k$ are mutually distinct. Then

$$\phi(n) = (p_1^{i_1} - p_1^{i_1 - 1}) \cdot (p_k^{i_k} - p_k^{i_k - 1}) = p_1^{i_1 - 1} \cdots p_k^{i_k - 1}(p_1 - 1) \cdots (p_k - 1).$$

As a motivation for the following section, we mention the following result:

4.2.15 Theorem (Euler). Consider, $a, n \in \mathbb{N}$, $a \perp n$. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Notice that the Theorem is a generalization of Little Fermat's theorem. Indeed, if you take $n = p$ to be a prime number, then $\phi(p) = p - 1$, so we exactly get what we already know.

It is possible to prove this theorem directly, but the group theory allows us to prove it in a much more elegant way. In fact, we are going to show in the next section that $a^{|G|} = e$ for any finite group G and any $a \in G$.

4.3 Subgroups

4.3.1 Definition. Let $(S, \cdot)$ be a semigroup. We say that a set $T \subseteq S$ forms a *subsemigroup* of if, for every $a, b \in T$, we have $a \cdot b \in T$.

4.3.2 Observation. Let $(S, \cdot)$ be a semigroup and $T \subset S$ a subsemigroup. Then $(T, \cdot)$ is a semigroup.

Proof. Exercise! □

The idea indeed is that a subsemigroup is just a subset, which itself is a semigroup *with respect to the same operation*.

4.3.3 Examples.

- $(\mathbb{N}, +)$ is a subsemigroup of $(\mathbb{Z}, +)$.
- $(\mathbb{R}^+, \cdot)$ is a subsemigroup of $(\mathbb{R}, \cdot)$.
- $(\mathrm{GL}_n, \cdot)$ is a subsemigroup of $(M_n, \cdot)$.
- $(\mathrm{GL}_n, +)$ is *not* a subsemigroup of $(M_n, +)$.

4.3.4 Definition. Let $(S, \cdot)$ be a monoid with a unit e. A subsemigroup $T \subset S$ is called a *submonoid* if $e \in T$.

4.3.5 Exercise. Go through the above examples of subsemigroups. Which of them are submonoids?

4.3.6 Remark. Again, a submonoid is just a subset, which is also a monoid with respect to the same operation *and the same unit*. The latter condition is essential! It can happen that a monoid has a subsemigroup, which is a monoid again, but it is not a submonoid as it has a different unit.

The simplest example can be constructed as follows. Consider $S = \{(a, b) \mid a, b \in \mathbb{Z}\}$ with an operation $(a, b) \cdot (c, d) = (ac, bd)$. This is a monid with the unit $(1, 1)$. Now, we can construct a subsemigroup $T = \{(a, 0) \mid a \in \mathbb{Z}\} \subset S$. It actually is a monoid with respect to the unit $e' = (1, 0)$. But since the unit is different, it is not a submonoid.

4.3.7 Definition. Let $(G, \cdot)$ be a group with a unit e. Then a subset $H \subset G$ forms a *subgroup* of G if

1. for all $x, y \in H$, we have $xy \in H$,

2. we have $e \in H$,
3. for all $x \in H$, we have $x^{-1} \in H$.

4.3.8 Proposition (Equivalent definition of a subgroup). Let $(G, \cdot)$ be a group. Then $H \subset G$ forms a subgroup if and only if $H \neq \emptyset$ and, for every $x, y \in H$, we have $xy^{-1} \in H$.

Proof. Exercise! □

4.3.9 Proposition. Let $(G, \cdot)$ be a group. Suppose $H_1, H_2 \subseteq G$ are subgroups. Then $H_1 \cap H_2$ is a subgroup.

Proof. Exercise! □

4.3.10 Definition. Let $(G, \cdot)$ be a group, $g_1, \ldots, g_n \in G$. We denote by $\langle g_1, \ldots, g_n \rangle$ the smallest[7] subgroup containing the elements $g_1, \ldots, g_n$. We say call it the subgroup *generated by* $g_1, \ldots, g_n$.

4.3.11 Exercise. Use Proposition 4.3.9 to prove that $\langle g_1, \ldots, g_n \rangle$ always exists.

4.3.12 Problem. What is the smallest subgroup of $(\mathbb{Z}, +)$ containing the element $3 \in \mathbb{Z}$?

Solution. Let us denote the subgroup by $\langle 3 \rangle$. Since it is supposed to be a subgroup, it must be closed under the operation $+$. So, it must contain also $3 + 3 = 6$, 9, 12, 15, ... It must also contain the neutral element 0. And it must also be closed under taking the inverse (opposite number), so it must also contain -3, -6, -9 ... We can guess that the solution is

$$\langle 3 \rangle = \{3j \mid j \in \mathbb{Z}\} = 3\mathbb{Z}.$$

It remains to show that this is indeed a subgroup.

4.3.13 Proposition. For any $k \in \mathbb{Z}$, the set

$$k\mathbb{Z} = \{jk \mid j \in \mathbb{Z}\}$$

forms a subgroup of $(\mathbb{Z}, +)$.

Proof. Take any $j_1, j_2 \in \mathbb{Z}$. Then $j_1 k - j_2 k = (j_1 - j_2)k \in k\mathbb{Z}$, which is according to Proposition 4.3.8 enough. □

4.3.14 Problem. In $(\mathbb{Z}_{35}, +)$, find $\langle [5] \rangle$, $\langle [7] \rangle$, $\langle [10] \rangle$, $\langle [6] \rangle$. How many elements do these subgroups have?

Solution. Let's start with $\langle [5] \rangle$. Since it is a subgroup, it must contain also [10], [15], ... and also [0]. That's actually enough. We claim that

$$\langle [5] \rangle = \{[0], [5], [10], [15], [20], [25], [30]\} = \{[5k] \mid k = 0, 1, \ldots, 6\}.$$

It is indeed a subgroup since $[5k] - [5l] = [5(k - l)]$ and the remainder of $5(k - l)$ when dividing by 35 must be between 0 and 34 and it clearly must be a multiple of

[7] Smallest with respect to the partial order *being a subgroup*. That is, if $H \subseteq G$ is a subgroup containing $g_1, \ldots, g_n$, then necessarily $\langle g_1, \ldots, g_m \rangle \subseteq H$.

five, so it must be one of the above numbers. As we can see, this subgroup has seven elements. (Note that $7 = 35/5$.)

For [7] it works the same. We find out that

$$\langle [7] \rangle = \{[0], [7], [14], [21], [28]\} = \{[7k] \mid k = 0, 1, 2, 3, 4\}.$$

This subgroup has five elements. Again, recall that $35 = 5 \cdot 7$. Coincidence? I think not.

For [10], it is a bit trickier. It must contain [0], [10], [20], [30], [40] = [5], [15], [25], and again [35] = [0]. After all, we find out that actually $\langle [10] \rangle = \langle [5] \rangle$.

Finally, maybe the most surprising is $\langle [6] \rangle$. It must contain [0], [6], [12], [18], [24], [30], [36] = [1], [7], [13] ... We could continue. But wait a moment. If it contains [1], it must contain [2], [3], [4] and so on. So, actually, it is the whole group! $\langle [6] \rangle = \mathbb{Z}_{35}$

The purpose of the following will be trying to understand the behaviour above.

4.3.15 Definition. Let $(G, \cdot)$ be a group, $H \subset G$ a subgroup. For any $g \in G$, we define it's **left coset** with respect to H as

$$gH = \{gh \mid h \in H\}.$$

We denote by $G/H = \{gH \mid g \in G\}$ the set of all left cosets.

4.3.16 Theorem. Let $(G, \cdot)$ be a group and $H \subset G$ its subgroup. Then G/H is a partition of G.

Proof. The cosets are clearly non-empty since any subgroup is non-empty (containing at least the identity). Secondly, the cosets clearly cover G as $g \in gH$ for every $g \in G$ (taking $h = e$. Finally, we have to show that the cosets are mutually disjoint. That is, taking $g_1, g_2 \in G$, we have to show that either $g_1H = g_2H$ or $g_1H \cap g_2H = \emptyset$. Assume that $g_1H \cap g_2H \neq \emptyset$. So, there are $h_1, h_2 \in H$ such that $g_1h_1 = g_2h_2$. But then, for any $h \in H$,

$$g_1h = g_1h_1h_1^{-1}h = g_2h_2h_1^{-1}h \in g_2H,$$

so $g_1H \subseteq g_2H$. Similarly, we show the opposite inclusion and prove the desired equality $g_1H = g_2H$. □

4.3.17 Corollary. There is an equivalence relation

$$g_1 \sim g_2 \quad \Leftrightarrow \quad g_1H = g_2H.$$

4.3.18 Exercise. Prove that $g_1 \sim g_2$ if and only if $g_2^{-1}g_1 \in H$.

4.3.19 Remark. We can also define *right cosets* as $Hg = \{hg \mid g \in G\}$ that would define another equivalence $g_1 \sim g_2$ if and only if $Hg_1 = Hg_2$, which holds if and only

if $g_2 g_1^{-1} \in H$. If the group is commutative, then these two notions are the same. If the group is not commutative, then they might and might not be the same.

4.3.20 Notation. If the opretaion is written *additively* (using the + sign), we write $g + H$ instead of gH.

4.3.21 Example. Take the group $(\mathbb{Z}, +)$ and its subgroup $n\mathbb{Z}$. Then the cosets are given by

$$j + n\mathbb{Z} = \{j + ki \mid i \in \mathbb{Z}\} = [j]_n.$$

So, they are the residue classes modulo n. That is, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$. What is the equivalence? Well, $i \sim j$ if and only if $[i] = [j]$ if and only if $i - j \in n\mathbb{Z}$. So, it is the congruence modulo n.

4.3.22 Exercise. Suppose $(G, \cdot)$ is a group and $\equiv$ is an equivalence on G such that

$$a \equiv b \wedge c \equiv d \quad \Rightarrow \quad a \cdot c \equiv b \cdot d. \tag{$*$}$$

Prove that $G/\equiv$ is a group with respect to the operation $[x] \cdot [y] = [x \cdot y]$. (Do not forget to prove that such an operation is well defined.) If e is the unit of G, prove that $[e]$ is a subgroup of G. Show that the associated cosets coincide with the equivalence classes, i.e. $x[e] = [x]$. Conversely, given any subgroup H, prove that the associated equivalence defined by Corollary 4.3.17 satisfies $(*)$ if and only if $gH = Hg$ for every $g \in G$.

4.3.23 Definition. Let $(G, \cdot)$ be a group, $H \subseteq G$ a subgroup. Then H is called **normal** if $gH = Hg$ for every $g \in G$. In this case, we define the **quotient group** to be the set of cosets G/H with respect to the operation $[g_1][g_2] = [g_1 g_2]$, where $[g] = gH$.

4.3.24 Definition. Let $(G, \cdot)$ be a group, $H \subseteq G$ a subgroup. Then the number of cosets $|G/H|$ is called the **index** of H and denoted by $[G\colon H]$.

4.3.25 Definition. Let $(G, \cdot)$ be a group. We define the **order** of G to be the number of its elements (if G is finite). If G has infinitely many elements, we say that the order is infinite.

4.3.26 Theorem (Lagrange). Let $(G, \cdot)$ be a finite group and $H \subseteq G$ its subgroup. Then $|G| = [G\colon H] \cdot [H]$.

Proof. It is a direct consequence of the following lemma. □

4.3.27 Lemma. Suppose H is finite. Then all left cosets have the same size $|gH| = |H|$.

Proof. Denote $H = \{h_1, \ldots, h_n\}$. Then $gH = \{gh_1, \ldots, gh_n\}$, so $|gH| \leq |H|$. But also $H = \{g^{-1}gh_1, \ldots, g^{-1}gh_n\}$, so actually $|H| = |gH|$. □

4.3.28 Notation. Let $(G, \cdot)$ be a group and e its identity. Take $a \in G$, $k \in \mathbb{N}$. We denote

$$a^0 = e, \quad a^k = \underbrace{a \cdot a \cdots a}_{k\times}, \quad a^{-k} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{k\times}.$$

So, in total we define a^k for any $k \in \mathbb{Z}$. If the operation is denoted by $+$, then we rather use ka instead of a^k.

4.3.29 Proposition. Let $(G, \cdot)$ be a group, $a \in G$. Then $\langle a \rangle = \{a^j \mid j \in \mathbb{Z}\}$.

Proof. The right-hand-side clearly is a subgroup as $a^j(a^k)^{-1} = a^{j-k}$. Conversely, any subgroup containing a must also contain a^j for any $j \in \mathbb{Z}$. □

4.3.30 Definition. Let $(G, \cdot)$ be a group, $a \in G$. The smallest $j \in \mathbb{N}$ such that $a^j = e$ is called the **order** of a. If there is no such j, we say that the order is infinite.

4.3.31 Observation. The order of a is the order of $\langle a \rangle$.

Proof. Exercise! □

4.3.32 Theorem. Let $(G, \cdot)$ be a finite group, $a \in G$. Then the order of a divides the order of G.

Proof. By Lagrange's theorem. □

4.3.33 Corollary (Euler's theorem). Let $a, n \in \mathbb{N}$, $a \perp n$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.

4.3.34 Definition. A group $(G, \cdot)$ is called **cyclic** if there is $a \in G$ such that $G = \langle a \rangle$.

4.3.35 Observation. All $(\mathbb{Z}_n, +)$ ass well as $(\mathbb{Z}, +)$ are cyclic.

Proof. Clearly $[1] \in \mathbb{Z}_n$ is a generator. For $\mathbb{Z}$, 1 is a generator. □

4.3.36 Theorem. $(\mathbb{Z}_p^\times, \cdot)$ is cyclic whenever p is a prime.

The proof of this theorem is beyond the scope of this subject, but let us check it for a couple of examples.

4.3.37 Problem. Show that $(\mathbb{Z}_7^\times, \cdot)$ is cyclic.

Solution. We just need to find a generator, i.e. an element $a \in \mathbb{Z}_7^\times$ of order 6. Let us do some trial and error.

[1] clearly has order one.

What is the order of [2]?

$$[2]^1 = [2], \quad [2]^2 = [4], \quad [2]^3 = [8] = [1],$$

so the order of [2] is 3.

What is the order of [3]?

$$[3]^1 = 3, \quad [3]^2 = [2], \quad [3]^3 = [6], \quad [3]^4 = [4], \quad [3]^5 = [5], \quad [3]^6 = 1.$$

That's it! We found a generator.

4.3.38 Problem. Show that $(\mathbb{Z}_8^\times, \cdot)$ is not cyclic.

Solution. First, we should determine, what are actually the elements of $\mathbb{Z}_8^\times$. These are all $[i]$ with $0 < i < 8$ such that $i \perp 8$, which just means that i is odd. That is $\mathbb{Z}_8^\times = \{[1], [3], [5], [7]\}$. We easily compute that

$$[3]^2 = [1], \quad [5]^2 = [1], \quad [7]^2 = [1],$$

so all elements (except for [1]) have order two.

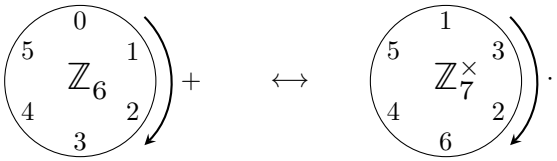
You might already have noticed the following fact:

4.3.39 Theorem. Every cyclic group is isomorphic to $(\mathbb{Z}_n, +)$ for some $n \in \mathbb{N}$ or $(\mathbb{Z}, +)$.

We did not define what *isomorphic to* actually means, so let us just give an idea of what we mean by this. Well, take any cyclic group $(G, \cdot)$, $G = \langle a \rangle$ for some $a \in G$. If it is finite of order n, then we have $G = \{a^i \mid i = 0, 1, \ldots, n\}$ and the group operation must be given by $a^i \cdot a^j = a^{i+j} = a^{(i+j) \bmod n}$. This is exactly how the group operation in $(\mathbb{Z}_n, +)$ works, right?

If G is infinite, then $G = \{a^i \mid i \in \mathbb{Z}\}$ and the group operation is just $a^i \cdot a^j = a^{i+j}$, which exactly corresponds to $(\mathbb{Z}, +)$.

You can see this on the example of $(\mathbb{Z}_7^\times, \cdot)$. We claim that it is isomorphic to $(\mathbb{Z}_6, +)$. Well, indead. Computing in $(\mathbb{Z}_6, +)$ is just like computing on a clock dial with five numbers 0, 1, 2, 3, 4, 5. Computing in $(\mathbb{Z}_7^\times, \cdot)$ actually works the same, except that somebody has shuffled the numbers.



Finally, let us get back to the problem, we started with. Take a cyclic group $(\mathbb{Z}_n, +)$ and choose some $[a] \in \mathbb{Z}_n$. Can you determine, what the order of $\langle [a] \rangle$ is?

4.3.40 Lemma. Let $(G, \cdot)$ be a group, $a \in G$. Then the order of a equals $r \in \mathbb{N}$ if and only if

1. $a^r = e$,
2. if $a^s = e$, then $r \mid s$.

Proof. The implication $\Leftarrow$ is clear. For the opposite, (1) is obvious, so let us prove (2). Take any $s \in \mathbb{N}$ such that $a^s = e$. Sinc r is the order, so the smallest number with such a property, we must have $s \geq r$. Let us do the division with remainder: $s = kr + z$, $0 \leq z < r$. Then $e = a^s = a^{kr+z} = a^{kr}a^z = a^z$. Since r is the order, we must have $z = 0$. □

4.3.41 Proposition. Let $(G, \cdot)$ be a group, $a \in G$. Let a be of order r. Then the order of a^i is given by $r' = r/\gcd(r, i)$.

Proof. We use the preceding lemma. So, we need to show that $(a^i)^{r'} = e$ and that if $(a^i)^s = e$, then $r' \mid s$. Denote $d := \gcd(r, i)$ and $l = i/d$.

For the first thing:

$$(a^i)^{r'} = a^{ir/d} = a^{rl} = e^l = e.$$

For the second, assume $e = a^{is}$. Then $r \mid is$, i.e. $r'd \mid is$, so in particular $r' \mid is$. We have $\gcd(r', i) = 1$, so by Euclid's lemma $r' \mid s$. □

4.3.42 Example. In Problem 4.3.14, we asked what is the order of [5], [7], [10], and [6] in $(\mathbb{Z}_{35}, +)$. We can easily answer this now using the above formula. Note that in $(\mathbb{Z}_n, +)$, we have that $[i] = i[1]$ for any $i \in \mathbb{Z}$ and that the order of [1] is n. So:

$$\begin{aligned}
|\langle[5]\rangle| &= 35/\gcd(35,5) = 35/5 = 7\\
|\langle[7]\rangle| &= 35/\gcd(35,7) = 35/7 = 5\\
|\langle[10]\rangle| &= 35/\gcd(35,10) = 35/5 = 7\\
|\langle[6]\rangle| &= 35/\gcd(35,6) = 35/1 = 35
\end{aligned}$$

As you can see from this example, we can in particular easily characterize the generators of any cyclic group.

4.3.43 Problem. How many distinct generators does $(\mathbb{Z}_n, +)$ have? (Any cyclic group of order n?)

Solution. Suppose $(G, \cdot)$ is a cyclic group of order n, $G = \langle a\rangle$ for some $a \in G$. That is, $G = \{a^i \mid 0 \le i < n\}$. The order of an element a^i is $n/\gcd(n,i)$, so a^i is a generator if and only if $\gcd(n,i) = 1$. Consequently, G has $\phi(n)$ generators.

4.3.44 Problem. Classify all subgroups of $(\mathbb{Z}_n, +)$ (any cyclic group of order n).

Solution. For any $d \mid n$, we obviously have the following subgroup of order $m = n/d$:

$$\langle[d]\rangle = \{[0], [d], [2d], \ldots, [n-d]\}.$$

We claim that there are no other subgroups. In fact, it holds that

$$\langle[i_1], \ldots, [i_k]\rangle = \langle[d]\rangle, \qquad \text{where } d = \gcd(n, i_1, \ldots, i_k).$$

We can prove that in two steps as follows:

1. For any $i \in \mathbb{Z}$, we have $\langle[i]\rangle = \langle[d]\rangle$, where $d = \gcd(n,i)$.
2. For any $i, j \mid d$, we have $\langle[i],[j]\rangle = \langle[d]\rangle$, where $d = \gcd(i,j)$.

Do it as an exercise!

4.4 Rings and fields

4.4.1 Definition. A **ring** is a triple $(R, +, \cdot)$ such that $(R, +)$ is a commutative group and $(R, \cdot)$ is a monoid and, in addition, the *distributive law* holds: For every $a, b, c \in R$,

$$\begin{aligned}
a \cdot (b + c) &= (a \cdot b) + (a \cdot c),\\
(b + c) \cdot a &= (b \cdot a) + (c \cdot a).
\end{aligned}$$

If the operation $\cdot$ is commutative, we call it a *commutative ring*.

4.4.2 Notation. We will always denote the first operation by $+$ and call it the *addition*, while the second will be denoted $\cdot$ and called *multiplication*. As with numbers, the dot is often ommited. We use the standard order of operations, where the multiplication has a higher precedence. We denote by $0 \in R$ the neutral element

of addition and by $1 \in R$ the neutral element of multiplication. Also recall that we denote by $-a$ the inverse of a with respect to addition. We also write $a-b := a+(-b)$.

4.4.3 Remark. Some authors do not assume the existence of 1, i.e. the neutral element of multiplication. You should always check the exact definition when studying some mathematical text about rings.

4.4.4 Theorem. Let $(R, +, \cdot)$ be a ring, $a, b, c \in R$. Then

1. $a(b-c) = ab - ac$, $(b-c)a = ba - ca$,
2. $0 \cdot a = 0 = a \cdot 0$,
3. $(-a)b = -(ab) = a(-b)$.

Proof. Let's prove that $0 \cdot a = 0$. Do the rest as an exercise.

$$0 \cdot a = (a-a) \cdot a = a \cdot a - a \cdot a = 0. \qquad \square$$

4.4.5 Remark. As a consequence, $0 \neq 1$ for any ring with more than one element. Indeed, if $0 = 1$, then $a = 1 \cdot a = 0 \cdot a = 0$ for all $a \in R$.

4.4.6 Examples.

- $(\mathbb{R}, +, \cdot)$ is a commutative ring,
- $(M_n, +, \cdot)$ is a non-commutative ring for any $n \in \mathbb{N}$, $n > 1$,
- $(\mathbb{Z}, +, \cdot)$ is a commutative ring,
- $(\mathbb{Z}_n, +, \cdot)$ is a commutative ring for any $n \in \mathbb{N}$.
- If R is a (commutative) ring, then $(R[x], +, \cdot)$ is a (commutative) ring, where $R[x]$ is the set of all polynomials with coefficients in R.

4.4.7 Definition. Let $(R, +, \cdot)$ be a ring. An element $a \in R$, $a \neq 0$ is called a **zero divisor** if there exists $b \in R$, $b \neq 0$ such that $ab = 0$.

4.4.8 Examples.

- In $\mathbb{Z}_6$, we have $[2] \cdot [3] = [6] = 0$.
- In M_2, we have

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \qquad \text{or} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

4.4.9 Lemma. Let $(R, +, \cdot)$ be a ring. If $ab \in R$ is a zero divisor, then it is not invertible.

Proof. Suppose a is invertible and $ab = 0$. Then

$$b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0 \qquad \square$$

4.4.10 Definition. A commutative ring without zero divisors is called an **integral domain**[8].

4.4.11 Definition. A ring $(R, +, \cdot)$ such that $(R \setminus \{0\}, \cdot)$ is a group is called a **field**.

4.4.12 Examples.

[8] The name might be slightly confusing. The adjective *integral* has nothing to do with integrals from analysis and the name *domain* has nothing to do with domains in analysis. The only point is that an integral domain has similar properties as the set (ring) of integers $\mathbb{Z}$.

- $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ are fields.
- $(\mathbb{Z}_p, +, \cdot)$ is a field if and only if p is a prime.
- There are so-called *Galois fields* $GF(p^k)$ that have p^k elements, where p is a prime and $k \in \mathbb{N}$. These are the only finite fields. (Every finite field is isomorphic to some Galois field.)
- $(M_n, +, \cdot)$ is not a field as not every non-zero matrix is invertible.
- $(\mathrm{GL}_n, +, \cdot)$ is not a field as invertible matrices are not closed under addition.

4.4.13 Theorem. Let $(F, +, \cdot)$ be a finite field. Then $(F \setminus \{0\}, \cdot)$ is a cyclic group.

This explains why $(\mathbb{Z}_p^\times, \cdot)$ is cyclic whenever p is prime. Nevertheless, we leave the theorem without proof.

4.5 Lattices and Boolean algebras

4.5.1 Definition. A **lattice**[9] is a triple $(L, \wedge, \vee)$, where $\wedge$ and $\vee$ are binary operations on L satisfying

- the associativity laws $(a \wedge b) \wedge c = a \wedge (b \wedge c)$, $(a \vee b) \vee c = a \vee (b \vee c)$,
- the commutativity laws $a \wedge b = b \wedge a$, $a \vee b = b \vee a$,
- the absorption laws $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$.

for every $a, b, c \in L$. The operation $\wedge$ is called the **meet** and $\vee$ is called the **join**.

4.5.2 Lemma. Let $(L, \wedge, \vee)$ be a lattice. Then the operations satisfy $a \wedge a = a$ and $a \vee a = a$ for every $a \in L$ (the *idempotent law*).

Proof. For the first, use the absorption laws: $a \wedge a = a \wedge (a \vee (a \wedge a)) = a$. Do the second as an exercise! □

4.5.3 Examples.

- For any set U, $(\mathscr{P}(U), \cap, \cup)$ is a lattice.
- $(\mathbb{R}, \min, \max)$ is a lattice. The same works with any $A \subset \mathbb{R}$.
- $(\mathbb{N}, \gcd, \mathrm{lcm})$ is a lattice.
- For a vector space L, denote by $S(V)$ the set of all its subspaces. Then $(S(V), \cap, +)$ is a lattice.

It seems that lattices are closely connected to orders. (Which order was it for the first example?) Let us now prove the correspondence.

4.5.4 Lemma. Let $(L, \wedge, \vee)$ be a lattice, $a, b \in L$. Then $a \wedge b = a$ if and only if $a \vee b = b$.

Proof. Assume $a \wedge b = a$. Then $a \vee b = (a \wedge b) \vee b = b$. Do the opposite as an exercise! □

[9] This is an unfortunate name. The notion *lattice* has also a different meaning in mathematics and physics. See `https://en.wikipedia.org/wiki/Lattice_(group)`.

4.5.5 Theorem. For every lattice $(L, \wedge, \vee)$, the relation

$$a \leq b \quad \Leftrightarrow \quad a \wedge b = a \quad (\Leftrightarrow \quad a \vee b = b)$$

is a partial order on L.

Proof. Exercise!

4.5.6 Remark. What is the meaning of $\wedge$ and $\vee$ then? If a and b are comparable, i.e. $a \leq b$ or $b \leq a$, then $a \wedge b$ is the smaller element, while $a \vee b$ is the larger one. What about if they are not comparable? Then $a \wedge b$ is the *infimum* of the set $\{a, b\}$. That is, the greatest element of L, which is smaller than both a and b (their *greatest lower bound*). Try to write a formal definition and prove this statement. Similarly, $a \vee b$ is in general the *supremum* (*least upper bound*) of $\{a, b\}$. Note that for a general partially ordered set an infimum or supremum of some given $\{a, b\}$ might not even exist. But here it does.

This also gives a hint on how to formulate a converse of this theorem. A set P equipped with a partial order $\leq$ is called a *lattice* if any two elements $a, b \in P$ have the greatest lower bound and the least upper bound. Denoting these two elements by $a \wedge b$ and $a \vee b$, these operations satisfy the axioms of a lattice according to Definition 4.5.1.

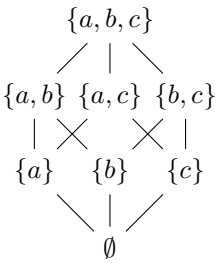
4.5.7 Definition. Let $(L, \wedge, \vee)$ be a lattice. An element $\mathbf{0}$ is called the **least** element of L if $\mathbf{0} \wedge a = \mathbf{0}$ (or, equivalently, $\mathbf{0} \vee a = a$) for every $a \in L$. An element $\mathbf{1}$ is called the **greatest** element of L if $\mathbf{1} \wedge a = a$ (or, equivalently, $\mathbf{1} \vee a = \mathbf{1}$) for every $a \in L$. A lattice that has both is called **bounded**.

It is convenient to depict finite lattices using diagrams. Remember the graphs we were drawing when dealing with relations. We will modify them here a bit. Given a lattice $(L, \wedge, \vee)$ and the corresponding order $\leq$, we will draw a line $a \to b$ if $a \leq b$ and there is no c such that $a \leq c \leq b$. Without the second condition, there would be too many lines. This way, it holds that $a \leq b$ if and only if there is a *path* from a to b.[10] In addition, we draw the elements in layers. Whenever $a \leq b$, we will draw a below b. In that way, we do not have to draw arrows, but simple edges. See the following examples, which should also reveal the reason for the name *lattice*.

4.5.8 Examples.

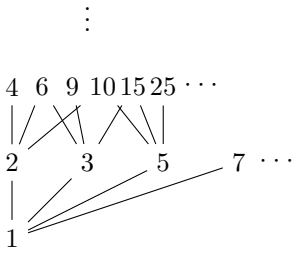
[10] Recall for instance the order *is ancestor of* on the set of people. This is an order, but drawing a family tree such that there is a line between any two people, where one is the ancestor of the other would be too messy. Instead, we draw the graph corresponding to the relation *is a parent of*, which is not an order. The order considered originally is, however, the *transitive closure* of the latter.

- Consider the set $U = \{a, b, c\}$. Then the power set $\mathscr{P}(U)$ has $2^3 = 8$ elements that can be arranged as follows:



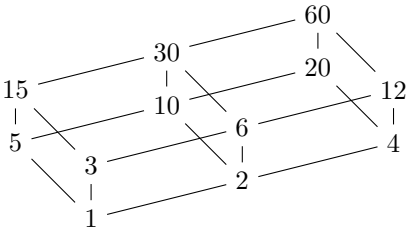
  Here, we have the least element $\mathbf{0} = \emptyset$ and the greatest element $\mathbf{1} = U = \{a, b, c\}$. It is maybe worth pointing out that in mathematics, we distinguish the notions *least* and *minimal* (as well as *greatest* and *maximal*). An element x of a partially ordered set is called *minimal* if there is no smaller element, i.e. for every $y \leq x$, we have $y = x$. If we remove $\emptyset$ from our set of subsets, then there will be no least element. That is, there will be no set $A \subset U$, which is a subset of all the others. But there will be three minimal elements $\{a\}$, $\{b\}$, and $\{c\}$.

- Consider the lattice $(\mathbb{N}, \gcd, \operatorname{lcm})$. Since $\mathbb{N}$ is infinite, we clearly cannot draw the whole diagram, but it would look approximately like this



  This set has a least element $\mathbf{0} = 1$. It does not have any greatest element (and actually even any maximal element). If we define $\gcd(0, k) = 0$ for any k and $\operatorname{lcm}(0, k) = k$ for every k (this corresponds to saying that everything divides zero or that zero is a multiple of anything, which makes sense as $0 \cdot k = 0$ for any k), then we can consider the lattice $(\mathbb{N}_0, \gcd, \operatorname{lcm})$ which already has a greatest element $\mathbf{1} = 0$.

- Consider the set $D_{60} := \{i \in \mathbb{N} \mid i \mid 60\}$ – the set of all divisors of 60. Then the diagram corresponding to $(D_{60}, \gcd, \mathrm{lcm})$ looks as follows



4.5.9 Definition. A lattice $(L, \wedge, \vee)$ is called **distributive** if the following distributive laws hold for every $a, b, c \in L$

$$a \wedge (b \vee c) = (a \wedge c) \vee (b \wedge c),$$
$$a \vee (b \wedge c) = (a \vee b) \wedge (b \vee c).$$

4.5.10 Remark. Actually, one already implies the other. Indeed, assume the first one, then

$$\begin{aligned}(a \vee b) \wedge (a \vee c) &= ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) \\ &= a \vee ((a \wedge c) \vee (b \wedge c)) = (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c))\end{aligned}$$

As an exercise, prove the other direction!

4.5.11 Definition. Let $(L, \wedge, \vee)$ be a bounded lattice, $a \in L$. We say that $b \in L$ is a complement of a if $a \wedge b = \mathbf{0}$ and $a \vee b = \mathbf{1}$.

4.5.12 Exercise. Which elements of D_{60} have a complement?

4.5.13 Theorem. Let $(L, \wedge, \vee)$ be a distributive lattice, $a, b, c \in L$. Then the equalities $a \vee b = a \vee c$ and $a \wedge b = a \wedge c$ imply $b = c$.

Proof. Assume the mentioned equalities. Then

$$\begin{aligned}b = (a \vee b) \wedge b = (a \vee c) \wedge b = (a \wedge b) \vee (c \wedge b) \\ = (a \wedge c) \vee (b \wedge c) = (a \vee b) \wedge c = (a \vee c) \wedge c = c.\end{aligned}$$ □

4.5.14 Corollary. In a bounded distributive lattice, every element has at most one complement.

We will denote the unique complement of a by $\bar{a}$.

4.5.15 Definition. A **Boolean algebra** is a bounded distributive lattice, where every element has a complement.

4.5.16 Theorem. Let $(B, \wedge, \vee)$ be a Boolean algebra. Then

1. $\bar{\mathbf{1}} = \mathbf{0}$, $\bar{\mathbf{0}} = \mathbf{1}$.
2. $\overline{a \wedge b} = \bar{a} \vee \bar{b}$, $\overline{a \vee b} = \bar{a} \wedge \bar{b}$.
3. $\bar{\bar{a}} = a$.

Proof. Exercise! □

4.5.17 Example. For any set U, the lattice $(\mathscr{P}(U), \cap, \cup)$ is a Boolean algebra.

4.5.18 Exercise. Fix a finite set U. If you wanted to represent the elements of $\mathscr{P}(U)$ in a computer, you would probably number the elements of U, so $U = \{x_1, \dots, x_n\}$ and then any given $A \subseteq U$ would be represented by an array of booleans $(b_1, \dots, b_n)$, $b_i \in \{0, 1\}$ (or $b_i \in \{\text{true}, \text{false}\}$), where $x_i \in A$ if and only if $b_i = 1$. Now, try to express the operations $\cap$ and $\cup$ in terms of the arrays $(b_1, \dots, b_n)$.

4.5.19 Example. Put $B = \{0, 1\}$. For $a, b \in B$, define

$$\begin{aligned} a \wedge b &= \min\{a, b\}, && (\text{so } 0 \wedge 0 = 0 \wedge 1 = 1 \wedge 0 = 0,\ 1 \wedge 1 = 1),\\ a \vee b &= \max\{a, b\}, && (\text{so } 0 \vee 0 = 0,\ 0 \vee 1 = 1 \vee 0 = 1 \vee 1 = 1). \end{aligned}$$

Then $(B, \wedge, \vee)$ is a Boolean algebra with $\mathbf{0} = 0$, $\mathbf{1} = 1$.

Now, define

$$B_n = \underbrace{B \times \cdots \times B}_{n\times} = \{(b_1, \dots, b_n) \mid b_1, \dots, b_n \in B\}.$$

We define the operations entrywise

$$\begin{aligned} (a_1, \dots, a_n) \wedge (b_1, \dots, b_n) &= (a_1 \wedge b_1, \dots, a_n \wedge b_n),\\ (a_1, \dots, a_n) \vee (b_1, \dots, b_n) &= (a_1 \vee b_1, \dots, a_n \vee b_n). \end{aligned}$$

Then $(B_n, \wedge, \vee)$ is again a Boolean algebra.

4.5.20 Theorem. Every finite Boolean algebra is isomorphic to B_n for some n.

5 Enumerative combinatorics

5.1 Problem. How many ordered pairs (i, j), $i = 1, \dots, n$, $j = 1, \dots, m$ are there?

Solution. For each fixed j, we have n pairs (i, j) as i can attain n different values. Since we have m possibilities for j, the answer is $n \cdot m$.

5.2 Problem. How many functions $\{1, 2, 3, 4\} \to \{1, 2, 3\}$ are there? In general, how many functions $\{1, \dots, n\} \to \{1, \dots, m\}$ are there?

Solution. A function $f\colon \{1, \dots, n\} \to \{1, \dots, m\}$ is determined by its function values. So, for each $x \in \{1, \dots, n\}$, we have to fix the corresponding $y = f(x)$. This means that such a function is precisely determined by a tuple $(y_1, \dots, y_n)$, $y_i = f(i)$. Each y_i can attain m different values. By a similar argumentation as in the previous problem, we can see that there are $m \cdot m \cdots m = m^n$ such tuples.

5.3 Observation. For any tuple of sets $A_1, \dots, A_k$, we have

$$\#(A_1 \times \cdots \times A_k) = \#A_1 \cdots \#A_k.$$

This gives us a tool how to solve certain counting problems, which is sometimes called the *multiplication principle*: Assume that a certain activity can be divided

into k independent steps. Suppose Step 1 can be done in n_1 ways, Step 2 in n_2 ways and so on. Then the total number of possibilities how to do the whole activity equals to the product $n_1 \cdot n_2 \cdots n_k$.

5.4 Problem. Suppose we have 4 kinds of dark chocolate, 5 kinds of milk chocolate, and 3 kinds of white chocolate. What is the number of ways we could choose two kinds of chocolate of different colours?

Solution. There are three possibilities of how to combine the colours. Either we take a dark and a milk chocolate, or we take a dark and a white one, or a milk and a white one. Now let us study these three cases separately first. If we decide to take a dark and a milk chocolate, there are, according to the multiplication principle, $4 \cdot 5 = 20$ ways of how to do that. Similarly, for the other two colour choices, we have $4 \cdot 3 = 12$ and $5 \cdot 3 = 15$ possibilities, respectively. So, in total, we can choose the chocolates in one of the total $20 + 12 + 15 = 47$ ways.

The final consideration, where we conclude that something can be done either n_1 ways or n_2 *different* ways (or n_3 other ones...) is called the *addition principle*. It is based on the following trivial observation:

5.5 Observation. Suppose $A_1, \ldots, A_k$ are pairwise disjoint sets. Then

$$\#(A_1 \cup \cdots \cup A_k) = \#A_1 + \cdots + \#A_k.$$

The next notion we would like to introduce is a *permutation*. This word can be understood from two slightly different viewpoints. In combinatorics, we usually take the *passive* viewpoint. A permutation of a set is a way of how to arrange its elements.

5.6 Definition. Let A be a finite set with n elements. A **permutation** of A is an ordered tuple $(a_1, \ldots, a_n)$ such that $A = \{a_1, \ldots, a_n\}$. (Since we assume that $\#A = n$, it follows that $a_i \neq a_j$ if $i \neq j$.)

5.7 Exercise. Equivalently, we may say that a permutation of A is any bijection $\{1, \ldots, n\} \to A$. Why?

Outside combinatorics, we often take the *active* viewpoint on permutations. We assume that the elements of A already are somehow arranged. Then a permutation is some rearrangement of A. We also use the verb *to permute*, which essentially means to shuffle.

5.8 Definition. Let A be a finite set. A **permutation** (active) of A is any bijection $A \to A$.

If we are counting permutations, it obviously does not matter, which definition/viewpoint we take.

5.9 Proposition. Any n-element set has $n! = n(n-1) \cdot 2 \cdot 1$ permutations.

Proof. Denote the respective set by A. We need to choose the n-tuple $(a_1, \ldots, a_n)$. We count the possibilities using the multiplication principle. There are n possibilities to choose a_1 as there are n elements of A. There are $n-1$ possibilities to choose a_2 as we can take any element of A except for a_1. We continue this way up to a_n for which we already have only one candidate as all the others were already used. □

5.10 Problem. In a shop, they sell 6 types of chocolate. How many ways are there to order them in a row?

Solution. We are exactly asking to count the permutations of the six types of chocolate. So, the answer is $6! = 720$.

5.11 Problem. How many permutations of letters A, B, C, D, E, F contain CDE as a substring?

Solution. If the result has to contain CDE as a substring, we are not allowed to permute these. We are essentially counting the permutations of the set $\{\mathrm{A}, \mathrm{B}, \mathrm{CDE}, \mathrm{F}\}$. Since the set has four elements, the number of permutations is $4! = 24$.

5.12 Definition. Let A be a finite set with n elements, $k \in \mathbb{N}_0$. A ***k*-permutation**[11] of A is any k-tuple $(a_1, \ldots, a_k)$ such that all $a_i \in A$ and $a_i \neq a_j$ if $i \neq j$.

5.13 Exercise. Try again to formulate an alternative definition using functions.

5.14 Proposition. Let A be a finite set with n elements, $k \in \mathbb{N}_0$. Then A has

$$P(n,k) = n(n-1)\cdots(n-k+1) = \frac{n!}{(n-k)!}$$

k-permutations. (The second expression works only if $k \leq n$. Otherwise the result clearly equals to zero.)

Proof. Exercise! □

5.15 Problem. How many 4-digit numbers are there, where no digit appears twice?

Solution. This sounds like a question for a direct application of the formula above. But we have to pay attention a bit. We have ten digits in total, but the first one is not allowed to be zero as otherwise we would not get a 4-digit number. So, we have 9 possibilities for the first digit, we have 9 possibilities for the second one (we cannot use the first digit, but we are allowed to use zero), 8 possibilities for the third, and 7 for the last. In total $9 \cdot 9 \cdot 8 \cdot 7 = 4536$.

5.16 Remark. One can also ask, how many possibilities are there to construct an ordered tuple $(a_1, \ldots, a_k)$ from elements of an n-element set A. Equivalently, how many functions $\{1, \ldots, k\} \to A$ are there in total. The answer is obviously n^k as we already mentioned in the solution of Problem 5.2. Such a process is sometimes called a *permutation with repetitions*.

5.17 Definition. Let A be a finite set, $k \in \mathbb{N}_0$. A ***k*-combination** of A is any k-element subset of A.

5.18 Proposition. Let A be a set with n elements, $k \in \mathbb{N}_0$. Then A has

$$C(n,k) = \binom{n}{k} = \frac{1}{k!}P(n,k) = \frac{n(n-1)\cdots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

k-combinations.[12] (The last expression works only if $k \leq n$. Otherwise the result clearly equals to zero.)

[11] In other languages, the word *permutation* is often reserved for the true permutations only. For a k-permutation a different word is used. Like *Variation* in German or *arrangement* in French.

[12] The notation $\binom{n}{k}$ is read "n choose k".

Proof. According to Proposition 5.14, there are $P(n,k) = n(n-1)\cdots(n-k+1)$ k-permutations. In the list of all k-permutations, each k-element subset of A is represented $k!$ times as k-element sets have $k!$ permutations. Hence, $P(n,k) = C(n,k)k!$. □

5.19 Theorem. Consider $k, n \in \mathbb{N}_0$, $k \leq n$. Then:

1. $\binom{n}{0} = 1$,
2. $\binom{n}{1} = n$,
3. $\binom{n}{k} = \binom{n}{n-k}$,
4. $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$.

All four statements can be proven using the defining formula of the numbers $\binom{n}{k}$. Nevertheless, we would like to use this opportunity to introduce a new proving technique called the *combinatorial proof*. If we have to prove that two integers are equal, it is enough to show that they are counting the same thing!

Proof. Denote $A = \{1, \ldots, n\}$.

1. There is clearly just one zero-element subset of A.

2. There are clearly n one-element subsets of A (we just have to choose one element and we have n possibilities of how to do that).

3. On the left-hand-side, there is the number of all k-element subsets of A. We have to show that the right-hand-side is counting the same thing. Well, it counts all $(n-k)$-element subsets, but we can take their complements relative to A and we obtain exactly all the k-element subsets.

4. Consider the set $\{1, \ldots, n+1\}$. The left-hand side counts all its k-element subsets. We can obtain these in two distinct ways. Either the subset does not contain $n+1$, so it is a subset of $\{1, \ldots, n\}$ – we have $\binom{n}{k}$ possibilities of doing that – or it does contain $n+1$, in which case we have to choose the remaining $k-1$ elements from the set $\{1, \ldots, n\}$, so we have $\binom{n}{k-1}$ possibilities of doing that. Now, use the addition principle. □

This theorem allows us to construct the numbers $\binom{n}{k}$ recursively. They are typically arranged in the *Pascal triangle*:

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
 & & & & & \vdots & & & & &
\end{array}$$

5.20 Theorem. For any $n \in \mathbb{N}$, $\sum_{k=0}^{n} \binom{n}{k} = 2^n$.

5.21 Exercise. Prove the theorem above! Doing it directly from the formula would be somewhat complicated. Instead try the following two approaches. First, do the proof by induction using Theorem 5.19. Secondly, do the combinatorial proof.

5.22 Theorem. For any $x, y \in \mathbb{R}$, $n \in \mathbb{N}$, we have

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k.$$

Proof. Exercise! (Use induction.) □

5.23 Problem. Having $n = 6$ kinds of chocolate, what is the number of ways, we can choose $k = 4$ chocolate bars? (Order is not important, repetition is allowed.)

Solution. I can perform the choosing procedure the following way. I will put the four different kinds of the chocolate next to each other and I will take a look at each and decide whether to take it. So, first I am staring on the first kind of chocolate. My options are: take it ($*$) or not to take it and move to the next one ($|$). If I choose to take it, then I will not move to the next kind of chocolate. I will continue staring at the first one and I will be thinking whether to take a second bar of the same chocolate. I will repeat that until I have enough and choose the option ($|$) of moving to the next one.

In total, my series of choices can look as follows: $**||*|*||$. Here, I chose twice the first one, I did not take the second, I took once the third and the fourth, and I did not take the fifth and sixth.

In general, the result of my decisions is a string of symbols $*$ and $|$, where the $*$ occurs k times (since I decided to take exactly k bars of chocolate) and the $|$ occurs $(n-1)$-times (it is the separator between the n types of chocolate). How many such strings are there? Well the total length of the string is $n+k-1$. Now the exact form of the string is determined by listing the positions, where the $*$ appears. This is a k-element subset of the total $n+k-1$ elements.

That is, a general formula for **combinations with repetitions** is

$$\left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}.$$

The last thing that we would like to address here is counting the elements of a union of sets. As one can easily check, we have

$$\#(A \cup B) = \#A + \#B - \#(A \cap B).$$

We can try to generalize this for three sets and obtain

$$\begin{aligned}\#(A_1 \cup A_2 \cup A_3) = {} & \#A_1 + \#A_2 + \#A_3 \\ & -\#(A_1 \cap A_2) - \#(A_1 \cap A_3) - \#(A_2 \cap A_3) + \#(A_1 \cap A_2 \cap A_3).\end{aligned}$$

In general, the following holds:

5.24 Theorem (Inclusion-exclusion principle). For any finite sets $A_1, \ldots, A_n$, we have

$$\#(A_1 \cup \cdots \cup A_n) = \sum_{k=1}^{n} (-1)^{k+1} \sum_{1 \le i_1 \le \cdots \le i_k \le n} \#(A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k}).$$

Proof. Take any $x \in A_1 \cup \cdots \cup A_n$. We need to prove that we are counting it exactly once on the right-hand-side. Without loss of generality, suppose that $x \in A_1, \ldots, A_l$ and $x \notin A_{l+1}, \ldots, A_n$ for some l. In that case, we are counting it the following many times:

$$\sum_{k=1}^{l}(-1)^{k+1}\sum_{1\le i_1\le\cdots\le i_k\le l} 1 = \sum_{k=1}^{n}(-1)^{k+1}\binom{l}{k}$$
$$= 1 - \sum_{k=0}^{n}(-1)^k\binom{l}{k} = 1-(1-1)^l = 1. \qquad \square$$

5.25 Problem. Count all *derangements* $\{1,\ldots,n\} \to \{1,\ldots,n\}$. A derangement means a bijection f that has no fixed point, i.e. $f(x) \neq x$ for all x.

Solution. The total number of permutations $\{1,\ldots,n\} \to \{1,\ldots,n\}$ is $n!$. We have to take out these permutations that have a fixed point. For any i, we have $\#\{f\colon \{1,\ldots,n\} \to \{1,\ldots,n\} \mid f \text{ is a bijection}, f(i) = i\}$ is clearly $(n-1)!$ because i is fixed and we are permuting the rest $(n-1)$ points. But it could happen that some permutation fixes two points i and j. So, actually, we need to use the inclusion-exclusion principle:

$$\begin{aligned}
\#\{f \text{ a derangement}\} &= \#\{f \text{ a permutation}\} - \#\bigcup_{i=1}^{n}\#\{f \text{ perm.} \mid f(i)=i\}\\
&= \#\{f \text{ a permutation}\} - \sum_{i=1}^{n}\#\{f \text{ perm.} \mid f(i)=i\}\\
&\quad + \sum_{i\le j}\#\{f \text{ perm.} \mid f(i)=i, f(j)=j\} - \cdots\\
&= n! - n(n-1)! + \binom{n}{2}(n-2)! - \binom{n}{3}(n-3)! + \cdots\\
&= \sum_{i=0}^{n}(-1)^n(n-1)!\binom{n}{i} = \sum_{i=0}^{n}(-1)^i\frac{n!}{i!}.
\end{aligned}$$

Now comes an extremely cool thing: Note that $\sum_{i=0}^{\infty}(-1)^i/i! = 1/e$. And this series converges pretty quickly. Consequently, the number of derangements equals to $n!/e$ rounded to the nearest integer. (This needs to be proven of course. We will not get into the details here.)

6 Graphs

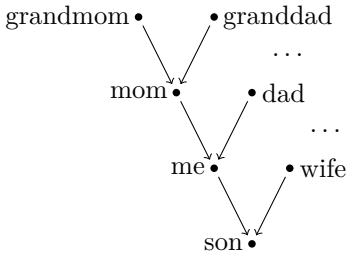
6.1 Basic definitions, examples

Informally, graph is a collection of points (vertices), where some of them are connected by a line or an arrow (edge). The vertices stand for some objects and the edges stand for some relation between them. So, mathematically, a graph is basically

the same thing as a relation. But we typically draw it as a picture (but we did that for relations as well).

6.1.1 Examples.

- Recall the relation R on the set of all people, where xRy if and only if y is a child of x. Let us denote the relation by an arrow $x \to y$ instead. We obtain a *directed graph*

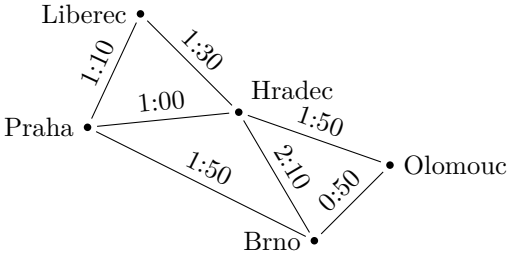


- If you have travelled by the Prague's underground, you have definitelly seen the following diagram

It features all the metro stations; two stations are connected by line if they are connected by some metro line. That is the diagram shows the graph for the relation R on the set of all stations with xRy if x is a neighbouring station of y. In addition, the lines are coloured according to the metro lines. Note in particular that the diagram does not show the actual shape of the network at all. The only information that is preserved is what is connected to what. Note also that there are no arrows as you can always travel both directions. The resulting graph is therefore *undirected*.

- Sometimes, it is useful to label the edges by some values related to the actual *cost* of the edges (their length, the time it takes to get through, or the price we have to pay when travelling). For instance, if you wanted to travel to Olomouc, you may consider going either through Hradec Králové or through Brno. If you are not sure, which way to take, it might be useful to draw a diagram like the

following one:



You can see that it is slightly quicker to go through Brno. A similar but far mor complicated *weighted graph* is stored in any navigation software. In this simple case, it is easy to find the shortest way. If the graph is much more complicated, it is worth looking for an effective algorithm.

6.1.2 Notation. For a set V, $k \in \mathbb{N}_0$ we will denote by $\binom{V}{k}$ the set of all k-element subsets of V.

6.1.3 Definition. A **(simple) graph** is a pair (V, E), where V is a set, whose elements are called **vertices**, and $E \subseteq \binom{V}{2}$, whose elements are called **edges**.

6.1.4 Remark. A graph according to the above definition is *undirected* ($\{v, w\} = \{w, v\}$, so the order is not important, therefore edges have no direction), contains no *loops* ($\{v, v\} = \{v\}$ is not a two-element set, so it cannot be an edge), and no *multiple edges* (E is a *set* of edges, so we do not distinguish how many times a given edge is contained).

6.1.5 Definition. A **directed graph** is a pair (V, E), where V is a set of **vertices**, $E \subseteq V \times V$ a set of (directed) **edges**.

6.1.6 Remark. In a directed graph (V, E), an edge (v, v), $v \in V$ is called a **loop**.

6.1.7 Definition. A **directed multigraph** is a triple (V, E, ϕ), where V and E are sets, $\phi\colon E \to V \times V$ is an **incidence function**.

Here, the elements of V are interpreted as vertices, the elements of E as edges and given an edge $e \in E$, denoting $\phi(e) = (v, w)$, we interpret e as an edge from v to w. Sometimes, v is called the *source* and w the *target*. This allows having more than one edge from v to w.

In the following text, we will mostly work in the framework of simple graphs. As an exercise, try to reformulate every statement and its proof for directed graphs or multigraphs. (Of course, some may not be true in these cases.)

6.1.8 Definition. In a graph $G = (V, E)$, two vertices $v, w \in V$ are called **adjacent** if they are connected with an edge, so $\{v, w\} \in E$. A vertex $v \in V$ is said to be **incident** with an edge $e \in E$ if it one of the vertices the edge connects, so $v \in e$.

6.1.9 Definition. Let $G = (V, E)$ be a graph. We define the **degree** of each vertex $v \in V$ to be the number of its neighbours (incident edges):

$$d_G(v) = \#\{w \in V \mid \{v, w\} \in E\}.$$

6.1.10 Remark. For directed graphs, we distinguish the *indegree* (number of incoming edges) and *outdegree* (number of outgoing edges).

6.1.11 Theorem. Let $G = (V, E)$ be a graph. Then $\sum_{v \in V} d_G(v) = 2\#E$.

Proof. On the left-hand-side, we sum the number of edges incident to all vertices. Since every edge is incident with exactly two vertices. Hence, each edge is counted exactly twice. □

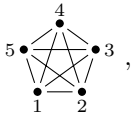
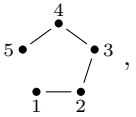
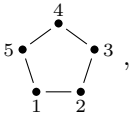
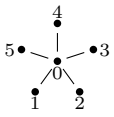
6.1.12 Corollary. Let $G = (V, E)$ be a graph. Then $\sum_{v \in V} d_G(v)$ is always even.

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

6.1.14 Remark. Either the theorem above or one of its corollaries is often refered to as the *Handshaking lemma*.

6.1.15 Examples.

- **Complete graph** $K_n = (V, E)$, $V = \{1, \dots, n\}$, $E = \binom{V}{2}$.
- **Path graph** $P_n = (V, E)$, $V = \{1, \dots, n\}$, $E = \{\{i, i+1\} \mid i = 1, \dots, n-1\}$.
- **Cycle graph** $C_n = (V, E)$, $V = \{1, \dots, n\}$, $E = \{\{i, i+1\} \mid i = 1, \dots, n-1\} \cup \{\{1, n\}\}$.
- **Star graph** $S_n = (V, E)$, $V = \{0, \dots, n\}$, $E = \{\{0, i\} \mid i = 1, \dots, n\}$.

$K_5 =$  , $P_5 =$  , $C_5 =$  , $S_5 =$ 

6.1.16 Definition. Let $G = (V, E)$ be a graph with $V = \{1, \dots, n\}$. We define its **adjacency matrix** A_G by

$$[A_G]_{ij} = \begin{cases} 1 & \text{if } \{i, j\} \in E, \\ 0 & \text{otherwise.} \end{cases}$$

6.1.17 Examples.

$$A_{K_5} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix}, \qquad A_{P_5} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix},$$

$$A_{C_5} = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix}, \qquad A_{S_5} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

6.2 Connectivity

6.2.1 Definition. Let $G = (V, E)$ be a graph.

- A **walk** (of **length** $k-1$, where $k \in \mathbb{N}$) is a sequence of vertices $v_1, \ldots, v_k$ such that $\{v_i, v_{i+1}\} \in E$ for every $i = 1, \ldots, k-1$.
- A **trail** is a walk in which all edges are distinct, i.e. $\{v_i, v_{i+1}\} \neq \{v_j, v_j + 1\}$ whenever $i \neq j$.
- A **path** is a walk in which all vertices are distinct, i.e. $v_i \neq v_j$ whenever $i \neq j$.
- A **circuit**[13] is a trail such that $v_1 = v_k$.
- A **cycle** is a circuit where $v_i \neq v_j$ for any $1 \leq i < j < k$.

6.2.2 Definition. Let $G = (V, E)$ be a graph. We say that vertices v and w are **connected** if there is a walk starting at v and ending at w in G.

6.2.3 Theorem. Being connected is an equivalence relation

6.2.4 Exercise. Prove the theorem above. Note that in this case it is indeed necessary to assume that the graph is directed. Why? Can you modify the definition such that it works also for directed graphs?

6.2.5 Definition. Let $G = (V, E)$ be a graph. The equivalence classes of the relation *being connected* are called the **(connected) components** of G. We say that G is **connected** if it has only one component. That is, G is connected if and only if there is walk from v to w for every pair $v, w \in V$.

6.3 Trees

6.3.1 Definition. A graph containing no cycles is called a **forest**. A connected forest is called a **tree**.

6.3.2 Theorem. Let $G = (V, E)$ be a graph. The following are equivalent:

1. G is a tree.
2. For every $v, w \in V$, there is a unique path from v to w.
3. G is connected and for every edge $e \in E$, the graph $(V, E \setminus \{e\})$ is not connected.

Proof. (1) $\Rightarrow$ (2): If G is a tree, then it must be connected, so there is a walk from v to w. It is easy to see that if there is a walk from v to w, there must also be a path from v to w. So, there is at least one path. We have to prove that it is unique. Well, if there were two paths connecting v and w, then we can easily construct a cycle. Indeed, denote by $v = a_1, \ldots, a_k = w$ and $v = b_1, \ldots, b_l = w$ the two paths. Denote by i, j the smallest indices such that $a_i = b_j$ (such an index must exist as $a_k = b_l$). Then $a_1, a_2, \ldots, a_i = b_j, b_{j-1}, \ldots, b_1 = a_1$ is a cycle.

(2) $\Rightarrow$ (3): If there is a path between each pair of vertices, then G must be connected. Now, take any edge $e = \{v, w\} \in E$. If we assume that any two points are connected by a unique path, the edge e forms the unique path connecting v and w. Removing this edge, the two points stop being connected.

[13] Here, I am inconsistent with the notes by M. Demlová from the earlier version of this subject. I believe my definition is more standard. See e.g. Wikipedia.

(3) $\Rightarrow$ (1): Assume G is connected, but contains a cycle. Then it is not true that removing any edge in the graph makes it disconnected as removing any edge from the mentioned cycle preserves connectivity (any walk using the edge can be modified by using the rest of the cycle). $\square$

6.3.3 Theorem. Let $G = (V, E)$ be a connected graph. Then G is a tree if and only if $\#E = \#V - 1$.

Proof. For the left-right implication, we proceed by induction. If $n = 1$, we have a graph with one vertex and no edge, which is a tree and satisfies the equation. Now, take any $n > 1$ and assume that any tree with the number of vertices smaller than n satisfies the equation. Take any edge e of G. Removing it, we obtain a disconnected graph with two connected components $G_i = (V_i, E_i)$, $i = 1, 2$. Since $\#V_i < n$, we can use the induction hypothesis, so $\#E_i = \#V_i - 1$. For the original graph, we have $E = E_1 \cup E_2 \cup \{e\}$ and $V = V_1 \cup V_2$, so

$$\#E = \#E_1 + \#E_2 + 1 = \#V_1 - 1 + \#V_2 - 1 + 1 = \#V - 1.$$

For the right-left implication, suppose we have $\#E = \#V - 1$, but G is not a tree. Then it must contain an edge such that, if you remove it, the graph remains connected. You can do that repeatedly until you obtain a tree $G' = (V, E')$. But, we already showed that such a tree must satisfy $\#E' = \#V - 1$. But since $\#E > \#E'$, this contradicts the original assumption. $\square$

6.3.4 Exercise. Prove that any tree must contain a vertex of degree 1 (actually at least two vertices if $\#V > 1$). There are actually two ways to prove that: either directly or using the formula $\#E = \#V - 1$. This can be used to formulate an alternative proof of Theorem 6.3.3: For ($\Rightarrow$) use induction again, but for the inductive step, remove the vertex of degree 1. For ($\Leftarrow$), also use induction removing the vertex of degree one.

Let us mention a couple of applications regarding trees. First, many structures are just naturally trees. Think, for instance, about the "family tree graph". Secondly, trees are widespread in programming as data structures. The reason is that they allow very effective algorithms for searching or sorting (cf. *heap sort*). The reason is that if you have a balanced tree with n entries, the number of *levels* is just $\log n$.

Finally, below we are going to study a third application called *spanning trees*. A typical problem that motivated studying this concept in history is as follows. In the beginning of 20. century when the electrical grids were built, a mathematician Otakar Borůvka got the task to design such a grid for South Moravia as cost effectively as possible. The problem is to connect every village to the grid while minimizing the length of the cables needed. In today's terms, this is a graph-theoretical problem of finding a minimal spanning tree.

6.3.5 Definition. Let $G = (V, E)$ be a graph. A subgraph $G' = (V, E')$, $E' \subseteq E$ which is a tree is called a **spanning tree** of G.

6.3.6 Observation. Any graph has a spanning tree if and only if it is connected.

How do you construct one? As follows from Theorem 6.3.2, it is enough to break all cycles. We actually used this idea already in the proof of Theorem 6.3.3. Now, let us formulate a more sophisticated problem:

6.3.7 Problem. Given a graph $G = (V, E)$ and a cost function $c\colon E \to (0, +\infty)$, find a subset $E' \subseteq E$ such that $G' = (V, E')$ is connected and $c(E') = \sum_{e \in E'} c(e)$ is minimal. Such a graph will be called a **minimal spanning tree**.

6.3.8 Algorithm (Kruskal 1956). Input: A connected weighted graph $G = (V, E, c)$. Output: It's minimal spanning tree.

1. **sort** E (according to c). That is, denote $E = \{e_1, \dots, e_m\}$ such that

$$c(e_1) \leq c(e_2) \leq \cdots \leq c(e_m)$$

2. $E' \leftarrow \emptyset$.
3. **for** every $i = 1, \dots, m$
4. **if** $E' \cup \{e_i\}$ contains no cycle
5. **then** $E' \leftarrow E' \cup \{e_i\}$

6.3.9 Exercise. What happens if the input is not connected? Checking whether a graph is connected beforehand might be ineffective. Can we easily see that the input was disconnected after running the algorithm?

6.3.10 Remark. We can make the algorithm slightly faster by breaking the for-loop when $\#E' = \#V - 1$.

6.3.11 Remark. It is a *greedy* algorithm.

6.3.12 Remark. Checking whether some given graph contains a cycle seems like a complex task. But in this particular case it is easy if we keep track of the components of $G' = (V, E')$. Indeed, $E' \cup \{e_i\}$ has a cycle if and only if e_i connects two vertices belonging to the same component of (V, E'). See example below.

6.3.13 Example. Consider the weighted graph $G = (V, E)$, where $V = \{1, \dots, 7\}$ and the edges and their weights are given by the following matrix

$$\begin{pmatrix} - & 6 & 9 & - & - & - & 9 \\ 6 & - & 2 & 1 & 3 & - & - \\ 9 & 2 & - & 1 & - & - & 15 \\ - & 1 & 1 & - & 10 & 13 & 3 \\ - & 3 & - & 10 & - & 10 & 1 \\ - & - & - & 13 & 10 & - & 15 \\ 9 & - & 15 & 3 & 1 & 15 & - \end{pmatrix},$$

where the numbers stand for weights and $-$ means no edge. It is a undirected graph, so the matrix is symmetric and all data is stored in the upper triangle.

So, first, let us sort the edges:

$$\begin{aligned}
e_1 &= \{2,4\}, \quad c(e_1) = 1, & e_8 &= \{1,3\}, \quad c(e_8) = 9,\\
e_2 &= \{3,4\}, \quad c(e_2) = 1, & e_9 &= \{1,7\}, \quad c(e_9) = 9,\\
e_3 &= \{5,7\}, \quad c(e_3) = 1, & e_{10} &= \{4,5\}, \quad c(e_{10}) = 10,\\
e_4 &= \{2,3\}, \quad c(e_4) = 2, & e_{11} &= \{5,6\}, \quad c(e_{11}) = 10,\\
e_5 &= \{2,5\}, \quad c(e_5) = 3, & e_{12} &= \{4,6\}, \quad c(e_{12}) = 13,\\
e_6 &= \{4,7\}, \quad c(e_6) = 3, & e_{13} &= \{3,7\}, \quad c(e_{13}) = 15,\\
e_7 &= \{1,2\}, \quad c(e_7) = 6, & e_{14} &= \{6,7\}, \quad c(e_{14}) = 15,
\end{aligned}$$

Now, we set $E' := \emptyset$ and go through all the edges and try to add them to E'. We keep track of the components we create. (At the beginning, all vertices are in their own component. We call them *singletons*.)

Adding $e_1 = \{2,4\}$ surely does not make a cycle, so we do that: $E' = \{e_1\}$. Now, we created the component $\{2,4\}$, the rest are singletons. Adding $e_2 = \{3,4\}$ also surely does not make a cycle, so we do it: $E' = \{e_1, e_2\}$. Now, we have the component $\{2,3,4\}$ and the rest are singletons. The edge $e_3 = \{5,7\}$ connects two singletons, so it does not make a cycle, we can add it to E' and we obtain $E' = \{e_1, e_2, e_3\}$ creating two components $\{2,3,4\}$ and $\{5,7\}$ while the rest are singletons.

Now the edge $e_4 = \{2,3\}$ connects two vertices that are in the component $\{2,3,4\}$, so adding it would create a cycle, so we do not do that. We can add $e_5 = \{2,5\}$, which connects the two components together, so we have $\{2,3,4,5,7\}$ and the rest are singletons. Adding $e_6 = \{4,7\}$ would make a cycle as both 4 and 7 are in the component. We can add $e_7 = \{1,2\}$, which enlarges the component to $\{1,2,3,4,5,7\}$. We cannot add $e_8 = \{1,3\}$, $e_9 = \{1,7\}$, or $e_{10} = \{4,5\}$ as this would create a cycle. We will add $e_{11} = \{5,6\}$ and obtain $E' = \{e_1, e_2, e_3, e_5, e_7, e_{11}\}$. The resulting graph has a single component containing all the vertices, which means it is connected and hence a tree. We are done!

Finally, we can determine the total cost of the graph we found:

$$c(E') = 1 + 1 + 1 + 3 + 6 + 10 = 22.$$

6.3.14 Theorem. The Kruskal's algorithm indeed constructs the minimal spanning tree.

The proof is not too hard, but a bit too technical, so we will skip it here.

6.3.15 Exercise. Is the minimal spanning tree determined uniquely? Try to construct an example of a weighted graph that has a unique minimal spanning tree. Try to construct an example of a weighted graph that has exactly two minimal spanning trees.

6.3.16 Definition. A **rooted tree** is a pair (G, r), where G is a tree and r is its vertex, which will be called the **root**.

6.3.17 Observation. A root in a tree uniquely defines a direction "from the root" to every edge. Indeed, for any other vertex v, there is a unique path from r to v by

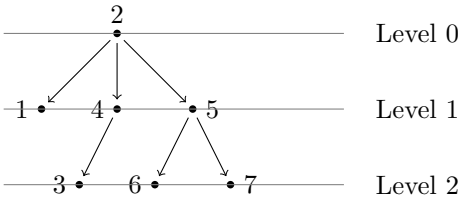
Theorem 6.3.2. Consequently, if we choose a root in a undirected tree, this induces a directed tree.

6.3.18 Definition. Let (G, r) be a rooted tree, $G = (V, E)$.

- A vertex $v \in V$ belongs to ***k*-th level** of (G, r) if there is a path from r to v of length k.
- The **height** of (G, r) is the maximum of the levels. That is, the length of the longest path starting at r.
- Let $u, v \in V$. We say that u is a **predecessor** (or **parent**) of v and that v is a **successor** (or a **child**) of u if $\{u, v\} \in E$ and v is on a greater level than u.
- A vertex is called a **leaf** if it has no successors.

6.3.19 Exercise. Following the "family terminology" think about what a *descendant* and *ancestor* should be. Write a formal definition.

6.3.20 Example. Take the tree $G' = (V, E')$ that we constructed in Example 6.3.13. Choose a root $r = 2$. Then the rooted tree looks as follows:



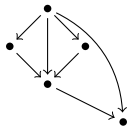
The height is 2. The leaves are vertices 1, 3, 6, and 7. Vertex 5 has successors 6 and 7 (but not 3), its predecessor is the root 2.

6.3.21 Definition. Let $k \in \mathbb{N}_0$. A ***k*-ary** tree is a rooted tree, where every vertex has at most k successors. A 2-ary tree is called a **binary** tree.

6.4 Directed acyclic graphs

6.4.1 Definition. A directed graph $G = (V, E)$ is called **acyclic** if there is no (directed) cycle.

6.4.2 Example. For instance, the following directed graph is acyclic:



Note that reversing any of the arrows creates a directed cycle and hence the graph stops being acyclic.

6.4.3 Example. For any lattice, the corresponding graph (e.g. Examples 4.5.8 if we draw the arrow always from top to bottom) is acyclic.

Note that in all the examples, we draw the directed edges *from top to bottom*. This clearly ensures that the graph is acyclic. Actually, the converse also holds as we are going to show below.

6.4.4 Definition. Let $G = (V, E)$ be a directed graph, $\#V = n$. A **topological sort** of vertices is an ordering $(v_1, \dots, v_n)$ of V such that $(v_i, v_j) \in E$ only if $i < j$.

6.4.5 Theorem. A directed graph is acyclic if and only if it has a topological sort of vertices.

Proof. As we mentioned above, the implication $\Leftarrow$ is clear: Suppose G has a topological sort of vertices $(v_1, \dots, v_n)$. If a graph G has a cycle $(v_{i_1}, \dots, v_{i_{k-1}}, v_{i_k} = v_{i_1})$, then by the definition of topological sort we must have $i_1 < \cdots < i_{k-1} < i_k = i_1$, which is a nonsense.

To prove the converse direction, we are going to formulate an algorithm that constructs the topological sort below. □

6.4.6 Lemma. In every finite acyclic directed graph, there is a vertex with no incoming edges.

Proof. Suppose there is no such vertex. Then take any $v_1 \in V$ and find $v_2 \in V$ such that $(v_2, v_1) \in E$. We can repeat this construction over and over finding $v_k \in V$ such that $(v_k, v_{k-1}) \in E$. Since the graph is finite, the vertices must eventually repeat, so there is $v_k = v_l$ for some $k > l$. But this means we have constructed a cycle $(v_k, v_{k-1}, \dots, v_l)$. □

6.4.7 Algorithm (Kahn 1962). Input: An acyclic directed graph $G = (V, E)$; Output: Topological sort $(v_1, \dots, v_n)$ of V

1. $L \leftarrow ()$
2. **while** $V \neq 0$ **do**
3. **append** any vertex $v \in V$ with no incoming edges to the list L
4. **remove** v from G

6.5 Strong connectivity

6.5.1 Definition. A directed graph $G = (V, E)$ is **strongly connected** if there is a (directed) path from u to v for each pair $u, v \in V$.

For a directed graph, we will say that it is connected if it is connected as an undirected graph, i.e. ignoring the directions of the edges.

6.5.2 Theorem. A directed graph is strongly connected if and only if it is connected and every edge is contained in a (directed) cycle.

Proof. ($\Rightarrow$): Take any edge $(u, v) \in E$. Since G is connected, there must be a path from $(v = v_1, \dots, v_k = u)$. Thus, we obtain a cycle $(v_1, \dots, v_k, v_1)$.

($\Leftarrow$): Take any pair of vertices $u, v \in V$. Since G is connected, there exists an undirected path $(u = v_1, \dots, v_k = v)$ in G. We can transform this to a directed path as follows. For any $i = 1, \dots, k-1$, if $(v_i, v_{i+1}) \in E$ do nothing, otherwise there must be an edge $(v_{i+1}, v_i) \in E$, which is a part of a cycle $(v_{i+1}, v_i, w_1, \dots, w_l, v_{i+1})$. So, add the vertices $w_1, \dots, w_l$ between v_i and v_{i+1} in our undirected path, which makes it a directed path. □

6.5.3 Definition. Let $G = (V, E)$ be a directed graph. Vertices $u, v \in V$ are said to be **strongly connected** if there is a directed path from u to v and a directed path from v to u.

6.5.4 Proposition. Being strongly connected is an equivalence relation.

Proof. Exercise. □

6.5.5 Definition. Let $G = (V, E)$ be a directed graph. The equivalence classes of the relation *being strongly connected* are called the **strongly connected components** of G.

6.5.6 Definition. Let $G = (V, E)$ be a directed graph. We define the **condensation** of G to be the graph $\bar{G} = (\bar{V}, \bar{E})$ defined as follows. $\bar{V}$ is the set of all strongly connected components of G. We put $(C, K) \in \bar{E}$ if there is $u \in C$ and $v \in K$ such that $(u, v) \in E$.

6.5.7 Remark. A condensation of a graph is a particular instance of a *quotient graph*: For any graph G, we can take a partition of its vertices $\bar{V}$ and define a graph $\bar{G} = (\bar{V}, \bar{E})$, where two elements $A, B \in \bar{V}$ are connected if they have representatives that are connected.

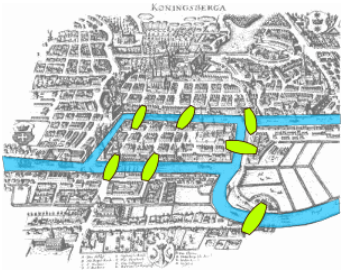
6.5.8 Proposition. The condensation of a directed graph is always acyclic.

Proof. Exercise. □

6.5.9 Exercise. Let G be a strongly connected directed graph on n vertices. Find the smallest and the largest number of edges that G can have.

6.6 Eulerian graphs

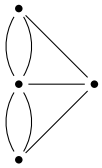
6.6.1 Problem (Seven bridges of Königsberg). This is a famous problem solved by Leonhard Euler in 1736. Below, there is a map[14] of Königsberg in Euler's time with seven bridges of the Pregel river highlighted. Can you cross all the bridges exactly once? If so, can you do it in such a way that you end where you started?



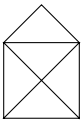
Solution. It is of course totally irrelevant, where the bridges exactly are, how far they are apart or what is the name of the river. The only important thing is that 1. the river divides the city into four parts and 2. which part is connected to which by how many bridges. The ideal way to formalize this in mathematics is using graph

[14] https://en.wikipedia.org/wiki/File:Konigsberg_bridges.png

theory. We replace city quarters by vertices and the bridges by edges. Now, the question is whether there is a trail or even a circuit that goes through all the edges. The answer to both questions is *no* as follows from the characterization below.



6.6.2 Problem (Haus vom Nikolaus). Can you draw the following picture in one stroke?



6.6.3 Definition. Let $G = (V, E)$ be a graph. An **Eulerian trail** is a trail that uses all edges exactly once. An **Eulerian circuit** is a circuit, where all edges are used exactly once. A graph is called **Eulerian** if it admits an Eulerian circuit.

6.6.4 Theorem. Let $G = (V, E)$ be a connected graph. Then G is Eulerian if and only if the degree of every vertex in G is even.

Proof. ($\Rightarrow$): For every vertex, its degree must be twice the number of times the Eulerian circuit visits the vertex.

($\Leftarrow$): We give a constructive proof: Pick any vertex. Start a walk in any direction and colour the edges you walk through. Never use the same edge twice. Since the degree of every vertex is even, you always have a possibility to continue unless you arive to the vertex where you started. If that happens, you have produced a circuit $(v_1, \ldots, v_k = v_1)$. If you used all the edges, you are done. Otherwise, pick some vertex v_i which is incident to a coloured edge as well as some uncoloured one. (It must exist, otherwise the graph is not connected.) Do the same avoiding the coloured edges (never repeat the edge you have already used in this walk or the walks before). This again must produce some circuit $(v_i = w_1, \ldots, w_l = v_i)$. We can now connect the two circuits in a big one as $(v_1, \ldots, v_i = w_1, \ldots, w_l = v_i, \ldots, v_k = v_1)$. If this still is not Eulerian, we continue in a similar way. □

6.6.5 Exercise. Try to reformulate the statement for directed graphs. What should be the condition in this case?

6.6.6 Theorem. Let $G = (V, E)$ be a connected graph. Then there is an Eulerian trail on G if and only if exactly two vertices in G have odd degree.

Proof. We can either repeat the proof above or note the following are equivalent:

- G has an Eulerian trail $(u = v_1, \ldots, v_k = v)$.
- $G' := (V \cup \{x\}, E \cup \{\{x, u\}, \{v, x\}\})$ has an Eulerian cycle $(x, u = v_1, \ldots, v_k = v, x)$. (Here, x is a new vertex not appearing in V.)
- G' has only vertices of even degree.
- G has only vertices of even degree except for u and v which have odd degree. □

If a graph does not satisfy the assumption that the degree of each edge is even, we can still try to solve the optimization problem: what is the shortest circuit that visits every edge? This is known as the *Chinese postman problem*. You are a postman and you want to go through every street at least once while keeping your route as short as possible.

6.7 Overview over some other areas of graph theory

In this section, we would like to give some other examples of application of graph theory. We will often start by formulating a certain (more or less famous) problem. For each problem, try to formulate it in the graph theoretical terms before reading further. (But do not try to solve it. The solution is usually hard.) The purpose is to gain some intuition in what kind of problems can be formulated in terms of graph theory and how do you do that. If you can do that, it is very likely that the corresponding algorithm is known and somebody has it already coded, so it is enough to load the corresponding library.

Hamiltonian graphs and the travelling salesman

6.7.1 Problem (Travelling salesman). Given a list of cities and distances between them what is the shortest path to visit all (and return to the original city)?

Solution. The graph-theoretical formulation is quite straightforward here. We have a weighted graph, where the vertices stand for cities and the weight of an edge between two vertices corresponds to their distance. The problem is now to find a circuit that visits all vertices and its length (the sum of the weights) is minimal. There is no exact algorithm that would solve this problem in polynomial time. The best known are exponential. (Actually the decision problem "Is there a circuit visiting all vertices of length l?" is proven to be NP-complete.) There are some approximation algorithms that are faster (but you are not guaranteed to get the optimal solution). See wikipedia for details.

We get an easier version of this concept if we consider just ordinary (not weighted) graphs.

6.7.2 Definition. Let $G = (V, E)$ be a graph, $n = \#V$. A **Hamiltonian path** is a path of length n (i.e. visiting all vertices). A **Hamiltonian cycle** is a cycle of length n. A graph is **Hamiltonian** if it contains a Hamiltonian cycle.

But there is no easy characterization here either. Again, the decision problem whether a graph is Hamiltonian is NP-complete. Nevertheless, there are some special cases, where we know the answer. For instance, by the theorem of Ore (1960), a graph is Hamiltonian if, for every pair of non-adjacent vertices, the sum of their degrees is greater or equal to n. This was further generalized in 1972 by Chvátal and 1976 by Bondy. We will not mention the exact formulations here.

Pairings and Hall's marriage problem

6.7.3 Problem (Hall's marriage problem). Consider a set of girls and boys such that each girl knows several boys. Under what condition can all the girls mary the boys such that each girl marries a boy she knows?

6.7.4 Theorem (Hall 1935). The problem has a solution if and only if, for every $k = 1, \dots, m := \#\{\text{girls}\}$, each set of k girls collectively knows at least k boys.

The actual solution is not that interesting as the new graph-theoretical concepts it introduces. We have a graph, where the set of vertices are the people (boys and girls) involved and there is an edge between girl and boy if the girl knows the boy. (We do not draw edges between girls or between boys as they are not relevant – the graph is *bipartite*.) The task is to find a *matching* – a set of mutually disjoint edges – that would cover all the girls.

6.7.5 Definition. Let $G = (V, E)$ be a graph. A **matching** in G is a subset $M \subset E$ such that, for every $e, f \in M$, $e \cap f = \emptyset$. The matching is called **perfect** if, for every $v \in V$, there is $e \in M$ with $v \in e$.

6.7.6 Examples.

- Organizing a tournament: The teams form the set of vertices. Before each round, we must decide, who will play against whom. We list all the possible pairs as the set of edges and find a perfect matching.
- Molecules of benzene rings: You might remember from chemistry the molecule of benzene having the structure $\leftrightarrow$  $\leftrightarrow$  . You can also combine the benzene rings to obtain more complicated aromatic compounds like napthtalene:  $\leftrightarrow$  $\leftrightarrow$ $\leftrightarrow$. Is there a chemical compound with the following formula  ?

Another thing worth noticing in the original problem, which also appears very often in graph theory, is that the set of vertices is divided into two subsets – boys and girls – and there are edges only connecting vertices of different parts.

6.7.7 Definition. A graph $G = (V, E)$ is called **bipartite** if there are V_1, V_2 such that $V = V_1 \cup V_2$ and $V_1 \cap V_2 = \emptyset$ and $E \cap \binom{V_1}{2} = \emptyset = E \cap \binom{V_2}{2}$.

There is a surprisingly simple characterization of bipartite graphs:

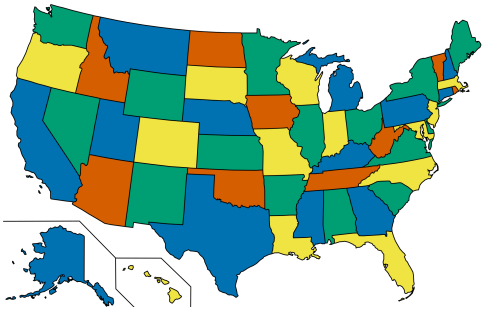
6.7.8 Theorem. A graph is bipartite if and only if it has no cycle of odd length.

Proof. Exercise! □

Planar graphs, colourings and the four-colour-theorem

6.7.9 Problem. Given a political map, what is the least amount of colours one has to use to colour the states such that neighbouring states always get a different colour? (As in the image[15].)

[15] `https://commons.wikimedia.org/wiki/File:Map_of_United_States_accessible_colors_shown.svg`



6.7.10 Thoerem (Four colour theorem). 4.[16]

Note that the proof of the four colour theorem is extremely complicated and involves a lot of brute force checking performed by a computer. Note also that it is relatively easy to prove that five colours are enough. But our aim is again just to understand what the statement says from the perspective of graph theory.

So, what we can do is to construct a graph where the vertices are the states and two states are connected by an edge if they share a border. The goal is to colour the vertices such that no two vertices of the same colour are connected.

6.7.11 Definition. Let $G = (V, E)$ be a graph, $k \in \mathbb{N}$. A ***k*-vertex colouring** of G is a map $\phi\colon V \to \{1, \dots, k\}$. It is called **proper** if for every edge $\{v, w\} \in E$ we have $\phi(v) \neq \phi(w)$. The minimal k such that a k-vertex colouring exists is called the **chromatic number** of the graph and denoted $\chi(G)$.

So, what do we mean by the four colour theorem. Is the chromatic number of every graph at most five? Certainly not! For instance, the full graph K_n clearly has the chromatic number equal to n. The point is that our graphs that come from maps are *planar*.

6.7.12 Informal definition. A graph $G = (V, E)$ is called **planar** if it can be drawn in a plane such that the edges do not cross.

6.7.13 Thoerem (Four colour theorem formulated properly). Let G be a planar graph. Then $\chi(G) \leq 4$.

Both the concept of planarity and colouring is very useful, so let us mention a couple of additional comments and applications.

6.7.14 Problem. Given a convex polyhedron, what is the relationship between the number of its vertices, edges, and faces?

For a planar graph, one can also define faces as the regions the plane is divided into by the edges. Here, you can ask the same question. Actually, any polyhedron can be deformed and identified with the plane, so the answer to both questions is actually the same.

[16] This is a joke. Please formulate theorems more precisely on the exam.

6.7.15 Theorem (Euler). For any connected planar graph, we have

$$\#\{\text{vertices}\} - \#\{\text{edges}\} + \#\{\text{faces}\} = 2.$$

Inspired by the concept of vertex colouring, we can study the same for edges:

6.7.16 Definition. Let $G = (V, E)$ be a graph, $k \in \mathbb{N}$. A ***k*-edge colouring** is a map $\phi\colon E \to \{1, \dots, k\}$. It is called **proper** if, for every $e, f \in E$, we have $\phi(e) = \phi(f)$ only if $e \cap f = \emptyset$.

6.7.17 Problem. Create a school timetable. You are given a set of teachers T a set of classes (groups) of students C and you know which teacher is supposed to each which class (and how many times a week). You are supposed to assign time slots to each lecture such that no teacher gives two lecture at the same time and no class is supposed to attend two lectures at the same time.

Solution. Define a bipartite graph with the set of vertices $V = T \cup C$; a teacher t is connected with a class c if t is supposed to teach c. (We can create a multigraph by using multiple edges if the class is more than once a week.) Now assigning the time slots just means that we have to find an edge colouring of the graph. Each colour then represents a certain time slot. The less colours we use, the better as it makes the timetable more compact.