01019 Part 2: Discrete Mathematics

Version 1.0:	Peter Beelen
Version 2.0:	Christian Henriksen
Version 2.1:	Johan Rosenkilde
Translation 2.1.e:	Sarah Van Dam

Version 2.1.e November 23, 2020

Contents

Chapter 1

Fundamentals of Combinatorics

Combinatorics is the art of counting. It may sound trivial, but a lot of things can be complicated to count. Even though a child can ask the question: "If you have ten Lego bricks, how many ways can they be assembled?". The number is astronomical and difficult to calculate if the Lego bricks are not of a simple structure.

Mathematically it is possible to count anything if it is described as elements in a set A. The number of elements in a set A is written $|A|$. For example:

$$\begin{aligned} |\emptyset| &= 0 \\ |\{1,2\}| &= 2 \\ |\{1,2,3,1\}| &= 3 \\ |\{x \mid x \text{ is a positive, even number under } 10\}| &= 4 \end{aligned}$$

The number of elements in A, $|A|$, is often called the cardinality of A.

In the following, we will thoroughly survey and proof all theorems. On one hand, some of the theorems can seem obvious and the proofs cumbersome, but proofs are very central in mathematics. This is why we have chosen to explain even the most trivial theorems.

On the other hand, for a student, who has just finished the logical part of the course "01019 Discrete Mathematics", our proofs can seem superficial and informal.

In the second part of the course, the proofs reflect how the mathematician works: The proofs are on a higher level of abstraction than what is wanted in the logical part of the course. In the logical part the automation of f.x. the proof process is a significant goal.

The development of mathematics is still something, which is done by people, because the intuition and imagination is still a very central role. This is reflected when mathematics is communicated, since theorems and proofs are written in a way, which makes it understandable to humans. On the

Notation We use $\mathbb{N}$ as a notation of the natural numbers including zero. Thus

$$\mathbb{N} = \{0, 1, 2, \ldots\}.$$

We use $\mathbb{Z}$ as a notation for all integers. That is to say

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}.$$

border between computer science and mathematics, there are many interesting topics with a complete formalisation - all the way down to axioms of mathematics - and partial automation of the proof techniques.

1.1 The Sum Rule

Sometimes it is possible to divide and conquer, when counting the amount of elements in a set, by splitting the problem into smaller sub-problems. It is easier to count the number of elements in a sub-problem and then sum all of these. For example, a deck of cards with one joker has

13	spades,
13	hearts,
13	diamonds,
13	clubs, and
1	joker

This gives a total sum of 53 cards.

The sum rule: If we can choose between k_1 options *or* k_2 other options, ..., *or* k_n other options, then we have in total

$$k_1 + k_2 + \cdots + k_n = \sum_{i=1}^{n} k_i$$

options to choose from (see the box on Page 8 for the $\sum$-sign).

More formally: if $A_1, A_2, \ldots, A_n$ are pairwise disjoint sets (i.e. $A_i \cap A_j = \emptyset$ when $i \neq j$), then we have

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n| = \sum_{i=1}^{n} |A_i|.$$

Proof: If $x \in A_i$ for some i, then $x \in A_1 \cup \ldots \cup A_n$, which means $|A_1 \cup \ldots \cup A_n| \leq |A_1| + \ldots + |A_n|$. If the equality does not hold, there must be an element x, which is counted two or more times on the right hand side, but only once on the left hand side. But this cannot happen since $A_i \cap A_j = \emptyset$ for $i \neq j$. □

In the example regarding the deck of cards, we can ask how many ways it is possible to draw one card. We can draw either a spade (13 options), a heart (13 options), a diamond (13 options), a club (13 options), or a joker (1 option). This gives 53 options in total. Meaning there is 53 cards in the deck.

It is important that all of the options are distinct, i.e. the sets we can choose between are disjoint. For example, if we wanted to count the amount of cards which are either a diamond or an ace, we know there are 13 diamonds and 4 aces, but there is only 16 cards which are either a diamond or an ace. This is because the set of diamonds and the set of aces are not disjoint.

The sum rule describes how we can count the amount of elements in a set, if we can divide the set into disjoint subsets.

But what if there *is* an overlap, similar to the example with the diamonds and aces in a deck of cards?

Theorem 1.1
For the sets A, B, and C it applies that

$$|A \cup B| = |A| + |B| - |A \cap B| \tag{1.1}$$

and

$$\begin{aligned} |A \cup B \cup C| = \quad & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C|. \end{aligned} \tag{1.2}$$

Proof: We start with Equation (1.1) For example by inspecting a Venn-diagram, it is possible to see that

$$\begin{aligned} A &= (A - B) \cup (A \cap B) \text{ , and} \\ A \cup B &= (A - B) \cup B \text{ .} \end{aligned}$$

By the sum rule, we get

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

Equation (1.2) is proven similar to Exercise 1.15 by using Equation (1.1). □

Example 1.1 Let's return to the example about the set of cards either being diamonds or aces. If R is the set of cards being diamonds, and E is the set of cards being aces. Then $R \cup E$ is the set of cards being either diamonds or aces, and $R \cap E$ is the set of cards being the ace of diamonds, i.e. only one card. Therefore $|R \cup E| = |R| + |E| - |R \cap E| = 13 + 4 - 1 = 16$.

Notation (The Summation symbol) The summation of a long sequence like $|A_1| + |A_2| + \cdots + |A_n|$ is very common in mathematics. A compact standardised notation was made in the form of a summation symbol $\sum$ (the Greek letter "sigma"). This means that

$$\sum_{i=1}^{10} |A_i| = |A_1| + |A_2| + \cdots + |A_{10}|.$$

The sub-script "$i = 1$" is the lower bound for the counting variable i, whos initial value is 1. The super-script is the upper bound, which in this case is the value 10. This means that i will assume all integer values from 1 to 10, both numbers included. Here are some examples:

$$\sum_{i=1}^{5} i = 1 + 2 + 3 + 4 + 5 = 15$$

$$\sum_{i=0}^{4} (2i + 1) = 1 + 3 + 5 + 7 + 9 = 25$$

$$\sum_{i=-5}^{5} i^2 = (-5)^2 + (-4)^2 + \ldots + \ldots + 5^2 = 2(1^2 + 2^2 + \ldots + 5^2)$$

$$\sum_{i=1}^{n} i^3 = 1 + 2^3 + 3^3 + \ldots + n^3$$

If the lower bound is greater than the upper bound, then the sum is zero, f.x. $\sum_{i=3}^{2} i = 0$.
The precedent rules, i.e. in which order to calculate the multiplications and additions within the summation symbol, is shown by the following examples:

$$\sum_{i=1}^{3} 2 \cdot i = 2 \cdot 1 + 2 \cdot 2 + 2 \cdot 3 = 12 \qquad \text{(multiply before } \textstyle\sum\text{)}$$

$$\sum_{i=1}^{3} i + 2 = \left(\sum_{i=1}^{3} i \right) + 2 = (1 + 2 + 3) + 2 = 8 \qquad \text{(addition after } \textstyle\sum\text{)}$$

$$\sum_{i=1}^{3} (i + 2) = (1 + 2) + (2 + 2) + (3 + 2) = 12 \qquad \text{(the parentes can make a difference).}$$

Occasionally, the elements, which are summed, is written as a set of elements. For example:

$$\sum_{s \in S} s^2 = 1^2 + 2^2 + 3^2 = 14 \qquad \text{where } S = \{1, 2, 3\}$$

$$\sum_{\substack{p \in P \\ p < 100}} p^2 = 2 + 3 + 5 + \ldots + 97 = 1060 \qquad \text{where } P = \{p \mid p \text{ is a prime number}\}$$

Exercise 1.1 Let us say that we have two dice: one red and one blue. Use Theorem 1.1 to calculate the number of ways to roll at least one six with the two dice. (To roll a 1 with the red dice and 2 with the blue dice is considered different than to roll a 2 with the red dice and 1 with the blue dice.)

Example 1.2 Let us say that we have one red, one green, and one blue dice. In how many ways can you roll a pair of sixes, i.e. at least 2 sixes?

We look at three sets, A is the set of rolls, in which the red and green dice are six, B is the set of rolls in which the red and the blue dice are six, and C is the set of rolls in which the green and the blue dice are six.

Therefore, we are interested in $|A \cup B \cup C|$.

$|A| = 6$, because when the the red and green dice both are six, the blue dice can show any of the 6 numbers. Equivalently, we have $|B| = |C| = 6$.

It also holds that $A \cap B = A \cap C = B \cap C = A \cap B \cap C$, since the four intersections all contains the roll of which all the dice are 6. Using the Theorem 1.1, we get

$$\begin{aligned} |A \cup B \cup C| = \; & 6 + 6 + 6 \\ & - 1 - 1 - 1 \\ & + 1. \end{aligned}$$

Thus 16 different ways of rolling a pair of sixes.

Exercise 1.2 In a study group of seven students, all the students attend at least one of the following classes: Advanced Mathematics 1 (AM1), Discrete Mathematics (DM), and Introduction to Programming (IP). Determine how many students are attending all three classes, if 6 students are attending AM1, 5 students are attending DM, 4 students are attending IP, 4 students are attending both AM1 and DM, 3 students are attending both AM1 and IP, and 3 students are attending both DM and IP.

1.2 The Product Rule

In the last section, we counted the amount of choices, when we had to choose between different choices, thus "*or*". In this section, we are going to look at making several choices at the same time, thus "*and*". We will start with an example.

Example 1.3 A restaurant has 3 different appetisers and 4 different main courses. How many menus containing an appetiser and a main course can the restaurant offer?

We divide the set of menus into three subsets according to the appetiser. Subset $A1$ is the ones ordering the first appetiser, subset $A2$ is the ones ordering the second appetiser, and subset $A3$ is the ones ordering the third appetiser. In each of the three subsets $A1$,

$A2$, and $A3$ there are 4 different elements, corresponding to each of the main courses. Thus according to the summation rule we have $4 + 4 + 4 = 3 \cdot 4 = 12$ different menus.

The restaurant now offers 2 desserts. How many menus containing an appetiser, a main course, and a dessert can the restaurant offer? We can divide the menus in two subsets: the ones ordering the first dessert and the ones ordering the second dessert. We know from the last example that both of these subsets have 12 combinations of appetisers and main courses. Thus, the summation rule states that there is $12 + 12 = 12 \cdot 2 = 3 \cdot 4 \cdot 2 = 24$ menus.

The menus in the example can be written as tuples with three values: (a, m, d), in which a is an appetiser, m is a main course, and d is a dessert. We can therefore choose a in three different ways, m in 4 different ways, and d in two different ways, and each of these choices are independent. Remember that if A and B are sets then their cross product is the set of pairs:

$$A \times B = \{(a, b) \mid a \in A \wedge b \in B\}.$$

The product rule: If we need to make n choices, of which we know that we have k_1 options for the first choice, hereafter k_2 options, etc., and at last k_n options, then we have in total

$$k_1 \cdot k_2 \cdot \cdots \cdot k_n$$

ways of making n choices.

Formally, if $A_1, A_2, \ldots, A_n$ are sets, and $A_1 \times A_2 \times \ldots \times A_n$ are their cross product, then

$$|A_1 \times A_2 \times \ldots \times A_n| = |A_1| \cdot |A_2| \cdot \ldots \cdot |A_n| \ .$$

Proof: We are proving the formal description with $n = 2$. Let $N = |A_1|$. Let $a_1, \ldots, a_N$ be all elements in A_1 in an arbitrary order. We can then write

$$A_1 \times A_2 = B_1 \cup B_2 \cup \ldots \cup B_N \ ,$$

of which $B_i = \{(a_i, b) \mid b \in A_2\}$. It is clear that all B_i are disjoint, which means we get the following by the rule of summation

$$|A_1 \times A_2| = \sum_{i=1}^{N} |B_i| = \sum_{i=1}^{N} |A_2| = |A_1||A_2| \ .$$

For $n > 2$, we have $A_1 \times \ldots \times A_n = (A_1 \times \ldots \times A_{n-1}) \times A_n$. Thus we can use the case of $n = 2$ to conclude

$$A_1 \times \ldots \times A_n = |A_1 \times \ldots \times A_{n-1}| \cdot A_n \ .$$

In the same way, it can be concludes that $|A_1 \times \ldots \times A_{n-1}| = |A_1 \times \ldots \times A_{n-2}| \cdot |A_{n-1}|$, which can be used continuously to conclude the wanted outcome. (This is an especially simple example of "Proof by Induction", which we will look further into in Chapter 3.) □

Exercise 1.3 You have 3 hats, 17 pairs of trousers, and 13 shirts in the wardrobe. Determine how many combinations of hats, trousers, and shirts we are able to create (while ignoring fashion and colour).

The very attentive reader will maybe have noticed that the formal and informal description of the product rule are not the same! In the formal description, it is very important that the different sets are given before hand, thus the options for the second choice does not depend on the first choice. The informal description allows this kind of dependency as long as the *number* of options does not change. Let us illustrate this with an example:

Example 1.4 You have a red, a yellow, and a green hat. You also have 17 pairs of trousers in each of the three colours, and you have 13 shirts in each of the colours. You are very colour aware and only want to wear a set of clothes with the exact same colour. How many sets of clothes are you able to construct?

The answer is the same as the previous exercise: $3 \cdot 17 \cdot 13$. When you have chosen a hat (3 options), then you are limiting yourself to only 17 pairs of the 51 pairs of trouser, which have the same colour, and likewise with the shirts. *The set* of trousers, which you are choosing between, is different depending on the colour of the hat, which you chose, but the amount is the same.

A formal description of this rule is arduous to formulate for an arbitrary number of choices n even though it is intuitively to use, when you have gotten used to it. To complete, there is a formal description of the simple case of $n = 2$, and the general case follows by repeatedly using this:

The product rule (2): Let A be a set and in addition let for each $a \in A$ be given by the set B_a. Assume that all B_a have the same amount of elements N. Then let S be given by

$$S = \{(a, b) \mid a \in A, b \in B_a\}$$

Thus $|S| = |A| \cdot N$.

Proof: The proof is completely analogous to the rule of multiplication of the case $n = 2$. □

Example 1.5 We have a red and a green 6-faced dice and ask how many ways we can roll an even and an odd number of eyes at the same time. There are 6 options for the red dice and the result of the roll is either even or odd. In both cases, there are 3 options for what the green dice must be. Thus we have in total $6 \cdot 3 = 18$ options.

Exercise 1.4 Let A be a set with $|A| = n$. Determine how many different subsets of A there exists. Tip: Name all of the elements of A as $a_1, \ldots, a_n$. First choose whether a_1 is in or out. Thereafter a_2 and so forth.

1.3 Arrangements

In this section, we will count the number of ways we can arrange a list of elements. That is how many distinct ways it is possible to arrange a list of n elements $x_1, \ldots, x_n$. Formally, the ordering of $x_1, \ldots, x_n$ is a tuple $(y_1, \ldots, y_n)$, where $y_i = x_j$ for each j, and for each x_j there exist exactly one i, which gives $y_i = x_j$. A ordering is also called a "permutation".

Definition 1.2
For a positive integer n we denote $n!$ (read: n factorial) as the product

$$n! = 1 \cdot 2 \cdot \ldots \cdot n \ .$$

0! is defined to be equal to 1.

Theorem 1.3
Let A be a set of n elements The number of permutations we can arrange these n elements is $n!$.

Proof: Let $x_1, \ldots, x_n$ be the elements in A and let $(y_1, \ldots, y_n)$ be a permutation of these elements. We can choose y_1 in n ways. For y_2 we have $n-1$ options to choose from, since we can choose any element except the element we chose as y_1. For y_3 we have $n-2$ options to choose from. We continue until y_n can only be chosen in one way. The rule of multiplication gives $n!$ ways to choose a permutation of the n elements. □

Notice that we above had to use the stronger rule of multiplication, in which the later choices are dependant on ealier choices, but the *number* of choices are still the same.

We can make a small table for the first values of the factorial function.

$$0! = 1$$
$$1! = 1$$
$$2! = 2 \cdot 1 = 2$$
$$3! = 3 \cdot 2 \cdot 1 = 6$$
$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$$
$$5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120$$
$$6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720$$

Exercise 1.5 Determine 7!.

Example 1.6 In a hundred meter run 6 athletes are competing. We determine how many ways the 6 athletes can reach the goal, when excluding the option of two athletes reaching the goal at the same time or that some of the athletes do not complete the run.

Since there are 6 runners, there are $6! = 720$ distinct permutations.

What if you are only interested in who gets the 1., 2., and 3.-place? The first place can be given to any of the six runners, which means that there are 5 runners left who can get second place. This means that there are 4 runners left who can get third place. According to the rule of multiplication there are $6 \cdot 5 \cdot 4 = 120$ options.

The second part of the example above regards the number of ways, where *not* all elements are used. We use the following notation:

Definition 1.4
For $0 \leq k \leq n$ we define:

$$P(n,k) = \frac{n!}{(n-k)!} = (n-k+1) \cdot (n-k+2) \cdot \ldots \cdot n$$

Theorem 1.5
Let A be a set of n elements and k be an integer, where $0 \leq k \leq n$. The number of permutations of k distinct elements in A is given by $P(n,k)$.

Proof: The theorem can be proved similarly to the proof of Theorem 1.3, but instead we will use that we have already proven Theorem 1.3. According to this, there are $n!$ permutation of all the n elements. If we only take the first k elements of each of these tuples, we get all k-permutations out of n elements - but each of them many times. How many: one for each permutation of the remaining $n-k$ elements, i.e. $(n-k)!$ times. Each k-permutation appears the same amount of times namely $(n-k)!$. This means that there are $\frac{n!}{(n-k)!}$ permutations of k elements in total. □

Exercise 1.6 How many positions of four distinct pieces are there on a chess board, if it does not matter if the chess position is valid or an option? (A chess board has 64 distinct fields.)

1.4 Combinations

Most times when counting, the important part is how many subsets there are with certain properties and not in which order the elements are in the subsets.

Example 1.7 Filling out a lottery ticket by choosing 6 numbers out of the numbers from 1 to 48. It does not matter in which order you choose the 6 numbers. It only matters which 6 numbers are chosen.

Definition 1.6
For $0 < k \leq n$ we define the notation

$$\binom{n}{k} = \frac{P(n,k)}{k!} = \frac{n!}{(n-k)! \cdot k!}$$

Furthermore, we define $\binom{n}{0} = 1$, and $\binom{n}{k} = 0$ for $k < 0$ and $k > n$.

$\binom{n}{k}$ is called a binomial coefficient and is pronounced "n choose k". Where the binomial coefficient comes from, is explained later on, but the statement "n choose k" comes from that the $\binom{n}{k}$ defines how many ways we can choose k out of n elements.

Theorem 1.7
Let A be a set of n elements and k an integer, $0 \leq k \leq n$. The number of subset $B \subseteq A$ with $|B| = k$ is given by $\binom{n}{k}$.

Proof: The number of permutations of k elements from A is $P(n,k)$ according to Theorem 1.5. Each subset $B \subseteq A$ with k elements are represented many times in these permutations: once for each permutation of the k elements in B, i.e. $k!$ times. Thus there are $\frac{P(n,k)}{k!}$ distinct subsets B. □

Example 1.8 Let us determine $\binom{5}{2}$. We have

$$\binom{5}{2} = \frac{5!}{3! \cdot 2!} = \frac{5 \cdot 4}{2 \cdot 1} = 10.$$

Here is a table over some small values of $\binom{n}{k}$:

n							
0	1						
1	1	1					
2	1	2	1				
3	1	3	3	1			
4	1	4	6	4	1		
5	1	5	10	10	5	1	
6	1	6	15	20	15	6	1
	0	1	2	3	4	5	6
				k			

Many concepts from combinatorics can be illustrated by combining letters.

Example 1.9 We can write all "words", consisting of $n = 1, 2, 3$ letters, if we can only use the letters X and Y. When $n = 1$ there are 2 words: X and Y. When $n = 2$ there are 4 words: XX, XY, YX, and YY. When $n = 3$ there are 8 words: XXX, XXY, XYX, XYY, YXX, YXY, YYX, and YYY. It follows from the rule of multiplication that there are 2^n words of the length n, which can be made of the letters X and Y.

Let us now see how many words of length $n = 3$ there are containing exactly k X's, where $k = 0, 1, 2, 3$.

$k = 0$ When there is no X's, all letters needs to be Y's. So there is one word, YYY. Notice that $\binom{3}{0} = 1$.

$k = 1$ There are 3 words with only one X, namely XYY, YXY, and YYX. This means that we need to choose one of the letters to be an X and the rest to be Y's. Thus $\binom{3}{1} = 3$ distinct words.

$k = 2$ Two out of three letter have to be X's. You need to choose two out of the three places to be X's, which can be done in $\binom{3}{2} = 3$ ways. The three words are XXY, XYX, and YXX.

$k = 3$ Three out of three letter needs to be X's. This can only be done in $\binom{3}{3} = 1$ ways.

Exercise 1.7 (a) Explain why there are 2^n "words" with the letters X and Y.

(b) Explain why there are exactly $\binom{n}{k}$ "words" with the letters X and Y, if there is exactly k X's.

Closely compare the previous example with the next example.

Example 1.10 Assume that x and y are variables. Consider the

expression $(x+y)^n$ for $n = 1, 2, 3$:

$$\begin{aligned}
(x+y)^1 &= x + y = \binom{1}{0}x + \binom{1}{1}y \\
(x+y)^2 &= xx + xy + yx + yy \\
&= x^2 + 2xy + y^2 = \binom{2}{0}x^2 + \binom{2}{1}xy + \binom{2}{2}y^2 \\
(x+y)^3 &= xxx + xxy + xyx + xyy + yxx + yxx + yxy + yyy \\
&= x^3 + 3xy^2 + 3x^2y + y^3 \\
&= \binom{3}{0}x^3 + \binom{3}{1}xy^2 + \binom{3}{2}x^2y + \binom{3}{3}y^3
\end{aligned}$$

This exemplifies for small values a beautiful correlation between $\binom{n}{k}$ and the binomials $(x+y)^n$.

Theorem 1.8
Let x and y be variables. For $n \in \mathbb{N}$ we have

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

Proof: If we expand $(x+y)^n$, then each term will be created by choosing either x or y in each of the n parentheses. A term has the form $x^k y^{n-k}$ exactly if we have chosen x k times. This can be done in exactly $\binom{n}{k}$ ways, cf. Theorem 1.7. □

Theorem 1.8 is a simpler version of Newton's Binomial Theorem and this is where the name "the binomial coefficient" comes from. It is really useful when proving other theorems, especially when x and/or y are given values. For example like the following:

Corollary 1.9
For $n \in \mathbb{N}$

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Proof: Use Theorem 1.8 with $x = y = 1$. □

Binomial coefficients have a lot of fun and surprising properties. We are going to present three here and more can be found later in the exercises. We are going to give "combinatorial proofs" of the properties, i.e. by using that $\binom{n}{k}$ counts the number of ways to choose k out of n elements. It is also possible to use the definition $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ to prove the identities.

Theorem 1.10
For $n, k \in \mathbb{N}$

$$\binom{n}{k} = \binom{n}{n-k}$$

Proof: To choose k elements from a set of n elements is the same as choosing $n-k$ elements, which must *not* be included. Therefore, the two ways of counting must be the same. □

Theorem 1.11
For $n, k \in \mathbb{N}$

$$\binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}$$

Proof: There are $\binom{n}{k}$ ways of choosing k out of n elements. But we can also count in a different way: Let x be one of the n elements. First, we can count the number of choice, in which x is one of the chosen elements, and thereafter count the number of choices, in which x is not chosen. The sum of these must be as before, i.e. $\binom{n}{k}$. But if x is already chosen then there are $\binom{n-1}{k-1}$ ways of chossing the rest of the $k-1$ elements. If x is *not* in the chosen elements, then there is $\binom{n-1}{k}$ ways of choosing all k elements. □

Theorem 1.11 can be used to "develop" the binomial coefficient, so we only need to use additions and not a single multiplication! It can seem surprising when looking at the definition $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. This leads to "Pascal's triangle", where every single element is equal to the sum of the two elements above it (you need to start with a border of 1's):

$n=0$						1					
$n=1$					1		1				
$n=2$				1		2		1			
$n=3$			1		3		3		1		
$n=4$		1		4		6		4		1	
$n=5$	1		5		10		10		5		1
$n=6$	1	6		15		20		15		6	1

Compare this triangle with the table of $\binom{n}{k}$, which was given earlier.

Theorem 1.12 (Chu-Vandermonde's convolution)
For $n, m, k \in \mathbb{N}$

$$\binom{n+m}{k} = \sum_{i=0}^{k} \binom{n}{i}\binom{m}{k-i}$$

Proof: If A is a set of $n+m$ elements, then there are $\binom{n+m}{k}$ ways of choosing k elements from the set A. But we can also count it in a different way: Let us say that n elements in A is "blue", and the remaining m elements are "red". To choose k elements from A, we first choose i blue elements, $0 \leq i \leq k$. Hereafter we take $k-i$ red elements, which can be done in $\binom{m}{k-i}$ ways. (Notice that these statements are true even if $i > n$ or $k-i > m$.) For each valid i, we can choose it in $\binom{n}{i}\binom{m}{k-i}$ ways, and the rule of summation states that the total amount is the sum of these. This must be equal to our first count $\binom{n+m}{k}$. □

1.5 Exercises

Exercise 1.8 At a 100-meter run, there is 7 participants. How many ways can the gold, silver, and bronze medals be distributed, if we assume that none of the medals are shared?

Exercise 1.9 If we have 7 different letters, how many "words" of three letters can be written? Assume that X is one of the letters. How many words of 3 letter is there with exactly one X?

Exercise 1.10 In how many ways can two white knights be places on a chess board?

Exercise 1.11 In this exercise, you must prove a fun property for binomial coefficients: For $n, k \in \mathbb{N}$, both greater than 0, we have

$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}.$$

There exists a combinatorial interpretation of this rule, but it can be a bit difficult to come up with. Try if you finish the other exercises.

Exercise 1.12 Prove the following surprising identity:

$$5^n = \sum_{k=0}^{n} \binom{n}{k} 4^k$$

For example is $5^3 = 1+3\cdot 4+3\cdot 4^2+4^3$. (Tip: Use Theorem 1.8 with the selected values for x and y.)

Exercise 1.13 What increases quicker: the factorial function or the exponential function? (I.e. for a given $a \in \mathbb{R}_+, a > 1$ is a^n greater than $n!$ for very large n or is it the other way around?) Discuss in groups; You do not need to give a formal proof.

Exercise 1.14 (a) How many "words" with 6 letters exists, if you need to use 2 X's, 2 Y's, and 2 Z's? (Tip: First, place the two X's within the 6 free places, thereafter place the two Y's within the 4 remaining places, and finally place the two Z's on the 2 remaining places.)

(b) (Only if you already have a computer open.) In maple, write `expand`$\big((x+y+z)^6\big)$. What is the coefficient in front of the term $x^2y^2z^2$?

(c) Let $k_1 + k_2 + k_3 = n$. How many "words" with $n = k_1 + k_2 + k_3$ letters does there exist, if you need to use k_1 X's, k_2 Y's, and k_3 Z's?

(d) Rewrite the answer to (a) to $\frac{6!}{2!\cdot 2!\cdot 2!}$ and the answer to (c) to $\frac{n!}{k_1!k_2!k_3!}$. The last is called a "trinomial" and is at times written $\binom{n}{k_1,k_2,k_3} = \frac{n!}{k_1!k_2!k_3!}$. Discuss why this proves the following generalisation of Theorem 1.8:

$$(x+y+z)^n = \sum_{\substack{0\leq a,b,c\leq n \\ a+b+c=n}} \binom{n}{a,b,c} x^a y^b z^c \ .$$

Exercise 1.15 Proof the second part of Theorem 1.1, i.e. we know the following for the sets A, B, and C:

$$\begin{aligned} |A \cup B \cup C| = \quad & |A| + |B| + |C| \\ & - |A \cap B| - |A \cap C| - |B \cap C| \\ & + |A \cap B \cap C|. \end{aligned}$$

Tip: Write $A \cup B \cup C = (A \cup B) \cup C$ and use the first part of Theorem 1.1 on the sets $(A \cup B)$ and C. Afterwards, you will need $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

Exercise 1.16 Give a combinatorial proof for Corollary 1.9. (Tip: What do we combinatorial count with the sum $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n}$?)

Exercise 1.17 In this exercise, we look at the more formal proofs for some of the properties of the binomial coefficients.

(a) Proof Theorem 1.10 by the use of the definition of $\binom{n}{k}$.

(b) Proof Theorem 1.11 by the use of the definition of $\binom{n}{k}$ and bring the right hand side to a common fraction.

(c) Proof Theorem 1.12 by the use of Theorem 1.8 (Tip: What is the coefficient of x^k in the expression $(x+1)^{m+n} = (x+1)^m (x+1)^n$?)

Exercise 1.18 In your company, you use the binomial coefficient all the time: in your software, in your department of logistics, and at your company Christmas lunch. Therefore, you decide to implement an efficient algorithm to calculate $\binom{n}{k}$. You have three options:

1. Use $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, and then calculate $n!$, $k!$, and $(n-k)!$ seperately and then finally perform the division. Discuss the problems with this procedure (Tip: Compare $\binom{20}{10}$ with 20!).
2. Another option is to use Theorem 1.11 repeatedly until getting $\binom{m}{0} = 1$ and then only using addition. How many additions do you need to calculate $\binom{n}{k}$ using this technique?
3. A third option is to use "the absorption rule" from Exercise 1.11. How many multiplications and divisions do you need to calculate $\binom{n}{k}$ by the help of this? Discuss the advantages and disadvantages between this and the addition method.

1.6 Extra material: Selections with Replacement

The material is not in the curriculum and can therefore be skipped.

If we have a bowl with 4 different balls and need to choose 2 of them, we have $P(4,2) = 12$ ways of doing so if the order is significant. There are $\binom{4}{2} = 6$ ways of doing so if the order is not significant. Here we decided that when having chosen one ball, we will not be able to choose it again.

But what if we could choose the same ball twice? We could after choosing a ball put it back in the bowl. There are two ways of counting. One of which the order means something and one of which it does not.

If the order means something then we have 4 ways of choosing the first ball, and also 4 ways of choosing the second ball. According to the rule of multiplication there is 4^2 ways of choosing the two balls.

Generally, if you have n different balls and need to choose k balls, where the order of them means something and you are allowed to choose the same ball more than once, then there is n^k different ways of doing it. It is said that there is n^k different k permutations with place back.

> **Exercise 1.19** A student has 3 exams, which is all graded based on the seven step grade scale. Calculate the amount of different exam results, which can be reached.

If the order does not have a meaning, the situation becomes more complicated. Let us start by looking at the case, of which we need to choose 5 balls out of 3 different balls. One is red (R), one is green (G), and one is blue (B). It is possible because we are allowing place back. One option could be 2 red balls, one green ball, and two blue balls, which can be written RRGBB. To clearly separate the different types of balls, we could also write RR|G|BB. If we instead choose two red balls, no green ones, and three blue balls, we could write RR||BBB. Because of the separation symbol |, we do not need to write R, G, or B, because the colour is depended on the position compared to the vertical lines. This means we could write **|*|** for two red balls, one green ball, and two blue balls. Meanwhile, **|***| means two red balls, three green balls, and no blue balls.

Ergo, each choice of 5 balls correspond to a "word" of 7 letters, of which we can choose between two letters: "*" and "|". We need 5 *'s and 2 |'s.

With this we can see that the solution to the problem corresponds to finding out how many words of seven letter there can be written with 5 *'s and 2 |'s. But this we can actually calculate because it is similar to choosing 2 elements out of 7 elements when the order does not matter. We need to choose two elements which is going to be |'s and the rest needs to be *'s. The number of ways of which 2 out of 7 elements can be chosen is $\binom{7}{2} = 21$. We can conclude that there is 21 ways of choosing 5 balls of three different ones, when the order does matter and place back is allowed.

The general case is not more difficult. If we imagine that we have n different balls and need to choose k, where the order matters and place back

is allowed. This corresponds to the number of words, which we can write with k *'s and $n-1$ |'s. The number of these kind of words are

$$\binom{n+k-1}{n-1}. \tag{1.3}$$

Example 1.11 In a tapas bar there is 17 different small dishes. We can calculate how many ways we can order 5 dishes. We are allowed to order the same dish multiple times. We get the solution by setting $n = 17$ and $k = 5$ in equation (1.3):

$$\binom{21}{16} = 20349$$

Exercise 1.20 If we have three different Easter eggs designs, how many ways can we paint 6 eggs?

To sum up, there are different ways of counting how many ways of choosing k elements out of n elements.

	The same elements can	
	at most be chosen once	be chosen multiple times
The order matters	$P(n,k)$	n^k
The order does not matter	$\binom{n}{k}$	$\binom{n+k-1}{n-1}$

Chapter 2

Recursive definitions

2.1 The Recursive only talk about themselves

> **Recursion**, *n. [L. recursio.]*
> *The act of recurring; return. [Obs.]*
> *[1913 Webster]*

For something to be "recursive" it means that the description of it referrers to the thing itself. It sounds like the serpent biting its own tail, which it also easily can be, if it is not thoroughly described. None the less, recursive definitions are very common in mathematics, because it is often a easy and natural way to describe and reason about objects.

Here is an example of a recursive definition of a function $f : \mathbb{N} \to \mathbb{Z}$.

$$f(n) = \begin{cases} 3 & \text{for } n = 0, \\ 2 + f(n-1) & \text{for } n > 0. \end{cases}$$

This is recursive, because $f(n-1)$ is contained in the definition of $f(n)$. This means that you need to know before hand what the function is. But the first basic case, $f(0) = 3$, is the thing that saves us and determines $f(n)$ unambiguously.

Notation When we write $f : \mathbb{N} \to \mathbb{Z}$, it means that $f(n)$ is a function, which is defined for any natural number $n \in \mathbb{N}$ and the value of the function $f(n)$ is an integer.

Therefore, we have:

$$\begin{aligned} f(1) &= 2 + f(0) = 2 + 3 = 5 \\ f(2) &= 2 + f(1) = 2 + 5 = 7 \\ f(3) &= 2 + f(2) = 2 + 7 = 9 \\ &\text{etc.} \end{aligned}$$

It can be seen that we can continue this way to determine the value of $f(n)$ for any n we deem fit. This can be very troublesome and often when starting with a recursive definition you want a "closed formula" for $f(n)$. I.e. more easily put, a mathematical expression, which allows us to calculate $f(n)$ with a number of calculations, which does not grow with n. It can be very difficult (at times impossible!) to achieve a closed formula and it often requires the proof technique called "induction", which will be taught next week.

In this case, it is maybe not as difficult to realise based on the first values, which was calculated, and based on the recursive definition. The closed formula is

$$f(n) = 2n + 3 \ .$$

Exercise 2.1 Let

$$g(n) = \begin{cases} 2 & \text{for } n = 0, \\ 2 \cdot g(n-1) - 1 & \text{for } n > 0. \end{cases}$$

Calculate $g(0)$, $g(1)$, and $g(2)$.

Example 2.1 In the last chapter we defined the factorial function $n! = 1 \cdot 2 \cdot \ldots \cdot n$. A recursive definition of $n!$ can be written as:

$$n! = \begin{cases} 1 & n = 0 \quad \text{(base case)} \\ n \cdot (n-1)! & n > 0 \quad \text{(recursion case)} \end{cases}$$

The reason that we were able to use the recursive definition to calculate $f(3)$ or $f(100)$ was by repeatedly using the recursion case to reduce the expression until the base case was reached. You need to be careful with recursive definitions because it does not take much before it is no longer possible to calculate the values of the functions in this way. For example take $h : \mathbb{N} \to \mathbb{Z}$

$$h(n) = \begin{cases} 1 & n = 0 \\ 2 + h(n+1) & n > 0 \ . \end{cases}$$

We see that $h(0) = 1$. But what is $h(1)$? To find $h(1)$ we need $h(2)$. To find $h(2)$ we need $h(3)$ and then we need $h(4)$ etc. – this is the screw without end! We actually have not defined a function for $h(1)$, which means it can be anything. The moral is, for the expression to make sense, we need to make sure to end with a base case when repeatedly using the definition.

Recursion: A *recursive definition* contains a reference to itself. A recursively defined expression is *well-defined*, if the definition contains one or more base cases without a reference to itself. Furthermore, the remaining cases need to be able to be reduced to the base cases by repeated use of the definition.

Exercise 2.2 Is the following function $f : \mathbb{N} \to \mathbb{Z}$ well-defined?

$$f(n) = \begin{cases} 1 & \text{when } n \text{ is odd} \\ 1 + f(n/2) & \text{when } n \text{ is even.} \end{cases}$$

Example 2.2 Sometimes, it can be very difficult to determine if a function is well-defined or not. Consider the following function $f : \mathbb{N} - \{0\} \mapsto \mathbb{Z}$:

$$f(n) = \begin{cases} 0 & \text{when } n = 1 \\ f(n/2) + 1 & \text{when } n \text{ is even} \\ f(3n+1) + 1 & \text{when } n \text{ is odd and } n > 1 \end{cases}$$

For example is

$$\begin{aligned} f(12) &= f(6) + 1 = f(3) + 2 = f(10) + 3 = f(5) + 4 = f(16) + 5 \\ &= f(8) + 6 = f(4) + 7 = f(2) + 8 = f(1) + 9 = 9 \ . \end{aligned}$$

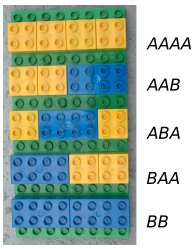
$f(n)$ counts the number of steps that the recursive definition goes through before it ends in $f(1) = 0$. For some n the path is very long: f.x. is $f(27) = 111$ and you need to go through $f(9232)$ during the calculation!

The incredible thing is that today it is still an unsolved problem if f is even well-defined! I.e. we do not know, if there exists a n that unfolds $f(n)$ by the recursive definition, which never leads to $f(1)$. This is called "the Collatz conjecture" or "the Syracuse problem" and the person, who solves this, will become very famous.

The following example shows that recursive definitions can occur naturally.

Assume we have two type of tiles: Type A is 1 unit wide, and type B is 2 units wide. We need to lay tiles on a strip which is n units wide. How many ways can we do this?

We let $f(n)$ denote the number of solutions and start with some special cases. If $n = 0$ we cannot lay down any tiles. So there is $f(0) = 1$ ways of doing this. If $n = 1$ there is only space to lay down one A tile. Meaning there is $f(1) = 1$ ways of doing it.



If $n = 2$ we can start by laying down either one A tile or one B tile. If we lay down a A tile, there is still space remaining, which means we need to lay down

another A tile. Alternatively, we can lay down a B tile. Therefore, there is $f(2) = 2$ different ways of doing this, namely AA and B. If $n = 3$ there is 3 possibilities AAA, AB, BA. If $n = 4$ there is 5 possibilities $AAAA$, AAB, ABA, BAA, BB. See the figure to the right.

Let us look at the general case $n > 1$. We can start by laying down one A tile, which mean we have a strip of length $n-1$ where we need to lay down tiles. Or we can lay down a B tile, which means we still have a remaining strip of length $n - 2$.

In the first case, there is $f(n-1)$ ways of laying down the remaining tiles, and in the second case, there is $f(n-2)$ ways of laying down the remaining tiles. Therefore, there is in total $f(n) = f(n-1) + f(n-2)$. Hereby, we can write a recursive definition for $f(n)$.

$$f(n) = \begin{cases} 1 & n = 0, 1 \\ f(n-1) + f(n-2) & n > 1. \end{cases}$$

This is very nice, but f.x. what is $f(10)$? The easiest way to calculate this is by making a table.

n	f(n)
0	1
1	1
2	2
3	3
4	5
5	8
6	13
7	21
8	34
9	55
10	89
⋮	⋮

The first two values in the table is the base case in the recursive definition. The next ones can be found by adding the two previous values.

Notice that it is way quicker to use a table than to use the definition repeatedly. In the base case f equals 1. So if we need to calculate $f(10)$ by repeatedly using the definition, we would. after many substitutions, get a sum of 89 1's.

The series of numbers $f(0), f(1), f(2), \ldots$ is very famous and has a name, namely the Fibonacci numbers.

2.2 More examples of recursive definitions

In this section we will see many of the functions, which we saw in the last chapter, can be written as recursive definitions.

We start with the summation symbol. Remember that for integers m and n it is denoted that

$$\sum_{k=m}^{n} f(k)$$

is the sum of all the terms $f(k)$, where k goes from m to n, thus $f(m) + f(m+1) + \cdots + f(n)$.

If the lower bound is greater than the upper bound, then the sum is set to 0. For example

$$\sum_{k=3}^{2} k = 0.$$

The meaning of the summation symbol can be defined recursively.

Definition 2.1
If $m, n \in \mathbb{Z}$ and $g(k)$ is an expression, then the symbol is $\sum_{k=m}^{n} g(k)$ defined by

$$\sum_{k=m}^{n} g(k) = \begin{cases} 0 & m > n \\ \sum_{k=m}^{n-1} g(k) + g(n) & m \leq n \end{cases}$$

Notice that the empty sum $m > n$ is set to 0. This is the base case. Consider why $\sum_{k=m}^{n} g(k)$ is well-defined.

We can use the definition to calculate the concrete sum. The following can be stated

$$\begin{aligned} \sum_{k=2}^{4} k^2 &= \sum_{k=2}^{3} k^2 + 4^2 \\ &= \sum_{k=2}^{2} k^2 + 3^2 + 4^2 \\ &= \sum_{k=2}^{1} k^2 + 2^2 + 3^2 + 4^2 \\ &= 0 + 2^2 + 3^2 + 4^2 \\ &= 29. \end{aligned}$$

The function $P(n, k)$ from the last chapter can be naturally defined using recursion. Remember that $P(n, k)$ determines that number of ways we can choose k balls out of n different ones, when the order matters.

If $k = 0$ then $P(n, k) = P(n, 0) = 1$. If $k > n$ then $P(n, k) = 0$, because it is not possible to choose more elements than there exists.

What about the general case $n \geq k > 0$? We have n different options for choosing the first element. No matter what we choose, subsequently we need to choose $k - 1$ elements between the remaining $n - 1$ elements. We can do this in $P(n-1, k-1)$ ways. Thus there is $nP(n-1, k-1)$ different k permutations, when $n \geq k > 0$. We can conclude that $P(n, k)$ have the recursive definition

$$P(n,k) = \begin{cases} 0 & k > n \\ 1 & k = 0 \\ nP(n-1,k-1) & n \geq k > 0 \end{cases} \tag{2.1}$$

Now we look at the number of k combinations. This means the number of ways to choose k elements from a set of n elements, when the order does not matter and we do not allow replacements. We introduced the notation $\binom{n}{k}$ for this amount and it is called a binomial coefficient, where $\binom{n}{0} = 1$ and if $k > n$ then $\binom{n}{k} = 0$. We still need to look at the general case where $n \geq k > 0$. Let us take one element in the set, which we call x_1. We split this in two cases:

Either we choose x_1 or we do not. If we choose x_1, we still need to choose $k - 1$ elements from the set of the remaining $n - 1$ elements. This can be done in $\binom{n-1}{k-1}$ different ways. If we do not choose x_1, we still need to choose k elements from a set of $n - 1$ elements. This can be done in $\binom{n-1}{k}$ ways. In total there is $\binom{n-1}{k-1} + \binom{n}{k-1}$ ways of doing this. Thus $\binom{n}{k}$ is recursively defined by

$$\binom{n}{k} = \begin{cases} 1 & k = 0 \\ 0 & r > n \\ \binom{n-1}{k-1} + \binom{n-1}{k} & n \geq k > 0. \end{cases}$$

2.3 More exercises

Exercise 2.3 What can the advantages be using a table when calculating a recursively defined function instead of using the definition repeatedly?

Exercise 2.4 A function is defined recursively for all natural number by

$$f(n) = \begin{cases} 1 & \text{if } n = 0 \\ f(n-1)^2 + 4 \cdot n & \text{if } n \geq 1 \end{cases}$$

Calculate the values $f(0), f(1), f(2)$, and $f(3)$ of the function.

Exercise 2.5 Show that $P(n, n) = n!$.

Exercise 2.6 We need to lay down tiles similarly to the previous example, but instead of the width being 1 and 2 units, they now have

the width of 2 and 5 units. How does the recursive definition of the number of tiles look now? Write a table of the values of the function from 0 to 10.

Tip: It can be practical to put $f(n) = 0$ for $n < 0$. The combinatorical problem does not make sense for $n < 0$, which means that we need to determine what $f(n)$ needs to be. If we use $f(n) = 0$ for $n < 0$, we get a simpler recursive expression.

Exercise 2.7 We need to lay down a 1m wide strip and have two types of tiles. The length of the strip is $n \cdot 0.5$m. Tile type A is $1\text{m} \times 0.5\text{m}$ with a homogeneous surface. One can be put across or two can be put along the strip. Tile type B is quadratic $1\text{m} \times 1\text{m}$ but with a asymmetrical surface drawing, which means it can be orientated in 4 different ways. Find a recursive formula for the number of ways the strip can be made, and calculate the first 10 values ($n = 1, 2, \ldots, 10$) of the function.

A biologist is working on making a model based on the growth of a population of rats. The biologist observes that the birth rate and the survival rate are dependent on the age of the rats.

The rats are divided into three different age groups: Those who are between 0 and 6 months old, those who are between 6 and 12 months old, and those who are between 12 and 18 months old. It is assumed that rats older than 18 months do not exist (it is a bad rat life to be a rat). A population of rats is described at a given time by three numbers:

u_0 : number of rats between 0 and 6 months,

v_0 : number of rats between 6 and 12 months, and

w_0 : number of rats between 12 and 18 months.

By studying the three age groups in the population of rats, the biologist finds how many rats die in the time frame of six months and how many rats are born in the time frame of six months. More precisely, the biologist observes for each of the age groups the following table of birth and survival rates:

Age (months)	Birth rate	Survival rate
$0-6$	0,1	0,8
$6-12$	0,7	0,8
$12-18$	0,1	0,0

Now answer the following questions:

Exercise 2.8 If $(u_0, v_0, w_0) = (15, 10, 5)$, how many rats will there approximately be in each of the age groups after six months?

Exercise 2.9 Find a recursion, which expresses (u_n, v_n, w_n) as the number of rats in the three age groups after six months with the starting values $(u_{n-1}, v_{n-1}, w_{n-1})$. The values for the base case $n = 0$ is given in the first question.

2.4 Extra: Recursion and software

This section is not within the curriculum.

Algorithms can also use recursion. Now and then, it can be practical that a method can call itself to solve a problem. Thus it is not only in mathematics that recursive definitions can make sense.

A famous example is `quicksort`. A quick algorithm, which can sort a list. We can describe loosely how is works. If you need to sort a list of numbers, you need to look at how many numbers are in the list. If there is 0 or 1 numbers, the list can be returned directly, since the numbers are already sorted. This is the base case. If there is 2 or more numbers, then you have to choose a random number x from the list. Then split the list in two: a list of the numbers smaller than the chosen number, A, and a list of numbers greater than (or equal) to the chosen number, B. The result is now the numbers in A sorted, followed by x, followed by the numbers in B sorted.

But how do we sort the numbers in A and B? This is done by calling `quicksort` again with respectively A and B as input. This means that `quicksort` is calling itself, which makes it a recursive algorithm.

For example let us assume that we will sort the numbers

$$7, 4, 3, 8$$

We choose a random number. Let us take the first one; 7. Thereafter, we construct the two lists: A is $4, 3$, namely the numbers less than 7 and B is 8, which is the only number greater than 7. Then we get

$$\texttt{quicksort}(7, 4, 3, 8) = \texttt{quicksort}(4, 3), 7, \texttt{quicksort}(8).$$

When $\texttt{quicksort}(4, 3)$ is being called, we choose a random number. Let us take again take the first number; 4. Then we split the remaining numbers (namely the number 3) in two lists: the list of numbers, which are smaller than 4 (it is 3) and the list of numbers, which are greater than 4, the empty list. Then we get

$$\texttt{quicksort}(4, 3) = \texttt{quicksort}(3), 4, \texttt{quicksort}().$$

The three function calls

$$\texttt{quicksort}(3), \texttt{quicksort}(), \text{ and } \texttt{quicksort}(8),$$

all corresponds to base cases. Therefore we get

$$\begin{aligned}\texttt{quicksort}(7, 4, 3, 8) &= \texttt{quicksort}(4, 3), 7, \texttt{quicksort}(8) \\ &= \texttt{quicksort}(3), 4, \texttt{quicksort}(), 7, \texttt{quicksort}(8) \\ &= 3, 4, 7, 8\end{aligned}$$

and we can see that the algorithm has sorted the 4 numbers.

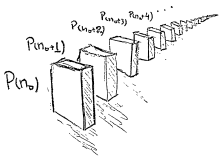
Chapter 3

Proofs by Induction

3.1 The principle of mathematical induction

It is important to be able to proof things. A lot of mathematics is about proving something. Even if it is something as simple as solving a single equation corresponds to proving that the solution is what it is. Even though it can be an advantage to show that a certain algorithm works in specific test cases, it is better to *prove* that the algorithm works in general. Proofs are our friends.

A forceful method to prove a statement about natural numbers are proof by induction. It can be useful to think about proof by induction as a way of tipping an infinite amount of dominoes. Imagine that an infinite amount of dominoes are lined op one after the other. **If** we know to things:



1. The first domino tips over and
2. tipping over one domino leads to the fall of the next domino.

Then what happens to the dominoes? The first one tips over, which makes the next one tip over, which makes the third one tip over, and so forth and so forth. They all tip over.

Imagine that instead of tipping over dominoes, we want to prove a statement $P(n)$ for $n \in \mathbb{N}$. If we can prove that

1. the statement is true for $n = 0$ and
2. that the statement is true for a value n, which makes it true for $n + 1$,

then the statement is true for all $n \in \mathbb{N}$. This is *the principle of mathematical induction.*

Assume that when a domino falls it leads to the next one falling, but we no longer know that the first domino falls. However we do know that

the domino n_0 falls. We can no longer conclude that all dominoes fall, but we can conclude that the dominoes from domino n_0 and onwards fall. This corresponds to the following phrasing of the principle of mathematical induction.

Mathematical Induction (weak form): Let $P(n)$ be a statement for $n \in \mathbb{N}$. If we can prove

1. $P(n_0)$ is true and
2. for all $n \in \mathbb{N}$, when $n \geq n_0$ $P(n) \Rightarrow P(n+1)$,

we know that $P(n)$ holds for all natural numbers $n \geq n_0$.

Thus, to show that $P(n)$ is true for all $n \geq n_0$, we need to show 1. *the base case* and 2. *the induction step*. In the induction step we need to assume that for any $n \geq n_0$ $P(n)$ is true and use this to prove that $P(n+1)$ is also true. This assumption is also called *the induction hypothesis*. The terms we use are therefore

1. $P(n_0)$ is true and — the base case
2. for all $n \in \mathbb{N}$ when $n \geq n_0$ is true that $\underbrace{P(n)}_{\text{induction hypothesis}} \Rightarrow P(n+1)$, — induction step

Now we are going to look at some examples of how to do proofs by induction. We will start with an example from matrix calculations. If $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{n \times n}$ then we know from linear algebra that it is true that

$$\det(\mathbf{AB}) = \det(\mathbf{A}) \det(\mathbf{B}).$$

What is true for $\det(\mathbf{A}^n)$ for $n \in \mathbb{N}$?

We can try to go from one end to the other. If $n = 0$ then $\mathbf{A}^n = \mathbf{A}^0 = \mathbf{E}$. Therefore it is true that $\det(\mathbf{A}^0) = \det(\mathbf{E}) = 1 = \det(\mathbf{A})^0$, since we have $x^0 = 1$ no matter what x is. If $n = 1$ then we have

$$\det \mathbf{A}^1 = \det(\mathbf{A})^1.$$

If $n = 2$ then we have

$$\det(\mathbf{A}^2) = \det(\mathbf{A}) \det(\mathbf{A}) = \det(\mathbf{A})^2.$$

If $n = 3$ then we have $\mathbf{A}^3 = \mathbf{A}\mathbf{A}^2$, which gives

$$\det(\mathbf{A}^3) = \det(\mathbf{A}) \det(\mathbf{A}^2) = \det(\mathbf{A}) \det(\mathbf{A})^2 = \det(\mathbf{A})^3.$$

If $n = 4$ then we have $\mathbf{A}^4 = \mathbf{A}\mathbf{A}^3$, which gives

$$\det(\mathbf{A}^4) = \det(\mathbf{A}) \det(\mathbf{A}^3) = \det(\mathbf{A}) \det(\mathbf{A})^3 = \det(\mathbf{A})^4.$$

Hereby, we know that $\det(\mathbf{A}^n) = \det(\mathbf{A})^n$, for $n = 0, 1, 2, 3, 4$.

We can now guess that for $n \in \mathbb{N}$ it is true that

$$\det(\mathbf{A}^n) = \det(\mathbf{A})^n. \tag{3.1}$$

But how can we prove it? We are able to do this simply and elegantly using proof by induction.

Proof. We can prove (3.1) by induction. We have already shown that base case: When $n = 0$ then we have $\det(\mathbf{A}^0) = 1 = \det(\mathbf{A})^0$. In the induction step we need to assume that given $n \geq 0$ it is true that

$$\det(\mathbf{A}^n) = \det(\mathbf{A})^n. \tag{3.2}$$

We can use this to prove that it is also true that

$$\det(\mathbf{A}^{n+1}) = \det(\mathbf{A})^{n+1}.$$

We are able to because of

$$\det(\mathbf{A}^{n+1}) = \det(\mathbf{A}\mathbf{A}^n) = \det(\mathbf{A})\det(\mathbf{A}^n)$$

and according to the induction hypothesis (3.2)

$$\det(\mathbf{A})\det(\mathbf{A}^n) = \det(\mathbf{A})\det(\mathbf{A})^n = \det(\mathbf{A})^{n+1}.$$

Thus we have completed the induction step. It then follows from the principle of induction that (3.1) is true for all $n \in \mathbb{N}$. □

We are going to show one more example. Prove that for all $n \in \mathbb{N}$ it is true that

$$\sum_{k=0}^{n} k = \frac{(n+1)n}{2}.$$

Proof. We are going to prove the equation by induction. In the base case $n = 0$ the left hand side is equal to zero and so is the right hand side. Assume that for an arbitrary $n \in \mathbb{N}$ it is true that

$$\sum_{k=0}^{n} k = \frac{(n+1)n}{2}.$$

Which means that we have

$$\begin{aligned}
\sum_{k=0}^{n+1} k &= \sum_{k=0}^{n} k + (n+1) && \text{and according to the induction hypothesis} \\
&= \frac{(n+1)n}{2} + n + 1 && \text{put on a common fraction} \\
&= \frac{2\cdot(n+1) + (n+1)n}{2} && \text{put outside the parentheses} \\
&= \frac{(n+1)(2+n)}{2} \\
&= \frac{(n+2)(n+1)}{2}.
\end{aligned}$$

Hereby, we have completed the induction step. According to the principle of induction the equation is fulfilled for all $n \in \mathbb{N}$. □

Exercise 3.1 What is a base case?

Exercise 3.2 What is an induction step?

Exercise 3.3 What is an induction hypothesis?

Exercise 3.4 What is the determinant of

$$\begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}^n ?$$

When you are starting out doing proofs by induction, it is a good idea to write down the proof after a model or template. In the following paragraph, what is written in black can be reused and what is written in blue needs to be adjusted to the current situation.

We prove $P(n)$ by induction. The base case is $P(n_0)$. Because *argument* is true for $P(n_0)$. This shows the base case.

For the induction step, it can be assumed that $P(n)$ is true for a given $n \geq n_0$. We need to show $P(n+1)$. Arguments. According to the induction hypothesis it is true that more arguments are true. This was what needed to be shown.

According to the principle of induction it is true that the equation/theorem/results holds for all $n \geq n_0$.

The difficult part of completing a proof by induction is of course to figure out what the blue text needs to be.

Let us give a proof of Bernoulli's inequality by the help of the template. Bernoulli's inequality is

$$\text{for all } x \geq -1 \text{ and for all } n \in \mathbb{N} \text{ it is true that } (1+x)^n \geq 1 + nx.$$

Here is the proof:

Proof. We want to prove *the inequality* by the help of induction.

The base case corresponds to

$$(1+x)^0 \geq 1 + 0 \cdot x,$$

because both the left hand side and the right hand side results in 1, which makes the inequality for $n = 0$ true.
This proves the base case.

For the induction step, it is assumed that $(1+x)^n \geq 1 + nx$ is true for a certain $n \geq 0$. We need to show that $(1+x)^{n+1} \geq 1 + (n+1)x$. We know $(1+x)^{n+1} = (1+x) \cdot (1+x)^n$. According to the induction hypothesis it is true that $(1+x)^n \geq 1 + nx$, and because we have assumed that $1 + x \geq 0$, we can conclude that

$$(1+x) \cdot (1+x)^n \geq (1+x) \cdot (1+nx) \ .$$

We reduce the parentheses and get

$$1 + nx + x + nx^2 \geq 1 + nx + x = 1 + (n+1)x \ .$$

It is therefore true that

$$(1+x)^{n+1} \geq 1 + (n+1)x.$$

This was what we needed to prove.

According to the principle of induction it is true that the inequality for all $n \geq 0$. □

We can use induction to prove many other things than just formulas and inequalities. As an example, we look at the solitaire game *The tower of Hanoi*. The tower of Hanoi is a puzzle consisting of a board with three verticals pins. On the first pin, there is a stack of rings of decreasing radius (see Figure 3.1). The purpose of the game is to move the stack of rings to the third pin. This should be done in consideration to the following rules:

- You can only move one ring at a time.
- You can only move a ring, which is on the top of a stack.
- A ring can never be placed on a smaller ring.

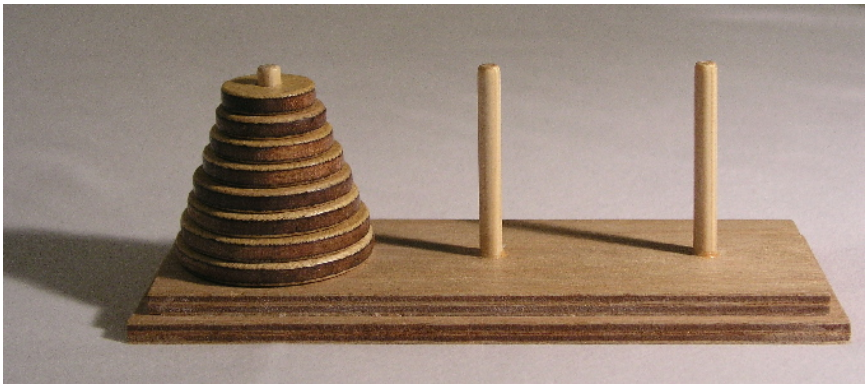


Figure 3.1: The tower of Hanoi.

With these rules you can start to move the rings to the other pins. But if there is a lot of rings, it is not immediately clear that it is possible to move the whole stack to the third pin.

Try to solve the game. Is it always possible to solve? We want to prove that

the tower of Hanoi always has a solution.

To begin with, we reformulate:

> For all $n \in \mathbb{N}$, of which $n \geq 1$, the tower of Hanoi with n rings have a solution.

Hereby, we have formulated the statement as a sentence, which can be proven by induction.

Proof. We use the principle of mathematical induction.

The base case $n = 1$ is simple. If there is only one ring, it can simply be moved from the first pin to the third pin.

Assume that we can solve the game, when there is n rings. Now consider a game with $n + 1$ rings. According to the induction hypothesis, the top n rings can be moved to the third pin. The $n + 1$'th ring is larger than all the others, which means that the moves, which are needed to move the n top rings are legal. There is no difference between pin 2 and 3 other than the number, which mean the n top rings can be moved to the second pin. This means that we can now move the largest ring from the first pin to the third pin. Again by the induction hypothesis we can move the n rings from the second pin to the third pin. Thus we have solved the game in the case of $n + 1$ rings. □

Exercise 3.5 Let $f(n)$ be recursively defined by

$$f(n) = \begin{cases} 0 & \text{for } n = 0, \\ 2f(n-1) + 1 & \text{for } n > 0. \end{cases}$$

Prove by induction that

$$f(n) = 2^n - 1$$

for all $n \in \mathbb{N}$.

Tip: It follows from the recursive definition that when $n \geq 0$, then $f(n + 1) = 2f(n) + 1$.

Exercise 3.6 What is wrong with the following proof, which says all set of balls have the same colour? Prove by induction using the amount of balls. If there is only one ball in the set, then they are all the same colour. Now assume that all sets consist of $n+1$ balls, which have the same colour, and consider an arbitrary set of $n + 1$ balls. If one ball is taken out, then by the induction hypothesis the remaining balls have the same colour. If a second ball is taken out, then the remaining balls also have the same colour. This means all balls must have the same colour. QED.

Exercise 3.7 The following statement is clearly not true: Any natural number n fulfils $n > 10$. Would the statement be correct by the induction hypothesis? What about the base case?

Exercise 3.8 Prove by induction the following closed formula for the sum of squares:

$$\sum_{k=1}^{n} k^2 = \frac{1}{6} n(n + 1)(2n + 1)$$

Exercise 3.9 Consider the game the tower of Hanoi from earlier. A "move" is to move one ring from one pin to anther. How many moves does the solution use to solve the tower of Hanoi described earlier?

Tip: Call the number of moves for $T(n)$, where n is the number of rings in the game. Write a recursive formula for $T(n)$. Do you recognise it? If not, then calculate $T(n)$ for small values of n. Guess a solution and use induction.

Exercise 3.10 We call x an intersection of the lines $L_1, L_2, \ldots, L_n$, if at least to of the lines intersect in x.

Show that n different lines at most can have $\sum_{k=1}^{n-1} k$ intersections.

Exercise 3.11 Two matrices $\mathbf{A}, \mathbf{B} \in \mathbb{C}^{m\times m}$ are called similar when there exists a regular matrix $\mathbf{V} \in \mathbb{C}^{m\times m}$ such that

$$\mathbf{A} = \mathbf{V}\mathbf{B}\mathbf{V}^{-1}.$$

When $\mathbf{A}$ and $\mathbf{B}$ are similar, it is written $\mathbf{A} \sim \mathbf{B}$.

(a) Show that if $\mathbf{A} \sim \mathbf{B}$ is true for all $n \in \mathbb{N}$ $\mathbf{A}^n \sim \mathbf{B}^n$.

(b) Afterwards, consider

$$\mathbf{A} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$$

and construct an example, where $\mathbf{A}^2 \sim \mathbf{B}^2$, but where it is not true that $\mathbf{A} \sim \mathbf{B}$.

Extra exercises (not part of the curriculum)

Exercise 3.12 Again, we look at the tower of Hanoi, but make the rules a bit more difficult than before: in a move you are still only allowed to place a smaller ring on top of a larger one, but now you are not allowed to move a ring directly from the first pin to the last pin. Thus, it is only allowed to move a ring between the outer pins and the middle pin.

Figure out a solution algorithm for this variant of the tower of Hanoi. Describe a recursive formula for the number of moves it uses. (There is not an immediate closed formula for this recursion).

Exercise 3.13 Theorem 1.1 describes the number of elements in a union of 2 or 3 sets from the amount of elements in different intersections. In this exercises you need to use induction to prove the general formula, which is at times called "the inclusion-exclusion-principle".

For the sets $A_1, \ldots, A_n$ it is true that:

$$|A_1 \cup \ldots \cup A_n| = \sum_{S\subset\{1,2,\ldots,n\}} (-1)^{|S|-1} \left| \bigcap_{s\in S} A_s \right|. \tag{3.3}$$

Here it means that $\bigcap_{s\in S} A_s = A_{s_1} \cap A_{s_2} \ldots \cap A_{s_{|S|}}$, in which $S = \{s_1, \ldots, s_{|S|}\}$ is all the elements in S.

The sum is an aggregation of all the subsets S of the set $\{1, 2, \ldots, n\}$, where each of them gives a small contribution, positive or negative, to the number of elements in the intersection of the A_*-sets, which are indexed by S.

(a) Verify that Equation (3.3) gives the same as Theorem 1.1 for $n = 2$ and $n = 3$.

(b) Expand Equation (3.3) completely for $n = 4$.

(c) Use induction to prove Equation (3.3). Tip: Write $A_1 \cup A_2 \cup \ldots \cup A_n = B_{n-1} \cup A_n$ where $B_{n-1} = A_1 \cup \ldots \cup A_{n-1}$ and use the theorem for $n = 2$. Afterwards make use of $B_{n-1} \cap A_n = (A_1 \cap A_n) \cup (A_2 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)$ and use the theorem for $n-1$ two times. Collect all the terms according to the unions which are represented by the different terms in the sum.

Exercise 3.14 Imagine a long circular track, where there is $n > 0$ fuel repositories. In the repositories there is exactly the amount of fuel, which is needed for a car to drive one lap around the track. Show that there exists one place on the track, where the car can start and complete a lap. Assume that the car starts with an empty tank, so it needs to start by one of the repositories.

Tip: If the car is by a repository, which contains enough fuel for the car to reach the next repository, so it resembles the case, where all the fuel had been at the first repository.

3.2 The strong version of the principle of induction

Let us return to the thought experiment about the dominoes. Assume that we know that the first domino falls as before. Furthermore, assume that for an arbitrary domino it is true that if all the dominoes before fall, this domino will also fall. Which dominoes will then fall?

The first one falls. Regarding the second, we know that all the previous have fallen, (namely the first one), so this will also fall. Regarding the third, we know that domino 1 and 2 fell, so domino 3 will also fall. And so forth and so forth. They all fall.

This leads us to the following stronger version of the principle of mathematical induction.

Mathematical Induction (strong form): Let $P(n)$ be a statement about the natural numbers. If it is true that

1. $P(n_0)$ for a $n_0 \in \mathbb{N}$ and
2. for all $n \geq n_0$

$$(\forall k \in \{n_0, n_0 + 1, \ldots, n\} P(k)) \quad \Rightarrow P(n+1)$$

then it must be true that $P(n)$ holds for all $n \geq n_0$.

The base case in the stronger version is the same as in the weak version. The induction step is different. When we need to prove that $P(n+1)$ is true,

we do not only allow to assume that $P(n)$ is true. We are allowed to assume that $P(k)$ is true for all k between n_0 and n, including both. This means that we in the induction step have a even stronger induction hypothesis to use, when we need to prove $P(n+1)$.

We want to use mathematical induction to prove that any $n \geq 2$ has a *prime factorisation*. For n to have a prime factorisation means that n can be written as a product of one or more prime numbers. For example, 3 is a prime number, which means it is a product of prime number, namely 3. The number 9 can be written as $3 \cdot 3$, which is a product of two prime numbers.

Before we prove anything, we need to refresh what we know about prime numbers. It is said that $k \in \mathbb{N}$ divides $n \in \mathbb{N}$, if there exists a $q \in \mathbb{N}$ such that $n = q \cdot k$. A short way to write k divides n is $k \mid n$. For example it is true that $7 \mid 14$ because $14 = 2 \cdot 7$. It is not true that $7 \mid 15$.

An integer $n \geq 2$ is called a *prime number*, if the two only natural number dividing n is 1 and n itself. An integer $n \geq 2$, which is not a prime number, is called a *composite* number.

Let us prove that all integers $n \geq 2$ can be written as a product of one or more prime numbers. We will prove this by induction.

Proof. The base case is $n = 2$. Since 2 is a prime number, we have already stated it as the product of one prime number, 2.

Induction step: Assume that all integers between 2 and n (inclusive) have a prime factorisation. Consider $n+1$. Either it is a prime number $n+1 = p$ and we are done. Or it is not a prime number, which means it can be written as $n + 1 = n_1 \cdot n_2$ where $n_1 \geq 2$ and $n_2 \geq 2$. Since $n_1 \geq 2$, n_2 must be less or equal to n, meaning $2 \leq n_2 \leq n$. Equivalently, we have $2 \leq n_1 \leq n$. According to the induction hypothesis, we can write both n_1 and n_2 as a product of prime numbers. Therefore, we can also write $n + 1 = n_1 \cdot n_2$ as a product of prime numbers, namely the collected product of the prime numbers, which we multiplied to get n_1 and the ones we multiplied to get n_2. □

Exercise 3.15 The Fibonacci numbers are recursively defined by $f(0) = f(1) = 1$ and $f(n+1) = f(n) + f(n-1)$ for $n = 1, 2, \ldots$. Prove that $f(n) \leq 2^n$ for all $n = 0, 1, 2, \ldots$. Tip: Since $2^{n-1} < 2^n$ then $2^n + 2^{n-1} < 2^n + 2^n = 2^{n+1}$.

The following shows that the principle of induction in the strong form follows from the principle of induction in the weak form. The following proof is not in the curriculum and can therefore be skipped.

Proof. Let $P(n)$ be a statement for all $n \geq n_0$. Let $Q(n)$ be the statement

$$\forall k \in \{n_0, n_0 + 1, \ldots, n\} P(k).$$

This applies if $Q(n)$ is fulfilled for all $n \geq n_0$, then $P(n)$ us also fulfilled for all $n \geq n_0$. To see this, assume that $Q(n)$ is fulfilled for all $n \geq n_0$. Let $n \geq n_0$ be arbitrary. Since $Q(n)$ is fulfilled, it leads to $P(k)$ being fulfilled for all k of which $n_0 \leq k \leq n$. Especially, $P(k)$ needs to be fulfilled for $k = n$.

This means that $P(n)$ is true. Since $n \geq n_0$ was arbitrary, we have showed what we wanted.

It follows that proving that $P(n)$ is fulfilled for all $n \geq n_0$ is enough to prove that $Q(n)$ is true for all $n \geq n_0$. What is needed to prove that $Q(n)$ is true for all $n \geq n_0$ using induction? The base case is that $Q(n_0)$ is true. The statement $Q(n_0)$ gives that $P(k)$ is true for all k when $n_0 \leq k \leq n_0$. Thus $Q(n_0) = P(n_0)$. So proving $Q(n_0)$ is the same as proving $P(n_0)$.

The induction step is to prove that for all $n \geq n_0$ it is true that $Q(n) \Rightarrow Q(n+1)$. Thus, $P(k)$ is fulfilled for k when $n_0 \leq k \leq n$ needs to imply that $P(k)$ is fulfilled for k when $n_0 \leq k \leq n+1$. But if $P(k)$ is fulfilled for k when $n_0 \leq k \leq n$ then it is also fulfilled for k between $n_0 \leq k \leq n+1$ if and only if $P(k)$ is fulfilled for $k = n+1$. Therefore, if and only if $P(n+1)$ is fulfilled. So showing that $Q(n)$ implies $Q(n+1)$ is equivalent to showing that $Q(n)$ implies $P(n+1)$.

To summarise. We can show that $P(n)$ is true for $n \geq n_0$ if we can prove that $Q(n)$ is true for $n \geq n_0$. We can proof that $Q(n)$ is fulfilled for $n \geq n_0$ if we can establish two things.

- $P(n_0)$ is fulfilled.
- $Q(n) \Rightarrow P(n+1)$ for all $n \geq n_0$.

But this is exactly the principle of induction in the strong version. □

Chapter 4

Euclid's algorithm

4.1 Greatest common divisor

Euclid[1]'s algorithm is an efficient algorithm to find the greatest common divisor of two integers. The algorithm will be useful, when we in the next chapter need to solve congruence equations. Later on, we will see that the algorithm not just works on two integers. It also works on two polynomials. Therefore, the algorithm is also interesting when solving equations, which involves polynomials. But first, we need to repeat some fundamentals regarding division.

First, we need the terms divisor, quotient, and the remainder. Take for example 14. The number can be written as $7 \cdot 2$. This means that 7 divides 14, which is the same as saying that 7 is a *divisor* in 14. This can also be written "$7 \mid 14$". It can also be said that 14 is a multiple of 7.

We have seen that 7 is a divisor of 14, but is it also true that 7 is a divisor of 15? Since we have $15 = 2 \cdot 7 + 1$. The integer quotient of 15 is divided by 7 is 2, and the remainder of this division is 1. This means that 7 is not one of the divisors of 15, because 7 does not divide 15. Formally, the quotient and the remainder is defined by the following theorem.

Theorem 4.1
Let $n, m \in \mathbb{Z}$ and $m \neq 0$. Then there exists two unambiguous numbers $q, r \in \mathbb{Z}$ which fulfil

$$n = qm + r, \text{ and } 0 \leq r < |m|.$$

The integers q and r is called respectively *the quotient* and *the remainder* of the division of n by m.

There exists a sneaky algorithm, which allows a fast calculation of the quotient and the remainder, which you probably already know from school.

[1] Euclid, Greek mathematician, ca. 340 B.C.

For example, let us divide 384 by 18. First we will write the calculation.

$$\begin{array}{r|l} 18 & \overline{384} \end{array}$$

The first two digits of 384 is 38, and 18 divides 38 twice. Therefore, we can write 2 and subtract $2 \cdot 18 = 36$ from 38.

$$\begin{array}{r|l} & 2 \\ 18 & \overline{384} \\ & -36 \\ & \overline{2} \end{array}$$

We pull down the number 4 and divide 24 by 18. This can be done once and the result is the following.

$$\begin{array}{rl} & 21 \quad \leftarrow \text{quotient} \\ 18 & \overline{384} \\ & -36 \\ & \overline{24} \\ & -18 \\ & \overline{6} \quad \leftarrow \text{remainder} \end{array}$$

The result is that 384 can be divided by 18 21 times with a remainder of 6.

There are different ways to write division, depending on the country one comes from. Below, we show how it is done in Denmark, the US and Germany.

$$\begin{array}{rl} & 21 \quad \leftarrow \text{quotient} \\ 18 & \overline{384} \\ & -36 \\ & \overline{24} \\ & -18 \\ & \overline{6} \quad \leftarrow \text{remainder} \end{array} \qquad \begin{array}{rl} & 21 \quad \leftarrow \text{quotient} \\ 18) & \overline{384} \\ & -36 \\ & \overline{24} \\ & -18 \\ & \overline{6} \quad \leftarrow \text{remainder} \end{array} \qquad \begin{array}{l} 384 : 18 = 21 \leftarrow \text{quotient} \\ \underline{36} \\ 24 \\ \underline{18} \\ 6 \quad \leftarrow \text{remainder} \end{array}$$

As mentioned earlier, a divisor of n is a number d, which divides n. Thus a number, where the remainder is 0 of the division of n by d.

Definition 4.2
A number $d \in \mathbb{Z}$ is called a *divisor* in $n \in \mathbb{Z}$, if there exists a $q \in \mathbb{Z}$ such that

$$n = qd.$$

If d is a divisor in n, it is said that n is a *multiple* of d, which we can write as $d \mid n$.

Exercise 4.1 Find the positive divisors when $n = 18$.

Exercise 4.2 What is the quotient and the remainder by the division of 30 by 7?

Definition 4.3
The set of multiples of $d \in \mathbb{Z}$ (thus the numbers, which d divides) is denoted

$$d\mathbb{Z}.$$

According to the definition, we have $d\mathbb{Z} = \{\ldots, -2d, -d, 0, d, 2d, \ldots\} = \{kd \mid k \in \mathbb{Z}\}$.

Notice that if d is a divisor of n, then $-d$ is a divisor too. The number n has the same divisors as $-n$. The number 1 has only the divisors 1 and -1. On the other hand 0 has any $d \in \mathbb{Z}$ as a divisor.

Exercise 4.3 Find the positive divisors for $n = 12$. Which positive divisors do $n = 12$ and $n = 18$ have in common? Which of the common divisors is greatest?

The greatest common divisor is useful in many contexts. To be sure that this is not misunderstood, we will define it formally:

Definition 4.4
For $n, m \in \mathbb{Z}$ when $n \neq 0 \vee m \neq 0$ the common divisor is a number d, which is both a divisor in n and m. The greatest of the common divisors is denoted $\gcd(n, m)$ and is called *the greatest common divisor* of n, m. We decide that $\gcd(0, 0) = 0$.

Notice that $\gcd(n, m) = \gcd(|n|, |m|)$. Furthermore, $\gcd(n, m) = \gcd(m, n)$ and $\gcd(n, 0) = \gcd(0, n) = |n|$.

There exists an alternative characterisation of the greatest common divisor. We will work our way towards this while looking at the coin exchange problem.

Example 4.1 Assume that there only exist coins of five and no other payment options. Which amount would then be possible to be exchanged between two people? Since a person only can give an integer amount of coins of five to another person, then the amount is on the form $5n$, where $n \in \mathbb{Z}$. The set of the amounts there can be exchanged is thus $5\mathbb{Z}$.

If we take an amount n that can be exchanged with coins of five (thus divisible by 5), then kn can also be exchanged for all $k \in \mathbb{Z}$. You will just need to pay with k times as many fives. It is also true that if $n \in 5\mathbb{Z}$ and $m \in 5\mathbb{Z}$, then it is also true that $n + m \in 5\mathbb{Z}$. It will be very useful that any set with these two properties is on the form $d\mathbb{Z}$ for a $d \in \mathbb{Z}$.

Theorem 4.5
Let $M \subseteq \mathbb{Z}$ be a set, which is not empty. If M has the following two properties:

- For all $n \in M$ and all $k \in \mathbb{Z}$ it is true that $kn \in M$; and

- for all $n \in M$ and $m \in M$ it is true that $n + m \in M$,

then there exists an unambiguous number $d \geq 0$ such that $M = d\mathbb{Z}$.

The first property in the theorem says that if you choose a number $n \in M$ then you stay within the set M, when you multiply n with any arbitrary integer k. The other property says that if you add to numbers within M then the sum is also within M.

Proof. First we show that d exists so $M = d\mathbb{Z}$. If $M = \{0\}$ we can choose $d = 0$. Otherwise M contains positive elements, because M needs to contain at least one $x \neq 0$, and the first property shows for M that $-1x = -x$ also needs to be within M. Therefore, there exists at least one positive element $d \in M$. Since $d \in M$ it is true that $kd \in M$ for all $k \in \mathbb{Z}$, according the the first property for M. This shows that $d\mathbb{Z} \subseteq M$.

Now we want to show that it is also true for $M \subseteq d\mathbb{Z}$. If it is not the case, there would be an integer $u \in M$, which is not divisible with d. We can write $u = dq + r$, where the remainder r fulfils $1 \leq r < d$. But since $r = u - dq$ and $-dq \in M$ according to property 1, then $r = u - dq$ will also be within M according to property 2. But this gives a contradiction, because $1 \leq r < d$ and d was the smallest positive element within M. Thus it must be true that $M \subseteq d\mathbb{Z}$, and we can conclude that $M = d\mathbb{Z}$.

We have proven that there always exists a $d > 0$ such that $M = d\mathbb{Z}$. We still need to prove that there only exists one such number. Assume that there exists another such number $d' > 0$. Then it is true that $d\mathbb{Z} = d'\mathbb{Z}$. Since $d \in d\mathbb{Z} = d'\mathbb{Z}$ it must be true that $d' \mid d$. In the same way, we can show that $d \mid d'$. And since both $d > 0$ and $d' > 0$ it must be true that $d = d'$. □

Exercise 4.4 Show that if $n \in 5\mathbb{Z}$ and $m \in 5\mathbb{Z}$ then it is true that $n + m \in 5\mathbb{Z}$.

Example 4.2 Assume that we only have two types of coins at our disposal. Coins, which have a value of 12 kroner and coins, which have a value of 18 kroner. By exchanging 12 kroner coins, we can pay an amount on the form $12n$ for all $n \in \mathbb{Z}$. By exchanging 18 kroner coins, we can pay amounts on the form $18m$ for all $m \in \mathbb{Z}$. Since we can use both 12 kroner coins and 18 kroner coins, we can pay amount on the form

$$12n + 18m, \quad n, m \in \mathbb{Z}.$$

Definition 4.6
For $a, b \in \mathbb{Z}$ we set

$$a\mathbb{Z} + b\mathbb{Z} = \{na + mb \mid n, m \in \mathbb{Z}\}.$$

Exercise 4.5 With this we can pay amounts in the set $M = 12\mathbb{Z} + 18\mathbb{Z}$, if we have 12 and 18 kroner coins at our disposal.

(a) Show that M fulfils the two requirements in the Theorem 4.5 and that it can be concluded that $12\mathbb{Z} + 18\mathbb{Z} = d\mathbb{Z}$ for a number $d \in \mathbb{Z}$.

You can interpret the result as the amounts, which can be payed if there only existed 12 and 18 kroner coins, which corresponds to the amounts you can pay, if there only exists a d kroner coin.

(b) Determine d.

Here is an alternative characterisation of the greatest common divisor.

Theorem 4.7
Let $a, b \in \mathbb{Z}$. Then there exists an unambiguous $d \in \mathbb{N}$ such that

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Actually, $d = \gcd(a, b)$.

Theorem 4.7 can be proven by using Theorem 4.5. This is done in exercise 4.15. The following result can be proven easily using Theorem 4.7. Therefore, it is called a corollary, which originates from the Latin word gift.

Corollary 4.8
Let $a, b \in \mathbb{Z}$. There exists $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$.

The next exercises is about using Theorem 4.7 to prove the corollary.

Exercise 4.6 Let $a, b \in \mathbb{Z}$ and set $d = \gcd(a, b)$.

- Explain why $d \in d\mathbb{Z}$.
- Explain why this means that $d \in a\mathbb{Z} + b\mathbb{Z}$.
- Explain why it can be concluded that there exists $s, t \in \mathbb{Z}$ such that $sa + tb = \gcd(a, b)$.

4.2 Euclid's algorithm

You may have calculated $\gcd(m, n)$ by finding the prime number factorisation of n and m and then multiplied the common divisors. It works well for small numbers, but it is difficult to do for larger numbers. Actually, there exists encryption systems, which rely on the difficulty of factorising large integers. Euclid's algorithm is an efficient algorithm for calculating $\gcd(a, b)$. Before we describe the general algorithm, we will show how it works in a specific case.

Example 4.3 Assume that there are two types of coins. A coin of the value 18 and a coin of the value 12. Notice that $18 - 12 = 6$, which means we can make a virtual coin of the value 6 by paying 18 kroner and getting 12 kroner back. So everything we can pay with 12 kroner

coins and 6 kroner coins, can also be paid with 18 and 12 kroner coins. On the other hand, if we have 12 and 6 kroner coins, we can also make a virtual 18 kroner coin. Namely by using a 12 kroner coin and a 6 kroner coin. We can formally write this as

$$18\mathbb{Z} + 12\mathbb{Z} = 12\mathbb{Z} + 6\mathbb{Z}.$$

If we have a 12 kroner coin and a 6 kroner coin, we can make a virtual 0 kroner coin by paying with a 12 kroner coin and getting two 6 kroner coins back. Therefore, everything which can be paid with 6 and 0 kroner coins can also be paid with 12 and 6 kroner coins. On the other hand, if we have 0 kroner coins and 6 kroner coins, we can virtually make a 12 kroner coin by using two 6 kroner coins. So everything which can be paid with 12 and 6 kroner coins, can also be paid with 6 and 0 kroner coins. In symbols

$$12\mathbb{Z} + 6\mathbb{Z} = 6\mathbb{Z} + 0\mathbb{Z}.$$

It is also clear that $6\mathbb{Z} + 0\mathbb{Z} = 6\mathbb{Z}$. Therefore, it is true that

$$18\mathbb{Z} + 12\mathbb{Z} = 6\mathbb{Z}.$$

It follows from Theorem 4.7 that $\gcd(18, 12) = 6$.

In the example, we saw that $18\mathbb{Z}+12\mathbb{Z} = 12\mathbb{Z}+6\mathbb{Z}$, because $6 = 18-12$. The following result generalises this.

Lemma 4.9
Let $a, b \in \mathbb{Z}$ be given and $q \in \mathbb{Z}$ be arbitrary. Set $c = a - qb$. Then it is true that

$$a\mathbb{Z} + b\mathbb{Z} = b\mathbb{Z} + c\mathbb{Z}.$$

Proof. We show that $a\mathbb{Z} + b\mathbb{Z} \subseteq b\mathbb{Z} + c\mathbb{Z}$ and $a\mathbb{Z} + b\mathbb{Z} \supseteq b\mathbb{Z} + c\mathbb{Z}$.

Let $x \in a\mathbb{Z}+b\mathbb{Z}$ be arbitrary. There exists a $r, s \in \mathbb{Z}$ such that $x = ra+sb$. Since $c = a - qb$ it is true that $a = c + qb$. Therefore, we have

$$x = r(c + qb) + sb = rc + rqb + sb = (rq + s)b + rc,$$

and it is also true that $x \in b\mathbb{Z} + c\mathbb{Z}$. It shows that $a\mathbb{Z} + b\mathbb{Z} \subseteq b\mathbb{Z} + c\mathbb{Z}$.

On the other hand, let $x \in b\mathbb{Z} + c\mathbb{Z}$ be arbitrary. We can then write $x = rb + sc$, for some integers $r, s \in \mathbb{Z}$. Since $c = a - qb$ it is true that

$$x = rb + s(a - qb) = rb + sa - sqb = sa + (r - sq)b.$$

Thus we have $x \in a\mathbb{Z} + b\mathbb{Z}$. We can conclude that $a\mathbb{Z} + b\mathbb{Z} \subseteq b\mathbb{Z} + c\mathbb{Z}$. □

Example 4.4 We can use the lemma to determine $\gcd(34, 8)$. It is true that $34\mathbb{Z} + 8\mathbb{Z} = 8\mathbb{Z} + c\mathbb{Z}$, when $c = 34 - 8q$ no matter what we choose q to be. We choose q such that c becomes positive and as small as possible. We can achieve this by choosing q to be an integer quotient by division of 34 with 8. We have $34 = 4 \cdot 8 + 2$, which means

that $q = 4$. With $q = 4$ we get $c = 34 - 4 \cdot 8 = 2$, thus the remainder by the division.

According to the lemma it is true that

$$34\mathbb{Z} + 8\mathbb{Z} = 8\mathbb{Z} + 2\mathbb{Z}.$$

Now we look at $8\mathbb{Z}+2\mathbb{Z}$ and use the lemma again. Since $8 = 4 \cdot 2 + 0$, we can choose $q = 4$ and then get $c = 0$. Therefore, the lemma shows that

$$8\mathbb{Z} + 2\mathbb{Z} = 2\mathbb{Z} + 0\mathbb{Z}.$$

Since $2\mathbb{Z} + 0\mathbb{Z} = 2\mathbb{Z}$, it is true that

$$34\mathbb{Z} + 8\mathbb{Z} = 2\mathbb{Z}.$$

According to Theorem 4.7 it is true that $\gcd(34, 8) = 2$.

Exercise 4.7 Explain why it is true that

$$384\mathbb{Z} + 18\mathbb{Z} = 18\mathbb{Z} + 6\mathbb{Z} = 6\mathbb{Z} + 0\mathbb{Z} = 6\mathbb{Z}.$$

Hereafter, compute $\gcd(384, 18)$.

Set $r_0 = 34$ and $r_1 = 8$. The example shows that if we set r_2 to the remainder of the division of r_0 by r_1, ergo $r_2 = 2$. We set r_3 to the remainder of the division of $r_1 = 8$ by $r_2 = 2$, ergo $r_3 = 0$. Then it is true that $r_0\mathbb{Z} + r_1\mathbb{Z} = r_k\mathbb{Z} + r_{k+1}\mathbb{Z}$ for $k = 0, 1, 2$. Since $r_3 = 0$, we can use this and Theorem 4.7 to conclude that $\gcd(r_0, r_1) = r_2$. We can generalise this, which gives us Euclid's algorithm.

Euclid's algorithm. The input to the algorithm is two integers a, b. We can assume that $a \geq b \geq 0$. The algorithm can calculate a row of numbers $r_0, r_1, \ldots, r_n$ and stops when $r_n = 0$. Firstly, we set $r_0 = a$ and $r_1 = b$. Hereafter, we set r_k to the remainder of the division of r_{k-2} with r_{k-1}, i.e. we calculate q_k and r_k such that

$$r_{k-2} = q_k r_{k-1} + r_k \ ,$$

and $0 \leq r_k < r_{k-1}$. We do this for $k = 2, 3, \ldots, n$ until $r_n = 0$. It is then true that $\gcd(a, b)$ is equal to the second to last calculated number r_{n-1}.

As an example, let us calculate $\gcd(384, 18)$.

k	r_k	q_k	explanation
0	384	-	r_0 is the first input
1	18	-	r_1 is the second input
2	6	21	since $384 = 21 \cdot 18 + 6$
3	0	3	since $18 = 3 \cdot 6 + 0$

We can read from the table that $\gcd(384, 18) = 6$.

There is a variant of Euclid's algorithm, which is very useful. It follows from Corollary 4.8 (Exercise 4.6) that there exists a $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. We can extend the algorithm such that it performs the necessary bookkeeping to determine the constants r and s.

Euclid's extended algorithm. The input to the algorithm is two integers a, b. We can assume that $a \geq b \geq 0$. The algorithm calculates a row of triples (r_0, s_0, t_0), (r_1, s_1, t_1), ..., (r_n, t_n, s_n) and stops when $r_n = 0$. Firstly, we set $(r_0, s_0, t_0) = (a, 1, 0)$ and $(r_1, s_1, t_1) = (b, 0, 1)$. Thereafter, we set

$$(r_k, s_k, t_k) = (r_{k-2}, s_{k-2}, t_{k-2}) - q_k(r_{k-1}, s_{k-1}, t_{k-1})$$

where q_k is the integer quotient by the division of r_{k-2} with r_{k-1}. We do this for $k = 2, 3, \ldots, n$ until $r_n = 0$. Notice that q_k normally is not saved, but it is very useful to name, when analysing the algorithm. It is then true that

$$\gcd(a, b) = r_{n-1} = s_{n-1}a + t_{n-1}b.$$

Let us again calculate $\gcd(384, 18)$, but this time with Euclid's extended algorithm.

k	r_k	q_k	s_k	t_k	explanation
0	384	-	1	0	
1	18	-	0	1	
2	6	21	1	-21	since $384 = 21 \cdot 18 + 6$
3	0	3	-3	64	since $18 = 3 \cdot 6 + 0$

We can read from the table that $\gcd(384, 18) = 6 = 1 \cdot 384 - 21 \cdot 18$.

Exercise 4.8 Euclid's algorithm is applied to 730 and 30, which gives the numbers $730, 30, 10, 0$. What can be concluded?

Here is the extended Euclidean algorithm as pseudo code:

$r_{-1} \leftarrow a,\ r_0 \leftarrow b,\ k \leftarrow ;$
$s_{-1} \leftarrow,\ s_0 \leftarrow;$
$t_{-1} \leftarrow,\ t_0 \leftarrow;$
repeat
  $r_k \leftarrow_{k-2} \mod r_{k-1};$
  $q_k = \lfloor r_{k-2}/r_{k-1} \rfloor;$
  $s_k \leftarrow_{k-2} -q_k s_{k-1};$
  $t_k \leftarrow_{k-2} -q_k t_{k-1};$
  $k \leftarrow +1;$
until $r_k = 0;$
return (s_{k-1}, t_{k-1})

4.3 Least common multiple

Let $a, b \in \mathbb{Z}$. The set $a\mathbb{Z}$ is a set of multiples of a, while the set $b\mathbb{Z}$ is a set of multiples of b. The intersection $a\mathbb{Z} \cap b\mathbb{Z}$ is the set of the common multiples of a and b. It is possible to see that the sets $a\mathbb{Z}$ and $b\mathbb{Z}$ fulfils the requirements in Theorem 4.5 and from this it follows that $a\mathbb{Z} \cap b\mathbb{Z}$ also fulfils the requirements. Theorem 4.5 has the following consequence.

Theorem 4.10
Let $a, b \in \mathbb{Z}$. There exists an unambiguous $m \geq 0$ such that

$$a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}.$$

Definition 4.11
The number m is given by Theorem 4.10 called *the least common multiple* of a, b and is denoted with $\operatorname{lcm}(a, b)$.

We can determine $\operatorname{lcm}(a, b)$ by the help of Euclid's algorithm, since the following is true.

Theorem 4.12
Let $a, b \in \mathbb{N}$. It is true that

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

4.4 More exercises

Exercise 4.9

(a) Find with the help of Euclid's algorithm the integers s and t such that $s \cdot 221 + t \cdot 357 = \gcd(221, 357)$.

(b) Can the fraction $221/357$ be reduced?

Exercise 4.10 Determine $\operatorname{lcm}(384, 18)$.

Exercise 4.11 Let u, v, and w be integers. Assume that $w \mid u \cdot v$ and that $\gcd(u, w) = 1$. The purpose of the exercise is to show that $w \mid v$.

(a) Use the assumption that $\gcd(u, w) = 1$ to show that there exists integers s and t such that

$$s \cdot u \cdot v + t \cdot w \cdot v = v.$$

(b) Show by the help of the above that $w \mid v$.

Exercise 4.12 The Fibonacci numbers are recursively defined by

$$F(n) := \begin{cases} 1 & \text{if } n = 0, \\ 1 & \text{if } n = 1, \\ F(n-1) + F(n-2) & \text{if } n \geq 2. \end{cases}$$

(a) Show by the help of induction that $\gcd(F(n-1), F(n)) = 1$ for $n \in \mathbb{N} - \{0\}$.

(b) Show that the calculation of $\gcd(F(n-1), F(n))$ for an arbitrary n is in the "worst case", i.e. for numbers in the same magnitude, Euclid's algorithm will take *the majority of* iterations (here it is meant the variant of Euclid's algorithm, which uses division.). (Tip: For Euclid's algorithm the worst case is that $q_i = 1$ for all the quotients. Express r_0 using r_1 and r_2, hereafter r_1 using r_2 and r_3 and so on.)

Exercise 4.13 Let $n, m \in \mathbb{Z}$. Euclid's extended algorithm will find the integers s and t such that $sn + tm = d = \gcd(n, m)$.

(a) For a given $k \in \mathbb{Z}$, Characterise when the equation $xn + ym = k$ has integer solutions (x, y), and use Euclid's extended algorithm to find a solution. This is called a linear Diophantine equation.

(b) Describe all solutions $(x, y) \in \mathbb{Z}^2$ to the equation $xn + ym = 0$.

(c) Describe all solutions $(x, y) \in \mathbb{Z}^2$ to the equation $xn + ym = k$.

(d) Find the "smallest" solution to the equation $x \cdot 21 + y \cdot 51 = 12$, where "smallest" means that $|x| + |y|$ needs to be minimised.

4.5 Extra-exercises (not part of the curriculum)

Exercise 4.14 In this exercise we want to prove **the fundamental theorem in arithmetic**, namely the unique prime number factorisation. Specifically: if $n \in \mathbb{N}$ then there is exactly one way to write

$$n = p_1 \cdot p_2 \cdot \ldots \cdot p_k \ ,$$

where $p_1, p_2, \ldots, p_k$ are the prime numbers such that $p_1 \leq p_2 \leq \ldots \leq p_k$.

Here are the steps we will take:

(a) Read and understand the proof for *the existence* of the prime number factorisation in Section 3.2.

(b) Use Exercise 4.11 to prove the following property of prime numbers: Let $a, b \in \mathbb{N}$ and let p be a prime number such that $p \mid ab$; then it is true that either $p \mid a$ or $p \mid b$.

(c) Prove the unique prime number factorisation. (Tip: Assume that it does not hold. Then there is a *smallest* number n which has two prime number factorisation. Write these and use the previous questions to show a contradiction.)

Exercise 4.15 In this exercise you need to construct a proof for Theorem 4.7. Let $a, b \in \mathbb{Z}$, and set $M = a\mathbb{Z} + b\mathbb{Z}$.

(a) Show that if $m \in M$ then it is true for all $k \in \mathbb{Z}$ that $km \in M$.

(b) Show that if $m_1 \in M$ and $m_2 \in M$ then it is true that $m_1 + m_2 \in M$.

(c) Use Theorem 4.5 to conclude $a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ for a $d \in \mathbb{N}$.

Hereby, the first half of the theorem is proved, and you just need to prove that $d = \gcd(a, b)$. Since $d \in d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$, there exists a $s, t \in \mathbb{Z}$ such that $d = sa + tb$. Set $c = \gcd(a, b)$

(d) Use that $d = sa + tb$ to show that $c \mid d$, and use this to show $c \leq d$.

(e) Show that d is a common divisor for a and b, thus that $d \mid a$ and $d \mid b$.

(f) Explain why it is true that $d = c$ so $d = \gcd(a, b)$.

Hereby, Theorem 4.7 is proven.

Exercise 4.16 The exercise shows why Euclid's extended algorithm finds the numbers s, t such that $\gcd(a, b) = sa + tb$. Let $a \geq b \geq 0$ be given and define the triples (r_k, s_k, t_k) like in Euclid's extended algorithm.

(a) Show that $r_0 = s_0 a + t_0 b$.

(b) Show that $r_1 = s_1 a + t_1 b$.

(c) Show that if $r_{k-2} = s_{k-2}a + t_{k-2}b$ and $r_{k-1} = s_{k-1}a + t_{k-1}b$, and we set

$$(r_k, s_k, t_k) = (r_{k-2} - qr_{k-1}, s_{k-2} - qs_{k-1}, t_{k-2} - qt_{k-1})$$

for an arbitrary $q \in \mathbb{Z}$, then it is true that

$$r_k = s_k a + t_k b.$$

(d) Explain why (a), (b), and (c) implies that

$$r_k = s_k a + t_k b$$

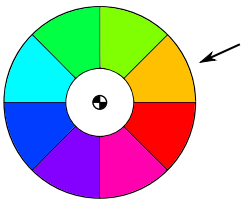
for all $k = 0, 1, 2, \ldots, n$.

Chapter 5

Modular arithmetic

This chapter is about the modulo operation. It plays an important and fundamental role in many contexts. To be able to make a statistical simulation it is important to be able to generate numbers, which look like random numbers. Such pseudo random numbers can be made with the help of the modulo operation. In cryptology it is more common to add and multiply modulo n than simply add and multiply normally. The modulo operation is therefore a basic skill.

5.1 Congruence



Imagine that we have a wheel with 8 fields and an arrow, which points to one field. See the figure to the right. If we spin the wheel, such that it spins past a fields, the arrow will point at a field A. If we instead spin the wheel, so it spins b fields, the arrow will point at a field B. If A and B is the same field, it is said that a and b is congruent modulo 8. It is written $a \equiv b \pmod 8$. For example, if we spin the wheel 7 fields clockwise or 1 fields counter clockwise, i.e., -1 field clockwise, then the arrow points at the red field in both cases. This means that $7 \equiv -1 \pmod 8$. A whole spin of the wheel corresponds to 8 fields and therefore it is true that $a \equiv b \pmod 8$, if and only if $a = b + 8k$ for a $k \in \mathbb{Z}$ or equivalently that 8 divides $b - a$.

We can generalise the expression to a wheel of n fields, where n is a positive integer. This generalisation is contained in the following definition.

Definition 5.1
Let n be a positive integer and $a, b \in \mathbb{Z}$. One says that a and b *is*

congruent modulo n, and it is written

$$a \equiv b \pmod{n},$$

if $n \mid (a-b)$. The statement $a \equiv b \pmod{n}$ is called a *congruence*, and n is in this context called *modulus*.

Exercise 5.1 Determine which of the following statements correspond to $a \equiv b \pmod{n}$.

- $a - b = qn$ for a $q \in \mathbb{Z}$,
- $a - b \in n\mathbb{Z}$,
- $n \mid (a-b)$,
- $(a-b) \mid n$.

Exercise 5.2 Determine which $x \in \{-2, 127, 219\}$ that satisfies

$$x \equiv 15 \pmod{17}.$$

The symbol $\equiv$ has a number of properties in common with the normal equality sign.

Lemma 5.2
Let a and b be integers and n be a positive natural number. Then it is true that

1. The integer a is congruent with itself: $a \equiv a \pmod{n}$.
2. If $a \equiv b \pmod{n}$, then it is true that $b \equiv a \pmod{n}$.
3. If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then it is true that $a \equiv c \pmod{n}$.

Proof.

1. Since $a - a = 0 = 0 \cdot n$, it is true that $a \equiv a \pmod{n}$ according to Definition 5.1.
2. If n divides $a - b$, then it will also divide $-(a-b) = b - a$. Therefore, if $a \equiv b \pmod{n}$, then it is true that $b \equiv a \pmod{n}$.
3. From the assumptions $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, it is seen that n divides $a - b$ and $b - c$. But then n will also divide their sum $(a-b)+(b-c)$, which is equal to $a-c$. Therefore it is true that $a \equiv c \pmod{n}$. □

We can visualise congruences with the help of a table. See Table 5.1.

A column in the table corresponds to all the numbers, which are congruent with each other modulo 7. Such sets of numbers are called *equivalence classes*. Some also use the term *congruence classes* or *residue classes*. When we calculate modulo 7, there are 7 different equivalence classes.

The formal definition of equivalence classes is as follows.

$0+7\mathbb{Z}$	$1+7\mathbb{Z}$	$2+7\mathbb{Z}$	$3+7\mathbb{Z}$	$4+7\mathbb{Z}$	$5+7\mathbb{Z}$	$6+7\mathbb{Z}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
-14	-13	-12	-11	-10	-9	-8
-7	-6	-5	-4	-3	-2	-1
0	1	2	3	4	5	6
7	8	9	10	12	13	14
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$

Table 5.1: If we write all the integers in a table with 7 columns as shown, then two numbers are congruent modulo 7 if and only if they are in the same column.

Definition 5.3
Let n be a positive integer and $k \in \mathbb{Z}$. The numbers, which are congruent to k, thus the set of solutions to

$$x \equiv k \pmod{n}$$

is called an equivalence class and it is denoted

$$k + n\mathbb{Z}.$$

We use the symbol $k + n\mathbb{Z}$ to denote the set

$$\{\ldots, k-2n, k-n, k, k+n, k+2n, \ldots\}.$$

Exercise 5.3 Is it true that $101 + 2\mathbb{Z} = 1 + 2\mathbb{Z}$? More generally, is it true that $k + n\mathbb{Z} = r + n\mathbb{Z}$, when r is the remainder of the division of k by n?

The following rules of arithmetic shows that we can manipulate with congruences in the same way that we can manipulate with equations.

Lemma 5.4
Let a, b, and c be integers and n be a positive natural number. Then it is true that

1. $a \equiv b \pmod{n}$ is equivalent to $a + c \equiv b + c \pmod{n}$,
2. if $a \equiv b \pmod{n}$ then it is true that $a \cdot c \equiv b \cdot c \pmod{n}$.

The lemma means that if we take two numbers a, a' from a column A in Table 5.1, and two numbers b, b' from a column B in the figure, then $a+b$ is in the same column as $a'+b'$. This suggests that we can determine a way to

add and multiply columns, thus enforce calculations on equivalence classes. This is a fruitful idea, though we will not expand on this here. Instead we will prove Lemma 5.4.

Proof.

1. It is enough to show that $a \equiv b \pmod{n} \Rightarrow a + c \equiv b + c \pmod{n}$, because using this rule, we can conclude that $a+c \equiv b+c \pmod{n} \Rightarrow a \equiv b \pmod{n}$, by adding $-c$ to both sides of the congruence relation. If n divides $a - b$, then it will also divide $(a + c) - (b + c)$, because $(a + c) - (b + c) = a - b$. Therefore if $a \equiv b \pmod{n}$, then it is also true that $a + c \equiv b + c \pmod{n}$.

2. If n divides $a-b$, then it will also divide $a \cdot c - b \cdot c$, because $a \cdot c - b \cdot c = (a-b) \cdot c$. Therefore if $a \equiv b \pmod{n}$, then it is also true that $a \cdot c \equiv b \cdot c \pmod{n}$. □

We can conclude with an example, which shows how the two lemmas can be used to calculate congruences in practise.

Example 5.1 Let us assume that we want to calculate $5a+b$ modulo 7, when we know that $a \equiv 5 \pmod{7}$ and $b \equiv 3 \pmod{7}$. We write

$$\begin{aligned} 5a + b &\equiv 5a + 3 \pmod{7} && \text{Using Lemma 5.4, 1.} \\ &\equiv 5 \cdot 5 + 3 \pmod{7} && \text{Using Lemma 5.4, 2.} \\ &\equiv 28 \pmod{7} \\ &\equiv 0 \pmod{7} && \text{as } 7 \mid 28 \end{aligned}$$

Using Lemma 5.2, 3. it is seen that

$$5a + b \equiv 0 \pmod{7}.$$

Exercise 5.4 Assume that $a \equiv 3 \pmod{7}$ and $b \equiv 4 \pmod{7}$. Work it out like the example and find a $k \in \{0, 1, \ldots, 6\}$ such that

$$5a + b \equiv k \pmod{7}.$$

Exercise 5.5 What is an equivalence class?

Exercise 5.6 Determine the modulus in the congruence $x \equiv 7 \pmod{5}$.

5.2 Congruence equations

In this section we will analyse the equations on the form

$$ax \equiv b \pmod{n}, \tag{5.1}$$

where $a, b \in \mathbb{Z}$ and $n > 0$ are the given integers and $x \in \mathbb{Z}$ is the variable, which we want to solve for. Such an equation is called a *congruence equation*. In the following we will see that we can determine precisely when a

congruence equation has a solution or not and find a method to determine the solutions.

Now, if only the congruence (5.1) had been an equation $ax = b$, and we did not require that the solution was an integer, then we would know exactly how to find the solutions. If $a \neq 0$, we would multiply by a^{-1} on both sides of the equality sign and see that $x = a^{-1}b$. What characterises the reciprocal a^{-1} is that $a^{-1}a = 1$. Now, we will determine a similar term for the modulo operation.

We start by looking at the very important case, where $b = 1$. Thus we look at the equation

$$ax \equiv 1 \pmod{n},$$

where $a \in \mathbb{Z}$ and $n > 0$ is given. A solution to this equation is called a multiplicative inverse of a modulo n.

Definition 5.5
Let $a \in \mathbb{Z}$ and n be a positive integer. An integer c, which fulfils

$$c \cdot a \equiv 1 \pmod{n},$$

is called *a multiplicative inverse of* $a \pmod{n}$, and is denoted a^{-1}, when modulus n appears from the context.

For example, it is true that a multiplicative inverse of 4 (mod 5) is 4, as $4 \cdot 4 = 16 = 1 + 3 \cdot 5 \equiv 1 \pmod{5}$. It is not always that there exists a multiplicative inverse modulo n. For example, look at the congruence equation

$$2 \cdot x \equiv 1 \pmod{4}.$$

If we wanted to solve this equation, there needs to exist a x such that $4 \mid (2x - 1)$. But since $2x - 1$ is odd, then it cannot be divided by 4.

We can generalise this counter example of the existence of the multiplicative inverse modulo n. Look at the general equation

$$ax \equiv 1 \pmod{n},$$

and set $d = \gcd(a, n)$. The congruence can be solved if there exists a x and q such that $ax - 1 = qn$ or equivalent $1 = ax - qn$. This means that there exists a solution if and only if $1 \in a\mathbb{Z} + n\mathbb{Z}$. Since $a\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, it corresponds to $d \mid 1$. The last thing can only be possible, when $d = 1$. In the example

$$2 \cdot x \equiv 1 \pmod{4},$$

we notice that $\gcd(2, 4) = 2$, which means there is not a multiplicative inverse like we also saw before.

When $\gcd(a, n) = 1$, we have seen that there exists a multiplicative inverse modulo n, but what is it? It follows from Corollary 4.8 that we can find s, t such that $sn + ta = 1$. If we set $c = t$ then it is true that

$$\begin{aligned} ac &\equiv ta \pmod{n} \\ &\equiv 1 - sn \pmod{n} \\ &\equiv 1 \pmod{n}. \end{aligned}$$

Namely, we have $a^{-1} \equiv t \pmod{n}$, when $sn + ta = 1$.

We summarise what we have learned so far.

Theorem 5.6
Let $a \in \mathbb{Z}$ and n be a positive integer. If $\gcd(n, a) \neq 1$, then a does not have a multiplicative inverse $\pmod{n}$. If $\gcd(n, a) = 1$, then there exists $s, t \in \mathbb{Z}$, such that $sn + ta = 1$, and t is a multiplicative inverse of $a \pmod{n}$, thus

$$t \cdot a \equiv 1 \pmod{n}.$$

The theorem shows not only when the multiplicative inverse exists, but also that it can be determined by the help of Euclid's extended algorithm.

Example 5.2 Let us see if we can find the multiplicative inverse of 5 $\pmod{27}$. We run Euclid's extended algorithm.

k	r_k	s_k	t_k	explanation
0	27	1	0	
1	5	0	1	
2	2	1	-5	since $27 = 5 \cdot 5 + 2$
3	1	-2	11	since $5 = 2 \cdot 2 + 1$
3	0	*	*	since $2 = 2 \cdot 1 + 0$

We see that $-2 \cdot 27 + 11 \cdot 5 = 1$. Therefore, 11 is a multiplicative inverse of 5 $\pmod{27}$. Control:

$$11 \cdot 5 = 55 = 54 + 1 = 2 \cdot 27 + 1 \equiv 1 \pmod{27}.$$

Example 5.3 If we use Euclid's algorithm on $27, 6$ we get the r_k's to $27, 6, 3, 0$, (we skip the intermediate results). This means that $\gcd(27, 6) = 3$, and 6 does not have any multiplicative inverse $\pmod{27}$.

Exercise 5.7 Find a number c such that $c \cdot 5 \equiv 1 \pmod{8}$.

Exercise 5.8 Let $a, b \in \mathbb{Z}$ be different from zero, $s, t \in \mathbb{Z}$, and assume that $sa + tb = 1$. Show that

$$sa \equiv 1 \pmod{b},$$

and

$$tb \equiv 1 \pmod{a}.$$

We turn our attention towards the general form of the congruence equation. (5.1).

Theorem 5.7
Consider the congruence equation

$$a \cdot x \equiv b \pmod{n},$$

where $a, b, n \in \mathbb{Z}$ and $n > 0$. Set $d = \gcd(n, a)$.

- If d does not divide b, then the congruence equation does not have any solutions.
- If d divides b, we can set $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, and $n' = \frac{n}{d}$, and it is true that the congruence equation is equivalent to

$$a' \cdot x \equiv b' \pmod{n'}.$$

Proof. First, assume that $\gcd(a, n)$ does not divide b and there anyways is a solution x. Then there exists an integer k such that $ax - b = nk$, which can be rewritten to $b = ax - nk$. Since $\gcd(a, n)$ divides both a and n, then $\gcd(a, n)$ also divides $ax - kn$, which is equal to b. This gives a contradiction, because we assumed that $\gcd(a, n)$ does not divide b.

Thereafter, assume that $d = \gcd(a, n)$ divides b. If x is a solution to $a \cdot x \equiv b \pmod{n}$, then there exists a $k \in \mathbb{Z}$, such that $ax - b = kn$. Since both a, b, and n is divisible by d, we get $a'x - b' = kn'$ when we divide by d. This equation is equivalent with $a'x \equiv b' \pmod{n'}$. On the other hand, if x is a solution to $a'x = b' \pmod{n'}$ it is true that $a'x - b' = kn'$ for a $k \in \mathbb{Z}$. If we multiply this equation by d, we get $ax - b = kn$, such that x is a solution to $ax \equiv b \pmod{n}$. □

Exercise 5.9 It is stated that $\gcd(22, 16) = 2$. Does the congruence $16x \equiv 5 \pmod{22}$ have any solutions? What about $16x \equiv 4 \pmod{22}$?

When we convert the congruence equation to $a'x \equiv b' \pmod{n'}$, we secure that a has a multiplicative inverse modulo n by dividing the congruence equation by $\gcd(a, n)$. This means that we now have that $\gcd(a', n') = 1$. This puts us in the position to solve the congruence equation, which the following theorem shows.

Theorem 5.8
Let $a, b \in \mathbb{Z}$ and n be a positive integer, and assume that $\gcd(n, a) = 1$. Then there exists $c \in \mathbb{Z}$ such that $ca \equiv 1 \pmod{n}$. The congruence equation

$$a \cdot x \equiv b \pmod{n}$$

is equivalent to

$$x \equiv cb \pmod{n}.$$

The set of solutions is

$$cb + n\mathbb{Z}.$$

Proof. We know from Theorem 5.6 that $c = a^{-1} \in \mathbb{Z}$ exists. If x solves $a \cdot x \equiv b \pmod{n}$ it is true that $ax - b = kn$ for a $k \in \mathbb{Z}$. We multiply by c on both sides of the equality sign, which gets us $x - a^{-1}b = (a^{-1}k)n$, which shows that $x \equiv cb \pmod{n}$. On the other side, if x is a solution to $x \equiv cb \pmod{n}$, it is true that $x - cb = kn$ for a $k \in \mathbb{Z}$. Now we multiply by a on both sides, leaving us with $ax - b = (ak)n$, which shows that $ax \equiv b \pmod{n}$. □

At this time, we know everything about solving the equation (5.1). Firstly, we can use Theorem 5.7 to either disproof that there are solutions, or make sure that $\gcd(a, n) = 1$. In the last case, we can use Theorem 5.8 to write all solutions. We will look at two examples.

Example 5.4 Let us solve

$$6x \equiv 3 \pmod{27}.$$

We can see that $\gcd(27, 6) = 3$. Since $3 \mid 3$, Theorem 5.8 shows us that the congruence equation is equivalent to the congruence equation

$$2x \equiv 1 \pmod{9}.$$

By running Euclid's algorithm or simply trying random numbers, we can see that $5 \cdot 2 \equiv 1 \mod 9$. A multiplicative inverse of 2 is 5. Therefore, the equation is equivalent with

$$x \equiv 5 \pmod{9},$$

of which we see the solution set is $5 + 9\mathbb{Z}$.

Example 5.5 The congruence equation

$$6x \equiv 4 \pmod{27},$$

has on the contrary no solutions. It is still true that $\gcd(27, 6) = 3$, but that 3 does not divide 4.

Exercise 5.10 It is true that $3 \cdot 2 \equiv 1 \pmod{5}$. What is the set of solutions to $3x \equiv 4 \pmod{5}$?

5.3 The Chinese remainder theorem

Now when we can solve a congruence equation, we can try to solve two or more simultaneously. In this section, we will look at a system of two congruence equations

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases}$$

which are equivalent to the congruence equation

$$x \equiv x_p \pmod{n_1 n_2}$$

for an appropriate value of x_p, when it is true that $\gcd(n_1, n_2) = 1$.

When $\gcd(n_1, n_2) > 1$, we can not be sure that there are solutions to the equations. But if we can find one solution, we can easily find them all.

Example 5.6 Look at the system of congruences

$$\begin{cases} x \equiv 2 \pmod 6, \\ x \equiv 2 \pmod 8. \end{cases}$$

It can quickly be seen that $x_p = 2$ solves both congruences. We now change variables by setting $x = x_p + y = 2 + y$. If we insert this into the equations, we get

$$\begin{cases} 2 + y \equiv 2 \pmod 6, \\ 2 + y \equiv 2 \pmod 8. \end{cases}$$

According to Lemma 5.4 it corresponds to

$$\begin{cases} y \equiv 0 \pmod 6, \\ y \equiv 0 \pmod 8. \end{cases}$$

The set of y, which solves both these congruences, is $6\mathbb{Z} \cap 8\mathbb{Z}$, which according to Theorem 4.10 is equal to $m\mathbb{Z}$, where $m = \operatorname{lcm}(6, 8) = 24$. Then the congruences are solved exactly when $y \in 24\mathbb{Z}$. Since $x = x_p + y = 2 + y$, the set of solutions to the two congruences, which we started with, is equal to $2 + 24\mathbb{Z}$. The single congruence $x \equiv 2 \pmod{24}$ has the same set of solutions. We can therefore conclude that the two congruences

$$\begin{cases} x \equiv 2 \pmod 6, \\ x \equiv 2 \pmod 8, \end{cases}$$

is equivalent to the one congruence

$$x \equiv 2 \pmod{24}.$$

The considerations in the example can be generalised and lead to the following theorem.

Theorem 5.9
Let n_1, n_2 be positive integers and $b_1, b_2 \in \mathbb{Z}$. If the system of congruence equations

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases}$$

has a solution x_p, then the two congruence equations are equivalent to

$$x \equiv x_p \pmod m,$$

where $m = \operatorname{lcm}(n_1, n_2)$. The set of solutions for both systems is

$$x_p + m\mathbb{Z}.$$

Exercise 5.11 Prove that 200 is a solution to the system of congruence equations

$$\begin{cases} x \equiv 20 \pmod{60}, \\ x \equiv 8 \pmod{32}. \end{cases}$$

Thereafter, specify the two integers x_p and m such that the system is equivalent with the one congruence equation

$$x \equiv x_p \pmod{m}.$$

As previous said, it is not always that

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2} \end{cases}$$

has a solution. Now we will see that when $\gcd(n_1, n_2) = 1$, then there is a solution.

We know from Corollary 4.8 that $\gcd(n_1, n_2) = 1$ means that there exists $u_1, u_2 \in \mathbb{Z}$ such that $u_1 n_1 + u_2 n_2 = 1$. We will now show that the number $x_p = u_1 n_1 b_2 + u_2 n_2 b_1$ is a solution to both the congruence equations. Since $u_1 n_1 \equiv 0 \pmod{n_1}$ and $u_1 n_1 + u_2 n_2 = 1$ it is true that $u_2 n_2 \equiv 1 \pmod{n_1}$. Therefore we have $u_2 n_2 b_1 \equiv b_1 \pmod{n_1}$. Since $u_1 n_1 b_2 \equiv 0 \pmod{n_1}$ is true, $x_p = u_1 n_1 b_2 + u_2 n_2 b_1$ solves the first congruence. In the same way, we can see that x_p is also a solution to the other congruence.

Now that we have found a solution, we can use Theorem 5.9. The theorem states that the system of congruences is equivalent to the one congruence equation,

$$x \equiv x_p \pmod{m},$$

where $m = \operatorname{lcm}(n_1, n_2)$. Since $\gcd(n_1, n_2) = 1$, we have $\operatorname{lcm}(n_1, n_2) = n_1 n_2$. Therefore the two congruence equations are equivalent to

$$x \equiv u_1 n_1 b_2 + u_2 n_2 b_1 \pmod{n_1 n_2}.$$

Hereby, we have proven the following Theorem.

The Chinese remainder theorem: Let b_1, b_2 be integers and n_1, n_2 be natural numbers such that $\gcd(n_1, n_2) = 1$. There exists $u_1, u_2 \in \mathbb{Z}$ such that $u_1 n_1 + u_2 n_2 = 1$. The system of congruence equations is given by

$$\begin{cases} x \equiv b_1 \pmod{n_1} \\ x \equiv b_2 \pmod{n_2}, \end{cases}$$

and has exactly the same solutions as the congruence equation

$$x \equiv u_1 n_1 b_2 + u_2 n_2 b_1 \pmod{n_1 n_2}.$$

Namely the set

$$(u_1 n_1 b_2 + u_2 n_2 b_1) + n_1 n_2 \mathbb{Z} \ .$$

This is a theorem, which have been known in China for more than 1700 years!

The Chinese remainder theorem allows us to solve systems of congruence equations of a more general form because we know from Theorem 5.7 and Theorem 5.8, how the more general congruence equation $ax \equiv b \pmod{n}$ can be reduced to the simpler form, where $a = 1$ if there is a solution. The result allows us to solve more than 2 congruence equations. For example, if there are 3, we can use the result two times and therefore end with a single congruence.

Example 5.7 We solve the system of congruences

$$\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 5 \pmod{19}, \end{cases}$$

By using Euclid's extended algorithm we can see that $\gcd(17, 19) = 1 = -8 \cdot 19 + 9 \cdot 17$. Therefore $x_p = -8 \cdot 19 \cdot 3 + 9 \cdot 17 \cdot 5 = 309$ is a solution. According to the Chinese remainder theorem, the two congruences are equivalent to the congruence

$$x \equiv 309 \pmod{17 \cdot 19}.$$

Since $17 \cdot 19 = 323$, we can conclude that the set of solutions is

$$309 + 323\mathbb{Z}.$$

Exercise 5.12 Find the set of solutions to the system of congruence equations given by

$$\begin{cases} x \equiv 7 \pmod{15} \\ x \equiv 14 \pmod{16}. \end{cases}$$

Exercise 5.13 Find the set of solutions to the system of congruence equations given by

$$\begin{cases} 4x \equiv 7 \pmod{15} \\ x \equiv 0 \pmod{4}. \end{cases}$$

Tip: First rewrite the first congruence equation into the form $x \equiv b \pmod{15}$.

Exercise 5.14 Let p be a prime number.

(a) Show that for every integer a between 1 and $p-1$ there exists an integer c between 1 and $p-1$ such that $ca \equiv 1 \pmod{p}$.

(b) Show the only solutions to the equation $x^2 \equiv 1 \pmod{p}$ between 1 and $p-1$ are the numbers 1 and $p-1$.
Tip: Factorise the polynomial $x^2 - 1$.

(c) Show Wilson's theorem: $(p-1)! \equiv -1 \pmod{p}$.
Tip: Which numbers between 1 and $p-1$ are its own multiplicative inverse modulo p?

Extra exercises – not part of the curriculum.

The next exercise is about proving Fermat's little theorem. This theorem is the theoretical foundation for a public key encryption system called RSA. To solve the exercise you can use, without proving, the result of Exercise 4.11: If $\gcd(w, u) = 1$ and $w \mid uv$ then it is true that $w \mid v$.

Exercise 5.15 Let p be a prime number and k be an integer between 1 and $p - 1$.

(a) Show $\gcd(p, k!) = 1$.
Tip: When p is a prime number then $\gcd(p, n)$ can be either 1 or p, and in the last case it is true that $p \mid n$.

(b) Show that $p \mid \binom{p}{k}$. Tip: Use that $k! \cdot \binom{p}{k} = p(p-1)\cdots(p-k+1) \equiv 0 \pmod{p}$.

The binomial formula says that for the integer $n \geq 0$ it is true that

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

(c) Use the binomial formula to show that $(a+b)^p \equiv a^p + b^p \pmod{p}$.

(d) Show Fermat's small equation: Let a be an integer. Then it is true that $a^p \equiv a \pmod{p}$. If it is assumed that $p \nmid a$, then it is true that $a^{p-1} \equiv 1 \pmod{p}$.
Tip: First show the result for $a \geq 0$ by the use of induction.

Chapter 6

Polynomials

One of the things that makes Euclid's algorithm so useful is that it is not only limited to natural numbers but it also works on polynomials. This is because polynomials and integers act algebraically alike. You can add and multiply both, and polynomials and integers fulfils the same fundamental operations. (They are both examples of the fields of integrity, and more precisely in Euclidean fields. You can learn all about this in the course 01018: Discrete Mathematics 2 - Algebra.)

6.1 Polynomials

We start by looking at what we mean by polynomials. First, we will look at how to add them, multiply them, and divide one polynomial by another. At last, we will look at how Euclid's algorithm can work on polynomials.

When we address polynomials in these notes, we will think about polynomials, which coefficients is either real or complex numbers. $P(x) = \frac{1}{2}x^2 + 2$ is an example of a polynomial.

Generally, a n'th degree polynomial $P(x)$ can be written as

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \tag{6.1}$$

where $a_n \neq 0$. This polynomial has degree n and we denote the degree of $P(x)$ with $\deg P(x)$. We call $a_n x^n$ for the highest degree term. The constant $P(x) = 0$ is also a polynomial, which we call the zero polynomial. We set the degree of the zero polynomial to -1, so $\deg(0) = -1$.

The constants a_n, a_{n-1}, ..., a_0 in (6.1) is called *the coefficients of the polynomial*. We call a_k the k'th degree coefficient of the polynomial for $k = 0, 1, \ldots, n$. There exists a practical notation for indicating the k'th degree coefficient, namely

$$[x^k]P(x).$$

If $P(x)$ is of degree n, then you set $[x^k]P(x) = 0$, when $k > n$.

Example 6.1 Look at the polynomial $P(x) = x^2 + 2x + 3$. Here the constant term is

$$[x^0]P(x) = 3,$$

the first degree coefficient is

$$[x^1]P(x) = 2,$$

and the second degree coefficient is

$$[x^2]P(x) = 1.$$

Since $P(x)$ is a second degree polynomial, it is true that

$$[x^3]P(x) = [x^4]P(x) = \ldots = 0.$$

Exercise 6.1 Determine

$$[x^k](x^3 + 2x + 2)$$

for $k = 0, 1, 2, 3, 4$.

We can add two polynomials. If we for example have $P(x) = x + 3$ and $Q(x) = 2x^2+2x+3$, then their sum is $P(x)+Q(x) = 2x^2+3x+6$. Generally, the sum of two polynomials $P(x)$ and $Q(x)$ is the polynomial $R(x)$, which is defined by

$$[x^k]R(x) = [x^k]P(x) + [x^k]Q(x).$$

Exercise 6.2 Determine $n(x) + m(x)$ when $n(x) = x^3 - x^2 + x - 1$ and $m(x) = x^3 + x^2 + x + 1$.

We can also multiply a polynomial by a constant. If $P(x) = x^2 + 2x + 3$ and c is a constant, then the product is $cP(x) = cx^2 + 2cx + 3c$. Thus the general form is

$$[x^k](cP(x)) = c[x^k].$$

Exercise 6.3 Determine $7n(x)$ when $n(x) = 7x + 7$.

We can also multiply two polynomials. If we for example have $P(x) = x + 3$ and $Q(x) = 2x^2 + 2x + 3$, which gives

$$\begin{aligned} P(x)Q(x) &= (x + 3)(2x^2 + 2x + 3) \\ &= x(2x^2 + 2x + 3) + 3(2x^2 + 2x + 3) \\ &= 2x^3 + 2x^2 + 3x + 6x^2 + 6x + 9 \\ &= 2x^3 + 8x^2 + 9x + 9. \end{aligned}$$

Let us try to look at the first degree term in the product above. You can get a first degree term by multiplying the constant term of $P(x)$ by the first degree term of $Q(x)$ and by multiplying the first degree term of $P(x)$ by the constant term of $Q(x)$. Therefore, it is true that

$$[x^1](P(x)Q(x)) = [x^0]P(x)[x^1]Q(x) + [x^1]P(x)[x^0]Q(x).$$

Generally, it is true that

$$[x^n](P(x)Q(x)) = \sum_{k=0}^{n} [x^k]P(x)[x^{n-k}]Q(x), \tag{6.2}$$

since you can get a $n'th$ degree term by multiplying a term of degree k by a term of degree $n-k$.

Exercise 6.4 Determine $P(x)Q(x)$, when $P(x) = x+3$ and $Q(x) = x^2-3$.

Exercise 6.5 Let k, n be integers where $0 \leq k \leq n$. Determine

$$[x^k](1+x)^n.$$

Tip: Use the binomial formula (Theorem 1.8 with $y = 1$).

Exercise 6.6 Let $a = \deg P(x)$ and $b = \deg Q(x)$. What is the degree of $P(x)$ times $Q(x)$, if none of the two polynomials are the zero polynomial?

A similarity between integers and polynomials is that we also have a division algorithm for polynomials. Let us for example divide $x^4+8x^3-2x^2+0x+16$ by $2x^2-4x+1$. Firstly, we write the division.

$$2x^2-4x+1 \overline{\big| x^4+8x^3-2x^2+0x+16}$$

The largest degree term of $2x^2-4x+1$ is $2x^2$, while the largest degree term of $x^4+8x^3-2x^2+0x+16$ is x^4. If we divide x^4 by $2x^2$, we get $\frac{1}{2}x^2$. We write this below.

$$2x^2-4x+1 \overline{\big| \begin{array}{r} \frac{1}{2}x^2 \\ \hline x^4+8x^3-2x^2+0x+16 \end{array}}$$

We multiply $2x^2-4x+1$ by $\frac{1}{2}x^2$ and subtract the result.

$$2x^2-4x+1 \overline{\big| \begin{array}{r} \frac{1}{2}x^2 \\ \hline x^4+8x^3\ -2x^2+0x+16 \\ -(x^4-2x^3+\frac{1}{2}x^2) \\ \hline 10x^3\ -\frac{5}{2}x^2+0x \end{array}}$$

Now $2x^2$ divides $10x^3$ exactly $5x$ times, which gives us the following.

$$2x^2-4x+1 \overline{\big| \begin{array}{r} \frac{1}{2}x^2+5x \\ \hline x^4+8x^3\ -2x^2+0x+16 \\ -(x^4-2x^3+\frac{1}{2}x^2) \\ \hline 10x^3\ -\frac{5}{2}x^2+0x \end{array}}$$

We multiply $2x^2 - 4x + 1$ by $5x$ and subtract the result.

$$\begin{array}{rl|l} & & \frac{1}{2}x^2 + 5x \\ \hline 2x^2 - 4x + 1 & x^4 + 8x^3 - 2x^2 + 0x + 16 & \\ & -(x^4 - 2x^3 + \frac{1}{2}x^2) & \\ \hline & 10x^3 - \frac{5}{2}x^2 + 0x & \\ & -(10x^3 - 20x^2 + 5x) & \\ \hline & \frac{35}{2}x^2 - 5x + 16 & \end{array}$$

If we divide $\frac{35}{2}x^2$ by $2x^2$, we get $\frac{35}{4}$. We write $\frac{35}{4}$ and subtract $\frac{35}{4}$ times $2x^2 - 4x + 1$.

$$\begin{array}{rl|ll} & & \frac{1}{2}x^2 + 5x + \frac{35}{4} & \leftarrow \text{quotient} \\ \hline 2x^2 - 4x + 1 & x^4 + 8x^3 - 2x^2 + 0x + 16 & & \\ & -(x^4 - 2x^3 + \frac{1}{2}x^2) & & \\ \hline & 10x^3 - \frac{5}{2}x^2 + 0x & & \\ & -(10x^3 - 20x^2 + 5x) & & \\ \hline & \frac{35}{2}x^2 - 5x + 16 & & \\ & -(\frac{35}{2}x^2 - 35x + \frac{35}{4}) & & \\ \hline & 30x + \frac{29}{4} & & \leftarrow \text{remainder} \end{array}$$

The term $2x^2$ has a larger degree than $30x$ and thus we are done. This was a bit hard, but it should be evident that division of polynomials can be calculated in almost the same way as divisions of integers.

You can see that $x^4 + 8x^3 - 2x^2 + 0x + 16$ divided by $2x^2 - 4x + 1$ is $\frac{1}{2}x^2 + 5x + \frac{35}{4}$ with the remainder $30x + \frac{29}{4}$. We can express this with the formula

$$x^4 + 8x^3 - 2x^2 + 16 = (2x^2 - 4x + 1) \cdot (\frac{1}{2}x^2 + 5x + \frac{35}{4}) + 30x + \frac{29}{4}.$$

The division algorithm shows the following result.

Theorem 6.1
Let $n(x), m(x)$ be two given polynomials, where $m(x)$ is not the zero polynomial. There exists two unambiguous polynomials $q(x), r(x)$, which fulfils

$$n(x) = q(x)m(x) + r(x), \text{ and } \deg(r(x)) < \deg(m(x)).$$

The polynomials $q(x)$ and $r(x)$ is called respectively *the quotient* and *the remainder* by the division of $n(x)$ by $m(x)$.

Exercise 6.7 Determine the quotient $q(x)$ and the remainder $r(x)$ by the division of $n(x) = x^2 - x - 2$ by $m(x) = x - 1$.

Exercise 6.8 Determine the quotient $q(x)$ and the remainder $r(x)$ by the division of $n(x) = x^2 - x - 2$ by $m(x) = x + 1$.

When the remainder is zero, we say that $m(x)$ is a divisor in $n(x)$.

Definition 6.2
We say that $m(x)$ is a divisor in $n(x)$ if there exists a polynomial $q(x)$ such that

$$n(x) = q(x)m(x).$$

If $m(x)$ is a divisor in $n(x)$, we say that $m(x)$ divides $n(x)$.

Exercise 6.9 Show that $x + 1$ and $x - 2$ are divisors in $n(x) = x^2 - x - 2$.

Exercise 6.10 Use the definition of the divisor to show that if $m(x) = x - x_0$ is a divisor in $n(x)$, then x_0 is a root in $n(x)$, which means that $n(x_0) = 0$. Hereafter, use Theorem 6.1 to show that it on the other hand is true that if $n(x)$ has the root x_0, then $m(x) = x - x_0$ is a divisor in $n(x)$.

Similarly to integers we can speak about a *greatest common divisor* for two polynomials $n(x)$ and $m(x)$, where a divisor $d_1(x)$ is greater than another $d_2(x)$ if the degree $\deg d_1(x)$ is greater than the degree $\deg d_2(x)$. It is intentionally that we say that *one* greatest divisor and not *the* greatest divisor, because divisors are only determined up to multiplication by a constant different from zero: If $d(x)$ is a divisor of $n(x)$ and $k \neq 0$ is a constant then $kd(x)$ is also a divisor in $n(x)$.

A greatest common divisor can be found by Euclid's algorithm, which is the same as Euclid's algorithm for integers, expect that the operations is done on polynomials.

Euclid's extended algorithm. Input to the algorithm is two polynomials $N(x), M(x)$, where $\deg(N(x)) \geq \deg(M(x))$. The algorithm calculates rows of triples $(r_0(x), s_0(x), t_0(x))$, $(r_1(x), s_1(x), t_1(x))$, $\ldots$, $(r_n(x), t_n(x), s_n(x))$ and stops when $r_n(x) = 0$. Firstly, we set

$$(r_0(x), s_0(x), t_0(x)) = (N(x), 1, 0)$$

and

$$(r_1(x), s_1(x), t_1(x)) = (M(x), 0, 1).$$

Thereafter, we set

$$(r_k(x), s_k(x), t_k(x)) = (r_{k-2}(x), s_{k-2}(x), t_{k-2}(x)) - q_k(x)(r_{k-1}(x), s_{k-1}(x), t_{k-1}(x))$$

where $q_k(x)$ is the quotient of the polynomial division of $r_{k-2}(x)$ by $r_{k-1}(x)$. We do this for $k = 2, 3, \ldots, n$ until $r_n(x) = 0$. Then it is true that

$$\gcd(N(x), M(x)) = r_{n-1}(x) = s_{n-1}(x)N(x) + t_{n-1}(x)M(x).$$

Example 6.2 Let us for example determine a greatest common divisor of $N(x) = x^4 + x^3 - 2x^2 + 2x - 2$, and $M(x) = x^2 + 2x - 3$. By the help of polynomial division, it can be calculated that

$$N(x) = (x^2 - x + 3)M(x) - 7x + 7, \tag{6.3}$$

and thereafter it can be calculated that

$$x^2 + 2x - 3 = -\frac{x+3}{7} \cdot (-7x + 7). \tag{6.4}$$

Thus we get

k	$r_k(x)$	$s_k(x)$	$t_k(x)$	explanation
0	$x^4 + x^3 - 2x^2 + 2x - 2$	1	0	
1	$x^2 + 2x - 3$	0	1	
2	$-7x + 7$	1	$-x^2 + x - 3$	according to (6.3)
3	0	*	*	according to (6.4)

Here we have written "*" for the elements, which calculations we have skipped.

We can read from the table that a greatest common divisor is $-7x + 7$ and that it is true that

$$-7x + 7 = 1 \cdot (x^4 + x^3 - 2x^2 + 2x - 2) + (-x^2 + x - 3) \cdot (x^2 + 2x - 3).$$

So Euclid's extended algorithm works.

Theorem 6.3
Euclid's extended algorithm is stopped in a final amount of steps. It is true that

$$r_k(x) = s_k(x)N(x) + t_k(x)M(x), \text{ for } k = 0, 1, \ldots, n,$$

and that we have

$$\gcd(N(x), M(x)) = r_{n-1}(x).$$

Exercise 6.11 Perform Euclid's extended algorithm on the polynomials $x^3 + x + 1$ and $x^2 + x + 1$, and find the polynomials $s(x)$ and $t(x)$ such that $s(x) \cdot (x^3 + x + 1) + t(x) \cdot (x^2 + x + 1) = 3$.

The algorithm calculates not only $\gcd(N(x), M(x))$ but also the two polynomials $s(x)$ and $t(x)$ such that $\gcd(N(x), M(x)) = s(x)N(x) + t(x)M(x)$. That such two polynomials exist has different important consequences. Here we can be satisfied by showing the following.

Theorem 6.4
The two polynomials $N(x)$ and $M(x)$ have a common root x_0 if and

only if $\gcd(N(x), M(x))$ has the root x_0.

Proof. Let $P(x)$ denote a greatest common divisor of $N(x), M(x)$. If x_0 is a root of both $N(x)$ and $M(x)$ then it is true that

$$P(x_0) = s(x_0)N(x_0) + t(x_0)M(x_0) = 0 \cdot s(x_0) + 0 \cdot t(x_0) = 0.$$

This means that x_0 is also a root of $P(x)$.

Now assume the opposite that $P(x_0) = 0$. Since $P(x) \mid N(x)$, a polynomial $Q(x)$ can be found such that $N(x) = Q(x)P(x)$. Therefore, we have

$$N(x_0) = Q(x_0) \cdot 0 = 0.$$

In the same way, x_0 is a root of $M(x_0)$. □

From example 6.2 we know that

$$\gcd(x^4 + x^3 - 2x^2 + 2x - 2, x^2 + 2x - 3) = -7x + 7.$$

The polynomial $-7x + 7$ has the root 1 and no other roots. It follows from Theorem 6.4 that $x^4 + x^3 - 2x^2 + 2x - 2$ and $x^2 + 2x - 3$ have the common root 1 and no other common roots. Often the degree of the greatest common divisor is less than that of the two original polynomials. Finding the roots of a polynomial is "easier" the lower the degree is.

Exercise 6.12 If $\gcd(N(x), M(x)) = 1$, does $N(x)$ and $M(x)$ have any common roots?

Exercise 6.13 Let $N(x) = x^5 + x^4 + x + 1$ and $M(x) = x^4 - 1$. Use Euclid's algorithm to determine if $N(x)$ and $M(x)$ have common roots.
Tip: It is not necessary to use Euclid's extended algorithm.

A polynomial $N(x)$ is said to have a *double root* x_0 if $(x - x_0)^2$ divides $N(x)$. It can be shown that $N(x)$ has a double root x_0 if and only if x_0 is a root both in $N(x)$ and the derivative $N'(x)$.

Exercise 6.14 (a) Determine if there exists values of the constant k, such that the polynomial $N(x) = x^2 + 2x + k$ has a double root in $\mathbb{R}$.

(b) Determine if there exists values of the constant k, such that the polynomial $M(x) = x^3 + x + k$ has a double root in $\mathbb{R}$.

Exercise 6.15 Let $f(x)$ be an arbitrary polynomial with coefficients in $\mathbb{R}$. Let then $g_n(x), n \in \mathbb{Z}$ be the following family of polynomials:

$$g_n(x) = f(x) + n \ .$$

(a) Prove that for an arbitrary $n \in \mathbb{Z} - \{0\}$, then $f(x)$ and $g_n(x)$ have no common roots.

(b) (Not in the curriculum): Prove that $\gcd(g_n(x), g_m(x)) = 1$ if $n \neq m$.

Exercise 6.16 Let $p(x) = \sum_{k=0}^{n} c_k x^k$ be a polynomial if the coefficients $c_0, \ldots, c_n$ are all integers where $c_0 \neq 0$ as well as $c_n \neq 0$. Let $\mathbb{Q}$ denominate the set of rational number, meaning fractions with integers in the numerator and the denominator. Then the following theorem is true:

> If $\frac{a}{b} \in \mathbb{Q}$ with $\gcd(a, b) = 1$, and if $p(\frac{a}{b}) = 0$, then it is true that $a \mid c_0$ and $b \mid c_n$.

(a) Show by the help of the above that the polynomial $p(x) = x^2 - 2$ does not have any rational roots.

(b) Conclude that $\sqrt{2} \notin \mathbb{Q}$.

(c) Conclude in a similar fashion that $\sqrt{5} \notin \mathbb{Q}$.

(d) Is it possible that $\sqrt{5} - \sqrt{2} \in \mathbb{Q}$? We actually do not know that yet. Show that $\sqrt{5} - \sqrt{2}$ is a root of the polynomial $q(x) = x^4 - 14x^2 + 9$. Show that $\sqrt{5} - \sqrt{2} \notin \mathbb{Q}$.

(e) (Extra, not in the curriculum) Prove the theorem in the beginning of the exercise. (Tip: Consider $p(\frac{a}{b}) = 0$ and multiply by the common denominator, such that all terms are integers. Thereafter use modulus arithmetic.)

Extra exercises – not in the curriculum.

Exercise 6.17 We will examine the execution time of Euclid's algorithm.

(a) Prove as a function of $\deg f(x)$ and $\deg g(x)$, how many iteration Euclid's algorithm uses at most, when it is executed on $f(x)$ and $g(x)$.

(b) Let $D(n)$ be an upper limit for the number of arithmetic operations it takes to execute a division of $f(x)$ by $g(x)$ with a remainder if $\deg f, \deg g \leq n$. By arithmetic operations we mean $+,-,\cdot$ or $/$ of elements from the field, thus $\mathbb{R}$ or $\mathbb{C}$. Argue that $D(n) \leq 2n^2$.

(c) Argue that Euclid's algorithm at most uses $2n^2(n+1)$ operations if $\deg f, \deg g \leq n$.

(d) But if we count more thoroughly, we see that it actually uses way less operations! Let $D(n,m)$ be an upper limit for the number of arithmetic operations it takes to execute the division of $f(x)$ by $g(x)$ with a remainder if $\deg f = n$ and $\deg g = m \leq n$. Argue that $D(n,m) \leq 2(n-m+1)(m+1)$.
Use this to show that Euclid's algorithm uses less than $4(n+1)^2$ operations with the input $f(x), g(x)$ with $\deg f, \deg g \leq n$. (Tip: Let $d_k = \deg r_k$ during Euclid's algorithm and express the number of operations as a sum over $2d_{k-1}(d_k - d_{k-1} + 1)$. Replace the first d_{k-1} with the upper limit d_0 and look at the total sum. Is there something which can be reduced?)

A "rational function" is a fraction with a polynomial in the numerator and denominator, for example $\frac{p(x)}{q(x)}$.

Exercise 6.18 As usual with fractions, they can be reduced such that given $\frac{p(x)}{q(x)}$ if you by chance know that there exists a $t(x)$ such that $p(x) = t(x)p_1(x)$ and $q(x) = t(x)q_1(x)$, then we have:

$$\frac{p(x)}{q(x)} = \frac{t(x)p_1(x)}{t(x)q_1(x)} = \frac{p_1(x)}{q_1(x)} \ .$$

If you are just given a rational function $\frac{p(x)}{q(x)}$, describe a course of action to calculate the completely reduced fraction.

The following exercise shows how a rational function sometimes can be written as a sum of the so called unit fractions. It can be useful when needing to find the primitive functions.

Exercise 6.19 Let $p(x)$ and $d(x)$ be polynomials both different from zero. Assume that $d(x) = d_1(x)d_2(x)$, where $\gcd(d_1(x), d_2(x)) = 1$, and assume that $\deg p(x) < \deg d(x)$. Show that there exists polynomials $p_1(x)$ and $p_2(x)$ such that

$$\deg p_1(x) < \deg d_1(x) \text{ and } \deg p_2(x) < \deg d_2(x),$$

and

$$\frac{p(x)}{d(x)} = \frac{p_1(x)}{d_1(x)} + \frac{p_2(x)}{d_2(x)}.$$

Tip: First multiply the wanted equation by $d(x)$.