

*Concepts in Abstract Mathematics*

Jean-Baptiste Campesato

<b>0</b>	<b>Logic and sets</b>	<b>1</b>
0.1	Sets . . . . .	1
0.2	Cartesian product . . . . .	2
0.3	Basic logic . . . . .	2
0.4	Quantifiers . . . . .	5
0.5	Functions . . . . .	6
0.6	Sigma notation . . . . .	7
<b>1</b>	<b>Natural numbers</b>	<b>8</b>
1.1	Peano axioms . . . . .	8
1.2	Addition, multiplication and order . . . . .	10
1.2.1	Addition . . . . .	10
1.2.2	Multiplication . . . . .	11
1.2.3	Order . . . . .	12
1.2.4	Summary . . . . .	14
1.3	Proof by induction . . . . .	15
1.3.1	Formal statement . . . . .	15
1.3.2	In practice . . . . .	15
1.3.3	Variants of the induction . . . . .	16
	Exercises . . . . .	18
<b>2</b>	<b>Integers</b>	<b>20</b>
2.1	Construction of the integers . . . . .	20
2.1.1	Definition . . . . .	20
2.1.2	Operations . . . . .	21
2.1.3	Order . . . . .	21
2.2	Absolute value . . . . .	23
2.3	Euclidean division . . . . .	23
2.4	Divisibility . . . . .	24
2.5	Greatest common divisor . . . . .	25
2.6	Euclid's algorithm . . . . .	27
2.7	Coprime integers . . . . .	28
2.8	A diophantine equation . . . . .	28
2.A	Properties of the strict order . . . . .	30
2.B	Implementation of Euclid's algorithm in Julia . . . . .	30
	Exercises . . . . .	31
<b>3</b>	<b>Prime numbers</b>	<b>34</b>
3.1	Prime numbers . . . . .	34
3.2	The fundamental theorem of arithmetic . . . . .	35
	Exercises . . . . .	37
<b>4</b>	<b>Modular arithmetic</b>	<b>39</b>
4.1	Congruences . . . . .	39
4.2	Applications: divisibility criteria . . . . .	41
4.3	Fermat's little theorem . . . . .	42
4.4	Wilson's theorem . . . . .	43
4.5	Chinese remainder theorem . . . . .	43
4.6	Euler's theorem . . . . .	44

4.A	Positional numeral system with base $b$	46
4.B	The Chinese Remainder Theorem for more than two equations	48
	Exercises	49
<b>5</b>	<b>The RSA algorithm</b>	<b>51</b>
5.1	Introduction	51
5.2	Generation of the keys	52
5.3	How to encrypt a message	52
5.4	How to decrypt a message	52
5.5	An example	53
5.6	In practice	53
5.A	A simple implementation in Julia	55
	Exercises	56
<b>6</b>	<b>The rationals and the reals</b>	<b>57</b>
6.1	Equivalence classes	57
6.2	Rational numbers	59
6.3	Infima and suprema	61
6.4	Real numbers	62
6.5	Decimal representation of real numbers	66
6.6	$\sqrt{2}$ is irrational	69
6.7	$e$ is irrational	72
	Exercises	73
<b>7</b>	<b>Cardinality</b>	<b>76</b>
7.1	Reviews about functions	77
7.2	Finite sets	78
7.3	Generalization to infinite sets	82
7.4	Countable sets	85
7.5	Cantor's diagonal argument	87
7.A	What is a set?	88
7.B	<i>Un morceau de choix</i>	91
7.C	Cheatsheet: recollection of some results about cardinality	92
	Exercises	94
<b>8</b>	<b>Sample solutions to the exercises</b>	<b>97</b>
8.1	Chapter 1	97
8.2	Chapter 2	104
8.3	Chapter 3	111
8.4	Chapter 4	116
8.5	Chapter 5	120
8.6	Chapter 6	122
8.7	Chapter 7	129
<b>9</b>	<b>Assessments (with solutions)</b>	<b>137</b>
	Problem Set 1	138
	Problem Set 2	142
	Problem Set 3	145
	Problem Set 4	148
	Problem Set 5	152
	Final exam	155

# Chapter 0

## Logic and sets

### 0.1 Sets

As in many areas of mathematics, we will use *sets* very often during this course. But we won't cover anything about axiomatic set theory. Instead we will only use a naive informal intuitive definition of what is a set and what is a function/map between two sets (you are already used to that from your linear algebra and calculus courses).

**Definition 0.1** (Informal). A *set* is a (well-defined) "collection" of elements (order doesn't matter). Two sets are equal if they contain the same elements, so  $\{1, 2, 2, 3\} = \{1, 2, 3\}$  since they contain 1, 2, 3.

**Remark 0.2.** We usually define a set either by giving explicitly the elements it contains, e.g.

$$S = \{\text{apple}, \pi, 5\}$$

or from an already constructed set by taking only the elements satisfying some property

$$S = \{n \in \mathbb{Z} : \exists k \in \mathbb{Z}, n = 2k\}$$

**Notation 0.3.** Given a set  $S$ , we write  $a \in S$  to express that  $a$  is an element of  $S$ . It is read " $a$  is in  $S$ " or " $a$  is an element of  $S$ ".

**Example 0.4.**

- $\text{apple} \in \{\text{apple}, \pi, 5\}$
- $\text{banana} \notin \{\text{apple}, \pi, 5\}$

**Notation 0.5.** Given two sets  $S$  and  $T$ , we write  $S \subset T$  to express that every element of  $S$  is an element of  $T$ , i.e.

$$\forall a \in S, a \in T$$

It is read " $S$  is a subset of  $T$ " or " $S$  is included in  $T$ ".

**Remark 0.6.** Two sets  $S$  and  $T$  are equal if and only if they have the same elements, i.e.

$$S = T \Leftrightarrow (S \subset T \text{ and } T \subset S)$$

**Remark 0.7.** There exists a unique set containing no element, it is denoted by  $\emptyset$  and called the *empty set*.

**Remark 0.8.** Given a set  $E$ , the set of subsets of  $E$  is well-defined, it is denoted by  $\mathcal{P}(E) := \{S : S \subset E\}$  and called the *powerset* of  $E$ .

## 0.2 Cartesian product

**Definition 0.9.** An  $n$ -tuple is an ordered list of  $n$  elements  $(x_1, \dots, x_n)$ . We say *couple* for a 2-tuple and *triple* for a 3-tuple.

**Fundamental property 0.10.**  $(x_1, \dots, x_n) = (y_1, \dots, y_n) \Leftrightarrow x_1 = y_1, x_2 = y_2, \dots, x_n = y_n$

**Remark 0.11.**

- $\{1, 2, 3\} = \{3, 2, 1\}$  (sets)
- $(1, 2, 3) \neq (3, 2, 1)$  (tuples)

**Remark 0.12.**

- $\{1, 2, 2, 3\} = \{1, 2, 3\}$  (sets)
- $(1, 2, 2, 3) \neq (1, 2, 3)$  (tuples)

**Theorem 0.13.** Given two sets  $A$  and  $B$ , the following set is well-defined

$$A \times B := \{(a, b) : a \in A, b \in B\}$$

It is called the cartesian product of  $A$  and  $B$ .

**Example 0.14.** Set  $A = \{\pi, e\}$  and  $B = \{1, \sqrt{2}, \pi\}$  then

$$A \times B = \{(\pi, 1), (\pi, \sqrt{2}), (\pi, \pi), (e, 1), (e, \sqrt{2}), (e, \pi)\}$$

**Theorem 0.15.** Given sets  $A_1, A_2, \dots, A_n$ , the following set is well-defined

$$A_1 \times A_2 \times \dots \times A_n := \{(a_1, a_2, \dots, a_n) : a_i \in A_i\}$$

**Remark 0.16.** We will often identify the following sets although they are not formally equal:

- $(A \times B) \times C \ni ((a, b), c)$
- $A \times (B \times C) \ni (a, (b, c))$
- $A \times B \times C \ni (a, b, c)$

## 0.3 Basic logic

**Definition 0.17.** A *statement* is a *sentence* which is either “true” ( $T$ ) or “false” ( $F$ ).

**Definition 0.18.** The *negation* of a statement  $P$  is the statement denoted by  $\neg P$  (or *no*  $P$ ) defined with the following truth table:

$P$	$\neg P$
$V$	$F$
$F$	$V$

**Definition 0.19.** The *disjunction* of two statements  $P$  and  $Q$  is the statement denoted by  $P \vee Q$  (or  $P$  or  $Q$ ) defined with the following truth table:

$P$	$Q$	$P \vee Q$
$V$	$V$	$V$
$V$	$F$	$V$
$F$	$V$	$V$
$F$	$F$	$F$

Beware: the disjunction is not exclusive.

**Definition 0.20.** The *conjunction* of two statements  $P$  and  $Q$  is the statement denoted by  $P \wedge Q$  (or  $P$  and  $Q$ ) defined with the following truth table:

$P$	$Q$	$P \wedge Q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$F$
$F$	$F$	$F$

**Definition 0.21.** Given two statements  $P$  and  $Q$ , we define the statement  $P \Rightarrow Q$  with the following truth table:

$P$	$Q$	$P \Rightarrow Q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$V$
$F$	$F$	$V$

It is called the *implication* (or *conditional statement*) and it is read as follows " $P$  implies  $Q$ " or "if  $P$  (is true) then  $Q$  (is true)".

**Definition 0.22.** The *converse* of  $P \Rightarrow Q$  is defined as  $Q \Rightarrow P$ .

**Definition 0.23.** Given two statements  $P$  and  $Q$ , we define the statement  $P \Leftrightarrow Q$  with the following truth table:

$P$	$Q$	$P \Leftrightarrow Q$
$V$	$V$	$V$
$V$	$F$	$F$
$F$	$V$	$F$
$F$	$F$	$V$

It is called the *equivalence* and it is read " $P$  is equivalent to  $Q$ " or " $P$  (is true) if and only if  $Q$  (is true)".

**Definition 0.24.** A *tautology* is a statement which is true whatever are the truth values of its components, we usually use the notation  $\models P$ .

**Definition 0.25.** We say that  $P$  and  $Q$  are *logically equivalent* when  $P \Leftrightarrow Q$  is a tautology. It simply means that  $P$  and  $Q$  have the same truth table.

**Remark 0.26.** The above logical connectives could have been defined in terms of the disjunction and the negation. Indeed:

- $P \wedge Q$  is equivalent to  $\neg((\neg P) \vee (\neg Q))$ .

$P$	$Q$	$\neg P$	$\neg Q$	$(\neg P) \vee (\neg Q)$	$\neg((\neg P) \vee (\neg Q))$	$P \wedge Q$
$V$	$V$	$F$	$F$	$F$	$V$	$V$
$V$	$F$	$F$	$V$	$V$	$F$	$F$
$F$	$V$	$V$	$F$	$V$	$F$	$F$
$F$	$F$	$V$	$V$	$V$	$F$	$F$

- $P \Rightarrow Q$  is equivalent to  $(\neg P) \vee Q$ .

$P$	$Q$	$\neg P$	$(\neg P) \vee Q$	$P \Rightarrow Q$
$V$	$V$	$F$	$V$	$V$
$V$	$F$	$F$	$F$	$F$
$F$	$V$	$V$	$V$	$V$
$F$	$F$	$V$	$V$	$V$

- $P \Leftrightarrow Q$  is equivalent to  $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$  or to  $(P \wedge Q) \vee ((\neg P) \wedge (\neg Q))$ .

**Example 0.27.** *Law of excluded middle:*  $\models P \vee (\neg P)$

$P$	$\neg P$	$P \vee (\neg P)$
$V$	$F$	$V$
$F$	$V$	$V$

The law of excluded middle simply means that either  $P$  is true, or its negation  $\neg P$  is true.

**Example 0.28.** The *modus ponens*:  $\models (P \wedge (P \Rightarrow Q)) \Rightarrow Q$

$P$	$Q$	$P \Rightarrow Q$	$P \wedge (P \Rightarrow Q)$	$(P \wedge (P \Rightarrow Q)) \Rightarrow Q$
$V$	$V$	$V$	$V$	$V$
$V$	$F$	$F$	$F$	$V$
$F$	$V$	$V$	$F$	$V$
$F$	$F$	$V$	$F$	$V$

It is the main inference rule in mathematics: if both  $P$  and  $P \Rightarrow Q$  are true then so is  $Q$ .

**Example 0.29.**  $\models (P \wedge Q) \Rightarrow P$

**Example 0.30.**  $\models P \Rightarrow (P \vee Q)$

**Proposition 0.31.** *The disjunction is commutative:*  $\models (P \vee Q) \Leftrightarrow (Q \vee P)$

**Proposition 0.32.** *The disjunction is associative:*  $\models ((P \vee Q) \vee R) \Leftrightarrow (P \vee (Q \vee R))$ .

**Proposition 0.33.** *The conjunction is commutative:*  $\models (P \wedge Q) \Leftrightarrow (Q \wedge P)$

**Proposition 0.34.** *The conjunction is associative :*  $\models ((P \wedge Q) \wedge R) \Leftrightarrow (P \wedge (Q \wedge R))$ .

**Proposition 0.35** (Double negation elimination).  $\models (\neg(\neg P)) \Leftrightarrow P$

*Proof.*

$P$	$\neg P$	$\neg(\neg P)$
$V$	$F$	$V$
$F$	$V$	$F$

■

**Proposition 0.36** (Morgan's laws).

- The negation of  $P \vee Q$  is  $(\neg P) \wedge (\neg Q)$ :

$$\models (\neg(P \vee Q)) \Leftrightarrow ((\neg P) \wedge (\neg Q))$$

- the negation of  $P \wedge Q$  is  $(\neg P) \vee (\neg Q)$ :

$$\models (\neg(P \wedge Q)) \Leftrightarrow ((\neg P) \vee (\neg Q))$$

*Mnemonic device: the negation changes conjunctions in disjunctions and vice-versa.*

*Proof.* I only prove the first one.

$P$	$Q$	$\neg P$	$\neg Q$	$(\neg P) \wedge (\neg Q)$	$P \vee Q$	$\neg(P \vee Q)$
$V$	$V$	$F$	$F$	$F$	$V$	$F$
$V$	$F$	$F$	$V$	$F$	$V$	$F$
$F$	$V$	$V$	$F$	$F$	$V$	$F$
$F$	$F$	$V$	$V$	$V$	$F$	$V$

■

**Proposition 0.37** (Distributivity).

- $\models (P \wedge (Q \vee R)) \Leftrightarrow ((P \wedge Q) \vee (P \wedge R))$
- $\models (P \vee (Q \wedge R)) \Leftrightarrow ((P \vee Q) \wedge (P \vee R))$

**Proposition 0.38** (Proof by contrapositive).

The statement  $P \Rightarrow Q$  is logically equivalent to its contrapositive  $(\neg Q) \Rightarrow (\neg P)$ .

*Proof.*

$P$	$Q$	$P \Rightarrow Q$	$\neg P$	$\neg Q$	$(\neg Q) \Rightarrow (\neg P)$
$V$	$V$	$V$	$F$	$F$	$V$
$V$	$F$	$F$	$F$	$V$	$F$
$F$	$V$	$V$	$V$	$F$	$V$
$F$	$F$	$V$	$V$	$V$	$V$

■

In some cases, it may be easier to prove  $(\neg Q) \Rightarrow (\neg P)$  rather than  $P \Rightarrow Q$ .

**Example 0.39.** Let  $n \in \mathbb{Z}$ . Prove that if  $n^2$  is odd then  $n$  is odd.

**Proposition 0.40** (Reductio ad absurdum).  $((\neg P) \Rightarrow Q) \wedge ((\neg P) \Rightarrow (\neg Q)) \Rightarrow P$  is a tautology.

In practice, in order to prove  $P$  by contradiction, we assume that  $\neg P$  is true and we look for a contradiction.

## 0.4 Quantifiers

**Definition 0.41.** A predicate  $P(x, y, \dots)$  is a statement whose truth value depends on variables  $x, y, \dots$  occurring in it.

**Definition 0.42** (Universal quantifier). The statement " $\forall x \in E, P(x)$ " means that  $P(x)$  is true for any  $x$  in  $E$ .

It is read "for all  $x$  in  $E$ ,  $P(x)$  is true".

**Definition 0.43** (Existential quantifier). The statement " $\exists x \in E, P(x)$ " means that there exists at least one  $x$  in  $E$  such that  $P(x)$  is true.

It is read "there exists  $x$  in  $E$  such that  $P(x)$  is true".

Here  $x$  is a bound variable:

- we may replace " $\forall x \in E, P(x)$ " by " $\forall y \in E, P(y)$ "
- we may replace " $\exists x \in E, P(x)$ " by " $\exists y \in E, P(y)$ ".

**Definition 0.44.** The statement " $\exists! x \in E, P(x)$ " means that  $P(x)$  is true for exactly one element  $x$  in  $E$ .

It is read "there exists a unique  $x$  in  $E$  such that  $P(x)$  is true".

As we see in the following example, we can't permute the quantifiers  $\forall$  and  $\exists$ .

- $\exists n \in \mathbb{N}, \forall p \in \mathbb{N}, p \leq n$
- $\forall p \in \mathbb{N}, \exists n \in \mathbb{N}, p \leq n$

Nonetheless, we may permute two existential quantifiers or two universal quantifiers.

**Remark 0.45.** It is common to write " $\forall x, y \in E$ " for " $\forall x \in E, \forall y \in E$ " (that's an ellipsis). The same holds for the existential quantifier  $\exists$ .

**Definition 0.46.** The negation of " $\forall x \in E, P(x)$ " is " $\exists x \in E, \neg P(x)$ ".

**Definition 0.47.** The negation of " $\exists x \in E, P(x)$ " is " $\forall x \in E, \neg P(x)$ ".

*Mnemonic device: the negation swaps  $\forall$  and  $\exists$ .*

**Axiom 0.48.** The statement " $\exists x \in \emptyset, P(x)$ " is false for any predicate.

**Proposition 0.49.** The statement " $\forall x \in \emptyset, P(x)$ " is true for any predicate.

*Proof.* Indeed,  $\exists x \in \emptyset, (\neg P(x))$  is false, so its negation  $\forall x \in \emptyset, P(x)$  is true.

■

## 0.5 Functions

**Definition 0.50** (informal). A *function* (or *map*) is the data of two sets  $A$  and  $B$  together with a "process" which assigns to each  $x \in A$  a unique  $f(x) \in B$ :

$$f : \begin{cases} A & \rightarrow & B \\ x & \mapsto & f(x) \end{cases}$$

Here,  $f$  is the name of the function,  $A$  is the *domain* of  $f$ , and  $B$  is the *codomain* of  $f$ .

**Remark 0.51.** The domain and codomain are part of the definition of a function. For instance

$$f : \begin{cases} \mathbb{R} & \rightarrow & [1, +\infty) \\ x & \mapsto & x^2 + 1 \end{cases} \quad \text{and} \quad g : \begin{cases} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & x^2 + 1 \end{cases}$$

are not the same function (the first one is surjective but not the second one).

A function is not simply a "formula", you need to specify the domain and the codomain.

**Definitions 0.52.** Given a function  $f : A \rightarrow B$ .

- The *image* of  $E \subset A$  by  $f$  is  $f(E) := \{f(x) : x \in E\} \subset B$ .
- The *image* of  $f$  (or *range* of  $f$ ) is  $\text{Range}(f) := f(A)$ .
- The *preimage* of  $F \subset B$  by  $f$  is  $f^{-1}(F) := \{x \in A : f(x) \in F\}$ .
- The *graph* of  $f$  is the set  $\Gamma_f := \{(x, y) \in A \times B : y = f(x)\}$ .
- We say that  $f$  is *injective* (or *one-to-one*) if  $\forall x_1, x_2 \in A, x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$  or equivalently by taking the contrapositive  $\forall x_1, x_2 \in A, f(x_1) = f(x_2) \implies x_1 = x_2$
- We say that  $f$  is *surjective* (or *onto*) if  $\forall y \in B, \exists x \in A, y = f(x)$
- We say that  $f$  is *bijective* if it is injective and surjective, i.e.  $\forall y \in B, \exists! x \in A, y = f(x)$

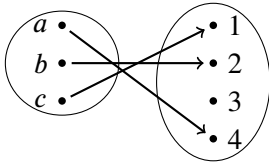


Figure 1: Injective

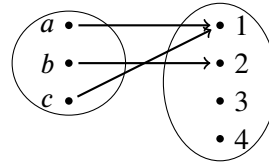


Figure 2: Not injective

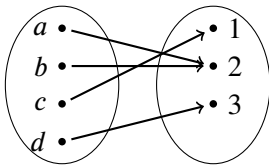


Figure 3: Surjective

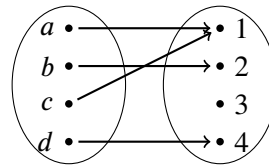


Figure 4: Not surjective

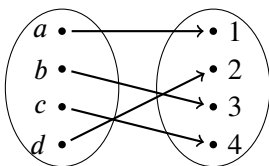


Figure 5: Bijective



**Proposition 0.53.**  $f : A \rightarrow B$  is bijective if and only if there exists  $g : B \rightarrow A$  such that  $\begin{cases} \forall x \in A, g(f(x)) = x \\ \forall y \in B, f(g(y)) = y \end{cases}$ .  
Then  $g$  is unique, it is called the inverse of  $f$  and denoted by  $f^{-1} : B \rightarrow A$ .

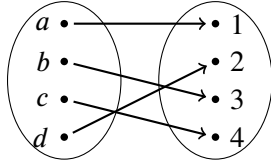


Figure 6: Bijective function

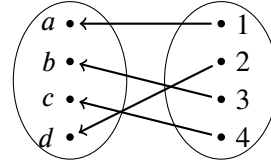


Figure 7: Its inverse

## 0.6 Sigma notation

**Definition 0.54.** For  $m, n \in \mathbb{Z}$ , we set

$$\sum_{i=m}^n a_i = a_m + a_{m+1} + \cdots + a_n$$

**Remark 0.55.** If  $m > n$  then  $\sum_{i=m}^n a_i = 0$  by convention.

**Example 0.56.**  $\sum_{i=3}^7 i^2 = 3^2 + 4^2 + 5^2 + 6^2 + 7^2 = 135$

**Remark 0.57.** If  $m \leq n$  then there are  $n - m + 1$  terms in the sum  $\sum_{i=m}^n a_i$ .

# Chapter 1

## Natural numbers

In this chapter we introduce the set  $\mathbb{N}$  of natural numbers. We will start with a minimal axiomatic description of it from which we will derive the main properties of  $\mathbb{N}$ .

Intuitively, we describe  $\mathbb{N}$  starting from 0 and repeatedly doing the operation  $+1$  (we say that we take the successor): 1 is the successor of 0, 2 is the successor of 1, 3 is the successor of 2 and so on... This operation is governed by a few rules in order to make sure that the set we obtain coincides with our intuitive expectation about what should be  $\mathbb{N}$ .

The method of *proof by induction* is closely related to the nature of  $\mathbb{N}$ . Hence we will study it at the end of this chapter.

I use the convention that  $\mathbb{N}$  is the set of non-negative integers, i.e.  $0 \in \mathbb{N}$ .

### 1.1 Peano axioms

All the results concerning the natural numbers will derive from the next theorem, that we admit, and which states the existence of  $\mathbb{N}$ .

**Theorem 1.1** (Peano axioms). *There exists a set  $\mathbb{N}$  together with an element  $0 \in \mathbb{N}$  read as zero and a function  $s : \mathbb{N} \rightarrow \mathbb{N}$  read as successor such that:*

(i) *0 is not the successor of any element of  $\mathbb{N}$ , i.e. 0 is not in the image of  $s$ :*

$$0 \notin s(\mathbb{N})$$

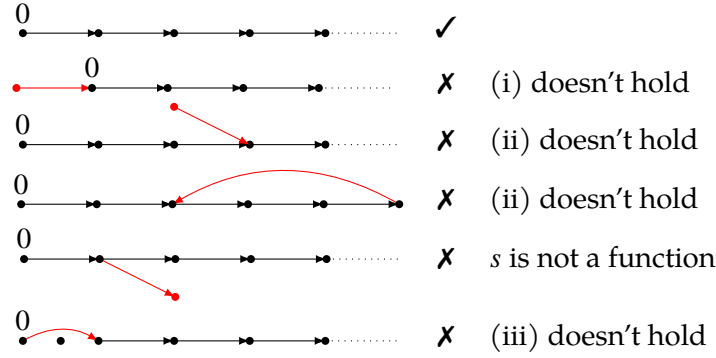
(ii) *If the successor of  $n$  equals the successor of  $m$  then  $n = m$ , i.e.  $s$  is injective:*

$$\forall n, m \in \mathbb{N}, s(n) = s(m) \implies n = m$$

(iii) *The induction principle. If a subset of  $\mathbb{N}$  contains 0 and is closed under  $s$  then it is  $\mathbb{N}$ :*

$$\forall A \subset \mathbb{N}, \left\{ \begin{array}{l} 0 \in A \\ s(A) \subset A \end{array} \right\} \implies A = \mathbb{N}$$

The set  $\mathbb{N}$  is the set of *natural numbers*. As we will see, all the results of  $\mathbb{N}$  will derive from the above basic properties. The last axiom basically means that all the elements of  $\mathbb{N}$  can be obtained from 0 by taking the successor iteratively. Intuitively, the successor of  $n$  is  $s(n) = n + 1$  (actually, it will become formal after we define the addition, see Remark 1.6).



Below are some basic propositions relying only on Peano axioms.

**Proposition 1.2.** Any non-zero natural number is the successor of a natural number, i.e.

$$\forall n \in \mathbb{N} \setminus \{0\}, \exists m \in \mathbb{N}, n = s(m)$$

*Proof.* Set  $A = s(\mathbb{N}) \cup \{0\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$
- $s(A) \subset s(\mathbb{N}) \subset A$

Hence, by the induction principle,  $A = \mathbb{N}$ .

Let  $n \in \mathbb{N} \setminus \{0\}$ , then  $n \in A$  but  $n \neq 0$ , therefore  $n \in s(\mathbb{N})$ . So there exists  $m \in \mathbb{N}$  such that  $n = s(m)$ . ■

**Proposition 1.3.** A natural number is never its own successor, i.e.

$$\forall n \in \mathbb{N}, n \neq s(n)$$

*Proof.* Set  $A = \{n \in \mathbb{N} : n \neq s(n)\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$  since  $0 \notin s(\mathbb{N})$  (particularly  $0 \neq s(0)$ )
- $s(A) \subset A$

Indeed, let  $m \in s(A)$ . Then  $m = s(n)$  for some  $n \in A$ . So  $s(n) \neq n$ .

Since  $s$  is injective, we get that  $s(s(n)) \neq s(n)$ , i.e.  $s(m) \neq m$ .

Hence  $m \in A$ .

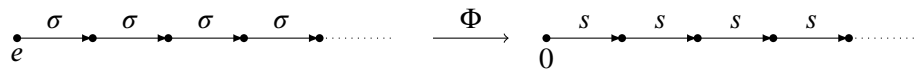
So, by the induction principle,  $A = \mathbb{N}$ . Thus, for every  $n \in \mathbb{N}$  we have that  $n \neq s(n)$ . ■

**Remark 1.4** (You can skip it). Up to a bijection,  $\mathbb{N}$  is uniquely defined by the Peano axioms.

More precisely, if there exists a set  $S$ , with an element  $e \in S$  and a function  $\sigma : S \rightarrow S$  such that

- (i)  $e \notin \sigma(S)$
- (ii)  $\forall x, y \in S, \sigma(x) = \sigma(y) \implies x = y$
- (iii)  $\forall A \subset S, \begin{cases} e \in A \\ \sigma(A) \subset A \end{cases} \implies A = S$

then there exists a bijection  $\Phi : S \rightarrow \mathbb{N}$  such that  $\Phi(e) = 0, s(\Phi(x)) = \Phi(\sigma(x))$ .



## 1.2 Addition, multiplication and order

### 1.2.1 Addition

The following proposition defines inductively the function *addition with  $a$* .

**Proposition 1.5.** *Let  $a \in \mathbb{N}$ . Then there exists a unique function  $(a + \bullet) : \mathbb{N} \rightarrow \mathbb{N}$  such that*

$$\begin{aligned} (i) \quad & a + 0 = a \\ (ii) \quad & \forall b \in \mathbb{N}, a + s(b) = s(a + b) \end{aligned}$$

*Proof.* This function is well defined by the induction principle (i.e. we didn't miss any element of the domain  $\mathbb{N}$  using this iterative definition).

Let's check that it is unique. Let  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  be such that  $\varphi(0) = a$  and  $\forall b \in \mathbb{N}, \varphi(s(b)) = s(\varphi(b))$ .

Set  $A = \{b \in \mathbb{N} : \varphi(b) = a + b\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$  since  $\varphi(0) = a = a + 0$ .
- $s(A) \subset A$ . Indeed, let  $c \in s(A)$ . Then  $c = s(b)$  for some  $b \in A$  and

$$\begin{aligned} \varphi(c) &= \varphi(s(b)) \quad \text{since } c = s(b) \\ &= s(\varphi(b)) \quad \text{by definition of } \varphi \\ &= s(a + b) \quad \text{since } b \in A \\ &= a + s(b) \quad \text{by definition of } a + \bullet \\ &= a + c \quad \text{since } s(b) = c \end{aligned}$$

Hence  $c \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . Thus, for every  $b \in \mathbb{N}$  we have that  $\varphi(b) = a + b$ . ■

**Remark 1.6.** We set  $1 := s(0)$ . Then, for  $n \in \mathbb{N}$ ,  $n + 1 = n + s(0) = s(n + 0) = s(n)$ . As expected...

Hence, from now on, I will use indistinctively  $n + 1$  or  $s(n)$  (depending on which notation seems to be the more convenient). Similarly, we set  $2 := s(1)$ ,  $3 := s(2)$ ,  $4 := s(3)$  and so on...

### Proposition 1.7.

1.  $\forall a, b, c \in \mathbb{N}, a + (b + c) = (a + b) + c$  (the addition is associative)
2.  $\forall a, b \in \mathbb{N}, a + b = b + a$  (the addition is commutative)
3.  $\forall a, b, c \in \mathbb{N}, a + b = a + c \implies b = c$  (cancellation)
4.  $\forall a, b \in \mathbb{N}, a + b = 0 \implies a = b = 0$

*Proof.*

1. Let  $a, b \in \mathbb{N}$ . Set  $A = \{c \in \mathbb{N} : a + (b + c) = (a + b) + c\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$ . Indeed,  $a + (b + 0) = a + b = (a + b) + 0$ .
- $s(A) \subset A$ . Indeed, let  $n \in s(A)$  then  $n = s(c)$  for some  $c \in A$ . Therefore

$$\begin{aligned} a + (b + n) &= a + (b + s(c)) \quad \text{since } n = s(c) \\ &= a + s(b + c) \\ &= s(a + (b + c)) \\ &= s((a + b) + c) \quad \text{since } c \in A \\ &= (a + b) + s(c) \\ &= (a + b) + n \end{aligned}$$

Hence  $n \in A$ .

Thus, by the induction principle,  $A = \mathbb{N}$  and for any  $c \in \mathbb{N}$ ,  $a + (b + c) = (a + b) + c$ .

## 2. Sketch of proof:

- (a) Prove that
- $\forall a \in \mathbb{N}, 0 + a = a + 0$
- using the induction principle.

*Hint:*  $0 + s(a) = s(0 + a) = s(a + 0) = s(a) = s(a) + 0$ 

- (b) Prove that
- $\forall a \in \mathbb{N}, s(a) = 1 + a$
- using the induction principle.

*Hint:*  $s(s(a)) = s(1 + a) = (1 + a) + 1 = 1 + (a + 1) = 1 + s(a)$ .

- (c) Let
- $a \in \mathbb{N}$
- . Prove that
- $\forall b \in \mathbb{N}, a + b = b + a$
- .

*Hint:*  $a + s(b) = s(a + b) = s(b + a) = b + s(a) = b + (1 + a) = (b + 1) + a = s(b) + a$ 3. Set  $A = \{a \in \mathbb{N} : \forall b, c \in \mathbb{N}, a + b = a + c \implies b = c\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$
- $s(A) \subset A$

Indeed, let  $n \in s(A)$ . Let  $b, c \in \mathbb{N}$  such that  $n + b = n + c$ . We want to prove that  $b = c$ .  
There exists  $a \in A$  such that  $n = s(a)$ . Then

$$\begin{aligned}
 n + b &= n + c \\
 \Rightarrow s(a) + b &= s(a) + c \\
 \Rightarrow b + s(a) &= c + s(a) \quad \text{by commutativity} \\
 \Rightarrow s(b + a) &= s(c + a) \quad \text{by construction of the addition} \\
 \Rightarrow b + a &= c + a \quad \text{since } s \text{ is injective} \\
 \Rightarrow a + b &= a + c \quad \text{by commutativity} \\
 \Rightarrow b &= c \quad \text{since } a \in A
 \end{aligned}$$

Hence  $n \in A$ .Thus, by the induction principle,  $A = \mathbb{N}$ .

4. Let
- $a, b \in \mathbb{N}$
- be such that
- $a + b = 0$
- . Assume by contradiction that
- $a \neq 0$
- or
- $b \neq 0$
- .

Without loss of generality, we may assume that  $b \neq 0$  (using commutativity).Then, by Proposition 1.2,  $b = s(n)$  for some  $n \in \mathbb{N}$ . So  $0 = a + b = a + s(n) = s(a + n)$ .Which is a contradiction since  $0 \notin s(\mathbb{N})$ . ■

## 1.2.2 Multiplication

The following proposition defines inductively the function *multiplication with a*.**Proposition 1.8.** Let  $a \in \mathbb{N}$ . Then there exists a unique function  $(a \times \bullet) : \mathbb{N} \rightarrow \mathbb{N}$  such that

(i)  $a \times 0 = 0$

(ii)  $\forall b \in \mathbb{N}, a \times s(b) = (a \times b) + a$

**Proposition 1.9.**

1.  $\forall a, b, c \in \mathbb{N}, a \times (b \times c) = (a \times b) \times c$  (the multiplication is associative)
2.  $\forall a, b \in \mathbb{N}, a \times b = b \times a$  (the multiplication is commutative)
3.  $\forall a, b, c \in \mathbb{N}, a \times (b + c) = a \times b + a \times c$  and  $(a + b) \times c = a \times c + b \times c$  ( $\times$  is distributive over  $+$ )
4.  $\forall a \in \mathbb{N}, a \times 1 = a$
5.  $\forall a, b \in \mathbb{N}, a \times b = 0 \implies (a = 0 \text{ or } b = 0)$
6.  $\forall a, b, c \in \mathbb{N}, \begin{cases} a \times b = a \times c \\ a \neq 0 \end{cases} \implies b = c$  (cancellation)

We prove these properties similarly to the ones of the addition.

**Remark 1.10.** It is common to omit the symbol  $\times$  when there is no possible confusion (i.e. to simply write  $ab$  for  $a \times b$ ).

### 1.2.3 Order

The following definition is a little bit informal, but it is enough for our purpose.

**Definition 1.11.** A **binary relation**  $\mathcal{R}$  on a set  $E$  consists in associating a truth value to every couple  $(x, y) \in E^2$  (beware, order matters here).

We say that  $x$  is *related to*  $y$  by  $\mathcal{R}$ , denoted  $x\mathcal{R}y$ , if the value *true* is assigned to  $(x, y)$ .

**Examples 1.12.**

1. Let  $E = \{a, b, c\}$ . Since  $E$  is finite, we can define a binary relation  $\mathcal{R}$  using a truth table as below:

$x \backslash y$	$a$	$b$	$c$
$a$	✓	✗	✗
$b$	✗	✗	✓
$c$	✓	✓	✗

Here  $a\mathcal{R}a$ ,  $a\mathcal{R}c$ ,  $b\mathcal{R}c$  and  $c\mathcal{R}b$ .

2. For  $E = \mathbb{R}$ , we can define a binary relation as follows:

$$x\mathcal{R}y \Leftrightarrow x^2 - y^2 = x - y$$

The following definition highlights the important properties of the order  $\leq$  that you intuitively know.

**Definition 1.13.** We say that a binary relation  $\mathcal{R}$  on a set  $E$  is an *order* if

- (i)  $\forall x \in E, x\mathcal{R}x$  (*reflexivity*)
- (ii)  $\forall x, y \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}x) \Rightarrow x = y$  (*antisymmetry*)
- (iii)  $\forall x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}z) \Rightarrow x\mathcal{R}z$  (*transitivity*)

**Definition 1.14.** We say that an order  $\mathcal{R}$  on a set  $E$  is *total* if

$$\forall x, y \in E, x\mathcal{R}y \text{ or } y\mathcal{R}x$$

**Definition 1.15.** We define the binary relation  $\leq$  on  $\mathbb{N}$  by

$$\forall a, b \in \mathbb{N}, (a \leq b \Leftrightarrow \exists k \in \mathbb{N}, b = a + k)$$

We read " $a$  is less than or equal to  $b$ " or " $b$  is greater than or equal to  $a$ " when  $a \leq b$  holds.

**Proposition 1.16.** The set of natural numbers  $\mathbb{N}$  is totally ordered for  $\leq$ .

*Proof.*

- (i) Reflexivity: let  $a \in \mathbb{N}$ , then  $a = a + 0$  with  $0 \in \mathbb{N}$ , hence  $a \leq a$ .
- (ii) Antisymmetry: let  $a, b \in \mathbb{N}$  be such that  $a \leq b$  and  $b \leq a$ .  
Then there exists  $k \in \mathbb{N}$  such that  $b = a + k$  and there exists  $l \in \mathbb{N}$  such that  $a = b + l$ .  
Therefore  $a = b + l = a + k + l$ . Hence  $0 = k + l$  and thus  $l = k = 0$  so that  $a = b$ .
- (iii) Transitivity: let  $a, b, c \in \mathbb{N}$  be such that  $a \leq b$  and  $b \leq c$ .  
Then there exists  $k \in \mathbb{N}$  such that  $b = a + k$  and there exists  $l \in \mathbb{N}$  such that  $c = b + l$ .  
Therefore  $c = b + l = a + (k + l)$  with  $k + l \in \mathbb{N}$ , i.e.  $a \leq c$ .
- (iv)  $\leq$  is total: let  $a \in \mathbb{N}$ . Set  $A = \{b \in \mathbb{N} : a \leq b \text{ or } b \leq a\}$ . Then
  - $A \subset \mathbb{N}$
  - $0 \in A$ , indeed  $a = 0 + a$  so that  $0 \leq a$ .
  - $s(A) \subset A$ .  
Indeed, let  $n \in s(A)$ . Then  $n = s(b)$  for some  $b \in A$ , i.e.  $a \leq b$  or  $b \leq a$ .  
If  $a \leq b$  then  $b = a + k$  for some  $k \in \mathbb{N}$ ,  $n = s(b) = b + 1 = a + k + 1$  with  $k + 1 \in \mathbb{N}$ , so that  $a \leq n$ .  
If  $b \leq a$  then  $a = b + l$  for some  $l \in \mathbb{N}$ . The case  $l = 0$  is covered by the above case, so we may assume that  $l \neq 0$ . Then  $l = \tilde{l} + 1$  for some  $\tilde{l} \in \mathbb{N}$ .  
Hence  $a = b + l = b + \tilde{l} + 1 = b + 1 + \tilde{l} = n + \tilde{l}$ , i.e.  $n \leq a$ .  
In both cases  $n \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . So, for all  $b \in \mathbb{N}$ , either  $a \leq b$  or  $b \leq a$ . ■

**Definition 1.17.** Given  $a, b \in \mathbb{N}$ , we write  $a < b$  for  $(a \leq b \text{ and } a \neq b)$ .

**Proposition 1.18.**

1.  $\forall a, b \in \mathbb{N}, a < b \Leftrightarrow a + 1 \leq b$ .
2. Given  $a, b \in \mathbb{N}$ , exactly one of the followings occurs: either  $a < b$ , or  $a = b$ , or  $b < a$ .  
Particularly, the negation of  $a \leq b$  is  $b < a$ .

*Proof.*

1.  $\Rightarrow$ : Let  $a, b \in \mathbb{N}$  be such that  $a < b$ . Then  $a \leq b$  so there exists  $k \in \mathbb{N}$  such that  $b = a + k$ .  
Assume by contradiction that  $k = 0$  then  $a = b$  which is false. Hence  $k \neq 0$  and there exists  $\tilde{k} \in \mathbb{N}$  such that  $k = \tilde{k} + 1$ . Then  $b = (a + 1) + \tilde{k}$ . We proved that  $a + 1 \leq b$  as expected.  
 $\Leftarrow$ : Assume that  $a + 1 \leq b$  then there exists  $k \in \mathbb{N}$  such that  $b = a + 1 + k$ .
  - Then  $b = a + (1 + k)$  with  $1 + k \in \mathbb{N}$  hence  $a \leq b$ .
  - Assume by contradiction that  $a = b$  then  $a = a + 1 + k$  hence  $0 = 1 + k$  from which we get  $0 = 1$ , so  $0 = s(0)$ . We get a contradiction with  $0 \notin s(\mathbb{N})$ .
2. This property derives from the fact that the order  $\leq$  is total. ■

**Proposition 1.19.**

1.  $\forall a \in \mathbb{N}, a \leq 0 \implies a = 0$
2.  $\forall a, b, c \in \mathbb{N}, a + b \leq a + c \implies b \leq c$
3. There is no  $a \in \mathbb{N}$  such that  $0 < a < 1$ .
4. There is no  $a \in \mathbb{N}$  such that  $\forall b \in \mathbb{N}, b \leq a$ .
5.  $\forall a, b, c \in \mathbb{N}, a \leq b \implies ac \leq bc$

- Proof.*
1. Let  $a \in \mathbb{N}$  be such that  $a \leq 0$ . Then there exists  $k \in \mathbb{N}$  such that  $0 = a + k$ . Hence  $a = k = 0$ .
  2. Let  $a, b, c \in \mathbb{N}$ . Assume that  $a + b \leq a + c$ . Then there exists  $k \in \mathbb{N}$  such that  $a + c = a + b + k$ . Then  $c = b + k$  so that  $b \leq c$  as expected.
  3. Let  $a \in \mathbb{N}$ . Assume that  $a < 1$ , then there exists  $l \in \mathbb{N} \setminus \{0\}$  such that  $1 = a + l$ . Since  $l \neq 0, l = k + 1$  for some  $k \in \mathbb{N}$ , and  $1 = a + k + 1$  so that  $0 = a + k$ . Therefore  $a = 0$ .
  4. Assume by contradiction that there exists  $a \in \mathbb{N}$  such that  $\forall b \in \mathbb{N}, b \leq a$ . Then  $a + 1 \leq a$  hence  $1 \leq 0$ , i.e.  $0 = 1 + k$  for some  $k \in \mathbb{N}$ . Therefore  $1 = 0$  which is a contradiction (otherwise  $0 = s(0)$  but  $0 \notin s(\mathbb{N})$ ).
  5. Let  $a, b, c \in \mathbb{N}$ . Assume that  $a \leq b$ . Then  $b = a + k$  for some  $k \in \mathbb{N}$ . Thus  $bc = (a + k)c = ac + kc$  with  $kc \in \mathbb{N}$ . Therefore  $ac \leq bc$ . ■

**Theorem 1.20** (The well-ordering principle). *The set  $\mathbb{N}$  is well-ordered for  $\leq$ .*

*A nonempty subset  $A$  of  $\mathbb{N}$  has a least element, i.e. there exists  $n \in A$  such that  $\forall a \in A, n \leq a$ .*

*Proof.* Let's prove the contrapositive, i.e. if a subset  $A \subset \mathbb{N}$  doesn't have a least element then it is empty.

Let  $B = \{a \in \mathbb{N} : \forall i \leq a, i \notin A\}$ .

- $B \subset \mathbb{N}$
- $0 \in B$  (otherwise 0 would be the least element of  $A$ ).
- $s(B) \subset B$

Indeed, if  $n \in s(B)$ , then  $n = s(a)$  for  $a \in B$ , i.e.  $\forall i \leq a, i \notin A$ . Note that  $n = a + 1 \notin A$  otherwise it would be the least element of  $A$ . Therefore  $\forall i \leq n, i \notin A$ , i.e.  $n \in B$ .

Thus, by the induction principle,  $B = \mathbb{N}$  so  $A$  is empty. ■

We proved that the induction principle implies the well-ordering principle, but they are actually equivalent. In the definition of  $\mathbb{N}$ , we could have replaced the induction principle by the well-ordering principle.

*Proof that the well-ordering principle implies the induction principle.*

Let  $A \subset \mathbb{N}$ . Assume that  $0 \in A$  and that  $s(A) \subset A$ . We want to prove that  $A = \mathbb{N}$ .

Assume by contradiction that  $\mathbb{N} \setminus A \neq \emptyset$ . Then, by the well-ordering principle,  $\mathbb{N} \setminus A$  admits a least element  $a \in A$ . Obviously,  $a \neq 0$  since  $0 \in A$ .

Since  $a \in \mathbb{N} \setminus \{0\}$ , there exists  $\tilde{a} \in \mathbb{N}$  such that  $a = s(\tilde{a})$ . Since  $s(A) \subset A$ ,  $\tilde{a} \notin A$  (otherwise  $a = s(\tilde{a}) \in A$ ).

But  $\tilde{a} < a$ . This contradicts the fact that  $a$  is the least element of  $A$ .

Hence  $\mathbb{N} \setminus A = \emptyset$  and  $A = \mathbb{N}$ . ■

**Proposition 1.21.**  $\forall a, b \in \mathbb{N}, ab = 1 \implies a = b = 1$ .

*Proof.* Let  $a, b \in \mathbb{N}$  be such that  $ab = 1$ . Since  $a = 0$  or  $b = 0$  implies that  $ab = 0$ , we know that  $a \neq 0$  and  $b \neq 0$ . We have  $0 \leq a$  and  $a \neq 0$  hence  $0 < a$  from which we get  $1 \leq a$ . Similarly  $1 \leq b$ .

Then  $a = 1 + k$  for some  $k \in \mathbb{N}$ . Then  $1 = ab = b + bk$ , i.e.  $b \leq 1$ . Hence  $b = 1$  and  $a = a \times 1 = ab = 1$ . ■

## 1.2.4 Summary

The main properties of  $(\mathbb{N}, +, \times, \leq, 0, 1)$ , where  $+, \times$  are two binary laws and  $\leq$  is a binary relation, are:

- $+$  is associative:  $\forall a, b, c \in \mathbb{N}, (a + b) + c = a + (b + c)$
- $+$  is commutative:  $\forall a, b \in \mathbb{N}, a + b = b + a$
- $0$  is the unit of  $+$ :  $\forall a \in \mathbb{N}, 0 + a = a + 0 = a$
- Cancellation rule:  $\forall a, b, c \in \mathbb{N}, a + b = a + c \Rightarrow b = c$
- $\forall a, b \in \mathbb{N}, a + b = 0 \implies a = b = 0$ .
- $\times$  is associative:  $\forall a, b, c \in \mathbb{N}, (a \times b) \times c = a \times (b \times c)$
- $\times$  is commutative:  $\forall a, b \in \mathbb{N}, a \times b = b \times a$
- $1$  is the unit of  $\times$ :  $\forall a \in \mathbb{N}, 1 \times a = a \times 1 = a$
- Cancellation rule: for  $\forall a, b, c \in \mathbb{N}, \begin{cases} a \times b = a \times c \\ a \neq 0 \end{cases} \Rightarrow b = c$
- $\times$  is distributive over  $+$ :  $\forall a, b, c \in \mathbb{N}, a \times (b + c) = a \times b + a \times c$  and  $(a + b) \times c = a \times c + b \times c$
- $\forall a, b \in \mathbb{N}, a \times b = 0 \implies (a = 0 \text{ or } b = 0)$
- $\forall a, b \in \mathbb{N}, ab = 1 \implies a = b = 1$
- $\leq$  is an order on  $\mathbb{N}$ , i.e.
  - Reflexivity:  $\forall a \in \mathbb{N}, a \leq a$
  - Antisymmetry:  $\forall a, b \in \mathbb{N}, (a \leq b \text{ and } b \leq a) \Rightarrow a = b$
  - Transitivity:  $\forall a, b, c \in \mathbb{N}, (a \leq b \text{ and } b \leq c) \Rightarrow a \leq c$

Besides, this order is total:  $\forall a, b \in \mathbb{N}, a \leq b \text{ or } b \leq a$

- Well-ordering principle: a nonempty subset  $A$  of  $\mathbb{N}$  has a least element.
- $\leq$  is compatible with  $+$ :  $\forall a, b, c \in \mathbb{N}, a \leq b \Rightarrow a + c \leq b + c$
- $\leq$  is compatible with  $\times$ :  $\forall a, b, c \in \mathbb{N}, a \leq b \Rightarrow ac \leq bc$
- ★  $\forall a, b, c, d \in \mathbb{N}, (a \leq b \text{ and } c \leq d) \Rightarrow a + c \leq b + d$
- ★  $\forall a, b, c, d \in \mathbb{N}, (a \leq b \text{ and } c \leq d) \Rightarrow ac \leq bd$
- $\forall a \in \mathbb{N}, a \leq 0 \implies a = 0$
- There is no  $a \in \mathbb{N}$  such that  $0 < a < 1$ .
- There is no  $a \in \mathbb{N}$  such that  $\forall b \in \mathbb{N}, b \leq a$ .
- $\forall a, b \in \mathbb{N}, a < b \Leftrightarrow a + 1 \leq b$ .
- For  $a, b \in \mathbb{N}$  we have (exclusively) either  $a < b$ , or  $a = b$ , or  $b < a$ .  
Particularly, the negation of  $a \leq b$  is  $b < a$ .

The properties with a star were not proved in this chapter but will be proved as practice questions. Except otherwise stated, you can directly use any of the above properties without proving them.



## 1.3 Proof by induction

In this section we are going to highlight the connection between the *principle of induction* as stated in Theorem 1.1 and the notion of *proof by induction* that you have already encountered.

### 1.3.1 Formal statement

*Proof by induction* is closely related to the fact that  $\mathbb{N}$  is defined by its initial term 0 and then by taking iteratively its successor. This fact is highlighted in the proof of the following theorem.

**Theorem 1.22** (Proof by induction). *Let  $P(n)$  be a statement depending on  $n \in \mathbb{N}$ . If  $P(0)$  is true and if  $P(n) \implies P(n+1)$  is true for all  $n \in \mathbb{N}$ , then  $P(n)$  is true for all  $n \in \mathbb{N}$ . Formally,*

$$\left\{ \begin{array}{l} P(0) \\ \forall n \in \mathbb{N}, (P(n) \implies P(n+1)) \end{array} \right\} \implies \forall n \in \mathbb{N}, P(n)$$

The informal idea is that since  $P(0)$  and  $P(0) \implies P(1)$  are true then  $P(1)$  is true. Then we can repeat the same process: since  $P(1)$  and  $P(1) \implies P(2)$  are true then  $P(2)$  is true, and so on...

This way  $P(0)$ ,  $P(1)$ ,  $P(2)$ ,  $P(3)$ , ... are all true.

*Proof of Theorem 1.22.*

We define the set  $A = \{n \in \mathbb{N} : P(n) \text{ is true}\}$ . Then:

- $A \subset \mathbb{N}$  by definition of  $A$ .
- $0 \in \mathbb{N}$  since  $P(0)$  is true.
- $s(A) \subset A$

Indeed, let  $n \in s(A)$ . Then  $n = s(m) = m + 1$  for some  $m \in A$ . By definition of  $A$ ,  $P(m)$  is true. But by assumption  $P(m) \implies P(m+1)$  is also true. Hence  $P(m+1)$  is true, meaning that  $n = m + 1 \in A$ .

Hence, by the *induction principle* of Theorem 1.1,  $A = \mathbb{N}$ . Finally, for every  $n \in \mathbb{N}$  we have that  $P(n)$  is true. ■

### 1.3.2 In practice

How to write a *proof by induction*? There are several steps that you should make sure they appear clearly!

- What statement are you proving? What is your  $P(n)$ ? Particularly, on which parameter are you doing the induction? You should make everything clear for the reader!
- **Base case:** prove that  $P(0)$  is true.
- **Induction step:** prove that if  $P(n)$  is true for some  $n \in \mathbb{N}$  then  $P(n+1)$  is also true.

It is important to clearly write the induction hypothesis and what you want to prove in this step (the reader shouldn't have to guess). Make sure that you used the induction hypothesis somewhere, otherwise there is something suspicious with your proof.

Below are two basic examples:

**Proposition 1.23.** *For any  $n \in \mathbb{N}$ , the sum  $0 + 1 + 2 + \dots + n$  is equal to  $\frac{n(n+1)}{2}$ .*

*Proof.* We are going to prove that  $\forall n \in \mathbb{N}, 0 + 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  by induction on  $n$ .

- **Base case:** Let  $n = 0$ . Then the sum in the left hand side is equal to 0. And  $\frac{n(n+1)}{2} = \frac{0 \cdot 1}{2} = 0$ . So the equality holds.
- **Induction step:** Assume that  $0 + 1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}$  for some  $n \in \mathbb{N}$  and let's prove that  $0 + 1 + 2 + 3 + \dots + n + (n+1) = \frac{(n+1)(n+2)}{2}$ .

$$\begin{aligned} 0 + 1 + 2 + 3 + \dots + n + (n+1) &= \frac{n(n+1)}{2} + (n+1) \text{ by the induction hypothesis} \\ &= \frac{n(n+1) + 2(n+1)}{2} = \frac{(n+1)(n+2)}{2} \end{aligned}$$

Which proves the induction step. ■

**Proposition 1.24.** *For any  $n \in \mathbb{N}$ , the sum of the first  $n$  odd numbers is equal to  $n^2$ .*

*Proof.* We are going to prove that  $\forall n \in \mathbb{N}, 1 + 3 + \dots + (2n - 1) = n^2$  by induction on  $n$ .

- **Base case:** Let  $n = 0$ . Then the sum in the left hand side is empty, so it is equal to 0. And  $n^2 = 0^2 = 0$ . So the equality holds.
- **Induction step:** Assume that the sum of the first  $n$  odd numbers is equal to  $n^2$  for some  $n \in \mathbb{N}$ , i.e.  $1 + 3 + \dots + (2n - 1) = n^2$ .  
Let's prove that  $1 + 3 + \dots + (2n - 1) + (2n + 1) = (n + 1)^2$ .

$$\begin{aligned} 1 + 3 + \dots + (2n - 1) + (2n + 1) &= n^2 + 2n + 1 \quad \text{by the induction hypothesis} \\ &= (n + 1)^2 \quad \text{by the binomial formula} \end{aligned}$$

Which proves the induction step. ■

### 1.3.3 Variants of the induction

#### Strong induction

The strong induction is equivalent to the usual induction (i.e. one may prove that Theorem 1.22 holds assuming Theorem 1.25, and that Theorem 1.25 holds assuming Theorem 1.22). Nonetheless, in some cases, it may be easier to write a strong induction rather than a usual one.

**Theorem 1.25** (Strong induction). *Let  $P(n)$  be a statement depending on  $n \in \mathbb{N}$ .*

*If  $P(0)$  is true and if  $(P(0), P(1), \dots, P(n)) \implies P(n + 1)$  is true for all  $n \in \mathbb{N}$ , then  $P(n)$  is true for all  $n \in \mathbb{N}$ . Formally,*

$$\left\{ \begin{array}{l} P(0) \\ \forall n \in \mathbb{N}, ((P(0), P(1), \dots, P(n)) \implies P(n + 1)) \end{array} \right\} \implies \forall n \in \mathbb{N}, P(n)$$

*Proof.* For  $n \in \mathbb{N}$ , we define  $R(n)$  by

$$R(n) \text{ is true} \Leftrightarrow P(0), P(1), \dots, P(n) \text{ are true}$$

Assume that  $P(0)$  is true and that  $(P(0), P(1), \dots, P(n)) \implies P(n + 1)$  is true for all  $n \in \mathbb{N}$ .

Then  $R(0)$  is true since  $P(0)$  is. And, for all  $n \in \mathbb{N}$ ,  $R(n) \implies R(n + 1)$  is true.

By the usual induction  $R(n)$  is true for any  $n \in \mathbb{N}$ . Particularly,  $P(n)$  is true for any  $n \in \mathbb{N}$  as expected. ■

#### Base case at $n_0$

It may be easier to write a proof by induction starting at a base  $n_0 \in \mathbb{N}$  which is not necessarily 0. Below is the corresponding statement for the usual induction, but it is possible to adapt the strong induction similarly.

**Theorem 1.26.** *Let  $n_0 \in \mathbb{N}$ . Let  $P(n)$  be a statement depending on a natural number  $n \geq n_0$ .*

*If  $P(n_0)$  is true and if  $P(n) \implies P(n + 1)$  is true for every natural number  $n \geq n_0$ , then  $P(n)$  is true for every natural number  $n \geq n_0$ . Formally,*

$$\left\{ \begin{array}{l} P(n_0) \\ \forall n \in \mathbb{N}_{\geq n_0}, (P(n) \implies P(n + 1)) \end{array} \right\} \implies \forall n \in \mathbb{N}_{\geq n_0}, P(n)$$

*Proof.* For  $n \in \mathbb{N}$ , we define  $R(n)$  by

$$R(n) \text{ is true} \Leftrightarrow P(n + n_0) \text{ is true}$$

Then  $R(0)$  is true since  $P(n_0)$  is. And, for all  $n \in \mathbb{N}$ ,  $R(n) \implies R(n + 1)$  is true.

By the usual induction  $R(n)$  is true for any  $n \in \mathbb{N}$ , i.e.  $P(n)$  is true for any  $n \in \mathbb{N}_{\geq n_0}$ . ■

Below is an example of induction starting at  $n_0 = 5$ .

**Proposition 1.27.** *For any integer  $n \geq 5$ ,  $2^n > n^2$ .*

*Proof.* We are going to prove that  $\forall n \geq 5$ ,  $2^n > n^2$  by induction on  $n$ .

- **Base case at  $n = 5$ :**  $2^5 = 32 > 25 = 5^2$ .

- **Induction step:** Assume that  $2^n > n^2$  for some  $n \geq 5$  and let's prove that  $2^{n+1} > (n+1)^2$ .

Note that  $2^{n+1} = 2 \times 2^n \geq 2n^2$  by the induction hypothesis. Hence it is enough to prove that  $2n^2 > (n+1)^2$  which is equivalent to  $n^2 - 2n - 1 > 0$ .

We study the sign of the polynomial  $x^2 - 2x - 1$ . It is a polynomial of degree 2 with positive leading coefficient and its discriminant is  $(-2)^2 - 4 \times (-1) = 8 > 0$ . Therefore

$x$	$-\infty$	$1 - \sqrt{2}$	$1 + \sqrt{2}$	$+\infty$	
$x^2 - 2x - 1$	+	0	-	0	+

Since  $5 > 1 + \sqrt{2}$ , we know that  $n^2 - 2n - 1 > 0$  for  $n \geq 5$ . Which proves the induction step. ■

**Remark 1.28.** The above example is interesting because the induction step holds for  $n \geq 3$ , but  $\mathcal{P}(3)$  and  $\mathcal{P}(4)$  are false: don't forget the base case! It is crucial!

## Exercises

### Exercise 1.

Using only the definition of the multiplication, the properties of the addition and Peano axioms, prove that:

1.  $\forall a \in \mathbb{N}, 0 \times a = a \times 0 = 0$
2.  $\forall a \in \mathbb{N}, a \times 1 = a$

### Exercise 2.

Given  $m \in \mathbb{N}$ , we define inductively the function  $m^\bullet : \mathbb{N} \rightarrow \mathbb{N}$  by  $m^0 = 1$  and  $\forall n \in \mathbb{N}, m^{s(n)} = m^n \times m$ .

Prove that:

1.  $\forall m \in \mathbb{N}, m^1 = m$
2.  $\forall a, b, n \in \mathbb{N}, (a \times b)^n = a^n \times b^n$
3.  $\forall a, m, n \in \mathbb{N}, a^{m+n} = a^m \times a^n$
4.  $\forall n \in \mathbb{N} \setminus \{0\}, 0^n = 0$
5.  $\forall n \in \mathbb{N}, 1^n = 1$

### Exercise 3.

For each of the followings, is the binary relation  $\mathcal{R}$  an order on  $E$ ? If so, is it total?

1.  $E = \mathbb{Z}$  and  $\forall x, y \in \mathbb{Z}, x\mathcal{R}y \Leftrightarrow x = -y$
2.  $E = \mathbb{R}$  and  $\forall x, y \in \mathbb{R}, x\mathcal{R}y \Leftrightarrow \cos^2 x + \sin^2 y = 1$
3.  $E = \mathcal{P}(S)$  is the set of subsets of a fixed set  $S$  and  $\forall A, B \in \mathcal{P}(S), A\mathcal{R}B \Leftrightarrow A \subset B$

### Exercise 4.

We define a binary relation  $\mathcal{R}$  on  $\mathbb{N}$  by  $\forall x, y \in \mathbb{N}, x\mathcal{R}y \Leftrightarrow \exists p, q \in \mathbb{N} \setminus \{0\}, y = px^q$ .

1. Prove that  $\mathcal{R}$  is an order.
2. Is it a total order?

### Exercise 5.

We define a binary relation  $<$  on  $\mathbb{N}^2$  by  $(x_1, y_1) < (x_2, y_2) \Leftrightarrow (x_1 \leq x_2 \text{ and } y_1 \leq y_2)$ .

1. Prove that  $<$  is an order.
2. Is it a total order?

### Exercise 6.

Prove that

1.  $\forall a, b, c, d \in \mathbb{N}, (a \leq b \text{ and } c \leq d) \Rightarrow a + c \leq b + d$
2.  $\forall a, b, c, d \in \mathbb{N}, (a \leq b \text{ and } c \leq d) \Rightarrow ac \leq bd$

### Exercise 7.

For which  $c \in \mathbb{N}$ , do we have  $\forall a, b \in \mathbb{N}, ac \leq bc \Rightarrow a \leq b$ ?

### Exercise 8.

Using the well-ordering principle, find an alternative proof of: *there is no natural number  $n$  between 0 and 1.*

### Exercise 9.

1. Prove that  $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, n^3 + 2n = 3k$ .
2. Prove that  $\forall n \in \mathbb{N}, \sum_{k=0}^n \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$ .

### Exercise 10.

We define a sequence  $(u_n)_{n \geq 1}$  by  $u_1 = 3$  and  $\forall n \in \mathbb{N} \setminus \{0\}, u_{n+1} = \frac{2}{n} \sum_{k=1}^n u_k$ .

Prove that  $\forall n \in \mathbb{N} \setminus \{0\}, u_n = 3n$ .

**Exercise 11.** *Bernoulli's inequality.*

Prove that  $\forall x \in [-1, +\infty), \forall n \in \mathbb{N}, (1+x)^n \geq 1+nx$ .  
(here we consider the usual order  $\geq$  on  $\mathbb{R}$ )

**Exercise 12.**

For  $n \in \mathbb{N}$ , we define the statement  $P(n)$  by  $2^n > n^2$ .

1. Prove that  $\forall n \geq 3, P(n) \implies P(n+1)$ .
2. For which  $n \in \mathbb{N}$ , is  $P(n)$  true?

**Exercise 13.**

What do you think about the following proof by induction?

We want to prove that for any  $n \geq 2$ ,  $n$  distinct points of the plane are always on the same line.

*Proof:*

- Base case: when  $n = 2$  the property is known to be true.
- Induction step: we assume that the property is true for some  $n \geq 2$  and we want to show that it also holds for  $n+1$ .

Let  $A_1, A_2, \dots, A_{n+1}$  be  $n+1$  distinct points of the plane. By the induction hypothesis, we have

- $A_1, A_2, \dots, A_n$  are on the same line  $L$ .
- $A_2, A_3, \dots, A_{n+1}$  are on the same line  $L'$ .

Then  $A_2, A_3, \dots, A_n$  are at the same time on  $L$  and  $L'$  so that  $L = L'$ .

Thus  $A_1, \dots, A_{n+1}$  are on the same line. Which ends the induction step. ■

**Exercise 14.**

Given  $n \in \mathbb{N} \setminus \{0\}$ , prove that there exists a unique couple  $(a, b) \in \mathbb{N}$  such that  $n = 2^a(2b+1)$ .

**Exercise 15.**

Find all the increasing functions  $f : \mathbb{N} \rightarrow \mathbb{N}$  such that  $f(2) = 2$  and  $\forall p, q \in \mathbb{N}, f(pq) = f(p)f(q)$ .

Recall that a function  $f : \mathbb{N} \rightarrow \mathbb{N}$  is increasing if  $\forall x, y \in \mathbb{N}, x < y \implies f(x) < f(y)$ .

**Exercise 16.**

1. Prove that if  $S \subset \mathbb{Z}$  admits a greatest element then it is unique.
2. Prove that a non-empty finite subset of  $\mathbb{Z}$  admits a greatest element.

**Exercise 17.**

Let  $n \in \mathbb{N} \setminus \{0\}$ . Prove that if one square of a  $2^n \times 2^n$  chessboard is removed, then the remaining squares can be covered by L-shaped trominoes.

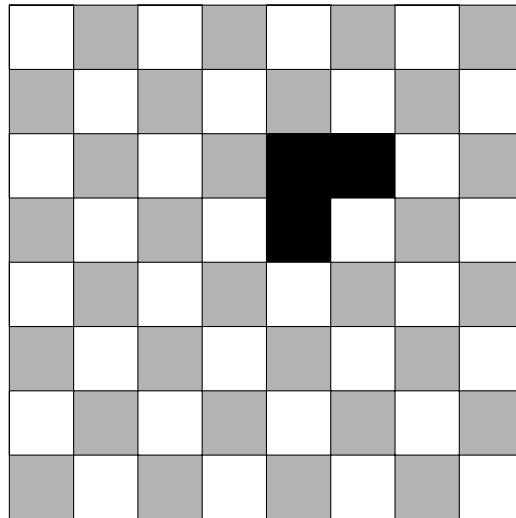
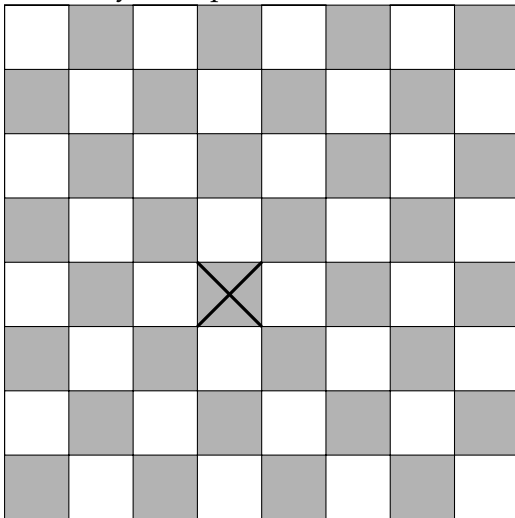
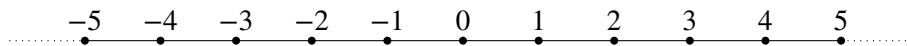


Figure 1.1: An  $8 \times 8$  chessboard with a removed square. Figure 1.2: An L-shaped tromino on a chessboard.

# Chapter 2

## Integers

In this chapter, we are going to construct the set  $\mathbb{Z}$  of integers and then to study its properties. The informal idea consists in extending  $\mathbb{N}$  by adding its *symmetry* with respect to 0:



For this purpose, we have to give a meaning to the notation  $-n$  where  $n$  is a natural number and then we have to extend from  $\mathbb{N}$  to  $\mathbb{Z}$  the operations  $(+, \times)$  and the order  $(\leq)$ .

There are several ways to formally do that. The usual one consists in defining  $\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$  for the equivalence relation  $(a, b) \sim (c, d) \Leftrightarrow a + d = b + c$ . Let me explain what does it mean: intuitively  $(a, b)$  stands for  $a - b$ , but, since such an expression is not unique (e.g.  $7 - 5 = 10 - 8$ ), we need to "identify" some couples (e.g.  $(7, 5) = (10, 8)$ ). This construction has several advantages (it is easy to extend  $+$ ,  $\times$  and  $\leq$ ) but it needs an additional layer of abstraction (equivalence relations, equivalence classes...).

Instead, I will use a more naive approach. The counterpart is that extending the operations will be a little bit tedious with several cases to handle (e.g. the definition of  $a + b$  will depend on the signs of  $a$  and  $b$ , so we have 4 cases just to define the addition...).

Note that what we are going to describe in a few lines took centuries to be developed and accepted: during the 18th century, most mathematicians were still reluctant about using negative numbers.

### 2.1 Construction of the integers

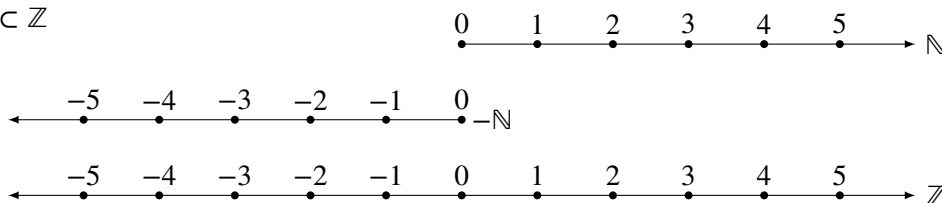
#### 2.1.1 Definition

**Definition 2.1.** For any  $n \in \mathbb{N} \setminus \{0\}$ , we formally introduce the symbol  $-n$  read as *minus n* and we fix the convention that  $-0 = 0$ .

We define the set  $-\mathbb{N} := \{-n : n \in \mathbb{N}\}$ . Then the *set of integers* is  $\mathbb{Z} := (-\mathbb{N}) \cup \mathbb{N}$ .

**Remark 2.2.**  $(-\mathbb{N}) \cap \mathbb{N} = \{0\}$

**Remark 2.3.**  $\mathbb{N} \subset \mathbb{Z}$



### 2.1.2 Operations

**Definition 2.4.** For  $m, n \in \mathbb{N}$ , we set:

- (i)  $m + n$  for the usual addition in  $\mathbb{N}$
- (ii)  $(-m) + (-n) = -(m + n)$
- (iii)  $m + (-n) = \begin{cases} k & \text{where } k \text{ is the unique natural integer such that } m = n + k \text{ if } n \leq m \\ -k & \text{where } k \text{ is the unique natural integer such that } n = m + k \text{ if } m \leq n \end{cases}$
- (iv)  $(-m) + n = n + (-m)$  where  $n + (-m)$  is defined in (iii)

We've just defined  $+$  :  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$   
 $(a, b) \mapsto a + b$ .

**Remark 2.5.** We have to check that the overlapping cases  $m = 0$  or  $n = 0$  are not contradictory.

**Definition 2.6.** For  $m, n \in \mathbb{N}$ , we set:

- (i)  $m \times n$  for the usual product in  $\mathbb{N}$
- (ii)  $(-m) \times (-n) = m \times n$
- (iii)  $m \times (-n) = -(m \times n)$
- (iv)  $(-m) \times n = -(m \times n)$

We've just defined  $\times$  :  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$   
 $(a, b) \mapsto a \times b$ .

**Remark 2.7.** We may simply write  $ab$  for  $a \times b$  when there is no possible confusion.

**Remark 2.8.** Note that the addition and product on  $\mathbb{Z}$  are compatible with the addition and product on  $\mathbb{N}$ .

**Definition 2.9.** For  $n \in \mathbb{N}$ , we set  $-(-n) = n$ . Then  $-a$  is well-defined for every  $a \in \mathbb{Z}$ .

**Proposition 2.10.**

- $+$  is associative:  $\forall a, b, c \in \mathbb{Z}, (a + b) + c = a + (b + c)$
- $0$  is the unit of  $+$ :  $\forall a \in \mathbb{Z}, a + 0 = 0 + a = a$
- $-a$  is the additive inverse of  $a$ :  $\forall a \in \mathbb{Z}, a + (-a) = (-a) + a = 0$
- $+$  is commutative:  $\forall a, b \in \mathbb{Z}, a + b = b + a$
- $\times$  is associative:  $\forall a, b, c \in \mathbb{Z}, (ab)c = a(bc)$
- $\times$  is distributive with respect to  $+$ :  $\forall a, b, c \in \mathbb{Z}, a \times (b + c) = ab + ac$  et  $(a + b)c = ac + bc$
- $1$  is the unit of  $\times$ :  $\forall a \in \mathbb{Z}, 1 \times a = a \times 1 = a$
- $\times$  is commutative:  $\forall a, b \in \mathbb{Z}, ab = ba$
- $\forall a, b \in \mathbb{Z}, ab = 0 \Rightarrow (a = 0 \text{ or } b = 0)$

The above properties are easy to prove but the proofs are tedious with several cases depending on the signs.

**Remark.** From now on, we may simply write  $a - b$  for  $a + (-b)$  and  $-a + b$  for  $(-a) + b$ .

**Corollary 2.11.**  $\forall a, b, c \in \mathbb{Z}, (ac = bc \text{ and } c \neq 0) \implies a = b$

*Proof.* Let  $a, b, c \in \mathbb{Z}$  be such that  $ac = bc$  and  $c \neq 0$ .

Then  $(a - b)c = 0$ . So either  $a - b = 0$  or  $c = 0$ . Since  $c \neq 0$ , we get  $a - b = 0$ , i.e.  $a = b$ . ■

### 2.1.3 Order

**Definition 2.12.** We define the binary relation  $\leq$  on  $\mathbb{Z}$  by

$$\forall a, b \in \mathbb{Z}, a \leq b \Leftrightarrow b - a \in \mathbb{N}$$

**Proposition 2.13.**  $\leq$  defines a total order on  $\mathbb{Z}$ .

*Proof.*

- *Reflexivity.* Let  $a \in \mathbb{Z}$ , then  $a - a = 0 \in \mathbb{N}$  so  $a \leq a$ .
- *Antisymmetry.* Let  $a, b \in \mathbb{Z}$ . Assume that  $a \leq b$  and that  $b \leq a$ . Then  $b - a \in \mathbb{N}$  and  $a - b \in \mathbb{N}$ . So  $a - b = -(b - a) \in (-\mathbb{N})$ . Hence  $a - b \in (-\mathbb{N}) \cap \mathbb{N} = \{0\}$  and thus  $a = b$ .

- *Transitivity.* Let  $a, b, c \in \mathbb{Z}$ . Assume that  $a \leq b$  and that  $b \leq c$ . Then  $b - a \in \mathbb{N}$  and  $c - b \in \mathbb{N}$ . Thus  $c - a = (c - b) + (b - a) \in \mathbb{N}$ , i.e.  $a \leq c$ .
- Let  $a, b \in \mathbb{Z}$ . Then  $b - a \in \mathbb{Z} = (-\mathbb{N}) \cup (\mathbb{N})$ .  
*First case:*  $b - a \in \mathbb{N}$  then  $a \leq b$ .  
*Second case:*  $b - a \in (-\mathbb{N})$ , then  $a - b = -(b - a) \in \mathbb{N}$  and  $b \leq a$ .  
Hence the order is total. ■

**Proposition 2.14.** *The order on  $\mathbb{Z}$  is compatible with the order on  $\mathbb{N}$ .*

*Proof.* Let  $a, b \in \mathbb{N}$ .

- Assume that  $a \leq_{\mathbb{Z}} b$ . Then  $k = b - a \in \mathbb{N}$ . So  $b = a + k$ , i.e.  $a \leq_{\mathbb{N}} b$ .
- Assume that  $a \leq_{\mathbb{N}} b$ . Then  $b = a + k$  for some  $k \in \mathbb{N}$ . Then  $b - a = k \in \mathbb{N}$ , i.e.  $a \leq_{\mathbb{Z}} b$ . ■

**Proposition 2.15.**

1.  $\mathbb{N} = \{a \in \mathbb{Z}, 0 \leq a\}$
2.  $\forall a, b, c \in \mathbb{Z}, a \leq b \Leftrightarrow a + c \leq b + c$
3.  $\forall a, b, c, d \in \mathbb{Z}, (a \leq b \text{ and } c \leq d) \Rightarrow a + c \leq b + d$
4.  $\forall a, b \in \mathbb{Z}, \forall c \in \mathbb{N} \setminus \{0\}, a \leq b \Leftrightarrow ac \leq bc$
5.  $\forall a, b \in \mathbb{Z}, \forall c \in (-\mathbb{N}) \setminus \{0\}, a \leq b \Leftrightarrow bc \leq ac$

*Proof.*

1. Let  $a \in \mathbb{Z}$ . Then  $0 \leq a \Leftrightarrow a = a - 0 \in \mathbb{N}$ .
2. Let  $a, b, c \in \mathbb{Z}$ . Then  $a \leq b \Leftrightarrow b - a \in \mathbb{N} \Leftrightarrow (b + c) - (a + c) \in \mathbb{N} \Leftrightarrow a + c \leq b + c$ .
3. Let  $a, b, c, d \in \mathbb{Z}$ . Assume that  $a \leq b$  and that  $c \leq d$ . Then  $b - a \in \mathbb{N}$  and  $d - c \in \mathbb{N}$ . Hence  $(b + d) - (a + c) = (b - a) + (d - c) \in \mathbb{N}$ , i.e.  $a + c \leq b + d$ .
4. Let  $a, b \in \mathbb{Z}$  and  $c \in \mathbb{N}$ .  
 $\Rightarrow$ : Assume that  $a \leq b$ . Then  $b - a \in \mathbb{N}$ , thus  $bc - ac = (b - a)c \in \mathbb{N}$ . Therefore  $ac \leq bc$ .  
 $\Leftarrow$ : Assume that  $c \neq 0$  and that  $ac \leq bc$ . Then  $bc - ac = (b - a)c \in \mathbb{N}$ . Assume by contradiction that  $(b - a) \in (-\mathbb{N}) \setminus \{0\}$  then, by definition of the multiplication,  $(b - a)c \in (-\mathbb{N}) \setminus \{0\}$ , which is a contradiction. Hence  $b - a \in \mathbb{N}$ , i.e.  $a \leq b$ .
5. Let  $a, b \in \mathbb{Z}$  and  $c \in (-\mathbb{N})$ .  
 $\Rightarrow$ : Assume that  $a \leq b$ . Then  $b - a \in \mathbb{N}$ , thus  $ac - bc = (b - a)(-c) \in \mathbb{N}$ . Therefore  $bc \leq ac$ .  
 $\Leftarrow$ : Assume that  $c \neq 0$  and that  $bc \leq ac$ . Then  $ac - bc = (b - a)(-c) \in \mathbb{N}$ . And we conclude as in 4. ■

**Remark 2.16.** Given  $a, b, c \in \mathbb{Z}$ , it is common to lighten the notation by writing  $a \leq b \leq c$  for  $(a \leq b \text{ and } b \leq c)$ .

**Theorem 2.17.**

1. *A non-empty subset  $A$  of  $\mathbb{Z}$  which is bounded from below has a least element, i.e.*

$$\exists m \in A, \forall a \in A, m \leq a$$

2. *A non-empty subset  $A$  of  $\mathbb{Z}$  which is bounded from above has a greatest element, i.e.*

$$\exists M \in A, \forall a \in A, a \leq M$$

*Proof.*

1. Assume that  $A$  is a non-empty subset of  $\mathbb{Z}$  which is bounded from below. Then there exists  $k \in \mathbb{Z}$  such that  $\forall a \in A, k \leq a$ . Define  $S = \{a - k : a \in A\}$ . Then  $S$  is a non-empty subset of  $\mathbb{N}$  (indeed,  $\forall a \in A, 0 \leq a - k$ ). By the well-ordering principle, there exists  $\tilde{m} \in S$  such that  $\forall a \in A, \tilde{m} \leq a - k$ . Then  $m = \tilde{m} + k$  is the least element of  $A$  (note that  $\tilde{m} \in S$  so  $m = \tilde{m} + k \in A$ ).
2. Assume that  $A$  is a non-empty subset of  $\mathbb{Z}$  which is bounded from above. Then  $(-A) = \{-a : a \in A\}$  is a non-empty subset of  $\mathbb{Z}$  which is bounded from below (prove it). By the above, there exists  $m \in (-A)$  such that  $\forall a \in A, m \leq -a$ . Hence  $\forall a \in A, a \leq -m$ . Thus  $M := -m$  is the greatest element of  $A$ . ■



## 2.2 Absolute value

**Definition 2.18.** For  $n \in \mathbb{Z}$ , we define the *absolute value* of  $n$  by  $|n| := \begin{cases} n & \text{if } n \in \mathbb{N} \\ -n & \text{if } n \in (-\mathbb{N}) \end{cases}$ .

**Proposition 2.19.**

- (i)  $\forall n \in \mathbb{Z}, |n| \in \mathbb{N}$
- (ii)  $\forall n \in \mathbb{Z}, n \leq |n|$
- (iii)  $\forall n \in \mathbb{Z}, |n| = 0 \Leftrightarrow n = 0$
- (iv)  $\forall a, b \in \mathbb{Z}, |ab| = |a||b|$
- (v)  $\forall a, b \in \mathbb{Z}, |a| \leq b \Leftrightarrow -b \leq a \leq b$
- (vi)  $\forall a, b \in \mathbb{Z}, |a + b| \leq |a| + |b|$  (triangle inequality)

*Proof.*

- (i) *First case:* if  $n \in \mathbb{N}$  then  $|n| = n \in \mathbb{N}$ .  
*Second case:* if  $n \in (-\mathbb{N})$  then  $n = -m$  for some  $m \in \mathbb{N}$  and  $|n| = -n = -(-m) = m \in \mathbb{N}$ .
- (ii) *First case:*  $n \in \mathbb{N}$ . Then  $n \leq n = |n|$ .  
*Second case:*  $n \in (-\mathbb{N})$ . Then  $n \leq 0 \leq |n|$ .
- (iii) Note that  $|0| = 0$  and that if  $n \neq 0$  then  $|n| \neq 0$ .
- (iv) You have to study separately the four cases depending on the signs of  $a$  and  $b$ .
- (v) If  $b < 0$  then  $|a| \leq b$  and  $-b \leq a \leq b$  are both false. So we may assume that  $b \in \mathbb{N}$ . Then  
*First case:*  $a \in \mathbb{N}$ . Then  $|a| \leq b \Leftrightarrow a \leq b \Leftrightarrow -b \leq a \leq b$ .  
*Second case:*  $a \in (-\mathbb{N})$ . Then  $|a| \leq b \Leftrightarrow -a \leq b \Leftrightarrow -b \leq a \Leftrightarrow -b \leq a \leq b$ .
- (vi) Since  $a + b \leq |a| + |b|$  and  $-(a + b) = -a - b \leq |-a| + |-b| = |a| + |b|$ , we get  $|a + b| \leq |a| + |b|$ . ■

## 2.3 Euclidean division

**Theorem 2.20** (Euclidean division).

Given  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z} \setminus \{0\}$ , there exists a unique couple  $(q, r) \in \mathbb{Z}^2$  such that

$$\begin{cases} a = bq + r \\ 0 \leq r < |b| \end{cases}$$

The integers  $q$  and  $r$  are respectively called the *quotient* and the *remainder* of the division of  $a$  by  $b$ .

*Proof.*

**Existence:**

*First case:* assume that  $0 < b$ .

We set<sup>1</sup>  $E = \{p \in \mathbb{Z} : bp \leq a\}$ .

- $E \neq \emptyset$ , indeed if  $0 \leq a$  then  $0 \in E$ , otherwise  $a \in E$ .
- $|a|$  is an upper bound of  $E$ .  
Indeed, let  $p \in E$ .  
If  $p \leq 0$  then  $p \leq 0 \leq |a|$ .  
Otherwise, if  $0 < p$  then  $1 \leq b \implies p \leq bp \leq a \leq |a|$ .

Thus  $E$  is a non-empty subset of  $\mathbb{Z}$  which is bounded from above.

Hence it admits a greatest element, i.e. there exists  $q \in E$  such that  $\forall p \in E, p \leq q$ .

We set  $r = a - bq$ . Since  $q \in E, r = a - bq \geq 0$ .

And  $q + 1 \notin E$  since  $q + 1 > q$  whereas  $q$  is the greatest element of  $E$ .

Therefore  $b(q + 1) > a$ , so  $r = a - bq < b = |b|$ .

We wrote  $a = bq + r$  with  $0 \leq r < |b|$  as expected.

<sup>1</sup>When  $b > 0$ , the informal idea of this proof consists in determining *how many times* we can add  $b$  before exceeding  $a$ , which will give the quotient. Then the remainder will be obtained by filling the difference in order to reach  $a$ . Intuitively, if the quotient exists, it has to be the greatest  $p$  such that  $bp \leq a$ . We have to prove the existence of such a number and then to check formally that this idea is actually correct.

*Second case: assume that  $b < 0$ .*

Then we apply the first case to  $a$  and  $-b > 0$ : there exists  $(q, r) \in \mathbb{Z}^2$  such that  $a = -bq + r = b(-q) + r$  with  $0 \leq r < -b = |b|$ .

**Uniqueness:** assume that we have two suitable couples  $(q, r)$  and  $(q', r')$ .

Then  $r' - r = (a - bq') - (a - bq) = b(q - q')$ . Besides

$$\begin{cases} 0 \leq r < |b| \\ 0 \leq r' < |b| \end{cases} \implies \begin{cases} -|b| < -r \leq 0 \\ 0 \leq r' < |b| \end{cases} \implies -|b| < r' - r < |b|$$

Thus  $-|b| < b(q - q') < |b|$ , from which we get  $|b||q - q'| = |b(q - q')| < |b|$ .

Since  $|b| > 0$ , we obtain  $0 \leq |q - q'| < 1$ .

But we proved in the first chapter that there is no natural number between 0 and 1.

Therefore  $|q - q'| = 0$ , which implies that  $q - q' = 0$ , i.e.  $q = q'$ .

Finally,  $r' = b - aq' = b - aq = r$ . ■

### Examples 2.21.

- Division of 22 by 5:  $22 = 5 \times 4 + 2$ .  
The quotient is  $q = 4$  and the remainder is  $r = 2$ .
- Division of  $-22$  by 5:  $-22 = 5 \times (-5) + 3$ .  
The quotient is  $q = -5$  and the remainder is  $r = 3$ .
- Division of 22 by  $-5$ :  $22 = (-5) \times (-4) + 2$ .  
The quotient is  $q = -4$  and the remainder is  $r = 2$ .
- Division of  $-22$  by  $-5$ :  $-22 = (-5) \times 5 + 3$ .  
The quotient is  $q = 5$  and the remainder is  $r = 3$ .

**Proposition 2.22.** Given  $n \in \mathbb{Z}$ ,

- either  $n = 2k$  for some  $k \in \mathbb{Z}$  (then we say that  $n$  is even),
- or  $n = 2k + 1$  for some  $k \in \mathbb{Z}$  (then we say that  $n$  is odd),

and these cases are exclusive.

*Proof.* Let  $n \in \mathbb{Z}$ . By the Euclidean division by 2, there exist  $k, r \in \mathbb{Z}$  such that  $n = 2k + r$  and  $0 \leq r \leq 1$ . But we know from the last chapter that there is no natural number between 0 and 1. Hence either  $r = 0$  or  $r = 1$ . These cases are exclusive by the uniqueness of the Euclidean division. ■

## 2.4 Divisibility

**Definition 2.23.** Given  $a, b \in \mathbb{Z}$ , we say that  $a$  is *divisible by*  $b$  if there exists  $k \in \mathbb{Z}$  such that  $a = bk$ . In this case we write  $b|a$  and we also say that  $b$  is *divisor of*  $a$  or that  $a$  is a *multiple of*  $b$ .

**Examples 2.24.** •  $(-5)|10$  •  $5 \nmid (-11)$

(we will study divisibility criteria later in the term)

**Remarks 2.25.**

- Any integer is a divisor of 0, i.e.  $\forall b \in \mathbb{Z}, b|0$ . Indeed,  $0 = b \times 0$ .
- Any integer is divisible by 1 and itself, i.e.  $\forall a \in \mathbb{Z}, 1|a$  and  $a|a$ . Indeed,  $a = 1 \times a = a \times 1$ .
- The only integer divisible by 0 is 0 itself, i.e.  $\forall a \in \mathbb{Z}, 0|a \implies a = 0$ .  
Indeed, then  $a = 0 \times k$  for some  $k \in \mathbb{Z}$  and hence  $a = 0$ .
- When  $b \neq 0$ ,  $b|a$  if and only if the remainder of the Euclidean division of  $a$  by  $b$  is  $r = 0$ .

**Proposition 2.26.**

1.  $\forall a, b \in \mathbb{Z}, (a|b \text{ and } b|a) \implies |a| = |b|$
2.  $\forall a, b, c \in \mathbb{Z}, (a|b \text{ and } b|c) \implies a|c$
3.  $\forall a, b, c, d \in \mathbb{Z}, (a|b \text{ and } c|d) \implies ac|bd$
4.  $\forall a, b, c, \lambda, \mu \in \mathbb{Z}, (a|b \text{ and } a|c) \implies a|(\lambda b + \mu c)$
5.  $\forall a \in \mathbb{Z}, a|1 \implies |a| = 1$

*Proof.*

1. Let  $a, b \in \mathbb{Z}$  satisfying  $a|b$  and  $b|a$ . If  $a = 0$  then  $b = 0$  (from  $0|b$ ). So we may assume that  $a \neq 0$ . There exist  $k, l \in \mathbb{Z}$  such that  $b = ak$  and  $a = bl$ . Then  $a = bl = ak l$ , thus  $1 = kl$  since  $a \neq 0$ . Therefore,  $1 = |1| = |kl| = |k| \times |l|$ . Since  $|k|, |l| \in \mathbb{N}$ , we get that  $|k| = |l| = 1$ . Finally,  $|a| = |bl| = |b| \times |l| = |b| \times 1 = |b|$ .
2. Let  $a, b, c \in \mathbb{Z}$  satisfying  $a|b$  and  $b|c$ . Then  $b = ak$  and  $c = bl$  for some  $k, l \in \mathbb{Z}$ . Therefore  $c = bl = ak l$ , so  $a|c$ .
3. Let  $a, b, c, d \in \mathbb{Z}$  satisfying  $a|b$  and  $c|d$ . Then  $b = ak$  and  $d = cl$  for some  $k, l \in \mathbb{Z}$ . Therefore  $bd = ackl$ , so  $ac|bd$ .
4. Let  $a, b, c \in \mathbb{Z}$  satisfying  $a|b$  and  $a|c$ . Then  $b = ka$  and  $c = la$  for some  $k, l \in \mathbb{Z}$ . Hence  $\lambda b + \mu c = \lambda ka + \mu la = (\lambda k + \mu l)a$ . Thus  $a|(\lambda b + \mu c)$ .
5. Let  $a \in \mathbb{Z}$ . Assume that  $a|1$ . Then  $a|1$  and  $1|a$ . So by the first item,  $|a| = 1$ . ■

**2.5 Greatest common divisor**

**Theorem 2.27.** Given  $a, b \in \mathbb{Z}$  not both zero, the set common divisors of  $a$  and  $b$  admits a greatest element denoted  $\gcd(a, b)$  and called the greatest common divisor of  $a$  and  $b$ .

*Proof.* Let  $a, b \in \mathbb{Z}$  not both zero. We set  $S = \{d \in \mathbb{Z} : d|a \text{ and } d|b\}$ .

- $S$  is non-empty since it contains 1.
- Since  $a$  and  $b$  are not both zero, we know that  $a \neq 0$  or  $b \neq 0$ . Without loss of generality, let assume that  $a \neq 0$ .

Let  $d \in S$  then  $a = dk$  for some  $k \in \mathbb{Z}$ . Note that  $k \neq 0$  (otherwise  $a = dk = 0$ ), hence  $1 \leq |k|$ .

Thus  $d \leq |d| \leq |d| \times |k| = |dk| = |a|$ . Hence  $S$  is bounded from above by  $|a|$ .

Therefore,  $S$  admits a greatest element (as an non-empty subset of  $\mathbb{Z}$  bounded from above). ■

**Remark 2.28.** Note that  $\gcd(a, b) \geq 1$  since 1 is a common divisor of  $a$  and  $b$  (particularly  $\gcd(a, b) \in \mathbb{N}$ ).

**Proposition 2.29.** Let  $a, b \in \mathbb{Z}$  not both zero and  $d \in \mathbb{N} \setminus \{0\}$ . Then

$$\left\{ \begin{array}{l} d|a \\ d|b \\ \forall \delta \in \mathbb{N}, (\delta|a \text{ and } \delta|b) \implies \delta|d \end{array} \right\} \implies d = \gcd(a, b)$$

**Remark 2.30.** We will see later that the converse holds (Proposition 2.35.(3)).

*Proof.* Let  $a, b \in \mathbb{Z}$  not both zero and  $d \in \mathbb{N} \setminus \{0\}$ . Assume that  $d|a$ ,  $d|b$  and that  $d$  is a multiple of every non-negative common divisors, i.e.

$$\forall \delta \in \mathbb{N}, (\delta|a \text{ and } \delta|b) \implies \delta|d$$

Then  $d$  is a common divisor of  $a$  and  $b$ . We need to prove that it is the greatest one.

Let  $\delta \in \mathbb{Z}$  be a common divisor of  $a$  and  $b$ .

- If  $\delta \leq 0$  then  $\delta \leq d$ .
- If  $\delta > 0$  then  $d = \delta k$  for some  $k \in \mathbb{Z}$ .

Note that  $k \geq 1$  since  $d, \delta > 0$ . Thus  $\delta \leq \delta k = d$ . ■

The following theorem is extremely useful! We will use it quite often to study gcd and also when studying modular arithmetic!

**Theorem 2.31** (Bézout's identity). *Given  $a, b \in \mathbb{Z}$  not both zero, there exist  $u, v \in \mathbb{Z}$  such that*

$$au + bv = \gcd(a, b)$$

**Example 2.32.**  $\gcd(15, 25) = 5 = 15 \times 2 + 25 \times (-1)$ .

We will see below an algorithm in order to find a suitable couple  $(u, v)$ .

**Remarks 2.33.**

- The couple  $(u, v)$  is not unique:  $5 = 15 \times 27 + 25 \times (-16)$ .
- The converse is false:  $2 = 3 \times 4 + 5 \times (-2)$  but  $\gcd(3, 5) = 1 \neq 2$ .  
Nonetheless, we will see later that there is a partial converse when  $\gcd(a, b) = 1$ .

*Proof of Theorem 2.31.* Let  $a, b \in \mathbb{Z}$  not both zero. Set  $S = \{n \in \mathbb{N} \setminus \{0\} : \exists u, v \in \mathbb{Z}, n = au + bv\}$ .

Without loss of generality we may assume that  $a \neq 0$ .

Note that  $S$  is not empty. Indeed,

- If  $a < 0$  then  $n = a \times (-1) + b \times 0$  is in  $S$ , or,
- If  $a > 0$  then  $n = a \times 1 + b \times 0$  is in  $S$ .

Thus, by the well-ordering principle,  $S$  admits a least element  $d$ .

Since  $d \in S$ , we know that  $d = au + bv$  for some  $u, v \in \mathbb{Z}$ .

Let's prove that  $d = \gcd(a, b)$ .

- By Euclidean division, there exist  $q, r \in \mathbb{Z}$  such that  $a = dq + r$  and  $0 \leq r < |d| = d$ .  
Assume by contradiction that  $r \neq 0$ .  
Then  $r = a - qd = a - q(au + bv) = a \times (1 - qu) + b \times (-qv)$  is in  $S$ . Which contradicts the fact that  $d$  is the least element of  $S$ . Hence  $r = 0$  and  $a = dq$ , i.e.  $d|a$ .
- Similarly  $d|b$ .
- Let  $\delta \in \mathbb{Z}$  be another common divisor of  $a$  and  $b$ .  
Since  $\delta|a$  and  $\delta|b$ ,  $a = \delta k$  and  $b = \delta l$  for some  $k, l \in \mathbb{Z}$ . Hence  $d = au + bv = \delta(ku + lv)$ , i.e.  $\delta|d$ .

Therefore, by Proposition 2.29,  $d = \gcd(a, b)$ .

Hence  $\gcd(a, b) = au + bv$  as requested. ■

**Proposition 2.34.**  $\forall a \in \mathbb{Z} \setminus \{0\}, \gcd(a, 0) = |a|$

*Proof.* By definition,  $\gcd(a, 0)$  is the greatest divisor of  $a$ .

Since  $a = |a| \times (\pm 1)$ , we know that  $|a|$  is a divisor of  $a$ . We have to check that it is the greatest one.

Let  $d$  be a non-negative divisor of  $a$ , then  $a = dk$  for some  $k \in \mathbb{Z}$ .

Since  $a \neq 0$ , we know that  $k \neq 0$ .

Hence  $1 \leq |k|$  from which we get that  $d \leq d|k| = |d| \times |k| = |dk| = |a|$ . ■

**Proposition 2.35.** *Let  $a, b \in \mathbb{Z}$  not both zero, then*

1.  $\gcd(a, b) = \gcd(b, a)$
2.  $\gcd(a, b) = \gcd(a, -b) = \gcd(-a, b) = \gcd(-a, -b)$
3.  $\forall \delta \in \mathbb{Z}, (\delta|a \text{ and } \delta|b) \implies \delta|\gcd(a, b)$
4.  $\forall \lambda \in \mathbb{Z} \setminus \{0\}, \gcd(\lambda a, \lambda b) = |\lambda| \gcd(a, b)$
5.  $\forall k \in \mathbb{Z}, \gcd(a + kb, b) = \gcd(a, b)$

*Proof.* I will just prove 3, 4 and 5, the first two being easy to prove.

3. Let  $a, b \in \mathbb{Z}$ . Let  $\delta \in \mathbb{Z}$ . Assume that  $\delta|a$  and  $\delta|b$ .  
By Bézout's theorem,  $\gcd(a, b) = au + bv$  for some  $u, v \in \mathbb{Z}$ .  
Since  $\delta|a$  and  $\delta|b$ , we have that  $\delta|au + bv = \gcd(a, b)$ .
4. Let  $a, b \in \mathbb{Z}$  let  $\lambda \in \mathbb{Z} \setminus \{0\}$ . Since  $|\lambda|$  divides  $\lambda a$  and  $\lambda b$ , then it divides  $\gcd(\lambda a, \lambda b)$  by the third item.  
Hence  $\gcd(\lambda a, \lambda b) = |\lambda| \times d$  for some  $d \in \mathbb{Z}$ . Let's prove that  $d = \gcd(a, b)$ .  
Let  $n \in \mathbb{Z}$ , then  $n|a, b \iff |\lambda|n|\lambda a, \lambda b \iff |\lambda|n|\gcd(\lambda a, \lambda b) \iff n|d$ .

5. Let  $a, b, k \in \mathbb{Z}$ .  $\gcd(a, b) | a, b$  hence  $\gcd(a, b) | a + kb$ . Thus  $\gcd(a, b) | \gcd(a + kb, b)$ .  
 Similarly,  $\gcd(a + kb, b) | a + kb, b$  hence  $\gcd(a + kb, b) | a + kb - kb = a$ . Thus  $\gcd(a + kb, b) | \gcd(a, b)$ .  
 Hence  $|\gcd(a + kb, b)| = |\gcd(a, b)|$ . Since they are both non-negative, we get  $\gcd(a + kb, b) = \gcd(a, b)$ . ■

## 2.6 Euclid's algorithm

Euclid's algorithm is an efficient way to compute the gcd of two numbers.

Let  $a, b \in \mathbb{Z}$  not both zero.

*Initialization of the algorithm.* We set  $a_0 := |a|$  and  $b_0 := |b|$ . Note that  $\gcd(a_0, b_0) = \gcd(\pm a, \pm b) = \gcd(a, b)$ .

*Iteration.* Assume that  $a_n, b_n \in \mathbb{Z}$  are already constructed with  $a_n, b_n \geq 0$  not both zero.

- If  $b_n = 0$  then  $\gcd(a_n, b_n) = a_n$  and the algorithm stops.
- Otherwise, by Euclidean division, there exist  $q_n, r_n \in \mathbb{R}$  such that  $a_n = b_n q_n + r_n$  and  $0 \leq r_n < b_n$ .  
 We set  $a_{n+1} := b_n$  and  $b_{n+1} := r_n$ , then  $a_{n+1} = b_n > 0$  and  $0 \leq b_{n+1} < b_n$ .  
 Moreover, using Proposition 2.35.(5),

$$\gcd(a_n, b_n) = \gcd(b_n q_n + r_n, b_n) = \gcd(r_n, b_n) = \gcd(b_n, r_n) = \gcd(a_{n+1}, b_{n+1})$$

We repeat the iterative process with  $a_{n+1}$  and  $b_{n+1}$ .

*Conclusion.* Since the  $b_n$  are natural numbers and  $0 \leq b_{n+1} < b_n$ , there exists  $N \in \mathbb{N}$  such that  $b_N = 0$ . It proves that the algorithm ends after finitely many steps. Furthermore

$$\gcd(a, b) = \gcd(a_0, b_0) = \gcd(a_1, b_1) = \cdots = \gcd(a_N, b_N) = a_N$$

So the algorithm computes  $\gcd(a, b)$  as expected.

**Algorithm:** Euclid's algorithm in pseudocode

**Result:**  $\gcd(a, b)$  where  $a, b \in \mathbb{Z}$  not both zero.

$a \leftarrow |a|$

$b \leftarrow |b|$

**while**  $b \neq 0$  **do**

$r \leftarrow a \% b$  (the remainder of the Euclidean division  $a = bq + r$  with  $0 \leq r < b$ )

$a \leftarrow b$

$b \leftarrow r$

**end**

**return**  $a$

**Example 2.36.** We want to compute  $\gcd(600, -136)$ :

$600 = 136 \times 4 + 56$	$a_0 = 600, \quad b_0 = 136$	$\gcd(600, -136) = \gcd(600, 136)$
$136 = 56 \times 2 + 24$	$a_1 = 136, \quad b_1 = 56$	$\gcd(600, 136) = \gcd(136, 56)$
$56 = 24 \times 2 + 8$	$a_2 = 56, \quad b_2 = 24$	$\gcd(136, 56) = \gcd(56, 24)$
$24 = 8 \times 3 + 0$	$a_3 = 24, \quad b_3 = 8$	$\gcd(56, 24) = \gcd(24, 8)$
	$a_4 = 8, \quad b_4 = 0$	$\gcd(24, 8) = \gcd(8, 0) = 8$

Hence  $\gcd(600, -136) = 8$ .

It is possible to obtain a suitable Bézout's identity from the above algorithm by going backward.

$8 = 56 + 24 \times (-2)$	since $8 = 56 - 24 \times 2$
$= 56 + (136 + 56 \times (-2)) \times (-2)$	since $24 = 136 - 56 \times 2$
$= 136 \times (-2) + 56 \times 5$	
$= 136 \times (-2) + (600 + 136 \times (-4)) \times 5$	since $56 = 600 - 136 \times 4$
$8 = 600 \times 5 + (-136) \times 22$	

## 2.7 Coprime integers

**Definition 2.37.** Let  $a, b \in \mathbb{Z}$  not both zero. We say that  $a$  and  $b$  are *coprime* (or *relatively prime*) if  $\gcd(a, b) = 1$ . The following result states that the converse of Bézout's identity holds **for coprime numbers**.

**Proposition 2.38.** Let  $a, b \in \mathbb{Z}$  not both zero. Then

$$\gcd(a, b) = 1 \Leftrightarrow \exists u, v \in \mathbb{Z}, au + bv = 1$$

*Proof.*

$\Rightarrow$ : it is simply Bézout's identity.

$\Leftarrow$ : let  $a, b \in \mathbb{Z}$  not both zero. Assume that  $au + bv = 1$  for some  $u, v \in \mathbb{Z}$ .

Set  $d = \gcd(a, b)$ . Then  $d|a$  and  $d|b$ , hence  $d|(au + bv) = 1$ . So  $|d| = 1$ . But since  $d \in \mathbb{N}$ , we get that  $d = 1$ . ■

**Theorem 2.39** (Gauss' lemma).  $\forall a, b, c \in \mathbb{Z}, \begin{cases} \gcd(a, b) = 1 \\ a|bc \end{cases} \implies a|c$

*Proof.* Let  $a, b, c \in \mathbb{Z}$  such that  $\gcd(a, b) = 1$  and  $a|bc$ . Then there exists  $k \in \mathbb{Z}$  such that  $bc = ka$ . By Bézout's identity, there exist  $u, v \in \mathbb{Z}$  such that  $1 = au + bv$ .

Thus  $c = (au + bv)c = auc + bcv = auc + kav = a(uc + kv)$ . Hence  $a|c$ . ■

The following result is very useful.

**Proposition 2.40.** Let  $a, b, c \in \mathbb{Z}$ . If  $a|c$ ,  $b|c$  and  $\gcd(a, b) = 1$  then  $ab|c$ .

*Proof.* Since  $a|c$  and  $b|c$ , there exist  $k, l \in \mathbb{Z}$  such that  $c = ak$  and  $c = bl$ .

Since  $\gcd(a, b) = 1$ , by Bézout's identity, there exists  $u, v \in \mathbb{Z}$  such that  $au + bv = 1$ .

Then  $c = auc + bvc = aubl + bvak = ab(ul + vk)$ , so that  $ab|c$ . ■

## 2.8 A diophantine equation

**Theorem 2.41.** Let  $a, b, c \in \mathbb{Z}$  with  $a$  and  $b$  not both zero.

Then the equation  $ax + by = c$  has an integer solution if and only if  $\gcd(a, b)|c$ .

*Proof.*

$\Rightarrow$ : Assume that  $ax + by = c$  for some  $(x, y) \in \mathbb{Z}^2$ .

Since  $\gcd(a, b)|a$  and  $\gcd(a, b)|b$ , we get that  $\gcd(a, b)|ax + by = c$ .

$\Leftarrow$ : Assume that  $\gcd(a, b)|c$ , then there exists  $k \in \mathbb{Z}$  such that  $c = k \gcd(a, b)$ .

By Bézout's identity, there exists  $(u, v) \in \mathbb{Z}^2$  such that  $au + bv = \gcd(a, b)$  hence  $aku + bkv = k \gcd(a, b) = c$ .

Therefore  $(ku, kv)$  is an integer solution of the equation. ■

How to find all the integer solutions of an equation of the form  $ax + by = c$  with  $a \neq 0$ ,  $b \neq 0$  and  $\gcd(a, b)|c$ ?

- **Step 1:** reduction to the case where  $\gcd(a, b) = 1$ .  
There exist  $\tilde{a}, \tilde{b}, \tilde{c} \in \mathbb{Z}$  such that  $a = \tilde{a} \gcd(a, b)$ ,  $b = \tilde{b} \gcd(a, b)$  and  $c = \tilde{c} \gcd(a, b)$ .  
Hence  $ax + by = c \Leftrightarrow \tilde{a}x + \tilde{b}y = \tilde{c}$ .  
Note that  $\gcd(a, b) = \gcd(\tilde{a} \gcd(a, b), \tilde{b} \gcd(a, b)) = \gcd(a, b) \gcd(\tilde{a}, \tilde{b})$ . Hence  $\gcd(\tilde{a}, \tilde{b}) = 1$ .
- **Step 2:** find a first solution.  
By Bézout's identity, there exist  $u, v \in \mathbb{Z}$  such that  $\tilde{a}u + \tilde{b}v = 1$  (we may find such a couple  $(u, v)$  using Euclid's algorithm).  
Thence  $\tilde{a}\tilde{c}u + \tilde{b}\tilde{c}v = \tilde{c}$ . Therefore we obtain a solution  $(x_0, y_0) = (\tilde{c}u, \tilde{c}v)$  of  $\tilde{a}x + \tilde{b}y = \tilde{c}$ .
- **Step 3:** study the other solutions.  
Let  $(x, y) \in \mathbb{Z}^2$  satisfying  $\tilde{a}x + \tilde{b}y = \tilde{c}$ . Then  $\tilde{a}(x - x_0) + \tilde{b}(y - y_0) = 0$ , i.e.  $\tilde{b}(y - y_0) = \tilde{a}(x_0 - x)$ .  
Since  $\tilde{a}|\tilde{b}(y - y_0)$  and  $\gcd(\tilde{a}, \tilde{b}) = 1$ , by Gauss' lemma,  $\tilde{a}|y - y_0$ , i.e. there exists  $k \in \mathbb{Z}$  such that  $k\tilde{a} = y - y_0$ , i.e.  $y = y_0 + k\tilde{a}$ .  
Then  $\tilde{a}(x_0 - x) = \tilde{b}(y - y_0) = k\tilde{a}\tilde{b}$ . Since  $\tilde{a} \neq 0$ , we get  $x_0 - x = k\tilde{b}$ , i.e.  $x = x_0 - k\tilde{b}$ .  
We proved that there exists  $k \in \mathbb{Z}$  such that  $(x, y) = (x_0 - k\tilde{b}, y_0 + k\tilde{a})$ .

- *Step 4: check the converse!*

We proved that if  $(x, y) \in \mathbb{Z}^2$  is a solution, then there exists  $k \in \mathbb{Z}$  such that  $(x, y) = (x_0 - k\tilde{b}, y_0 + k\tilde{a})$ . It means that the solutions are among  $(x, y) \in \{(x_0 - k\tilde{b}, y_0 + k\tilde{a}) : k \in \mathbb{Z}\}$ .

Otherwise stated, it means that  $\{(x, y) \in \mathbb{Z}^2 : \tilde{a}x + \tilde{b}y = \tilde{c}\} \subset \{(x_0 - k\tilde{b}, y_0 + k\tilde{a}) : k \in \mathbb{Z}\}$ .

It doesn't mean that they are all solutions, we need to check that separately, i.e. we need to prove the other inclusion.

Conversely, let's prove that for every  $k \in \mathbb{Z}$ ,  $(x, y) = (x_0 - k\tilde{b}, y_0 + k\tilde{a})$  is a solution:

$$\tilde{a}(x_0 - k\tilde{b}) + \tilde{b}(y_0 + k\tilde{a}) = \tilde{a}x_0 + \tilde{b}y_0 = \tilde{c}$$

- *Step 5: Conclusion!*

The solutions are exactly the  $(x, y) = (x_0 - k\tilde{b}, y_0 + k\tilde{a})$  for  $k \in \mathbb{Z}$ .

**Example 2.42.** We want to solve  $20x + 16y = 500$  for  $(x, y) \in \mathbb{Z}$ .

1. Note that  $\gcd(20, 16) = 4 \mid 500$ , hence this equation admits a solution.  
Moreover, dividing by 4, we get that  $20x + 16y = 500 \Leftrightarrow 5x + 4y = 125$ .
2. Let's find a first solution starting from a Bézout relation  $5u + 4v = 1$ .  
In this example, there is an obvious Bézout relation:  $5 \times 1 + 4 \times (-1) = 1$ .  
(otherwise, we can use Euclid's algorithm to find one)  
Hence  $5 \times 125 + 4 \times (-125) = 125$ . So  $(125, -125)$  is a solution
3. Let's find all the solutions.  
Let  $(x, y)$  be a solution then  $5x + 4y = 125$  and  $5 \times 125 + 4 \times (-125) = 125$ .  
Thus  $5(x - 125) + 4(y + 125) = 0$ , so  $4 \mid 5(x - 125)$ .  
Since  $\gcd(4, 5) = 1$ , by Gauss' lemma,  $4 \mid x - 125$ . So  $x = 4k + 125$  for some  $k \in \mathbb{Z}$ .  
Then  $5(4k) + 4(y + 125) = 0$ , i.e.  $5k + y + 125 = 0$ , so that  $y = -5k - 125$ .  
Therefore  $(x, y) = (4k + 125, -5k - 125)$ .
4. Conversely,  $(4k + 125, -5k - 125)$  is a solution for every  $k \in \mathbb{Z}$ :  
indeed,  $20x + 16y = 20(4k + 125) + 16(-5k - 125) = 500$ .
5. Conclusion: the solutions are  $(4k + 125, -5k - 125)$ ,  $k \in \mathbb{Z}$ .

For general diophantine equations, there are no recipes (Fermat's Last Theorem is about some diophantine equations and took 4 centuries to be solved).

**Example 2.43.** We want to find integer solutions of  $x^2 - y^2 = 401$ .

Note that  $x^2 - y^2 = 401 \Leftrightarrow (x - y)(x + y) = 401$ .

Since 401 is a prime number (I am sure you can look in the future for next Thursday lecture), then

$$\text{either } \begin{cases} x - y = 1 \\ x + y = 401 \end{cases} \quad \text{or} \quad \begin{cases} x - y = -1 \\ x + y = -401 \end{cases} \quad \text{or} \quad \begin{cases} x - y = 401 \\ x + y = 1 \end{cases} \quad \text{or} \quad \begin{cases} x - y = -401 \\ x + y = -1 \end{cases}$$

So either  $(x, y) = (201, 200)$ , or  $(x, y) = (-201, -200)$  or  $(x, y) = (201, -200)$  or  $(x, y) = (-201, 200)$ .

## Appendix 2.A Properties of the strict order

Recall that given  $a, b \in \mathbb{Z}$ ,  $a < b$  means  $(a \leq b \text{ and } a \neq b)$ .

The following properties of  $<$  are easy to derive from the ones of  $\leq$ .

- $\forall a, b, c \in \mathbb{Z}, (a < b \text{ and } b \leq c) \implies a < c$
- $\forall a, b, c \in \mathbb{Z}, (a \leq b \text{ and } b < c) \implies a < c$
- $\forall a, b, c, d \in \mathbb{Z}, (a < b \text{ and } c \leq d) \implies a + c < b + d$
- $\forall a, b, c \in \mathbb{Z}, a < b \implies a + c < b + c$   
(that's a special case of the previous one where  $d = c$ )
- $\forall a, b, c \in \mathbb{Z}, (a < b \text{ and } c > 0) \implies ac < bc$
- $\forall a, b, c \in \mathbb{Z}, (a < b \text{ and } c < 0) \implies ac > bc$
- $\forall a, b \in \mathbb{Z}, a < b \Leftrightarrow a + 1 \leq b$
- Given  $a, b \in \mathbb{Z}$ , exactly one of the following occurs:
  - (i)  $a < b$
  - (ii)  $a = b$
  - (iii)  $a > b$

Particularly, the negation of  $a \leq b$  is  $a > b$ .

## Appendix 2.B Implementation of Euclid's algorithm in Julia

Euclid's algorithm in Julia (iterative)

```

1 function euclid(a::Integer, b::Integer)
2     a != 0 || b != 0 || error("a and b must not be both zero")
3     a = abs(a)
4     b = abs(b)
5     while b != 0
6         r = a%b
7         a = b
8         b = r
9     end
10    return a
11 end

```

Actually, it is not important to replace  $a$  and  $b$  by their respective absolute values in the initialization. In this case, the sequence  $(b_n)$  is eventually non-negative so the algorithm stops as earlier and we just have to make sure that we return the absolute value of  $a$  at the end.

That being said, you should be careful because most programming languages don't use the above convention for Euclidean division. Instead, they require the remainder  $r$  to have the same sign as  $b$ , i.e.  $r$  satisfies  $0 \leq r < b$  if  $b > 0$  or  $b < r \leq 0$  if  $b < 0$ .

But it doesn't matter for Euclid's algorithm: indeed, with this convention, the sequence  $|b_n|$  is still decreasing, so the algorithm stops.

Therefore, we can simply write the following program (here  $\text{gcd}(0, 0) = 0$  by convention).

Euclid's algorithm in Julia (recursive)

```

1 function euclid(a::Integer, b::Integer)
2     b != 0 || return abs(a)
3     return euclid(b, a%b)
4 end

```



## Exercises

### Exercise 1.

Let  $a, b \in \mathbb{Z}$ . Prove that if  $a^2 = b^2$  then  $|a| = |b|$ .

### Exercise 2.

Let  $n \in \mathbb{N} \setminus \{0\}$ . Prove that given  $n$  consecutive integers, one is divisible by  $n$ .

*The above result is very useful and from now on you can use it without proving it again.*

### Exercise 3.

1. Compute  $\gcd(816, 2260)$ .
2. Find  $(u, v) \in \mathbb{Z}^2$  such that  $816u + 2260v = \gcd(816, 2260)$ .

### Exercise 4.

1. Does the divisibility relation  $|$  define an order on  $\mathbb{Z}$ ? If so, is it total?
2. Does the divisibility relation  $|$  define an order on  $\mathbb{N}$ ? If so, is it total?

### Exercise 5.

Prove that  $\forall n \in \mathbb{N}, 7 \mid 3^{2n+1} + 2^{4n+2}$

### Exercise 6.

Let  $a, b, c, d \in \mathbb{Z}$  be such that  $ad + bc \neq 0$ . Prove that if  $ad + bc$  divides  $a, b, c, d$  then  $|ad + bc| = 1$ .

### Exercise 7.

Prove that  $\forall n \in \mathbb{N}, \gcd(n^2 + n, 2n + 1) = 1$

### Exercise 8.

Let  $a, b \in \mathbb{Z}$ . Prove that if  $\gcd(a, b) = 1$  then  $\gcd(a^2, b^2) = 1$ .

### Exercise 9.

Prove that

1.  $\forall a, b \in \mathbb{Z} \setminus \{0\}, a^2 \mid b^2 \implies a \mid b$
2. Prove that  $\forall a, b, c \in \mathbb{Z} \setminus \{0\}, \gcd(a, b) = 1$  and  $c \mid b \implies \gcd(a, c) = 1$

### Exercise 10.

For each of the following statements: is it true? If so, prove it. Otherwise, give a counter-example.

1. If  $a, b \in \mathbb{Z}$  are coprime then  $a + b$  and  $ab$  are too.
2. If  $a, b \in \mathbb{Z}$  are coprime then  $a + b$  and  $a^2 + b^2$  are too.

*We say that  $a$  and  $b$  are coprime if  $\gcd(a, b) = 1$ .*

### Exercise 11.

Seven friends have a dinner in a restaurant. When he brings the bill, the waiter makes the following offer: "I'll put on each of your foreheads a sticky note with a day of the week<sup>2</sup> written on it, so that each of you will see the other six notes but not yours. Then you will have to guess the day written on your note (by secretly writing your guess on your napkin). If at least one of you has the correct answer, then the bill is on me. By the way, there is no rule concerning my choices for the days, for instance I can assign several times the same day."

While the waiter left to write the sticky notes, one of the friends, who happens to be a mathematician, exclaims: "I found a way so that we are 100% sure that one of us is correct!"

And then he explains his winning strategy to his friends.

Can you guess what it is?

---

<sup>2</sup>Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.

**Exercise 12.**

1. Prove that among 42 distinct integers, there are always two distinct integers  $a$  and  $b$  such that  $b - a$  is a multiple of 41.
2. Prove that among five integers, there are always three with sum divisible by 3.

**Exercise 13.**

Compute  $\gcd(3^{123} - 5, 25)$ .

**Exercise 14.**

Prove that  $\forall n \in \mathbb{Z}, 6 \mid n(n+1)(n+2)$

**Exercise 15.**

1. Prove that  $\forall n \in \mathbb{Z}, \gcd(2n, 2n+2) = 2$ .
2. Prove that  $\forall n \in \mathbb{Z}, \gcd(2n-1, 2n+1) = 1$ .
3. Prove that for  $a, b \in \mathbb{Z}$  not both zero,  $\gcd(5a+3b, 13a+8b) = \gcd(a, b)$ .

**Exercise 16.**

Find all the integer solutions of

- (a)  $xy = 2x + 3y$       (b)  $\frac{1}{x} + \frac{1}{y} = \frac{1}{5}$       (c)  $x + y = xy$   
 (d)  $9x + 15y = 11$       (e)  $9x + 15y = 18$       (f)  $1665x + 1035y = 45$

**Exercise 17.**

1. Prove that if  $a, b \in \mathbb{Z}$  are not both zero then there exist  $a', b' \in \mathbb{Z}$  such that  $\gcd(a', b') = 1$ , and  $a = da'$  and  $b = db'$  where  $d = \gcd(a, b)$ .
2. Prove that  $\forall a, b, c \in \mathbb{Z} \setminus \{0\}, c \mid ab \implies c \mid (\gcd(a, c) \gcd(b, c))$

**Exercise 18.**

1. Prove *Sophie Germain's identity*:  $a^4 + 4b^4 = ((a+b)^2 + b^2)((a-b)^2 + b^2)$ .
2. Prove that  $3^{44} + 4^{29}$  is a composite number.
3. Prove that for every natural number  $n > 1$ ,  $n^4 + 4^n$  is a composite number.  
*Hint: study the parity of  $n$ .*

**Exercise 19.**

Prove that there are infinitely many integers that can't be written as the sum of a square with a prime number.

*Hint: look at  $(3k+2)^2$  for  $k \in \mathbb{N} \setminus \{0\}$ .*

**Exercise 20.**

Prove that  $\forall n \in \mathbb{N}, n \mid (n-1)! + 1 \implies n$  is prime.

**Exercise 21.**

Let  $n \in \mathbb{N} \setminus \{0\}$ . Find  $n$  consecutive natural numbers such that none of them is a prime number.

**Exercise 22.**

Prove that the following numbers are not rationals using the prime factorization theorem.

1.  $\log_{10} 2$
2.  $\sqrt{2}$

For this question you can use what you know about  $\mathbb{Q}$  and  $\mathbb{R}$ .

**Exercise 23.**

Prove that  $\forall n \in \mathbb{Z}, 49 \nmid n^3 - n^2 - 2n + 1$

**Exercise 24.**

Prove that there are infinitely many prime numbers of the form  $p = 4k + 3$  where  $k \in \mathbb{N}$ .

**Exercise 25.** *Goldbach's theorem about Fermat numbers*

1. Prove that  $\forall n \in \mathbb{N}, \forall k \in \mathbb{N} \setminus \{0\}, 2^{2^{n+k}} - 1 = (2^{2^n} - 1) \times \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1)$ .
2. Let  $m, n \in \mathbb{N}$ . Prove that if  $m \neq n$  then  $2^{2^m} + 1$  and  $2^{2^n} + 1$  are coprime.

**Exercise 26.**

Let  $a, n \geq 2$  be two natural numbers.

1. Prove that if  $a^n - 1$  is prime then  $a = 2$  and  $n$  is prime.  
A number of the form  $M_n = 2^n - 1$  is called a Mersenne number.
2. Is the converse true?

**Exercise 27.**

Three brothers inherit  $n$  gold pieces weighing  $1, 2, \dots, n$ .

For what  $n \in \mathbb{N} \setminus \{0\}$  can they be split into three equal heaps?

**Exercise 28.**

A sea pirate wants to share a treasure with its sailors.

The treasure is made of 69 diamonds, 1150 pearls and 4140 gold coins.

He is able to share fairly the treasure such that everyone (including himself) receive the same amount of each object.

How many sailors are there?

## Chapter 3

# Prime numbers

Informally, prime numbers are the integers greater than 1 which can't be factorized further. More precisely they are the natural numbers admitting exactly two positive divisors. Otherwise stated, a natural number  $n \geq 2$  is a prime number if and only if its only positive divisors are 1 and  $n$  itself.

They play a crucial role in number theory since every natural number admit a unique expression as a product of prime numbers. They will also appear quite often later when we will study modular arithmetic.

All the results presented below were already known in *Euclid's Elements* (circa 300BC). Nonetheless, there are still many conjectures involving prime numbers which are easy to state but still open (some of them despite several centuries of attempts). For instance:

- *Goldbach conjecture* (1742): any even natural number greater than 2 may be written as a sum of two prime numbers (e.g.  $4 = 2 + 2$ ,  $6 = 3 + 3$ ,  $8 = 5 + 3$ ,  $10 = 5 + 5 = 7 + 3 \dots$ ).
- *The twin prime conjecture* (1849): there are infinitely many prime numbers  $p$  such that  $p+2$  is also prime (e.g.  $(3, 5)$ ,  $(5, 7)$ ,  $(11, 13) \dots$ ).
- *Legendre conjecture* (1912): given  $n \in \mathbb{N} \setminus \{0\}$ , we may always find a prime between  $n^2$  and  $(n+1)^2$ .

### 3.1 Prime numbers

**Definition 3.1.** We say that a natural number  $p$  is a *prime number* if it has exactly two distinct positive divisors. A positive natural number with more than 2 positive divisors is said to be a *composite number*.

**Remark 3.2.**

- 0 is not a prime number since any natural number is a divisor of 0.
- 1 is not a prime number because it has only one positive divisor.

Hence a natural number  $p$  is prime if and only if  $p \geq 2$  and the only positive divisors of  $p$  are 1 and  $p$ .

**Example 3.3.** The first prime numbers are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97...

We face two natural questions:

1. How to check whether a natural number is a prime number?
2. How many prime numbers are there?

**Proposition 3.4.** Let  $n \in \mathbb{N}$ . Then  $n$  is composite if and only if there exist  $a, b \in \mathbb{N} \setminus \{0, 1\}$  such that  $n = ab$ .

*Proof.* Let  $n \in \mathbb{N}$ .

$\Rightarrow$  assume that  $n$  is a composite number, then it admits a divisor  $k \in \mathbb{N}$  such that  $k \neq 1$  and  $k \neq n$ .

So  $n = km$  for some  $m \in \mathbb{N}$ . Note that  $k, m \neq 0$  since otherwise  $n = 0$ . Note that  $m \neq 1$  since otherwise  $k = n$ .

$\Leftarrow$  Assume that  $n = ab$  for some  $a, b \in \mathbb{N} \setminus \{0, 1\}$ .

Note that  $a \neq n$ , since otherwise  $b = 1$  and that  $n \neq 1$  since otherwise  $a|1$ , i.e.  $a = 1$ .

Therefore 1,  $a$ ,  $n$  are three distinct positive divisors of  $n$ , so that  $n$  is a composite number. ■

**Proposition 3.5.** *A composite number  $a$  admits a positive divisor  $b$  such that  $1 < b^2 \leq a$ .*

*Proof.* Write  $a = b_1 b_2$  for some  $b_1, b_2 \in \mathbb{N} \setminus \{0, 1\}$ . Then  $b_1^2, b_2^2 > 1$ .

Assume by contradiction that both  $b_1^2 > a$  and  $b_2^2 > a$ . Then  $a^2 = (b_1 b_2)^2 = b_1^2 b_2^2 > a^2$ . Hence a contradiction. ■

**Example 3.6.** We want to prove that 97 is a prime number.

Since  $10^2 = 100 > 97$ , it is enough to check that none of 2, 3, 4, 5, 6, 7, 8 and 9 are divisors of 97.

We will see later criteria to check divisibility.

**Lemma 3.7.** *A natural number  $n \geq 2$  has at least one prime divisor.*

*Proof.* We are going to prove with a strong induction that every natural number  $n \geq 2$  has a prime divisor.

**Base case at  $n = 2$ :** 2 admits a prime divisor (itself).

**Induction step:** assume that all the natural numbers  $2, \dots, n$  admit a prime divisor for some  $n \geq 2$ .

- First case:  $n + 1$  is a prime number, then it has a prime divisor (itself).
- Second case:  $n + 1$  is a composite, then  $n + 1 = ab$  where  $a, b \in \mathbb{N} \setminus \{0, 1\}$ .

Note that  $a \neq n + 1$  since otherwise  $b = 1$ .

Since  $2 \leq a \leq n$ ,  $a$  admits a prime divisor  $p$  by the induction hypothesis, i.e.  $a = pk$  for some  $k \in \mathbb{N}$ .

Then  $n + 1 = ab = pkb$ . Thus the prime number  $p$  is a divisor of  $n + 1$ .

Which proves the induction step. ■

**Theorem 3.8.** *There are infinitely many prime numbers.*

*Proof.* Assume by contradiction that there exist only finitely many prime numbers  $p_1, p_2, \dots, p_n$ .

We set  $q = p_1 p_2 \dots p_n + 1$ . By Lemma 3.7,  $q$  has a prime divisor. Thus there exists  $i \in \{1, 2, \dots, n\}$  such that  $p_i | q$ .

Then, since  $p_i | p_1 p_2 \dots p_n$  and  $p_i | q$ , we have that  $p_i | (q - p_1 p_2 \dots p_n)$ , i.e.  $p_i | 1$ .

Therefore  $p_i = 1$ , which is a contradiction because 1 is not a prime number. ■

## 3.2 The fundamental theorem of arithmetic

**Lemma 3.9** (Euclid's lemma). *Let  $a, b \in \mathbb{Z}$  and  $p$  be a prime number. If  $p | ab$  then  $p | a$  or  $p | b$  (or both).*

*Proof.* Let  $a, b \in \mathbb{Z}$  and  $p$  be a prime number such that  $p | ab$ .

Assume that  $p \nmid a$  then  $\gcd(a, p) = 1$  since the only positive divisors of  $p$  are 1 and itself.

Hence, by Gauss' lemma,  $p | b$ . ■

**Theorem 3.10** (The fundamental theorem of arithmetic). *Any integer greater than 1 can be written as a product of primes, moreover this expression as a product of primes is unique up to the order of the prime factors.*

**Remark 3.11.** The above theorem states two things: the **existence** of a prime factorization, and its **uniqueness**.

*Proof.*

- **Existence.** We are going to prove with a strong induction that  $n \geq 2$  admits a prime factorization.

*Base case for  $n = 2$ :* 2 is a prime number, so there is nothing to do.

*Induction step:* assume that all the integers  $2, 3, \dots, n$  have a prime factorization for some  $n \geq 2$ .

We want to prove that  $n + 1$  admits a prime factorization.

By Lemma 3.7,  $n + 1$  admits a prime factor, so  $n + 1 = pk$  where  $p$  is a prime number and  $k \in \mathbb{N} \setminus \{0\}$ .

If  $k = 1$  then there is nothing to do. So we may assume that  $k \geq 2$ .

Since  $1 < p$ , we have that  $k < pk = n + 1$ .

Since  $2 \leq k \leq n$ , by the induction hypothesis,  $k$  admits a prime factorization  $k = p_1 p_2 \dots p_l$ .

Finally  $n + 1 = p p_1 p_2 \dots p_l$ , which proves the induction step.

- **Uniqueness (up to order).**

Assume by contradiction that there exists an integer greater than 1 with (at least) two distinct prime factorizations. Denote by  $n$  the least such integer (which exists by the well-ordering principle).

Let  $n = p_1 p_2 \dots p_r$  and  $n = q_1 q_2 \dots q_s$  be two distinct prime factorizations of  $n$ .

Then  $p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ .

By Euclid's lemma  $p_1$  divides one of the  $q_j$ .

Up to reordering the indices, we may assume that  $p_1 | q_1$ .

Since  $q_1$  is a prime number, either  $p_1 = 1$  or  $p_1 = q_1$ .

And thus  $p_1 = q_1$  since  $p_1$  is also a prime number (and 1 is not).

Therefore, by cancellation,  $m = p_2 \dots p_r = q_2 \dots q_s$  is a number with two distinct prime factorizations.

Note that  $m > 1$  since otherwise  $n = p_1 = q_1$  is not two distinct prime factorizations.

And, since  $1 < p_1$  we get that  $m = p_2 \dots p_r < p_1 p_2 \dots p_r = n$ .

Which contradicts the fact that  $n$  is the least integer greater than 1 with two prime factorizations. ■

**Corollary 3.12.** Any natural number  $n \in \mathbb{N} \setminus \{0\}$  admits a unique expression  $n = \prod_{p \text{ prime}} p^{\alpha_p}$  where  $\alpha_p \in \mathbb{N}$

(i.e. the  $\alpha_p$  are uniquely determined).

**Remarks 3.13.**

- The above product is finite since all but finitely many exponents are equal to 0.
- 1 is the special case when  $\alpha_p = 0$  for all prime numbers  $p$ .

**Example 3.14.**  $60798375 = 3^2 \times 5^3 \times 11 \times 17^3$

**Corollary 3.15.** Write  $a = \prod_{p \text{ prime}} p^{\alpha_p}$  and  $b = \prod_{p \text{ prime}} p^{\beta_p}$  with  $\alpha_p, \beta_p \in \mathbb{N}$  all but finitely many equal to 0. Then

- $a|b$  if and only if for every prime number  $p$ ,  $\alpha_p \leq \beta_p$ .
- $\gcd(a, b) = \prod_{p \text{ prime}} p^{\min(\alpha_p, \beta_p)}$ .

**Example 3.16.**  $\gcd(3^2 \times 5^3 \times 11 \times 17^3, 3 \times 5^5 \times 17^2 \times 23) = 3 \times 5^3 \times 17^2$

**Corollary 3.17.** Write  $n = \prod_{p \text{ prime}} p^{\alpha_p}$  with  $\alpha_p \in \mathbb{N}$  all but finitely many equal to 0. Then the positive divisors of  $n$  are exactly the numbers of the form  $n = \prod_{p \text{ prime}} p^{\gamma_p}$  with  $0 \leq \gamma_p \leq \alpha_p$  for all prime numbers  $p$ .

Particularly,  $n$  has  $\prod_{p \text{ prime}} (\alpha_p + 1)$  positive divisors.

## Exercises

### Exercise 1.

1. Prove that  $\forall n \in \mathbb{N}, 5|2^{2n+1} + 3^{2n+1}$
2. Prove that  $\forall n \in \mathbb{N}, 17|2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1}$

### Exercise 2.

Find all the  $x \in \mathbb{Z}$  such that  $x^2 + 3 \equiv 0 \pmod{7}$ .

### Exercise 3.

1. Determine the remainder of the Euclidean division of  $2^n$  by 5 for  $n \in \mathbb{N}$ .
2. Determine the remainder of  $1357^{2021}$  by 5.

### Exercise 4.

1. Find a criterion for divisibility by 5.
2. Find a criterion for divisibility by 8.  
Use it on 958547 and on 123456789336.
3. Find a criterion for divisibility by 11.  
Use it on 123456789 and 715.

### Exercise 5.

1. Find the integer solutions of  $x^2 - 5y^2 = 3$ .
2. Find the integer solutions of  $15x^2 - 7y^2 = 9$ .
3. Find the integer solutions of  $x^2 + y^2 = 4003$  (Hint: work modulo 4).

### Exercise 6.

Prove that  $13|3^{126} + 5^{126}$ .

### Exercise 7.

- For which  $n \in \mathbb{N}$ , is it true that  $8|3^n + 4n + 1$ ?
- For which  $n \in \mathbb{N}$ , is it true that  $21|2^{2^n} + 2^n + 1$ ?

### Exercise 8.

1. Prove that  $\forall a, b \in \mathbb{Z}, (3|a \text{ and } 3|b) \Leftrightarrow 3|(a^2 + b^2)$ .
2. Prove that  $\forall a, b \in \mathbb{Z}, (7|a \text{ and } 7|b) \Leftrightarrow 7|(a^2 + b^2)$ .
3. Prove that  $\forall a, b \in \mathbb{Z}, 21|(a^2 + b^2) \implies 441|(a^2 + b^2)$ .

### Exercise 9.

Compute  $\gcd(2^{445} + 7, 15)$ .

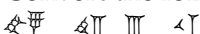
### Exercise 10.

Find all the prime numbers  $p$  such that  $2^p + p^2$  is also prime.

### Exercise 11.

What is the last digit in the decimal expansion of  $7^{3^{84}}$ ?

### Exercise 12.

1. Convert the following number from the Babylonian cuneiform numeral system to base 10:  

2. Convert the following number from decimal to the Babylonian cuneiform numeral system: 42137.
3. Convert the following number from hexadecimal (with digits 0, 1, 2, ..., 9, A, B, ..., F) to base 10:  $\overline{F420C}^{16}$ .
4. Convert the following number from decimal to hexadecimal: 11211.
5. Compute in hexadecimal (without converting to decimal):  $\overline{9AB7}^{16} + \overline{3C0D}^{16}$ .
6. Perform the above computation using decimals. Is it easier?

**Exercise 13.**

The scene takes place on an island inhabited by chameleons which are either blue, green, or red.

When two chameleons of different colors meet, they both change to the third color (for instance, if a green chameleon and a red chameleon meet, then they both become blue).

Cherge, one of the chameleons, is a retired mathematician who likes funny mathematical riddles and tongue twisters. While he stands at the highest place on the island, he is able to see all the chameleons: 17 of them are blue, 15 are green and 13 are red (including himself).

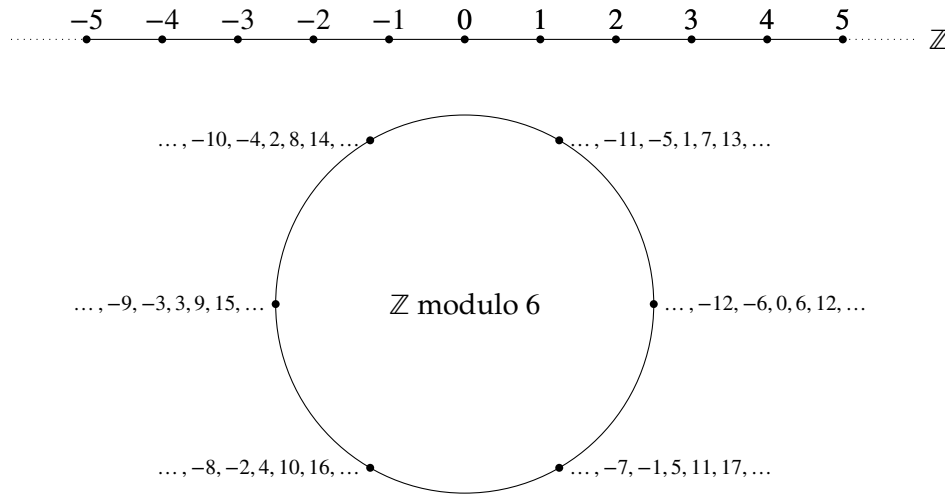
Then he wonders about a new riddle "*Could the island become monochromatic?*". What do you think?



## Chapter 4

# Modular arithmetic

Modular arithmetic was introduced by Gauss during the beginning of the 19th century. Working modulo a natural number  $n > 0$  means that, given an integer  $a$ , we identify it with its remainder  $r$  for the Euclidean division by  $n$ . Basically, it means that we *force*  $a$  to be equal to  $r$  (of course, not as integers, but equal *modulo*  $n$ ). Informally, we wind  $\mathbb{Z}$  on itself as represented below.



This extra layer of abstraction allowed Gauss, and subsequently other mathematicians, to obtain simpler proofs of already known results concerning integers but also to prove new theorems, simply by introducing this new efficient notation which has many good properties.

### 4.1 Congruences

**Definition 4.1.** We say that a binary relation  $\mathcal{R}$  on a set  $E$  is an *equivalence relation* if

- (i)  $\forall x \in E, x\mathcal{R}x$  (*reflexivity*)
- (ii)  $\forall x, y \in E, x\mathcal{R}y \implies y\mathcal{R}x$  (*symmetry*)
- (iii)  $\forall x, y, z \in E, (x\mathcal{R}y \text{ and } y\mathcal{R}z) \implies x\mathcal{R}z$  (*transitivity*)

**Definition 4.2.** Let  $n \in \mathbb{N} \setminus \{0\}$  and  $a, b \in \mathbb{Z}$ . We say that  $a$  and  $b$  are *congruent modulo*  $n$  if  $n|a - b$ , which we denote by  $a \equiv b \pmod{n}$ .

**Proposition 4.3.** Congruence modulo  $n$  is an equivalence relation on  $\mathbb{Z}$ .

*Proof.*

- *Reflexivity.* Let  $a \in \mathbb{Z}$  then  $n|0 = a - a$ . Hence  $a \equiv a \pmod{n}$ .
- *Symmetry.* Let  $a, b \in \mathbb{Z}$  be such that  $a \equiv b \pmod{n}$ . Then  $n|b - a = -(a - b)$  hence  $b \equiv a \pmod{n}$ .
- *Transitivity.* Let  $a, b, c \in \mathbb{Z}$  be such that  $a \equiv b \pmod{n}$  and  $b \equiv c \pmod{n}$ . Then  $n|a - b$  and  $n|b - c$ . Hence  $n|a - c = (a - b) + (b - c)$ . Thus  $a \equiv c \pmod{n}$ . ■

**Proposition 4.4.** Let  $n \in \mathbb{N} \setminus \{0\}$  and  $a, b \in \mathbb{Z}$ . Then  $a \equiv b \pmod{n}$  if and only if  $a$  and  $b$  have same remainder for the Euclidean division by  $n$ .

*Proof.*

$\Rightarrow$ . Assume that  $a \equiv b \pmod{n}$ , then  $b - a = kn$  for some  $k \in \mathbb{Z}$ . By Euclidean division,  $a = nq + r$  for  $q, r \in \mathbb{Z}$  satisfying  $0 \leq r < n$ . Hence  $b = a + kn = nq + r + kn = (q + k)n + r$ .

$\Leftarrow$ . Assume that  $a$  and  $b$  have same remainder for the Euclidean division by  $n$ , then  $a = nq_1 + r$  and  $b = nq_2 + r$  where  $q_1, q_2, r \in \mathbb{Z}$  with  $0 \leq r < n$ .

Hence  $a - b = nq_1 + r - (nq_2 + r) = n(q_1 - q_2)$ . Thus  $n|a - b$ , i.e.  $a \equiv b \pmod{n}$ . ■

**Proposition 4.5.** Let  $n \in \mathbb{N} \setminus \{0\}$  and  $a \in \mathbb{Z}$ . Then  $a$  is congruent modulo  $n$  to exactly one element of  $\{0, 1, \dots, n-1\}$ .

*Proof.* By Euclidean division  $a = nq + r$  where  $0 \leq r < n$  so that  $a \equiv r \pmod{n}$ .

Conversely, if  $a \equiv r' \pmod{n}$  where  $r' \in \{0, 1, \dots, n-1\}$ , then  $a - r' = nq$  for some  $q \in \mathbb{Z}$ . So  $a = nq + r'$ .

By uniqueness of the Euclidean division,  $r = r'$ . ■

**Proposition 4.6.** Let  $a, b, c, d \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Assume that  $a \equiv b \pmod{n}$  and that  $c \equiv d \pmod{n}$  then

- $a + c \equiv b + d \pmod{n}$
- $ac \equiv bd \pmod{n}$

*Proof.* Let  $a, b, c, d \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Assume that  $a \equiv b \pmod{n}$  and that  $c \equiv d \pmod{n}$ . Hence  $a - b = nk$  and  $c - d = nl$  for some  $k, l \in \mathbb{Z}$ . Then

- $(a + c) - (b + d) = (a - b) + (c - d) = nk + nl = n(k + l)$ , hence  $a + c \equiv b + d \pmod{n}$ .
- $ac - bd = (b + nk)(d + nl) - bd = bnl + dnk + n^2kl = n(bl + dk + nkl)$ , hence  $ac \equiv bd \pmod{n}$ . ■

**Example 4.7.**  $1729 \times 16 \equiv 12 \times (-1) \pmod{17} \equiv -12 \pmod{17} \equiv 5 \pmod{17}$

**Corollary 4.8.** Let  $a, b \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Then  $\forall k \in \mathbb{N}$ ,  $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$ .

*Proof.* We prove the statement by induction on  $k$ .

Base case at  $k = 0$ :  $a^0 = b^0 = 1$  hence  $a^0 \equiv b^0 \pmod{n}$ .

Induction step: assume that  $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$  for some  $k \in \mathbb{N}$ .

If  $a \equiv b \pmod{n}$  then by induction hypothesis we also have  $a^k \equiv b^k \pmod{n}$ . Hence, combining both previous congruences, we get that  $a^k a \equiv b^k b \pmod{n}$ , i.e.  $a^{k+1} \equiv b^{k+1} \pmod{n}$ . Which proves the induction step. ■

**Remark 4.9.** Therefore addition, subtraction (which is a special case of addition in  $\mathbb{Z}$ ), multiplication and exponentiation are compatible with congruences.

Beware: division is **not** compatible with congruences:  $10 \equiv 4 \pmod{6}$  but  $5 \not\equiv 2 \pmod{6}$ .

**Proposition 4.10.** Let  $a \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Then  $a$  has a multiplicative inverse modulo  $n$  if and only if  $\gcd(a, n) = 1$ .

Otherwise stated,

$$\exists b \in \mathbb{Z}, ab \equiv 1 \pmod{n} \Leftrightarrow \gcd(a, n) = 1$$

*Proof.*  $\exists b \in \mathbb{Z}, ab \equiv 1 \pmod{n} \Leftrightarrow \exists b, c \in \mathbb{Z}, ab + nc = 1 \Leftrightarrow \gcd(a, n) = 1$  ■

**Remark 4.11.** Then the multiplicative inverse is unique modulo  $n$ . Indeed if  $ab \equiv 1 \pmod{n} \equiv ab' \pmod{n}$  then  $n|(b - b')a$ . Since  $\gcd(a, n) = 1$ , using Gauss' lemma, we get that  $n|b - b'$ , i.e.  $b \equiv b' \pmod{n}$ .

**Remark 4.12.** There is no cancellation law for congruences. For instance,  $50 \equiv 20 \pmod{15}$  but  $5 \not\equiv 2 \pmod{15}$ .

Nonetheless, we have the following proposition.

**Proposition 4.13.** Let  $n \in \mathbb{N} \setminus \{0\}$  and  $a, x, y \in \mathbb{Z}$  satisfying  $ax \equiv ay \pmod{n}$  and  $\gcd(a, n) = 1$ . Then  $x \equiv y \pmod{n}$ .

*Proof.* Since  $\gcd(a, n) = 1$ ,  $a$  admits an inverse modulo  $n$ , i.e. there exists  $b \in \mathbb{Z}$  such that  $ab \equiv 1 \pmod{n}$ .

Then  $ax \equiv ay \pmod{n} \implies bax \equiv bay \pmod{n} \implies x \equiv y \pmod{n}$ . ■

## 4.2 Applications: divisibility criteria

In our everyday life, we usually use a base ten positional notation. It allows use to write all natural numbers using only 10 digits although  $\mathbb{N}$  is infinite. The idea is that the position of a digit changes its value.

Indeed, using the well-ordering principle and Euclidean division, it is possible to prove that any  $n \in \mathbb{N}$  can be uniquely written as  $n = \sum_{k=0}^r a_k 10^k$  where  $a_k \in \{0, 1, \dots, 9\}$  and  $a_r \neq 0$  (see the appendix for a proof).

We usually write  $\overline{a_r a_{r-1} \dots a_0}^{10}$  for  $\sum_{k=0}^r a_k 10^k$  but we may omit the line over the digits when there is no possible confusion. For instance,  $590743 = 5 \times 10^5 + 9 \times 10^4 + 0 \times 10^3 + 7 \times 10^2 + 4 \times 10^1 + 3 \times 10^0$ .

Note that we also use other bases: base 2 and base 16 are quite common nowadays in computer sciences. And other bases were also commonly used by human beings in various places in the past: we still have the influence of a base 60 positional system when describing time (1 hour is 60 minutes), and the influence of a base 20 positional system in several languages (in French 96 is literally pronounced  $4 \times 20 + 16$ ).

In this section, we are going to use modular arithmetic in order to prove some divisibility criteria using our base ten positional notation.

**Proposition 4.14.**  $3 | \overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $3 | \sum_{k=0}^r a_k$ .

*Proof.* Note that  $10 \equiv 1 \pmod{3}$ , hence

$$\overline{a_r a_{r-1} \dots a_0}^{10} = \sum_{k=0}^r a_k 10^k \equiv \sum_{k=0}^r a_k 1^k \pmod{3} \equiv \sum_{k=0}^r a_k \pmod{3}$$

Thus,

$$\begin{aligned} 3 | \overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{3} \\ &\Leftrightarrow \sum_{k=0}^r a_k \equiv 0 \pmod{3} \\ &\Leftrightarrow 3 | \sum_{k=0}^r a_k \end{aligned}$$

■

**Examples 4.15.**

- 91524 is divisible by 3 since  $9 + 1 + 5 + 2 + 4 = 21 = 7 \times 3$  is.
- Let's study whether 8546921469 is a multiple of 3 or not:

$$\begin{aligned} 3 | 8546921469 &\Leftrightarrow 3 | 8 + 5 + 4 + 6 + 9 + 2 + 1 + 4 + 6 + 9 = 54 \\ &\Leftrightarrow 3 | 5 + 4 = 9 \end{aligned}$$

But  $9 = 3 \times 3$ , hence  $3 | 8546921469$ .

**Proposition 4.16.**  $9 | \overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $9 | \sum_{k=0}^r a_k$ .

*Proof.* That's a similar proof since  $10 \equiv 1 \pmod{9}$ .

■

**Proposition 4.17.**  $4|\overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $4|\overline{a_1 a_0}^{10}$ .

*Proof.* Note that  $10^2 = 4 \times 25$  hence  $10^k \equiv 0 \pmod{4}$  for  $k \geq 2$ . Hence

$$\begin{aligned} 4|\overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{4} \\ &\Leftrightarrow \sum_{k=0}^r a_k 10^k \equiv 0 \pmod{4} \\ &\Leftrightarrow a_1 \times 10 + a_0 \equiv 0 \pmod{4} \\ &\Leftrightarrow \overline{a_1 a_0}^{10} \equiv 0 \pmod{4} \\ &\Leftrightarrow 4|\overline{a_1 a_0}^{10} \end{aligned}$$

■

**Examples 4.18.**

- $4 \nmid 856987454251100125$  since  $4 \nmid 25$ .
- $4|98854558715580$  since  $4|80 = 4 \times 20$ .

### 4.3 Fermat's little theorem

**Lemma 4.19.** Let  $p$  be a prime number. Then  $\forall n \in \{1, \dots, p-1\}$ ,  $\binom{p}{n} \equiv 0 \pmod{p}$ .

*Proof.* Let  $n \in \{1, \dots, p-1\}$ . Remember that  $n \binom{p}{n} = p \binom{p-1}{n-1}$ . Hence,  $p|n \binom{p}{n}$ .

Since  $\gcd(p, n) = 1$ , by Gauss' lemma, we get that  $p|\binom{p}{n}$ .

■

**Theorem 4.20** (Fermat's little theorem, version 1).

Let  $p$  be a prime number and  $a \in \mathbb{Z}$ . Then  $a^p \equiv a \pmod{p}$ .

*Proof.* We first prove the theorem for  $a \in \mathbb{N}$  by induction.

Base case at  $a = 0$ :  $0^p = 0 \equiv 0 \pmod{p}$ .

Induction step: assume that  $a^p \equiv a \pmod{p}$  for some  $a \in \mathbb{N}$ . Then

$$\begin{aligned} (a+1)^p &= \sum_{n=0}^p \binom{p}{n} a^n \text{ by the binomial formula} \\ &\equiv a^p + 1 \pmod{p} \quad \text{since, by the above lemma, } p|\binom{p}{n} \text{ for } 1 \leq n \leq p-1 \\ &\equiv a + 1 \pmod{p} \quad \text{by the induction hypothesis} \end{aligned}$$

Which ends the induction step.

We still need to prove the theorem for  $a < 0$ . Then  $-a \in \mathbb{N}$ , hence, from the first part of the proof,  $(-a)^p \equiv -a \pmod{p}$ . Multiplying both sides by  $(-1)^p$  we get that  $a^p \equiv (-1)^{p+1} a \pmod{p}$ .

If  $p = 2$  then either  $a \equiv 0 \pmod{2}$  or  $a \equiv 1 \pmod{2}$ , and the statement holds for both cases.

Otherwise,  $p$  is odd, and hence  $(-1)^{p+1} = 1$ . Thus  $a^p \equiv a \pmod{p}$ .

■

**Theorem 4.21** (Fermat's little theorem, version 2).

Let  $p$  be a prime number and  $a \in \mathbb{Z}$ . If  $\gcd(a, p) = 1$  then  $a^{p-1} \equiv 1 \pmod{p}$ .

*Proof.* By the first version of Fermat's little theorem,  $a^p \equiv a \pmod{p}$ . Hence  $p|a^p - a = a(a^{p-1} - 1)$ .

Since  $\gcd(a, p) = 1$ , by Gauss' lemma,  $p|a^{p-1} - 1$ . Thus  $a^{p-1} \equiv 1 \pmod{p}$ .

■

**Remark 4.22.** Note that both versions of Fermat's little theorem are equivalent.

## 4.4 Wilson's theorem

**Lemma 4.23.** *Let  $p$  be a prime number. Then*

$$\forall a \in \mathbb{Z}, a^2 \equiv 1 \pmod{p} \implies (a \equiv -1 \pmod{p} \text{ or } a \equiv 1 \pmod{p})$$

*Proof.* Let  $p$  be a prime number and  $a \in \mathbb{Z}$  satisfying  $a^2 \equiv 1 \pmod{p}$ . Then  $p|a^2 - 1 = (a - 1)(a + 1)$ . By Euclid's lemma, either  $p|a - 1$  or  $p|a + 1$ , i.e.  $a \equiv 1 \pmod{p}$  or  $a \equiv -1 \pmod{p}$ . ■

**Theorem 4.24** (Wilson's theorem). *Let  $n \in \mathbb{N} \setminus \{0, 1\}$ . Then  $n$  is prime if and only if  $(n - 1)! \equiv -1 \pmod{n}$ .*

*Proof.* Let  $n \in \mathbb{N} \setminus \{0, 1\}$ .

- Assume that  $n$  is a composite number. Then there exists  $k \in \mathbb{N}$  such that  $k|n$  and  $1 < k < n$ . Assume by contradiction that  $(n - 1)! \equiv -1 \pmod{n}$  then  $n|(n - 1)! + 1$  and hence  $k|(n - 1)! + 1$ . But  $k|(n - 1)!$ , thus  $k|((n - 1)! + 1 - (n - 1)!)$ , i.e.  $k|1$ . So  $k = 1$  which leads to a contradiction.
- Assume that  $n$  is prime. Let  $a \in \{1, 2, \dots, n - 1\}$  then  $\gcd(a, n) = 1$ . Hence  $a$  admits a multiplicative inverse modulo  $n$ , so there exists  $b \in \{1, 2, \dots, n - 1\}$  such that  $ab \equiv 1 \pmod{n}$ . Note that this  $b$  is unique by Remark 4.11. By the above lemma,  $a = 1$  and  $a = n - 1$  are the only  $a$  as above being their self-multiplicative inverse (i.e. such that  $a^2 \equiv 1 \pmod{n}$ ). Otherwise  $b \neq a$ . Thus  $(n - 1)! = 1 \times 2 \times \dots \times (n - 1) \equiv 1 \times (n - 1) \pmod{n} \equiv -1 \pmod{n}$ . Indeed, in the previous product each term simplifies with its multiplicative inverse except 1 and  $n - 1$ . ■

**Examples 4.25.**

- Take  $p = 17$  then  $(17 - 1)! + 1 = 20922789888001 = 17 \times 1230752346353$ .
- Take  $p = 15$  then  $(15 - 1)! + 1 = 87178291201 = 15 \times 5811886080 + 1$ .

**Remark 4.26.** Wilson's theorem is a very inefficient way to check whether a number is prime or not. Nonetheless, it has some interesting theoretical applications.

## 4.5 Chinese remainder theorem

**Theorem 4.27** (Chinese remainder theorem).

Let  $n_1, n_2 \in \mathbb{N} \setminus \{0, 1\}$  be such that  $\gcd(n_1, n_2) = 1$  and let  $a_1, a_2 \in \mathbb{Z}$ .

Then there exists  $x \in \mathbb{Z}$  satisfying 
$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Besides, if  $x_1, x_2 \in \mathbb{Z}$  are two solutions of the above system then  $x_1 \equiv x_2 \pmod{n_1 n_2}$ .

*Proof.*

- *Existence.* By Bézout's identity, there exist  $m_1, m_2 \in \mathbb{Z}$  such that  $n_1 m_1 + n_2 m_2 = 1$ . Note that  $n_1 m_1 \equiv 0 \pmod{n_1}$  and that  $n_1 m_1 \equiv n_1 m_1 + n_2 m_2 \pmod{n_2} \equiv 1 \pmod{n_2}$ . Similarly  $n_2 m_2 \equiv 0 \pmod{n_2}$  and  $n_2 m_2 \equiv 1 \pmod{n_1}$ . Thus, if we set  $x = a_2 n_1 m_1 + a_1 n_2 m_2$  then
  - $x \equiv a_2 \times 0 + a_1 \times 1 \pmod{n_1} \equiv a_1 \pmod{n_1}$ ,
  - $x \equiv a_2 \times 1 + a_1 \times 0 \pmod{n_2} \equiv a_2 \pmod{n_2}$ .
- *Uniqueness modulo  $n_1 n_2$ .* Let  $x_1, x_2 \in \mathbb{Z}$  be two solutions. Then  $x_1 - x_2 \equiv 0 \pmod{n_1}$  so  $x_1 - x_2 = kn_1$  for some  $k \in \mathbb{Z}$ . Similarly  $n_2|x_1 - x_2 = kn_1$ . Since  $\gcd(n_1, n_2) = 1$ , by Gauss' lemma,  $n_2|k$ . So there exists  $l \in \mathbb{Z}$  such that  $k = n_2 l$ . Thus  $x_1 - x_2 = ln_1 n_2$  and therefore  $x_1 \equiv x_2 \pmod{n_1 n_2}$ . ■

## 4.6 Euler's theorem

**Definition 4.28.** Euler's totient function is the function  $\varphi : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N} \setminus \{0\}$  defined by

$$\varphi(n) := \# \{k \in \mathbb{N} : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\}$$

**Proposition 4.29.**  $\forall n_1, n_2 \in \mathbb{N} \setminus \{0\}, \gcd(n_1, n_2) = 1 \implies \varphi(n_1 n_2) = \varphi(n_1) \varphi(n_2)$

*Proof.* If  $n_1 = 1$  or  $n_2 = 1$  then there is nothing to prove. So let's assume that  $n_1, n_2 \geq 2$ .

Define

$$S_i = \{r \in \mathbb{N} : 1 \leq r \leq n_i \text{ and } \gcd(r, n_i) = 1\}, i = 1, 2$$

and

$$T = \{k \in \mathbb{N} : 1 \leq k \leq n_1 n_2 \text{ and } \gcd(k, n_1 n_2) = 1\}$$

For  $k \in T$ , write the Euclidean divisions  $k = n_1 q_1 + r_1$  with  $0 \leq r_1 < n_1$  and  $k = n_2 q_2 + r_2$  where  $0 \leq r_2 < n_2$ . Let's prove that  $r_i \in S_i$ :

- Assume that  $r_i = 0$  then  $n_i | k$  and  $n_i | n_1 n_2$  so that  $n_i | \gcd(k, n_1 n_2) = 1$ : contradiction. So  $1 \leq r_i < n_i$ .
- $\gcd(r_i, n_i) = \gcd(k - n_i q_i, n_i) = \gcd(k, n_i) | \gcd(k, n_1 n_2) = 1$ , hence  $\gcd(r_i, n_i) = 1$ .

Therefore we can define  $f : T \rightarrow S_1 \times S_2$  by  $f(k) = (r_1, r_2)$ . Let's prove that  $f$  is a bijection.

Let  $(r_1, r_2) \in S_1 \times S_2$ . Then by the Chinese remainder theorem, there exists a unique  $k \in \{1, 2, \dots, n_1 n_2\}$  such that  $k \equiv r_1 \pmod{n_1}$  and  $k \equiv r_2 \pmod{n_2}$ .

Note that  $\gcd(k, n_1) = \gcd(r_1 + l n_1, n_1) = \gcd(r_1, n_1) = 1$  (for some  $l \in \mathbb{Z}$ ).

Similarly  $\gcd(k, n_2) = \gcd(r_2, n_2) = 1$ .

Then  $\gcd(k, n_1 n_2) = 1$  by Exercise 3 of Problem Set 2, so that  $k \in T$ .

We proved that  $\forall (r_1, r_2) \in S_1 \times S_2, \exists! k \in T, (r_1, r_2) = f(k)$ , i.e. that  $f$  is bijective.

Therefore,  $\#T = \#(S_1 \times S_2) = \#S_1 \#S_2$ , i.e.  $\varphi(n_1 n_2) = \varphi(n_1) \varphi(n_2)$ . ■

**Proposition 4.30.** Let  $p_1, \dots, p_r$  be pairwise distinct prime numbers and  $\alpha_1, \dots, \alpha_r \in \mathbb{N} \setminus \{0\}$ , then

$$\varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

*Proof.*

- *First case:* let  $p$  be a prime number and  $\alpha \in \mathbb{N} \setminus \{0\}$ . Then  $\gcd(p^\alpha, m) > 1$  if and only if  $p | m$ . Hence  $\varphi(p^\alpha) = \#(\{1, 2, \dots, p^\alpha\} \setminus \{1 \times p, 2 \times p, \dots, p^{\alpha-1} \times p\}) = p^\alpha - p^{\alpha-1}$ .
- *General case:* using Proposition 4.29 and the first case, we get that

$$\varphi\left(\prod_{i=1}^r p_i^{\alpha_i}\right) = \prod_{i=1}^r \varphi(p_i^{\alpha_i}) = \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$
■

**Remark 4.31.** Assuming that we have already some knowledge about  $\mathbb{Q}$ , we can also write for  $n = \prod_{i=1}^r p_i^{\alpha_i}$ :

$$\varphi(n) = n \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

**Theorem 4.32** (Euler's theorem). Let  $n \in \mathbb{N} \setminus \{0\}$  and  $a \in \mathbb{Z}$  such that  $\gcd(a, n) = 1$ . Then  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

**Remark 4.33.** Note that Fermat's little theorem is a special case of Euler's theorem: indeed, if  $p$  is a prime number then  $\varphi(p) = p - 1$ .

*Proof of Euler's theorem.*

Write  $S = \{k \in \mathbb{N} : 1 \leq k \leq n \text{ and } \gcd(k, n) = 1\} = \{k_1, k_2, \dots, k_{\varphi(n)}\}$ .

We will use the following two facts:

- (i) Given  $k_i \in S$ , there exists  $k_j \in S$  such that  $ak_i \equiv k_j \pmod{n}$ .  
 Let  $k_i \in S$  then  $\gcd(ak_i, n) = 1$  by Exercise 3 of Problem Set 2.  
 Thus  $ak_i \equiv k_j \pmod{n}$  for some  $k_j \in S$ .
- (ii)  $\forall k_i, k_j \in S, ak_i \equiv ak_j \pmod{n} \implies k_i = k_j$ .  
 Indeed, then  $n|a(k_i - k_j)$  and hence  $n|k_i - k_j$  by Gauss' lemma.  
 Thus  $k_i \equiv k_j \pmod{n}$ .  
 Finally,  $k_i = k_j$  since  $1 \leq k_i, k_j \leq n$ .

For  $i \in \{1, 2, \dots, \varphi(n)\}$ , there exists a unique  $l_i \in \{0, 1, \dots, n-1\}$  such that  $l_i \equiv ak_i \pmod{n}$ .

Then,  $\{l_1, l_2, \dots, l_{\varphi(n)}\} = \{k_1, k_2, \dots, k_{\varphi(n)}\}$ .

Indeed, by (i),  $\{l_1, l_2, \dots, l_{\varphi(n)}\} \subset \{k_1, k_2, \dots, k_{\varphi(n)}\}$ . And by (ii),  $\#\{l_1, l_2, \dots, l_{\varphi(n)}\} = \#\{k_1, k_2, \dots, k_{\varphi(n)}\}$ .

Hence  $\prod_{i=1}^{\varphi(n)} k_i = \prod_{i=1}^{\varphi(n)} l_i \equiv \prod_{i=1}^{\varphi(n)} ak_i \pmod{n} \equiv a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} k_i \pmod{n}$ .

Therefore  $n|(a^{\varphi(n)} - 1) \prod_{i=1}^{\varphi(n)} k_i$ .

Since  $\gcd\left(n, \prod_{i=1}^{\varphi(n)} k_i\right) = 1$  by Exercise 3 of Problem Set 2, we deduce from Gauss' lemma that  $n|a^{\varphi(n)} - 1$ ,  
 i.e.  $a^{\varphi(n)} \equiv 1 \pmod{n}$ . ■

## Appendix 4.A Positional numeral system with base $b$

**Theorem 4.34.** Let  $b \geq 2$  be an natural number. Then any natural number  $n \in \mathbb{N}$  admits a unique expression

$$n = \sum_{k \geq 0} a_k b^k$$

where  $a_k \in \{0, 1, \dots, b-1\}$  and  $a_k = 0$  for all but finitely many  $k \geq 0$ .

**Notation 4.35.** We write  $\overline{a_r a_{r-1} \dots a_1 a_0}^b$  for  $\sum_{k=0}^r a_k b^k$ .

*Proof of Theorem 4.34.*

**Existence.**

We are going to prove by strong induction that for any  $n \geq 0$ , there exist  $a_k \in \{0, 1, \dots, b-1\}$ ,  $k \in \mathbb{N}$ , all but finitely many equal to 0 such that  $n = \sum_{k \geq 0} a_k b^k$ .

- *Base case at  $n = 0$ :*  $0 = \sum_{k \geq 0} 0b^k$ .
- *Induction step.* Assume that  $0, 1, \dots, n$  admit an expression in base  $b$ , for some  $n \geq 0$ .  
By Euclidean division,  $n+1 = bq + r$  where  $q, r \in \mathbb{N}$  satisfy  $0 \leq r < b$ .  
Note that if  $q \neq 0$  then  $q < bq \leq bq + r = n+1$ . Thus  $0 \leq q \leq n$ .  
Therefore, by the induction hypothesis,  $q = \sum_{k \geq 0} a_k b^k$  where  $a_k \in \{0, 1, \dots, b-1\}$  and  $a_k = 0$  for all but finitely many  $k \geq 0$ .  
Hence,  $n+1 = bq + r = \sum_{k \geq 0} a_k b^{k+1} + rb^0$ .

**Uniqueness.**

Write  $\sum_{k \geq 0} a_k b^k = \sum_{k \geq 0} a'_k b^k$  where  $a_k, a'_k \in \{0, 1, \dots, b-1\}$  are zero for all but finitely many  $k \geq 0$ .

Assume by contradiction there exists  $k \geq 0$  such that  $a_k \neq a'_k$ .

Since  $\{k \in \mathbb{N} : a_k \neq a'_k\}$  is finite and non-empty, it admits a greatest element  $\ell$ .

WLOG, we may assume that  $a_\ell < a'_\ell$ .

Then  $0 = \sum_{k \geq 0} a_k b^k - \sum_{k \geq 0} a'_k b^k = \sum_{k \geq 0} (a_k - a'_k) b^k = \sum_{k=0}^{\ell} (a_k - a'_k) b^k$ . So that  $(a'_\ell - a_\ell) b^\ell = \sum_{k=0}^{\ell-1} (a_k - a'_k) b^k$ .

Therefore  $(a'_\ell - a_\ell) b^\ell \leq \sum_{k=0}^{\ell-1} |a_k - a'_k| b^k \leq \sum_{k=0}^{\ell-1} (b-1) b^k = b^\ell - 1 < b^\ell \leq (a'_\ell - a_\ell) b^\ell$ .

Hence a contradiction. ■

**Remark 4.36.** In order to pass from a base 10 expression to a base  $b$  expression, we can perform successive Euclidean divisions as shown below (to pass from a base  $b$  expression to a base 10 we may simply compute the sum).

**Example 4.37.**

$$\begin{aligned} 42 &= 2 \times 21 + 0 \\ &= 2 \times (2 \times 10 + 1) + 0 \\ &= 2 \times (2 \times (2 \times 5 + 0) + 1) + 0 \\ &= 2 \times (2 \times (2 \times (2 \times 2 + 1) + 0) + 1) + 0 \\ &= 2 \times (2 \times (2 \times (2 \times (2 \times 1 + 0) + 1) + 0) + 1) + 0 \\ &= 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 0 \times 2^2 + 1 \times 2^1 + 0 \times 2^0 \end{aligned}$$

Hence  $\overline{42}^{10} = \overline{101010}^2$ .



The first known positional numeral system is the Babylonian one (circa 2000BC) whose base is 60 and whose digits are:

0		10	𐎶	20	𐎵𐎶	30	𐎶𐎵𐎶	40	𐎶𐎶𐎶	50	𐎶𐎶𐎶𐎶
1	𐎶	11	𐎶𐎶	21	𐎵𐎶𐎶	31	𐎶𐎶𐎶𐎶	41	𐎶𐎶𐎶𐎶𐎶	51	𐎶𐎶𐎶𐎶𐎶𐎶
2	𐎶𐎶	12	𐎶𐎶𐎶	22	𐎵𐎶𐎶𐎶	32	𐎶𐎶𐎶𐎶𐎶	42	𐎶𐎶𐎶𐎶𐎶𐎶	52	𐎶𐎶𐎶𐎶𐎶𐎶𐎶
3	𐎶𐎶𐎶	13	𐎶𐎶𐎶𐎶	23	𐎵𐎶𐎶𐎶𐎶	33	𐎶𐎶𐎶𐎶𐎶𐎶	43	𐎶𐎶𐎶𐎶𐎶𐎶𐎶	53	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
4	𐎶𐎶𐎶𐎶	14	𐎶𐎶𐎶𐎶𐎶	24	𐎵𐎶𐎶𐎶𐎶𐎶	34	𐎶𐎶𐎶𐎶𐎶𐎶𐎶	44	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	54	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
5	𐎶𐎶𐎶𐎶𐎶	15	𐎶𐎶𐎶𐎶𐎶𐎶	25	𐎵𐎶𐎶𐎶𐎶𐎶𐎶	35	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	45	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	55	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
6	𐎶𐎶𐎶𐎶𐎶𐎶	16	𐎶𐎶𐎶𐎶𐎶𐎶𐎶	26	𐎵𐎶𐎶𐎶𐎶𐎶𐎶𐎶	36	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	46	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	56	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
7	𐎶𐎶𐎶𐎶𐎶𐎶𐎶	17	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	27	𐎵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	37	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	47	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	57	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
8	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	18	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	28	𐎵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	38	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	48	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	58	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶
9	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	19	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	29	𐎵𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	39	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	49	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶	59	𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶𐎶

Let's say that we want to write 13655 using Babylonian cuneiform numerals. For that, we perform successive Euclidean divisions by 60 as follows:

$$13655 = 60 \times 227 + 35 = 60 \times (60 \times 3 + 47) + 35 = 3 \times 60^2 + 47 \times 60^1 + 35 \times 60^0$$

Hence it was written: 𐎶𐎶𐎶 𐎶𐎶𐎶𐎶 𐎶𐎶𐎶

Originally, there was no positional zero and an empty space was used instead (which can be confusing: 𐎶𐎶𐎶 𐎶 and 𐎶𐎶𐎶 𐎶 are not equal). The more convenient symbol 𐎶 was later used instead of the empty space (but it is not the number 0, just a placeholder symbol for the positional numeral system).

See below a problem set submission by a MAT246 student circa 1700BC.



Figure 4.1: YBC 7289, clay tablet, between 1800BC and 1600BC.

It shows (extremely accurate) approximations of  $\sqrt{2} \simeq 1 + \frac{24}{60} + \frac{51}{60^2} + \frac{10}{60^3}$

and of  $30\sqrt{2} \simeq 42 + \frac{25}{60} + \frac{35}{60^2}$  (diagonal of the square of side length 30, see above de square)

Yale Babylonian Collection,

Original picture from <https://commons.wikimedia.org/wiki/File:YBC-7289-OBV-REV.jpg>

## Appendix 4.B The Chinese Remainder Theorem for more than two equations

You won't need the following result in MAT246, I've just added it because it was asked on Piazza (@82).

**Theorem 4.38** (Chinese remainder theorem). *Let  $k \in \mathbb{N} \setminus \{0, 1\}$ .*

*Let  $n_1, n_2, \dots, n_k \in \mathbb{N} \setminus \{0, 1\}$  be pairwise coprime, i.e.  $\forall i, j \in \{1, \dots, k\}, i \neq j \implies \gcd(n_i, n_j) = 1$ .*

*Let  $a_1, \dots, a_k \in \mathbb{Z}$ . Then there exists  $x \in \mathbb{Z}$  satisfying*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

The proof follows closely the one of Theorem 4.27 but applied to  $n_i$  and  $n_1 \dots n_{i-1} n_{i+1} \dots n_k$ .

*Proof.* Let  $i \in \{1, \dots, k\}$ . Then  $\gcd(n_i, n_1 \dots n_{i-1} n_{i+1} \dots n_k) = 1$ .

So, by Bézout's identity, there exists  $u_i, v_i \in \mathbb{Z}$  such that  $u_i n_i + v_i n_1 \dots n_{i-1} n_{i+1} \dots n_k = 1$ .

Set  $e_i = v_i n_1 \dots n_{i-1} n_{i+1} \dots n_k$  then  $e_i \equiv 1 \pmod{n_i}$ , and for  $j \in \{1, \dots, k\} \setminus \{i\}$ ,  $e_i \equiv 0 \pmod{n_j}$ .

Therefore  $x = \sum_{i=1}^k a_i e_i$  is a suitable solution. ■

## Exercises

### Exercise 1.

Find the remainder of the Euclidean division of  $24^{103}$  by 103.

### Exercise 2.

Prove that  $\forall n \in \mathbb{Z}, \frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \in \mathbb{Z}$ .

*You may already use  $\mathbb{Q}$  for this question.*

*Hint: introduce  $A_n = 35 \left( \frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} \right)$ .*

### Exercise 3.

Let  $p$  be an odd prime number. Prove that  $\forall n \in \mathbb{Z}, (n+1)^p - (n^p + 1) \equiv 0 \pmod{2p}$ .

### Exercise 4.

Let  $p$  be a prime number. Prove that  $\forall k \in \mathbb{N}, \forall n \in \mathbb{Z} \setminus \{0\}, \gcd(n, p) = 1 \implies (n^{p-1})^{p^k} \equiv 1 \pmod{p^{k+1}}$ .

### Exercise 5.

Let  $p$  and  $q$  be two distinct prime numbers. Prove that  $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ .

### Exercise 6.

Prove that  $x^4 + 781 = 3y^4$  has no integer solution.

### Exercise 7.

Let  $n \in \mathbb{N}$  be such that  $n \geq 5$ . Prove that if  $n+2$  is prime then  $n! - 1$  is composite.

### Exercise 8.

Let  $p$  be an odd prime number. Prove that  $2(p-3)! \equiv -1 \pmod{p}$ .

### Exercise 9. A characterization of twin prime numbers.

Let  $n \in \mathbb{N} \setminus \{0, 1\}$ . Prove that if  $n$  and  $n+2$  are both prime numbers then

$$4((n-1)! + 1) + n \equiv 0 \pmod{n(n+2)}$$

*(Actually the converse holds too, but it's a little bit more difficult to prove)*

### Exercise 10.

Let  $p$  be a prime number. Prove that  $\forall n \in \mathbb{Z}, p | n^p + (p-1)!n$ .

### Exercise 11.

Either prove or find a counter-example to  $\forall a, b \in \mathbb{N} \setminus \{0\}, \varphi(ab) = \varphi(a)\varphi(b)$ .

### Exercise 12.

What's the remainder of the Euclidean division of  $1 + 2 + 2^2 + 2^3 + \dots + 2^{100}$  by 125?

### Exercise 13.

Find the last 3 digits of  $3^{2021}$  (written in decimal).

### Exercise 14.

Prove that  $\forall n, k \in \mathbb{N} \setminus \{0\}, \varphi(n^k) = n^{k-1}\varphi(n)$ .

**Exercise 15.**

Prove that  $\forall a, b \in \mathbb{N} \setminus \{0\}, \gcd(a, b) = 1 \implies a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ .

**Exercise 16.**

Let  $a \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Prove that if  $\gcd(a, n) = \gcd(a - 1, n) = 1$  then  $\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0 \pmod{n}$ .

**Exercise 17.**

Prove that  $\forall a \in \mathbb{N} \setminus \{0, 1\}, \forall k \in \mathbb{N} \setminus \{0\}, k | \varphi(a^k - 1)$ .

**Exercise 18.**

We define a sequence by  $u_0 \in \mathbb{N} \setminus \{0\}$  and  $u_{k+1} = \varphi(u_k) \in \mathbb{N} \setminus \{0\}$  for  $k \in \mathbb{N}$ .  
Prove that the sequence  $(u_k)_k$  is eventually constant equal to 1.

## Chapter 5

# The RSA algorithm

### 5.1 Introduction

How can someone send a secret message in a way that only the recipient could read the content even if the message happens to have been intercepted by a third party? There are several ways to do so.

Early cipher algorithms relied on a unique key which had to be used both by the sender to encrypt the message and by the recipient to decrypt it. A very simple example is Caesar's cipher which consists in shifting letters according to the key.

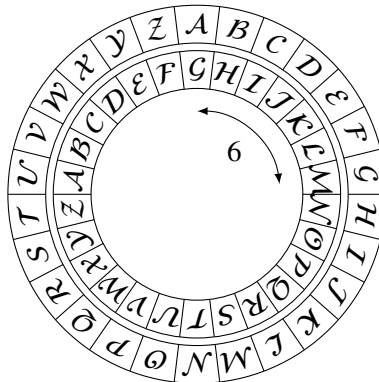
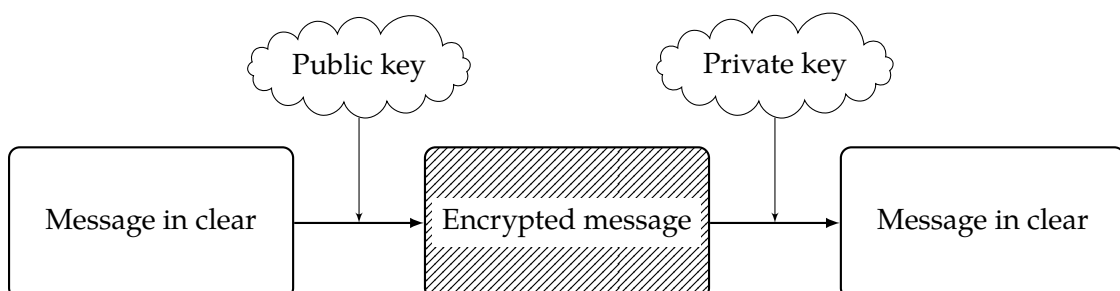


Figure 5.1: Caesar ciphering with key=6

A major weakness of such a system is that the key has to be disclosed to all the participants, increasing the risk for the key to be compromised by a third party.

Asymmetric algorithms allow to reduce this weakness by using two keys: a public key which is used to encrypt messages and which can be widely shared without compromising the exchanges, and a private key which is kept only by the recipient to decrypt the data. The idea is that anyone can encrypt messages using the public key but only the recipient can decrypt them with his private key. Particularly, the knowledge of the public key should not be enough to decrypt messages.



Asymmetric cryptographic systems were theoretically developed in the mid 70s and the first concrete algorithm of this kind was the RSA algorithm which appeared in 1978 and is named from the initials of its authors (Ron Rivest, Adi Shamir, and Leonard Adleman). Actually, the British secret service developed a similar algorithm as early as 1973 but it was kept confidential until the 90s.

In this chapter, we are going to explain the RSA algorithm which relies on modular arithmetic. The original proof of work used Fermat's little theorem but the RSA algorithm is actually easier to explain using Euler's theorem (which is a generalization of Fermat's little theorem, as you already know).

The robustness of this cipher relies on the fact that we don't know yet an efficient algorithm in order to find the prime decomposition of a given positive integer. This last difficult problem will not be addressed in this chapter.

## 5.2 Generation of the keys

The recipient, that we will call Alice, picks two distinct prime numbers  $p$  and  $q$ . She sets  $n := pq$  and then she chooses  $e \in \mathbb{N}$  such that  $\gcd(e, \varphi(n)) = 1$ . Then the public key is  $(n, e)$ . Alice can publicly provide this key to people willing to send her a crypted message.

Since  $\gcd(e, \varphi(n)) = 1$ ,  $e$  admits a multiplicative inverse modulo  $\varphi(n)$ , i.e. there exists  $d \in \mathbb{N}$  such that  $ed \equiv 1 \pmod{\varphi(n)}$ . Indeed, there exist  $u, v \in \mathbb{Z}$  such that  $eu + \varphi(n)v = 1$  (and we can easily find such a Bézout's relation using Euclid's algorithm). Then we take  $d = u + k\varphi(n)$  for a suitable  $k \in \mathbb{Z}$  for  $d$  to be positive. Then the private key is  $(n, d)$ . Alice should not share this key with anyone else.

Note that in order to find a suitable  $d$ , it is necessary to know  $\varphi(n)$  and  $e$ . Alice knows the prime numbers  $p$  and  $q$  that she used to define  $n$  so she can easily compute  $\varphi(n) = (p-1)(q-1)$ . But the shared information is only the public key  $(n, e)$ . Although it is theoretically possible to find  $\varphi(n)$ , there is no known efficient algorithm to compute  $\varphi(n)$  directly from  $n$ . Nonetheless, if a third party were able to quickly compute the prime factorization of a positive integer, then it could compute  $\varphi(n)$  allowing him to recover  $(n, d)$  from  $(n, e)$ .

The prime numbers  $p$  and  $q$  should be chosen wisely so that there is no known efficient algorithm to recover  $p$  and  $q$  from  $n$  using our current computing power. For instance, not only  $p$  and  $q$  should be large enough but  $\delta = |p - q|$  should be large too. Indeed, assume that  $p < q$  then  $q = p + \delta$ . Thus  $\sqrt{n} = p\sqrt{1 + \frac{\delta}{p}} \sim p + \frac{\delta}{2}$ . Hence, according to Proposition 3 of Chapter 3, it is enough to check whether numbers less than  $\sqrt{n}$  divides  $n$ , and from the above estimation,  $p$  could be obtained after less than  $\frac{\delta}{2}$  attempts (starting from  $\sqrt{n}$ ).

## 5.3 How to encrypt a message

The sender, that we are going to call Bob, wants to send a secret message to Alice. But he wants to make sure that only her can read the content. First, Bob obtains her public key  $(n, e)$ .

A message is going to be an element  $m \in \{0, 1, \dots, n-1\}$  (in practice, Alice and Bob need to agree on how to reduce a human readable message into a sequence of natural numbers less than  $n$ , that's the goal of the various protocols used in computer sciences).

Then, there exists a unique  $c \in \{0, 1, \dots, n-1\}$  such that  $c \equiv m^e \pmod{n}$ . It is going to be the crypted message. Bob sends  $c$  to Alice, and Alice will use her private key in order to recover  $m$  from  $c$ .

## 5.4 How to decrypt a message

Alice just received the secret message  $c$  from Bob. He told her that it was encrypted using her public key  $(n, e)$ . Since she knows her private key  $(n, d)$ , Alice can find the unique  $k \in \{0, 1, \dots, n-1\}$  such that

$$k \equiv c^d \pmod{n}.$$

We claim that  $m = k$ . Indeed, since  $ed = 1 + l\varphi(n)$  for some  $l \in \mathbb{N}$ , we obtain using Euler's theorem that

$$k \equiv c^d \pmod{n} \equiv m^{ed} \pmod{n} = m^{1+l\varphi(n)} \pmod{n} \equiv m \times (m^{\varphi(n)})^l \pmod{n} \equiv m \times 1^l \pmod{n} \equiv m \pmod{n}$$

We conclude since  $k$  has a unique representative in  $\{0, 1, \dots, n-1\}$  and  $m, k \in \{0, 1, \dots, n-1\}$ .

Note that the above proof doesn't work when  $\gcd(m, n) \neq 1$ , i.e. when  $p|m$  or  $q|m$  (because we can't apply Euler's theorem). Nonetheless, it is still true that  $m^{ed} \equiv m \pmod{n}$  in this case (you will prove it during next week tutorials).

## 5.5 An example

Alice wants to create a pair of keys for the RSA algorithm so that people could send her secret messages. She picked the prime numbers  $p = 13$  and  $q = 17$  then  $n = 221$  and  $\varphi(n) = 12 \times 16 = 192$ . Then she picks  $e = 11$ , which is a suitable choice since  $\gcd(192, 11) = 1$ .

Using Euclid's algorithm, Alice obtains the Bézout relation  $192 \times (-2) + 11 \times (35) = 1$ . Therefore, she sets  $d = 35$  so that  $ed \equiv 1 \pmod{192}$ . Finally, she shares the public key  $(n, e) = (221, 11)$  on her website and preciously keeps the private key  $(n, d) = (221, 35)$  for herself only.

Later, Bob wants to send the private message  $m = 149 \in \{0, 1, 2, \dots, 220\}$  to Alice. He finds on her website her public key and computes  $m^e = 149^{11} \equiv 89 \pmod{221}$ . So the encrypted message is  $c = 89 \in \{0, 1, 2, \dots, 220\}$ . He sends it to Alice by e-mail.

After receiving the e-mail, Alice computes  $c^d = 89^{35} \equiv 149 \pmod{221}$  and she recovers the original message  $m = 149$ .

## 5.6 In practice

It is not difficult to find a Bézout relation using Euclid's algorithm. But two other things seem not to be very practical in the above example:

1. How to generate the prime numbers  $p$  and  $q$ ?
2. The computations seem to involve very large numbers which are not suitable to computers ( $149^{11}$  is already a very large number).

The first problem is a little bit tricky. In practice we generate a random odd number  $k$  of the wanted order of magnitude and we check whether it is prime or not. If not, we take the next odd number and we repeat the process. According to the prime number theorem<sup>1</sup> we could expect a prime number before  $\frac{\ln(k)}{2}$  attempts.

Nonetheless, we don't know efficient algorithms to check whether a number is prime or not. Instead, we usually use probabilistic primality tests (so they can fail, but with a very low probability).

Some algorithms rely on Fermat's little theorem: if  $p$  is prime then  $\forall a \in \mathbb{Z}, a^p \equiv a \pmod{p}$ .

Therefore, since  $24^{221} \equiv 176 \pmod{221}$ , we know that 221 is not prime.

Nonetheless, it is possible for such a congruence to hold even for a non-prime number  $a$ , for instance we have  $2^{341} \equiv 2 \pmod{341}$  although  $341 = 11 \times 31$ .

The second problem has easy workarounds. First, note that we don't need to actually compute  $m^e$ . Indeed, we only need a representative modulo  $n$ . More precisely, given  $m, e, n \in \mathbb{N}$ , we want to find (the unique)  $c \in \{0, 1, \dots, n-1\}$  such that  $m^e \equiv c \pmod{n}$ . One naive way to avoid very large numbers consists in iteratively multiplying by  $c$  and to reduce to a representative in  $\{0, \dots, n\}$  before the next step.

For instance, in order to compute  $149^{11} \pmod{221}$ , we would do:

<sup>1</sup>For  $k$  large enough, there are *about*  $\frac{k}{\ln(k)}$  prime numbers less than or equal to  $k$ .

- |   |   |
|---|---|
| 1. $149^1 \equiv 149 \pmod{221}$                          | 7. $149^7 = 220 \times 149 = 32780 \equiv 72 \pmod{221}$      |
| 2. $149^2 = 149 \times 149 = 22201 \equiv 101 \pmod{221}$ | 8. $149^8 = 72 \times 149 = 10728 \equiv 120 \pmod{221}$      |
| 3. $149^3 = 101 \times 149 = 15049 \equiv 21 \pmod{221}$  | 9. $149^9 = 120 \times 149 = 17880 \equiv 200 \pmod{221}$     |
| 4. $149^4 = 21 \times 149 = 3129 \equiv 35 \pmod{221}$    | 10. $149^{10} = 200 \times 149 = 29800 \equiv 186 \pmod{221}$ |
| 5. $149^5 = 35 \times 149 = 5215 \equiv 132 \pmod{221}$   | 11. $149^{11} = 186 \times 149 = 27714 \equiv 89 \pmod{221}$  |
| 6. $149^6 = 132 \times 149 = 19668 \equiv 220 \pmod{221}$ |   |

Note that no involved number exceeded 32780 whereas  $149^{11} = 803616698647447868139149$  (actually  $149 \times 220 = 32780$  is the largest number we could have obtained).

We even have even far more efficient algorithms.

First, write the exponent in binary  $e = \overline{a_r a_{r-1} \dots a_1 a_0}^2 = \sum_{i=0}^r a_i 2^i$  where  $a_i \in \{0, 1\}$ . Then

$$m^e = m^{\sum a_i 2^i} = \prod_{i=0}^r \left(m^{2^i}\right)^{a_i}$$

So we just need to compute successive squares:  $m^{2^{i+1}} = \left(m^{2^i}\right)^2$  (actually we only need it modulo  $n$ ).

Implementation in Julia:

```

1 function fastpowmod(m,e,n::Integer)
2     n > 0 || error("n must be positive")
3     e >= 0 || error("e must be non-negative")
4     r = 1
5     while e > 0
6         if (e & 1) > 0
7             r = (r*m)%n
8         end
9         e >>= 1
10        m = (m^2)%n
11    end
12    return r>0 ? r : r+n
13 end

```

Output:

```
julia> fastpowmod(149,11,221)
89
```



## Appendix 5.A A simple implementation in Julia

Source:

```

1  using Primes
2
3  struct PublicKey
4      n::Integer
5      e::Integer
6  end
7
8  struct PrivateKey
9      n::Integer
10     d::Integer
11 end
12
13 function gen_keys(p::Integer, q::Integer, e::Integer)
14     isprime(p) || error("p must be a prime number")
15     isprime(q) || error("q must be a prime number")
16     e>0 || error("e must be positive")
17     phi = (p-1)*(q-1)
18     (g,u,v) = gcdx(e,phi)
19     g == 1 || error("phi(n) and e must be coprime")
20     u<0 ? d=(u%phi)+phi : d=u%phi
21     n = p*q
22     return PublicKey(n,e),PrivateKey(n,d)
23 end
24
25 function encrypt(m::Integer, k::PublicKey)
26     0 <= m || error("m must be non-negative")
27     m < k.n || error("m is too large")
28     return powermod(m,k.e,k.n)
29 end
30
31 function decrypt(c::Integer, k::PrivateKey)
32     0 <= c || error("c must be non-negative")
33     c < k.n || error("c is too large")
34     return powermod(c,k.d,k.n)
35 end
36
37 (pbk,pvk) = gen_keys(13,17,11)
38 println("The public key is (n,e)=($(pbk.n),$(pbk.e)), give it to people
39     willing to send you a secret message!")
39 println("The private key is (n,d)=($(pvk.n),$(pvk.d)), don't share it!")
40 m = 149
41 println("Original message: $m")
42 c = encrypt(m, pbk)
43 println("Encrypted message: $c")
44 println("Decrypted message: $(decrypt(c,pvk))")

```

Output:

```

[mat246@Pavilion mat246]$ julia rsa.j
The public key is (n,e)=(221,11), give it to people willing to send you a
secret message!
The private key is (n,d)=(221,35), don't share it!
Original message: 149
Encrypted message: 89
Decrypted message: 149

```

## Exercises

### Exercise 1.

Assume that  $n = pq$  where  $p, q$  are distinct prime numbers.

Find a way to easily recover  $p$  and  $q$  from the knowledge of  $n$  and  $\varphi(n)$ .

### Exercise 2.

In order to prove that RSA works, we check that if  $p$  and  $q$  are two distinct prime numbers then

$$\forall l \in \mathbb{N}, \forall m \in \mathbb{Z}, m^{1+l\varphi(pq)} \equiv m \pmod{pq} \quad (5.1)$$

The proof seen in class relies on Euler's theorem:  $m^{1+l\varphi(pq)} = m \times (m^{\varphi(pq)})^l \equiv m \times 1^l \pmod{pq} \equiv m \pmod{pq}$ . Therefore it holds only when  $\gcd(m, pq) = 1$ , i.e. it doesn't hold when  $p|m$  or  $q|m$ .<sup>2</sup>

Prove that (5.1) holds with no restriction on  $m$ .

### Exercise 3.

1. Check that  $(n, e) = (5917, 17)$  and  $(n, d) = (5917, 2033)$  are suitable respectively public and private keys.  
Note that  $n = 61 \times 97$ .
2. Bob wants to send the message  $m = 42$  to Alice using the above keys. What should he send to Alice?  
You don't have to compute it by hand.  
Check that Alice can decrypt this message.
3. Alice just received the ciphered message  $c = 3141$  from Bob. What is the original message?

### Exercise 4.

Eve intercepted the message  $c = 271$  sent to Alice from Bob.

She finds Alice's public key  $(n, e) = (1003, 11)$  on her website.

What is the original message sent by Bob?

### Exercise 5. Digital signature

Another common problem related to communications is the following: how can the recipient be sure that the sender is not an impostor?

Explain how RSA can be used to solve this issue.

<sup>2</sup>That's already quite good: it works for  $m \in \{0, 1, \dots, pq-1\} \setminus (\{p, 2p, \dots, (q-1)p\} \cup \{q, 2q, \dots, (p-1)q\})$  but  $\frac{pq-(p-1)-(q-1)}{pq} = 1 + \frac{2}{pq} - \frac{1}{q} - \frac{1}{p}$  is small when  $p$  and  $q$  are large, so this proof works for almost all possible messages.

## Chapter 6

# The rationals and the reals

Positive rational numbers  $\frac{p}{q}$  are systematically studied in Euclid's elements (circa 300BC), but they already appeared in ancient Egyptian mathematical writings.

In this chapter we are going to formally construct the set  $\mathbb{Q}$  of rational numbers. The basic idea would be to set

$$\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{Z} \setminus \{0\} \right\}$$

as it is often written in elementary introductions to mathematics. Nonetheless that's not a fully satisfactory definition since a same rational number may have different quotient expressions, for instance we want to have  $\frac{10}{14} = \frac{5}{7}$ . In order to formally solve this issue we are going to introduce the notion of *equivalence classes* and *quotient sets*.

The oldest known texts referring to irrational numbers are the Śulbasūtras. They contain the fact that the diagonal of a square sacrificial altar<sup>1</sup> is uncommensurable with the side length (i.e. the side and the diagonal can't be integral multiples of another length).

The Pythagorean Hippasus of Metapontum (circa 500BC) is often credited to have discovered the first proof of irrationality (it is known for sure that Pythagoreans were aware that  $\sqrt{2}$  and  $\varphi$  are irrational, but there is a lot of confusion about the first author divulging irrationality, probably because of the subsequent damages to the dogma of the Pythagorean school). In ancient Greece, mathematics had a geometric flavour with a focus on constructions: therefore that was a geometric proof of uncommensurability (I will give an example later in this chapter).

There are several tales concerning the fate of the discoverer of uncommensurable lengths. In the most favorable version, he was expelled for his impiety (it was Pythagorean dogma that lengths are commensurable, and more generally that all the things in the world are commensurable, such as melodic intervals). In other versions, the discoverer was sentenced to death by drowning<sup>2</sup>. That was for sure the beginning of a deep philosophical crisis.

The second part of this chapter is devoted to the set  $\mathbb{R}$  of real numbers. It allows us to take these irrational numbers into account. I will give several proofs of irrationality (disclaimer: no ancient greek philosopher has been harmed during the preparation of this text).

### 6.1 Equivalence classes

Recall that a binary relation  $\sim$  on a set  $E$  is an *equivalence relation* if

- (i)  $\forall x \in E, x \sim x$  (*reflexivity*)
- (ii)  $\forall x, y \in E, x \sim y \implies y \sim x$  (*symmetry*)
- (iii)  $\forall x, y, z \in E, (x \sim y \text{ and } y \sim z) \implies x \sim z$  (*transitivity*)

---

<sup>1</sup>Irrational numbers seem to always appear in a deadly context...

<sup>2</sup>I warned you that irrational numbers seem to always appear under deadly circumstances.

In what follows, we fix  $E$  a set together with an equivalence relation  $\sim$  on it. We define the *equivalence class* of  $x \in E$  by

$$[x] = \{y \in E : x \sim y\}$$

and we say that  $x$  is a *representative* of  $[x]$ .

We may easily prove that equivalence classes satisfy the following properties:

- $\forall x \in E, x \in [x]$
- $\forall x, y \in E, x \sim y \Leftrightarrow [x] = [y]$
- $\forall x, y \in E, [x] = [y] \text{ or } [x] \cap [y] = \emptyset$

*Proof.*

- Let  $x \in E$ . Since  $x \sim x$ , we have that  $x \in [x]$ .
- Let  $x, y \in E$ .  
 $\Rightarrow$  Assume that  $x \sim y$ . Let  $z \in [x]$ , then  $x \sim z$ . By transitivity  $y \sim z$  so that  $z \in [y]$ .  
 We proved that  $[x] \subset [y]$ . We may similarly prove that  $[y] \subset [x]$ . Hence  $[x] = [y]$ .  
 $\Leftarrow$  Assume that  $[x] = [y]$ . Then  $x \in [x] = [y]$ , so  $y \sim x$  (and thus  $x \sim y$ ).
- Let  $x, y \in E$ . Assume that  $[x] \cap [y] \neq \emptyset$ , then there exists  $z \in [x] \cap [y]$ .  
 Therefore  $x \sim z$  and  $y \sim z$ . By transitivity, we get that  $x \sim y$ , thus  $[x] = [y]$ . ■

The set

$$E/\sim := \{[x] : x \in E\}$$

of equivalence classes of  $\sim$  is called the *quotient set* of  $E$  for  $\sim$ .

An element of  $E/\sim$  is a subset of  $E$  made of elements which are all equivalent for  $\sim$ .

According to the above properties the elements of  $E/\sim$  form a partition of  $E$ :

$$E = \bigsqcup_{S \in E/\sim} S$$

The idea is that we want to identify all the elements which are equivalent:  $x \sim y$  becomes  $[x] = [y]$  in  $E/\sim$ . That's a very convenient tool to construct new sets from already constructed ones.

**Example 6.1.** For instance  $\mathbb{Z}/\text{mod } 6$  contains 6 equivalence classes:

- $[0] = \{n \in \mathbb{Z} : n \equiv 0 \pmod{6}\} = \{\dots, -12, -6, 0, 6, 12, \dots\}$
- $[1] = \{n \in \mathbb{Z} : n \equiv 1 \pmod{6}\} = \{\dots, -11, -5, 1, 7, 13, \dots\}$
- $[2] = \{n \in \mathbb{Z} : n \equiv 2 \pmod{6}\} = \{\dots, -10, -4, 2, 8, 14, \dots\}$
- $[3] = \{n \in \mathbb{Z} : n \equiv 3 \pmod{6}\} = \{\dots, -9, -3, 3, 9, 15, \dots\}$
- $[4] = \{n \in \mathbb{Z} : n \equiv 4 \pmod{6}\} = \{\dots, -8, -2, 4, 10, 16, \dots\}$
- $[5] = \{n \in \mathbb{Z} : n \equiv 5 \pmod{6}\} = \{\dots, -7, -1, 5, 11, 17, \dots\}$

Note that  $-5, 1$  and  $7$  are representatives of  $[-5] = [1] = [7]$ .

Congruences become an actual equality in  $\mathbb{Z}/\text{mod } 6$ :  $a \equiv b \pmod{6} \Leftrightarrow [a] = [b]$ .

In this example, it is easy to see that the equivalence classes form a partition of  $\mathbb{Z} = [0] \sqcup [1] \sqcup [2] \sqcup [3] \sqcup [4] \sqcup [5]$ . Indeed, an integer  $n \in \mathbb{Z}$  is an element of exactly one of the equivalence classes (depending on its remainder for the Euclidean division by 6).

**Remark 6.2.** An equivalence relation is entirely characterized by its equivalence classes.

Indeed if we have a partition  $E = \bigsqcup_{i \in I} S_i$  then

$$x \sim y \Leftrightarrow (\exists i \in I, x, y \in S_i)$$

defines an equivalence relation on  $E$ .

## 6.2 Rational numbers

**Proposition 6.3.** *The relation  $\sim$  on  $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  defined by*

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc$$

*is an equivalence relation.*

*Proof.*

- *Reflexivity.* Let  $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  then  $ab = ba$  so that  $(a, b) \sim (a, b)$ .
- *Symmetry.* Let  $(a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ . Assume that  $(a, b) \sim (c, d)$  then  $ad = bc$ . Thus  $cb = da$ , i.e.  $(c, d) \sim (a, b)$ .
- *Transitivity.* Let  $(a, b), (c, d), (e, f) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ . Assume that  $(a, b) \sim (c, d)$  and that  $(c, d) \sim (e, f)$ . Then  $ad = bc$  and  $cf = de$ . Therefore  $adf = bcf = bde$ . Since  $d \neq 0$ , by cancellation,  $af = be$ , i.e.  $(a, b) \sim (e, f)$ . ■

**Definition 6.4.** We define the set of *rational numbers* by  $\mathbb{Q} := (\mathbb{Z} \times \mathbb{Z} \setminus \{0\}) / \sim$  and we denote the equivalence class of  $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  by  $\frac{a}{b} := [(a, b)]$ .

**Remark 6.5.** Note that  $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc$ .

**Remark 6.6.** With the above definition, we may formally write that  $\frac{12}{14} = \frac{6}{7}$ : indeed  $(12, 14) \sim (6, 7)$  since  $12 \times 7 = 84 = 14 \times 6$ .

**Remark 6.7.** We defined a rational number as a set of couples, but what really matters is how the usual operations and the order are defined on rational numbers  $\frac{a}{b} \in \mathbb{Q}$ .

**Remark 6.8.** Note that for  $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$ , we have  $\frac{-a}{b} = \frac{a}{-b}$ . Hence we set  $-\frac{a}{b} := \frac{-a}{b} = \frac{a}{-b}$ .

**Remark 6.9.** Note that  $\frac{a}{b} = 0 \Leftrightarrow a = 0$  and that if  $\frac{a}{b} = \frac{a'}{b'} \neq 0$  then  $\frac{b}{a} = \frac{b'}{a'}$ .

Hence, if  $x = \frac{a}{b} \neq 0$ , we set  $x^{-1} := \frac{b}{a}$  which doesn't depend on the representative of  $x$ .

**Proposition 6.10.** *Given  $x \in \mathbb{Q}$ , there exists a unique couple  $(a, b) \in \mathbb{Z} \times \mathbb{N} \setminus \{0\}$  such that  $x = \frac{a}{b}$  and  $\gcd(a, b) = 1$ . Then we say that  $x = \frac{a}{b}$  is written in lowest form.*

*Proof.* Let  $x \in \mathbb{Q}$ .

**Existence.** There exist  $\alpha \in \mathbb{Z}$  and  $\beta \in \mathbb{Z} \setminus \{0\}$  such that  $x = \frac{\alpha}{\beta}$ .

Write  $d = \gcd(\alpha, \beta)$ , then there exist  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z} \setminus \{0\}$  such that  $\alpha = da$  and  $\beta = db$ .

We have  $d = \gcd(\alpha, \beta) = \gcd(da, db) = d \gcd(a, b)$ , so  $\gcd(a, b) = 1$ .

Besides  $\frac{\alpha}{\beta} = \frac{\text{sign}(b)a}{|b|}$  since  $\text{sign}(b)a\beta = \text{sign}(b)adb = |b|da = |b|\alpha$ .

**Uniqueness.** Assume that  $\frac{a}{b} = \frac{a'}{b'}$  where  $a, a' \in \mathbb{Z}$ ,  $b, b' \in \mathbb{N} \setminus \{0\}$ ,  $\gcd(a, b) = 1$ ,  $\gcd(a', b') = 1$ .

Then  $ab' = a'b$ . By Gauss' lemma, since  $b|ab'$  and  $\gcd(a, b) = 1$ , we get that  $b|b'$ . Similarly  $b'|b$ .

Since  $b|b'$  and  $b'|b$ , we get  $|b| = |b'|$ , and thus  $b = b'$ .

Then, using the cancellation rule,  $ab' = a'b$  gives  $a = a'$  since  $b = b' \neq 0$ . ■

**Remark 6.11.** Note that the function  $\varphi : \begin{matrix} \mathbb{Z} & \rightarrow & \mathbb{Q} \\ n & \mapsto & \frac{n}{1} \end{matrix}$  is injective. Indeed,  $\forall n, m \in \mathbb{Z}$ ,  $\frac{n}{1} = \frac{m}{1} \Leftrightarrow n = m$ .

Therefore we may see  $\mathbb{Z}$  as a subset of  $\mathbb{Q}$  by setting  $n := \frac{n}{1} \in \mathbb{Q}$  for  $n \in \mathbb{Z}$ .

More formally,  $\varphi(\mathbb{Z}) \subset \mathbb{Q}$  and we may identify  $\mathbb{Z}$  with  $\varphi(\mathbb{Z})$  since  $\varphi : \mathbb{Z} \rightarrow \varphi(\mathbb{Z})$  is bijective.

**Proposition 6.12.** The addition  $+$  :  $\begin{matrix} \mathbb{Q} \times \mathbb{Q} & \rightarrow & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ad+bc}{bd} \end{matrix}$  is well-defined.

*Proof.* We need to prove that the addition doesn't depend on the choice of the representatives, i.e. that if  $\frac{a}{b} = \frac{a'}{b'}$  and  $\frac{c}{d} = \frac{c'}{d'}$  then  $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ .

Assume that  $\frac{a}{b} = \frac{a'}{b'}$  and  $\frac{c}{d} = \frac{c'}{d'}$ , i.e.  $ab' = ba'$  and  $cd' = dc'$ .

Therefore  $(ad + bc)(b'd') = adb'd' + bcb'd' = ba'dd' + dc'bb' = (a'd' + b'c')(bd)$ , i.e.  $\frac{ad+bc}{bd} = \frac{a'd'+b'c'}{b'd'}$ . ■

**Remark 6.13.** Note that the addition defined on  $\mathbb{Q}$  is compatible with the one on  $\mathbb{Z}$ . Indeed, if  $m, n \in \mathbb{Z}$  then  $\frac{m}{1} + \frac{n}{1} = \frac{m+n}{1}$ .

**Proposition 6.14.** The multiplication  $\times$  :  $\begin{matrix} \mathbb{Q} \times \mathbb{Q} & \rightarrow & \mathbb{Q} \\ \left(\frac{a}{b}, \frac{c}{d}\right) & \mapsto & \frac{ac}{bd} \end{matrix}$  is well-defined.

*Proof.* We need to prove that the multiplication doesn't depend on the choice of the representatives, i.e. that if  $\frac{a}{b} = \frac{a'}{b'}$  and  $\frac{c}{d} = \frac{c'}{d'}$  then  $\frac{a}{b} \times \frac{c}{d} = \frac{a'}{b'} \times \frac{c'}{d'}$ .

Assume that  $\frac{a}{b} = \frac{a'}{b'}$  and  $\frac{c}{d} = \frac{c'}{d'}$ , i.e.  $ab' = ba'$  and  $cd' = dc'$ .

Therefore  $(ac)(b'd') = ab'cd' = ba'dc' = (a'c')(bd)$ , i.e.  $\frac{ac}{bd} = \frac{a'c'}{b'd'}$  as desired. ■

**Remark 6.15.** Note that the multiplication defined on  $\mathbb{Q}$  is compatible with the one on  $\mathbb{Z}$ . Indeed, if  $m, n \in \mathbb{Z}$  then  $\frac{m}{1} \times \frac{n}{1} = \frac{m \times n}{1}$ .

**Definition 6.16.** We define the binary relation  $\leq$  on  $\mathbb{Q}$  by

$$\frac{a}{b} \leq \frac{c}{d} \Leftrightarrow 0 \leq (bc - ad)bd$$

where the order on the RHS of the equivalence is the order of  $\mathbb{Z}$ .

**Remark 6.17.** The idea behind the above definition is the following:

- We want that  $\frac{a}{b} \leq \frac{c}{d}$  if and only if  $0 \leq \frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd}$ , and,
- we also want that  $0 \leq \frac{e}{f}$  if and only if  $0 \leq ef$  (i.e. the sign rule).

**Remark 6.18.** We have to check that the order doesn't depend on the choice of representatives.

**Remark 6.19.** Note that the relation  $\leq$  defined on  $\mathbb{Q}$  is compatible with the usual order  $\leq$  on  $\mathbb{Z}$ . Indeed, let  $m, n \in \mathbb{Z}$  then  $\frac{m}{1} \leq \frac{n}{1} \Leftrightarrow 0 \leq n - m \Leftrightarrow m \leq n$ .

**Theorem 6.20.**  $(\mathbb{Q}, +, \times, \leq)$  is a (totally) ordered field, meaning that

- $+$  is associative:  $\forall x, y, z \in \mathbb{Q}, (x + y) + z = x + (y + z)$
- $0$  is the unit of  $+$ :  $\forall x \in \mathbb{Q}, x + 0 = 0 + x = x$
- $-x$  is the additive inverse of  $x$ :  $\forall x \in \mathbb{Q}, x + (-x) = (-x) + x = 0$
- $+$  is commutative:  $\forall x, y \in \mathbb{Q}, x + y = y + x$
- $\times$  is associative:  $\forall x, y, z \in \mathbb{Q}, (xy)z = x(yz)$
- $\times$  is distributive with respect to  $+$ :  $\forall x, y, z \in \mathbb{Q}, x(y + z) = xy + xz$  and  $(x + y)z = xz + yz$
- $1$  is the unit of  $\times$ :  $\forall x \in \mathbb{Q}, 1 \times x = x \times 1 = x$
- If  $x \neq 0$  then  $x^{-1}$  is the multiplicative inverse of  $x$ :  $\forall x \in \mathbb{Q} \setminus \{0\}, xx^{-1} = x^{-1}x = 1$
- $\times$  is commutative:  $\forall x, y \in \mathbb{Q}, xy = yx$
- $\leq$  is reflexive:  $\forall x \in \mathbb{Q}, x \leq x$
- $\leq$  is antisymmetric:  $\forall x, y \in \mathbb{Q}, (x \leq y \text{ and } y \leq x) \Rightarrow x = y$
- $\leq$  is transitive:  $\forall x, y, z \in \mathbb{Q}, (x \leq y \text{ and } y \leq z) \Rightarrow x \leq z$
- $\leq$  is total:  $\forall x, y \in \mathbb{Q}, x \leq y \text{ or } y \leq x$
- $\forall x, y, r, s \in \mathbb{Q}, (x \leq y \text{ and } r \leq s) \Rightarrow x + r \leq y + s$
- $\forall x, y, z \in \mathbb{Q}, (x \leq y \text{ and } z > 0) \Rightarrow xz \leq yz$

**Remark 6.21.** If  $\frac{c}{d} \neq 0$ , we set  $\frac{\frac{a}{b}}{\frac{c}{d}} := \left(\frac{c}{d}\right)^{-1} \frac{a}{b} = \frac{ad}{bc}$ .

**Proposition 6.22.**  $\forall x, y \in \mathbb{Q}, x < y \implies (\exists z \in \mathbb{Q}, x < z < y)$

*Proof.* Let  $x, y \in \mathbb{Q}$  be such that  $x < y$ . Then  $z = \frac{x+y}{2}$  is a suitable choice. Indeed,  $x < y$  implies  $2x < x + y$  and thus  $x < z$ . Similarly  $x + y < 2y$ , and thus  $z < y$ . ■

**Theorem 6.23** ( $\mathbb{Q}$  is archimedean).  $\forall \varepsilon \in \mathbb{Q}_{>0}, \forall A \in \mathbb{Q}_{>0}, \exists N \in \mathbb{N}, N\varepsilon > A$ .

*Proof.* Since  $\frac{A}{\varepsilon} > 0$ , we may find a representative  $\frac{a}{b} = \frac{A}{\varepsilon}$  where  $a, b \in \mathbb{N} \setminus \{0\}$ . Then  $a + 1 - \frac{A}{\varepsilon} = a + 1 - \frac{a}{b} = \frac{a(b-1)+b}{b} > 0$ , thus  $(a+1)\varepsilon > A$ . So  $N = a + 1$  is a suitable choice. ■

**Remark 6.24.** The above theorem means that  $\lim_{n \rightarrow +\infty} \frac{1}{n} = 0$ , or equivalently that  $\mathbb{Q}$  doesn't contain infinitesimal elements (i.e. there is not infinitely large or infinitely small elements).

This property may seem obvious at first glance, but, even if it is a little bit beyond the scope of this course, it is not too difficult to construct a (totally) ordered field with infinitesimal elements (i.e. with a positive element which is less than or equal to any other positive elements).

**Remark 6.25.** Note that  $\mathbb{Q}$  is not well-ordered.

Indeed  $\mathbb{Q}_{>0} = \{x \in \mathbb{Q} : x > 0\}$  is non-empty (and even bounded from below) but it has no least element.

**Theorem 6.26** (The rational root theorem).

Let  $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  be a polynomial with integer coefficients  $a_k \in \mathbb{Z}$ .

If  $x = \frac{p}{q}$  is a rational root of  $f$  written in lowest terms (i.e.  $\gcd(p, q) = 1$ ), then  $p|a_0$  and  $q|a_n$ .

*Proof.* By assumption we have that

$$a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0$$

Therefore

$$a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$$

Thus  $p|a_0 q^n$ . Since  $\gcd(p, q) = 1$ , by Gauss' lemma we obtain that  $p|a_0$ .

Similarly  $q|a_n$ . ■

### 6.3 Infima and suprema

Recall that a binary relation  $\leq$  on a set  $E$  is an *order* if

- (i)  $\forall x \in E, x \leq x$  (*reflexivity*)
- (ii)  $\forall x, y \in E, (x \leq y \text{ and } y \leq x) \implies x = y$  (*antisymmetry*)
- (iii)  $\forall x, y, z \in E, (x \leq y \text{ and } y \leq z) \implies x \leq z$  (*transitivity*)

**Definition 6.27.** Let  $(E, \leq)$  be an ordered set and  $A \subset E$ .

- We say that  $m \in A$  is the *least element* of  $A$  if  $\forall a \in A, m \leq a$ .
- We say that  $M \in A$  is the *greatest element* of  $A$  if  $\forall a \in A, a \leq M$ .

**Remark 6.28.** Note that, if it exists, the least element (resp. greatest element) of  $A$  is in  $A$  by definition.

**Remark 6.29.** The least (resp. greatest) element may not exist, but if it exists then it is unique.

For instance  $\{n \in \mathbb{Z} : n \leq 0\} \subset \mathbb{Z}$  and  $\{x \in \mathbb{Q} : 0 < x < 1\}$  have no least element.

For the uniqueness, it is easy to prove: assume that  $m, m'$  are two least elements of  $A$ , then

- $m \leq m'$  since  $m$  is a least element of  $A$  and  $m' \in A$ , and,
- $m' \leq m$  since  $m'$  is a least element of  $A$  and  $m \in A$ .

Hence  $m = m'$ .

**Definition 6.30.** Let  $(E, \leq)$  be an ordered set and  $A \subset E$ .

- We say that  $A$  is *bounded from below* if it admits a *lower bound*, i.e.

$$\exists c \in E, \forall a \in A, c \leq a$$

- We say that  $A$  is *bounded from above* if it admits an *upper bound*, i.e.

$$\exists C \in E, \forall a \in A, a \leq C$$

- We say that  $A$  is *bounded* if it is bounded from below and from above.

**Definition 6.31.** Let  $(E, \leq)$  be an ordered set and  $A \subset E$ .

- If the greatest lower bound of  $A$  exists, we denote it  $\inf(A)$  and call it the *infimum* of  $A$ .
- If the least upper bound of  $A$  exists, we denote it  $\sup(A)$  and call it the *supremum* of  $A$ .

**Remark 6.32.** If it exists, the greatest element of the set of lower bounds of  $A$  is unique (as shown above), therefore the infimum is unique (if it exists). And similarly for the supremum.

However, it may not exist:

- If  $A = \{n \in \mathbb{Z} : n \leq 0\} \subset \mathbb{Z}$  then the set of lower bounds of  $A$  is empty, so  $A$  has no infimum.
- If  $A = \{x \in \mathbb{Q} : x > 0 \text{ and } x^2 > 2\} \subset \mathbb{Q}$  then the set of lower bounds of  $A$  is not empty but has no greatest element, so  $A$  has no infimum.

Note that the infimum (resp. supremum) may not be an element of  $A$ , but if it is then it is the least (resp. greatest) element of  $A$ . For instance, the infimum of  $A = \{x \in \mathbb{Q} : 0 < x < 1\} \subset \mathbb{Q}$  is  $0 \notin A$ .

## 6.4 Real numbers

The following results concerning  $\mathbb{R}$  that you learnt during your first year calculus course are equivalent:

- The Least Upper Bound principle
- The Monotone Convergence Theorem for sequences
- The Extreme Value Theorem
- The Intermediate Value Theorem
- Rolle's Theorem/The Mean Value Theorem
- A continuous function on a segment line is Riemann-integrable
- Bolzano-Weierstrass Property of  $\mathbb{R}$ : a bounded sequence in  $\mathbb{R}$  admits a convergent subsequence
- Cut property:

$$\left. \begin{array}{l} A, B \neq \emptyset \\ \forall A, B \subset \mathbb{R}, \quad \mathbb{R} = A \cup B \\ \forall a \in A, \forall b \in B, a < b \end{array} \right\} \implies \exists! c \in \mathbb{R}, \forall a \in A, \forall b \in B, a \leq c \leq b$$

We say that  $\mathbb{R}$  is Dedekind-complete to state that the above statements hold.

Intuitively, the Dedekind-completeness of the real line tells us two things:

1. There is no infinitely small positive real number (*Archimedean property*, which is already true for  $\mathbb{Q}$ ):

$$\forall \epsilon > 0, \forall A > 0, \exists n \in \mathbb{N}, n\epsilon > A$$

2. There is no gap in the real line (e.g. any sequence of digits is the decimal expansion of a real number).

That's the difference with  $\mathbb{Q}$ . See for instance the following examples involving  $\sqrt{2} \notin \mathbb{Q}$ :

- LUB:  $\sqrt{2} = \sup \{x \in \mathbb{Q} : x^2 < 2\}$ .
- MCT: define a sequence by  $x_0 = 1$  and  $x_{n+1} = \frac{x_n}{2} + \frac{1}{x_n}$ .  
Then  $(x_n)$  converges to some limit  $l$  by the MCT. But this limit must satisfy  $l^2 = 2$ .
- IVT: let  $f(x) = x^2 - 2$ . Then  $f(0) < 0$  and  $f(2) > 0$ .  
Hence we deduce from the IVT that  $f$  has a root, i.e.  $\exists x \in \mathbb{R}, x^2 - 2 = 0$ .



The Dedekind-completeness of the real line has several consequences that you already know:

- The various results connecting the sign of  $f'$  to the monotonicity of  $f$ .
- $ACV \implies CV$  (for series and improper integrals).
- The Fundamental Theorem of Calculus.
- L'Hôpital's rule.
- The BCT and the LCT (for series and improper integrals).
- Cauchy-completeness of  $\mathbb{R}$ : any Cauchy sequence converges.  
*Beware, despite very close names, without the Archimedean property Cauchy-completeness is strictly weaker than Dedekind-completeness.*
- ...

Hence a first year calculus course is basically about the Dedekind-completeness of  $\mathbb{R}$  and its consequences.

**Theorem 6.33.** *Up to isomorphism<sup>3</sup>, there exists a unique (totally) ordered field  $(\mathbb{R}, +, \times, \leq)$  which is Dedekind-complete, i.e. such that:*

- $+$  is associative:  $\forall x, y, z \in \mathbb{R}, (x + y) + z = x + (y + z)$
- $0$  is the unit of  $+$ :  $\forall x \in \mathbb{R}, x + 0 = 0 + x = x$
- Existence of the additive inverse:  $\forall x \in \mathbb{R}, \exists (-x) \in \mathbb{R}, x + (-x) = (-x) + x = 0$
- $+$  is commutative:  $\forall x, y \in \mathbb{R}, x + y = y + x$
- $\times$  is associative:  $\forall x, y, z \in \mathbb{R}, (xy)z = x(yz)$
- $\times$  is distributive with respect to  $+$ :  $\forall x, y, z \in \mathbb{R}, x(y + z) = xy + xz$  and  $(x + y)z = xz + yz$
- $1$  is the unit of  $\times$ :  $\forall x \in \mathbb{R}, 1 \times x = x \times 1 = x$
- Existence of the multiplicative inverse:  $\forall x \in \mathbb{R} \setminus \{0\}, \exists x^{-1} \in \mathbb{R}, xx^{-1} = x^{-1}x = 1$
- $\times$  is commutative:  $\forall x, y \in \mathbb{R}, xy = yx$
- $\leq$  is reflexive:  $\forall x \in \mathbb{R}, x \leq x$
- $\leq$  is antisymmetric:  $\forall x, y \in \mathbb{R}, (x \leq y \text{ and } y \leq x) \implies x = y$
- $\leq$  is transitive:  $\forall x, y, z \in \mathbb{R}, (x \leq y \text{ and } y \leq z) \implies x \leq z$
- $\leq$  is total:  $\forall x, y \in \mathbb{R}, x \leq y \text{ or } y \leq x$
- $\forall x, y, r, s \in \mathbb{R}, (x \leq y \text{ and } r \leq s) \implies x + r \leq y + s$
- $\forall x, y, z \in \mathbb{R}, (x \leq y \text{ and } z > 0) \implies xz \leq yz$
- $\mathbb{R}$  is Dedekind-complete (for instance a non-empty subset which is bounded from above admits a supremum).

The theorem contains two parts: existence and uniqueness.

For the existence part, there are several ways to construct a field satisfying the above properties. Usually each construction gives easily a version of the Dedekind-completeness from which we derive the other equivalent statements.

One very common construction consists in defining  $\mathbb{R}$  as equivalence classes of rational Cauchy sequences: this way we obtain easily the archimedean property and the Cauchy-completeness (which are together equivalent to the Dedekind-completeness).

Another common construction relies on Dedekind cuts (that I present in the appendix). This one gives the cut property for free, from which we easily derive the least upper bound principle (quite often the LUB principle is the start point of first year calculus courses).

The uniqueness part is a little bit delicate and I won't prove it in this course. Nonetheless, let me try to explain the rough idea.

Assume that we are given two fields  $\mathbb{R}$  and  $\tilde{\mathbb{R}}$  satisfying the above properties. Note that each of them contains a copy of  $\mathbb{Q}$ . Then we can construct a order-preserving bijection  $\varphi : \mathbb{R} \rightarrow \tilde{\mathbb{R}}$  compatible with the addition and the multiplication as follows: first we map the copy of  $\mathbb{Q}$  in  $\mathbb{R}$  to the one in  $\tilde{\mathbb{R}}$  and then we use the Dedekind-completeness to extend the bijection from  $\mathbb{Q}$  to  $\mathbb{R}$  (the idea is to *fill the gaps* similarly in  $\mathbb{R}$  and  $\tilde{\mathbb{R}}$ ).

<sup>3</sup>It means that if we have two such fields, then there is a bijection between them preserving the addition, the multiplication and the order, i.e. they are basically the same.

Nonetheless, there is no need to give an explicit construction of  $\mathbb{R}$ : we can use the above properties as axioms and then study their consequences. That's the usual strategy in a first year calculus course. In the sequel, concerning the Dedekind-completeness of  $\mathbb{R}$ , we assume that the least upper bound principle holds:

**LUB Principle.** A non-empty subset of  $\mathbb{R}$  which is bounded from above admits a supremum.

**Proposition 6.34.**  $\mathbb{Q} \subset \mathbb{R}$  and  $+, \times, <$  for  $\mathbb{R}$  are compatible with the ones for  $\mathbb{Q}$ .

*Proof.* That's a sketch of proof (for concision I use equality instead of identification/bijection).

1.  $\mathbb{N} \subset \mathbb{R}$ : if  $n \in \mathbb{N}$  then  $n = 1 + 1 + \dots + 1 \in \mathbb{R}$ . So  $\mathbb{N} \subset \mathbb{R}$ .
2.  $\mathbb{Z} \subset \mathbb{R}$ : if  $n \in \mathbb{N}$  then  $-n \in \mathbb{R}$ . So  $\mathbb{Z} \subset \mathbb{R}$ .
3.  $\mathbb{Q} \subset \mathbb{R}$ : if  $(a, b) \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$  then  $\frac{a}{b} := ab^{-1} \in \mathbb{R}$ . So  $\mathbb{Q} \subset \mathbb{R}$ . ■

**Proposition 6.35.**

- $\forall x, y, z \in \mathbb{R}, x \leq y \Rightarrow x + z \leq y + z$
- $\forall x, y, z \in \mathbb{R}, (x \leq y \text{ and } 0 \leq z) \Rightarrow xz \leq yz$
- $\forall x, y, u, v \in \mathbb{R}, (x \leq y \text{ and } u \leq v) \Rightarrow x + u \leq y + v$
- $\forall x \in \mathbb{R}, 0 < x \Leftrightarrow 0 < \frac{1}{x}$
- $\forall x, y \in \mathbb{R}, \forall z \in \mathbb{R}_+^*, x \leq y \Leftrightarrow xz \leq yz$
- $\forall x, y, u, v \in \mathbb{R}, (0 \leq x \leq y \text{ and } 0 \leq u \leq v) \Rightarrow xu \leq yv$
- $\forall x, y \in \mathbb{R}, 0 < x < y \Leftrightarrow \frac{1}{y} < \frac{1}{x}$

**Definition 6.36.** We define the *absolute value* by  $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}$  :

$$x \mapsto |x| := \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x \leq 0 \end{cases}$$

**Proposition 6.37.**

- $\forall x \in \mathbb{R}, |x| = \max(x, -x)$
- $\forall x \in \mathbb{R}, |x| \geq 0$
- $\forall x \in \mathbb{R}, x = 0 \Leftrightarrow |x| = 0$
- $\forall x, y \in \mathbb{R}, |x| = |y| \Leftrightarrow (x = y \text{ or } x = -y)$
- $\forall x, y \in \mathbb{R}, |xy| = |x||y|$
- $\forall x \in \mathbb{R} \setminus \{0\}, \left| \frac{1}{x} \right| = \frac{1}{|x|}$
- $\forall x, y \in \mathbb{R}, |x + y| \leq |x| + |y|$  (*triangle inequality*)
- $\forall x, y \in \mathbb{R}, ||x| - |y|| \leq |x - y|$  (*reverse triangle inequality*)

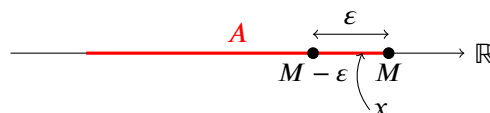
**Proposition 6.38.** For  $x, a \in \mathbb{R}$ ,

- $|x| \leq a \Leftrightarrow -a \leq x \leq a$
- $|x| < a \Leftrightarrow -a < x < a$
- $|x| \geq a \Leftrightarrow (x \geq a \text{ or } x \leq -a)$
- $|x| > a \Leftrightarrow (x > a \text{ or } x < -a)$
- If  $a \geq 0$  then  $|x| = a \Leftrightarrow (x = a \text{ or } x = -a)$

**Proposition 6.39.** Let  $A \subset \mathbb{R}$  and  $M \in \mathbb{R}$ . Then

$$M = \sup(A) \Leftrightarrow \begin{cases} \forall x \in A, x \leq M \\ \forall \varepsilon > 0, \exists x \in A, M - \varepsilon < x \end{cases}$$

The first condition ensures that  $M$  is an upper bound of  $A$ . The second one means it is the smallest one.



Beware, for simplicity I represented  $A$  as an interval in the above figure, but it may not be an interval!

*Proof.*

$\Rightarrow$  Assume that  $M = \sup(A)$ . Then  $M$  is an upper bound of  $A$  so  $\forall x \in A, x \leq M$ .

We know that if  $T$  is an other upper bound of  $A$  then  $M \leq T$  (since  $M$  is the least upper bound).

So, by taking the contrapositive, if  $T < M$  then  $T$  isn't an upper bound of  $A$ .

Let  $\varepsilon > 0$ . Since  $M - \varepsilon < M$ , we know that  $M - \varepsilon$  is not an upper bound of  $A$ , meaning that there exists  $x \in A$  such that  $M - \varepsilon < x$ .

$\Leftarrow$  Assume that

$$\begin{cases} \forall x \in A, x \leq M \\ \forall \varepsilon > 0, \exists x \in A, M - \varepsilon < x \end{cases}$$

Then, by the first condition,  $M$  is an upper bound of  $A$ . Let's prove it is the least one.

We will show the contrapositive: if  $T < M$  then  $T$  isn't an upper bound of  $A$ .

Let  $T \in \mathbb{R}$ . Assume that  $T < M$ . Set  $\varepsilon = M - T > 0$ . Then there exists  $x \in A$  such that  $M - \varepsilon < x$ , i.e.  $T < x$ . Hence  $T$  isn't an upper bound of  $A$  ■

We have a similar characterization for the infimum.

**Proposition 6.40.** *Let  $A \subset \mathbb{R}$  and  $m \in \mathbb{R}$ . Then*

$$m = \inf(A) \Leftrightarrow \begin{cases} \forall x \in A, m \leq x \\ \forall \varepsilon > 0, \exists x \in A, x < m + \varepsilon \end{cases}$$

**Proposition 6.41.** *Given  $A, B \subset \mathbb{R}$  two non-empty subsets of  $\mathbb{R}$ , we set*

- $A + B = \{x \in \mathbb{R} : \exists a \in A, \exists b \in B, x = a + b\}$
- $-A = \{x \in \mathbb{R} : -x \in A\}$

*Then*

- *If  $A$  and  $B$  are bounded from above then  $A + B$  is too and  $\sup(A + B) = \sup(A) + \sup(B)$ .*
- *If  $A$  is bounded from above then  $-A$  is bounded from below and  $\inf(-A) = -\sup(A)$ .*
- *If  $A$  and  $B$  are bounded from above then  $A \cup B$  is too and  $\sup(A \cup B) = \max(\sup(A), \sup(B))$*

**Theorem 6.42** ( $\mathbb{R}$  is archimedean).  $\forall \varepsilon > 0, \forall A > 0, \exists n \in \mathbb{N}, n\varepsilon > A$

*Proof.* Let  $\varepsilon > 0$  and  $A > 0$ .

Assume by contradiction that  $\forall n \in \mathbb{N}, n\varepsilon \leq A$ . Then  $E = \{n\varepsilon : n \in \mathbb{N}\}$  is non-empty and bounded from above so it admits a supremum  $M = \sup E$  by the least upper bound principle.

Since  $M - \varepsilon < M$ ,  $M - \varepsilon$  is not an upper bound of  $E$ , so there exists  $n \in \mathbb{N}$  such that  $n\varepsilon > M - \varepsilon$ .

Therefore  $(n + 1)\varepsilon > M$ , hence a contradiction. ■

**Proposition 6.43.** *For every  $x \in \mathbb{R}$ , there exists a unique  $n \in \mathbb{Z}$  such that  $n \leq x < n + 1$ .*

*We say that  $n$  is the integer part (or the floor function value) of  $x$  and we denote it by  $\lfloor x \rfloor$ .*

*Proof.* Let  $x \in \mathbb{R}$ .

**Existence.**

- *First case: if  $x \geq 0$ .*

We set  $E = \{k \in \mathbb{N} : x < k\}$ .

By the archimedean property (with  $\varepsilon = 1$ ), there exists  $m \in \mathbb{N}$  such that  $m > x$ . Hence  $E \neq \emptyset$ .

By the well-ordering principle,  $E$  admits a least element  $p$ .

We have that  $x < p$  since  $p \in E$  and that  $p - 1 \leq x$  since  $p - 1 \notin E$ .

Therefore  $n = p - 1$  satisfies  $n \leq x < n + 1$ .

- *Second case: if  $x < 0$ .* We show similarly that  $n = -\min \{k \in \mathbb{N} : -x \leq k\}$  suits the definition of  $\lfloor x \rfloor$ .

**Uniqueness.** Assume that  $n, n' \in \mathbb{Z}$  are two suitable integers, then

$$n \leq x < n + 1 \tag{6.1}$$

and

$$n' \leq x < n' + 1$$

We deduce from the last inequality that

$$-n' - 1 < -x \leq -n' \quad (6.2)$$

Summing (6.1) and (6.2), we get that  $n - n' - 1 < 0 < n - n' + 1$ .

Hence  $n - n' < 1$ , i.e.  $n - n' \leq 0$ , and  $-1 < n - n'$  i.e.  $0 \leq n - n'$ .

Therefore  $n = n'$ . ■

**Remark 6.44.** We have  $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ , from which we derive  $x - 1 < \lfloor x \rfloor \leq x$ .

**Theorem 6.45** ( $\mathbb{Q}$  is dense in  $\mathbb{R}$ ).  $\forall x, y \in \mathbb{R}, x < y \Rightarrow (\exists q \in \mathbb{Q}, x < q < y)$

*Proof.* Let  $x, y \in \mathbb{R}$  be such that  $x < y$ . Set  $\varepsilon = y - x > 0$ .

By the archimedean property, there exists  $n \in \mathbb{N} \setminus \{0\}$  such that  $n\varepsilon > 1$ , i.e.  $\frac{1}{n} < \varepsilon$ .

Set  $m = \lfloor nx \rfloor + 1$ . Then  $nx < m \leq nx + 1$ , so  $x < \frac{m}{n} \leq x + \frac{1}{n} < x + \varepsilon = y$ . ■

**Remark 6.46.** The above theorem is equivalent to the fact that any real number is the limit of a sequence of rational numbers (that you will prove in Problem Set).

**Definition 6.47.** A subset  $I \subset \mathbb{R}$  is an *interval* if  $\forall x, y \in I, \forall z \in \mathbb{R}, (x \leq z \leq y \Rightarrow z \in I)$ .

**Proposition 6.48.** If  $I \subset \mathbb{R}$  is a non-empty interval not reduced to a singleton then  $I \cap \mathbb{Q} \neq \emptyset$ .

*Proof.* Since  $I$  is non-empty and not reduced to a singleton, there exist  $x, y \in I$  with  $x < y$ .

Then, since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ , there exists  $q \in \mathbb{Q}$  such that  $x < q < y$ .

Since  $I$  is an interval,  $q \in I$ . Hence  $q \in I \cap \mathbb{Q} \neq \emptyset$ . ■

**Corollary 6.49.**  $\forall x, y \in \mathbb{R}, x < y \Rightarrow (\exists s \in \mathbb{R} \setminus \mathbb{Q}, x < s < y)$

*Proof.* Let  $x, y \in \mathbb{R}$  be such that  $x < y$ .

By Theorem 6.45, there exists  $q \in \mathbb{Q}$  such that  $x < q < y$ .

Still by Theorem 6.45, there exists  $p \in \mathbb{Q}$  such that  $x < p < q$ .

Hence we obtained  $p, q \in \mathbb{Q}$  such that  $x < p < q < y$ .

Set  $s = p + \frac{\sqrt{2}}{2}(q - p)$ . Then  $s \in \mathbb{R} \setminus \mathbb{Q}$  (otherwise, by contradiction,  $\sqrt{2}$  would be in  $\mathbb{Q}$ , which is not the case as you proved in the Week 4 of tutorials) and  $p < s < q$  (notice that  $0 < \frac{\sqrt{2}}{2} < 1$  so  $s$  is a number between  $p$  and  $q$ ).

We obtained  $s \in \mathbb{R} \setminus \mathbb{Q}$  such that  $x < s < y$ . ■

**Proposition 6.50.** If  $I \subset \mathbb{R}$  is an interval which is non-empty and not reduced to a singleton then  $I \cap (\mathbb{R} \setminus \mathbb{Q}) \neq \emptyset$ .

## 6.5 Decimal representation of real numbers

It is possible to generalize the decimal numeral system used to describe integers in order to describe real numbers. In what follows I only work with decimal expansions but all the statements/proofs work if we replace 10 by  $b \geq 2$ .

We start with a lemma that we will use several times in this section.

**Lemma 6.51.** Let  $(a_k)_{k \geq 1}$  be a sequence such that  $\forall k \in \mathbb{N} \setminus \{0\}, a_k \in \{0, 1, \dots, 9\}$ . Then the series

$$S = \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$$

is convergent and  $S \geq 0$ .

*Proof.*

Note that  $0 \leq \frac{a_k}{10^k} \leq \frac{9}{10^k}$  and that  $\sum_{k=1}^{+\infty} \frac{9}{10^k}$  is convergent (geometric series with ratio  $\frac{1}{10} < 1$ ).

Therefore we may conclude using the BCT. ■

**Remark 6.52.** Unfortunately the decimal representation may not be unique:

$$0.9999 \dots = \sum_{k=1}^{+\infty} \frac{9}{10^k} = \frac{9}{10} \times \frac{1}{1 - \frac{1}{10}} = 1.000 \dots$$

In order to achieve uniqueness we are going to restrict to expansions which don't end with infinitely many 9, see the definition below.

**Definition 6.53.** Let  $x \in \mathbb{R}$ . We say that

$$\lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$$

is a *proper decimal expansion* of  $x$  if

(i)  $\forall k \in \mathbb{N} \setminus \{0\}, a_k \in \{0, 1, \dots, 9\}$

(ii)  $\forall n \in \mathbb{N} \setminus \{0\}, \sum_{k=1}^n \frac{a_k}{10^k} \leq x - \lfloor x \rfloor < \sum_{k=1}^n \frac{a_k}{10^k} + \frac{1}{10^n}$

**Proposition 6.54.** If  $\lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$  is a proper decimal expansion of  $x \in \mathbb{R}$  then

$$1. \ x = \lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$$

$$2. \ \forall N \in \mathbb{N} \setminus \{0\}, \exists k > N, a_k \neq 9$$

Then we simply write  $x = \lfloor x \rfloor . a_1 a_2 a_3 \dots$

**Remark 6.55.** The last item means that a proper decimal expansion can't end with infinitely many 9.

*Proof.*

1. We already proved that  $S = \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$  is convergent. Hence we get  $S \leq x - \lfloor x \rfloor \leq S$ . So  $x = \lfloor x \rfloor + S$ .

2. Assume by contradiction that there exists  $N \in \mathbb{N} \setminus \{0\}$  such that  $\forall k > N, a_k = 9$ .

Then  $x - \lfloor x \rfloor = \sum_{k=1}^{+\infty} \frac{a_k}{10^k} = \sum_{k=1}^N \frac{a_k}{10^k} + \sum_{k=N+1}^{+\infty} \frac{9}{10^k} = \sum_{k=1}^N \frac{a_k}{10^k} + \frac{1}{10^N}$ . Which contradicts the definition of proper decimal expansion (the strict inequality in 6.53.(ii)). ■

**Theorem 6.56.** A real number  $x$  admits a unique proper decimal expansion.

*Proof.* Let  $x \in \mathbb{R}$ . Up to replacing  $x$  with  $x - \lfloor x \rfloor$ , we may assume that  $\lfloor x \rfloor = 0$ .

Assume that  $\sum_{k=1}^{+\infty} \frac{a_k}{10^k}$  is a proper decimal expansion of  $x$ .

Then, from 6.53.(ii), we get that

$$a_n \leq 10^n \left( x - \sum_{k=1}^{n-1} \frac{a_k}{10^k} \right) < a_n + 1$$

So the only possible suitable sequence  $(a_n)$  is given by  $a_1 = \lfloor 10x \rfloor$  and  $a_{n+1} = \left\lfloor 10^{n+1} \left( x - \sum_{k=1}^n \frac{a_k}{10^k} \right) \right\rfloor$ .

It proves the uniqueness, but we still need to check that it is valid.

- (i) Since  $\lfloor x \rfloor = 0$ , we have  $0 \leq x < 1$ . Thus  $0 \leq 10x < 10$ . Therefore  $a_1 = \lfloor 10x \rfloor \in \{0, 1, \dots, 9\}$ .  
Let  $n \in \mathbb{N} \setminus \{0\}$ , then

$$0 \leq 10^n \left( x - \sum_{k=1}^{n-1} \frac{a_k}{10^k} \right) - a_n < 1$$

Thus

$$0 \leq 10^{n+1} \left( x - \sum_{k=1}^n \frac{a_k}{10^k} \right) < 10$$

Therefore  $a_{n+1} \in \{0, 1, \dots, 9\}$ .

- (ii) We have  $\forall n \in \mathbb{N} \setminus \{0\}$ ,  $\sum_{k=1}^n \frac{a_k}{10^k} \leq x < \sum_{k=1}^n \frac{a_k}{10^k} + \frac{1}{10^n}$  by construction. ■

**Remark 6.57.** It is easy to compute the decimal expansion of a rational number. Indeed, let  $x = \frac{a}{b}$  where  $a \in \mathbb{Z}$  and  $b \in \mathbb{N} \setminus \{0\}$ .

By Euclidean division,  $a = bq_0 + r_0$  where  $0 \leq r_0 < b$ . Hence  $\frac{a}{b} = q_0 + \frac{r_0}{b}$ . Note that  $q_0 = \left\lfloor \frac{a}{b} \right\rfloor$ .

Now, again by Euclidean division,  $10r_0 = bq_1 + r_1$  where  $0 \leq r_1 < b$ .

And we repeat:  $10r_k = bq_{k+1} + r_{k+1}$  where  $0 \leq r_{k+1} < b$ .

According to the *pigeonhole principle* (or the *Dirichlet's drawer principle*), since there are only  $b$  possible remainders, the process will start looping after at most  $b$  steps.

But note that the  $(q_k)_{k \geq 1}$  defines exactly the decimal expansion of  $x$ .

Therefore the decimal expansion of a rational is eventually periodic.

**Definition 6.58.** We say that a proper decimal expansion is eventually periodic if

$$\exists r \in \mathbb{N}, \exists s \in \mathbb{N} \setminus \{0\}, \forall k \in \mathbb{N}, a_{r+k+s} = a_{r+k}$$

It means that

$$\begin{aligned} x &= \lfloor x \rfloor . b_1 b_2 \dots b_r \underline{c_1 c_2 \dots c_s} \\ &:= \lfloor x \rfloor . b_1 b_2 \dots b_r c_1 c_2 \dots c_s c_1 c_2 \dots c_s c_1 \dots \end{aligned}$$

**Example 6.59.** We want to find the decimal expansion of  $\frac{1529327}{24975}$ .

1.  $1529327 = 24975 \times 61 + 5852$
2.  $58520 = 24975 \times 2 + 8570$
3.  $85700 = 24975 \times 3 + 10775$
4.  $107750 = 24975 \times 4 + 7850$
5.  $78500 = 24975 \times 3 + 3575$
6.  $35750 = 24975 \times 1 + 10775$

And we start to loop. Therefore  $\frac{1529327}{24975} = 61.234314$

**Theorem 6.60.** A real number  $x$  is rational if and only if its proper decimal expansion is eventually periodic.

*Proof.*

$\Rightarrow$  That's exactly Remark 6.57.

$\Leftarrow$  Assume that the proper decimal expansion  $x = \lfloor x \rfloor + \sum_{k=1}^{+\infty} \frac{a_k}{10^k}$  is eventually periodic,

i.e.  $\exists r \in \mathbb{N}, \exists s \in \mathbb{N} \setminus \{0\}, \forall k \in \mathbb{N}, a_{r+k+s} = a_{r+k}$ .

Then  $x = \lfloor x \rfloor + \sum_{k=1}^r \frac{a_k}{10^k} + 10^{-r} \sum_{k=1}^{+\infty} \frac{a_{r+k}}{10^k}$ .

Hence it is enough to prove that  $y = \sum_{k=1}^{+\infty} \frac{a_{r+k}}{10^k} \in \mathbb{Q}$ .

Note that  $10^s y = N + y$  where  $N = \overline{a_{r+1} a_{r+2} \dots a_{r+s}}_{10} \in \mathbb{N}$ . Hence  $y = \frac{N}{10^s - 1} \in \mathbb{Q}$ . ■

**Remark 6.61.** According to the above proof,

$$\begin{aligned}
 a_t a_{t-1} \dots a_0 . b_1 b_2 \dots b_r \overline{c_1 c_2 \dots c_s} &= \overline{a_t a_{t-1} \dots a_0}^{10} + \sum_{k=1}^r \frac{b_k}{10^k} + 10^{-r} \frac{\overline{c_1 c_2 \dots c_s}^{10}}{10^s - 1} \\
 &= \overline{a_t a_{t-1} \dots a_0}^{10} + \frac{\overline{b_1 b_2 \dots b_r}^{10}}{10^r} + \frac{\overline{c_1 c_2 \dots c_s}^{10}}{10^{r+s} - 10^r} \\
 &= \frac{\overline{a_t a_{t-1} \dots a_0 b_1 b_2 \dots b_r c_1 c_2 \dots c_s}^{10}}{10^{r+s} - 10^r}
 \end{aligned}$$

**Example 6.62.**

$$\begin{aligned}
 \bullet \quad 61.\underline{234314} &= \frac{61234314 - 61234}{10^6 - 10^3} = \frac{61173080}{999000} \\
 \bullet \quad 0.\underline{3} &= \frac{3 - 0}{10 - 1} = \frac{3}{9} \qquad \bullet \quad 42.\underline{012} = \frac{42012 - 42}{10^3 - 1} = \frac{41970}{999}
 \end{aligned}$$

## 6.6 $\sqrt{2}$ is irrational

Using the IVT, we may prove that there exists a unique positive real number  $x > 0$  such that  $x^2 = 2$ . We denote it by  $\sqrt{2}$ .

**Theorem 6.63.**  $\sqrt{2} \notin \mathbb{Q}$

Below are some of my favorite proofs for the irrationality of  $\sqrt{2}$ .

*Proof 1 (Fundamental Theorem of Arithmetic).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ . Then  $2b^2 = a^2$ .

The prime factorization of the LHS has an odd number of primes (counted with exponents) whereas the RHS has an even number of primes (counted with exponents).

Which is impossible since the prime factorization is unique up to order. ■

*Proof 2 (Euclid's lemma).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  written in lowest form.

Then  $2b^2 = a^2$ . Therefore  $2|a^2$ . By Euclid's lemma,  $2|a$ , so  $a = 2k$ .

Thus  $2b^2 = 4k^2$ , from which we get  $b^2 = 2k^2$ . By Euclid's lemma,  $2|b$ .

Hence  $2|\gcd(a, b) = 1$ , which is a contradiction. ■

*Proof 3 (Gauss' lemma).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  written in lowest form.

Then  $2b^2 = a^2$ . Therefore  $b|a^2$ .

Since  $\gcd(a, b) = 1$ , by Gauss' lemma (applied twice),  $b|1$  and hence  $b = 1$  (since  $b \in \mathbb{N} \setminus \{0\}$  in lowest form).

Hence  $a^2 = 2$ . Which is impossible (2 is not a perfect square:  $\forall x \in \mathbb{Z}$ ,  $x^2 \equiv 0 \pmod{3}$  or  $x^2 \equiv 1 \pmod{3}$ ). ■

*Proof 4 (proof by infinite descent).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  where  $a \in \mathbb{N}$  and  $b \in \mathbb{N} \setminus \{0\}$ .

Then  $2b^2 = a^2$ . Then  $a(a - b) = a^2 - ab = 2b^2 - ab = b(2b - a)$ . Hence  $\sqrt{2} = \frac{a}{b} = \frac{2b-a}{a-b}$ .

Note that  $1 < \sqrt{2} = \frac{a}{b}$ , thus  $0 < a - b$ . Therefore  $0 < 2b - a$ , so  $a - b < b$ .

Therefore we obtained another expression of  $\sqrt{2}$  with a smaller positive denominator.

By repeating this process, we may construct an infinite sequence  $\sqrt{2} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \dots$  such that  $a_k > 0$  and  $0 < b_{k+1} < b_k$ .

Which is a contradiction since there is no decreasing infinite sequence of natural numbers. ■

*Proof 5 (by congruences).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  written in lowest form. Then  $2b^2 = a^2$ .

Since  $\gcd(a, b) = 1$ , we can't have  $a \equiv 0 \pmod{3}$  and  $b \equiv 0 \pmod{3}$  simultaneously (otherwise  $3 \mid \gcd(a, b)$ ).

- Either  $a \equiv \pm 1 \pmod{3}$  and  $b \equiv 0 \pmod{3}$ , then  $a^2 - 2b^2 \equiv 1 \pmod{3}$ ,
- or  $a \equiv 0 \pmod{3}$  and  $b \equiv \pm 1 \pmod{3}$ , then  $a^2 - 2b^2 \equiv 1 \pmod{3}$ ,
- or  $a \equiv \pm 1 \pmod{3}$  and  $b \equiv \pm 1 \pmod{3}$ , then  $a^2 - 2b^2 \equiv 2 \pmod{3}$ .

Therefore  $a^2 - 2b^2 \not\equiv 0 \pmod{3}$  and so  $a^2 - 2b^2 \neq 0$ . Which is a contradiction. ■

*Proof 6 (by the well-ordering principle).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ . Then  $a = \sqrt{2}b$ .

Therefore  $E = \{n \in \mathbb{N} : n\sqrt{2} \in \mathbb{N} \setminus \{0\}\}$  is not empty since it contains  $|b|$  as  $\sqrt{2}|b| = |a|$ .

By the well-ordering principle,  $E$  admits a least element  $p$ . Then  $p\sqrt{2} \in \mathbb{N} \setminus \{0\}$ .

Set  $q = p\sqrt{2} - p$ . Then  $q \in \mathbb{Z}$ . Besides  $q = p(\sqrt{2} - 1)$  so that  $0 < q < p$ .

But  $q\sqrt{2} = 2p - p\sqrt{2} = p - q \in \mathbb{N} \setminus \{0\}$ . So  $q \in E$ .

Which is a contradiction since  $p$  is the least element of  $E$  and  $q < p$ . ■

*Proof 7 (by the rational root theorem).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  written in lowest form.

Since  $\sqrt{2} = \frac{a}{b}$  is a root of  $x^2 - 2 = 0$ , we deduce from the rational root theorem that  $a \mid 2$  and  $b \mid 1$ .

So either  $\sqrt{2} = \pm 1$  or  $\sqrt{2} = \pm 2$ .

We obtain a contradiction in both cases since  $(\pm 1)^2 = 1 \neq 2$  and  $(\pm 2)^2 = 4 \neq 2$ . ■

*Proof 8 (by the archimedean property).*

For  $n \in \mathbb{N}$ , set  $u_n = (\sqrt{2} - 1)^n$ . We may prove either by induction or using the binomial formula, that for every  $n$ , there exist  $a_n, b_n \in \mathbb{Z}$  such that  $u_n = a_n + b_n\sqrt{2}$ .

Since<sup>4</sup>  $0 < \sqrt{2} - 1 < \frac{1}{2}$ , we may also prove that  $0 < u_n \leq \frac{1}{2^n}$ .

Assume by contradiction that  $\sqrt{2} = \frac{p}{q} \in \mathbb{Q}$ , then

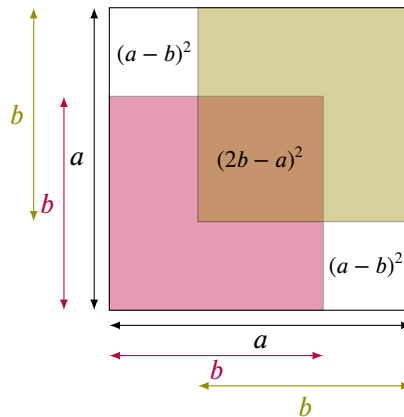
$$u_n = a_n + b_n\sqrt{2} = a_n + b_n\frac{p}{q} = \frac{qa_n + pb_n}{q}$$

Since  $u_n > 0$  we get that  $|qa_n + pb_n| \geq 1$  and that  $u_n \geq \frac{1}{|q|}$ .

Therefore  $\forall n \in \mathbb{N}$ ,  $0 < \frac{1}{|q|} \leq u_n \leq \frac{1}{2^n}$ . Which contradicts the archimedean property. ■

*Proof 9 (geometric version of proof 4).*

Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$  where  $a \in \mathbb{N}$  and  $b \in \mathbb{N} \setminus \{0\}$ . Then  $a = \sqrt{2}b > b$ .



<sup>4</sup>Use the fact that  $(0, +\infty) \ni x \rightarrow x^2 \in \mathbb{R}$  is increasing and that  $2 \leq \left(\frac{3}{2}\right)^2$  to conclude that  $\sqrt{2} \leq \frac{3}{2}$ .



By a direct computation of the side length, the square at the center has an area of  $\mathcal{A} = (2b - a)^2$ .

But, by inclusion-exclusion,  $\mathcal{A}$  also satisfies  $2(a - b)^2 + 2b^2 - \mathcal{A} = a^2$ .

So  $\mathcal{A} = 2(a - b)^2 + 2b^2 - a^2 = 2(a - b)^2$  since  $a^2 = 2b^2$ .

Therefore  $2(a - b)^2 = \mathcal{A} = (2b - a)^2$ . Thus  $2 = \frac{(2b-a)^2}{(a-b)^2}$ .

Hence  $\sqrt{2} = \frac{2b-a}{a-b}$  with<sup>5</sup>  $0 < 2b - a$  and  $0 < a - b < b$ .

By repeating this process, we may construct an infinite sequence  $\sqrt{2} = \frac{a}{b} = \frac{a_1}{b_1} = \frac{a_2}{b_2} = \dots$  such that  $a_k > 0$  and  $0 < b_{k+1} < b_k$ .

Which is a contradiction since there is no decreasing infinite sequence of natural numbers. ■

*Proof 10 (Pythagoras flavored).*

Let  $ABC$  be a isosceles right triangle in  $A$ . By the Pythagorean theorem  $\frac{BC}{AB} = \sqrt{2}$ .

Assuming that  $\sqrt{2}$  is rational means geometrically that  $\overline{BC}$  and  $\overline{AB}$  are commensurable, i.e. they are both integral multiple of a another length  $d$ <sup>6</sup>.

Put  $D$  on  $[BC]$  such that  $\overline{BD} = \overline{AB}$ .

Define  $E$  as the intersection of  $(AC)$  with the line through  $D$  which is perpendicular to  $(BC)$ .

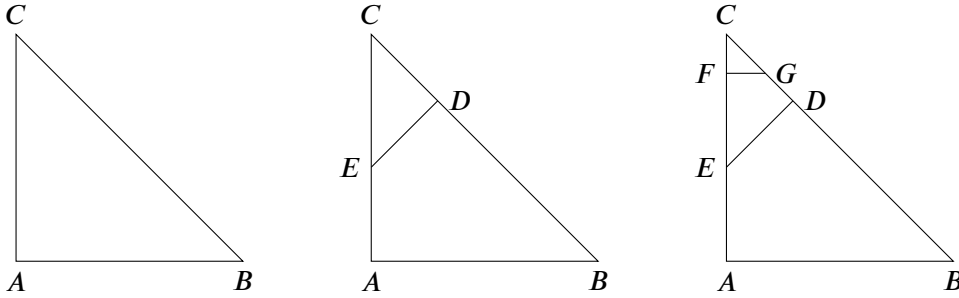
Note that<sup>7</sup>  $\overline{AE} = \overline{ED} = \overline{DC}$ .

Thus  $\overline{CD} = \overline{BC} - \overline{AB}$  and  $\overline{EC} = \overline{AC} - \overline{AE} = \overline{AB} - (\overline{BC} - \overline{AB}) = 2\overline{AB} - \overline{BC}$ .

Therefore  $\overline{CD}$  and  $\overline{EC}$  are integral multiple of  $d$ .

Besides  $DEC$  is a isosceles right triangle in  $D$ , therefore we may repeat this construction on the triangle  $DEC$  in order to construct an infinite sequence of segment lines  $(AC, EC, FC, \dots, \text{see below})$  which are all integral multiple of  $d$  and with decreasing length.

Which is impossible.



The above proof is actually another geometric version of Proof 4:

Algebraically:  $\frac{2b-a}{a-b} = \frac{2-a/b}{a/b-1} = \frac{2-\sqrt{2}}{\sqrt{2}-1} = \sqrt{2}$ .

Geometrically:  $\sqrt{2} = \frac{\overline{EC}}{\overline{CD}} = \frac{2\overline{AB} - \overline{BC}}{\overline{BC} - \overline{AB}}$ .

*Proof 11 (my favorite one).*

The proof is left as an exercise to the reader. ■

<sup>5</sup>See Proof 4 for  $0 < 2b - a$ .

<sup>6</sup>That is the geometric version of *irrationality* used by ancient Greeks:

if  $\sqrt{2} = \frac{a}{b}$ , set  $d = \frac{AB}{b}$  then  $\overline{AB} = bd$  and  $\overline{BC} = \sqrt{2} \times \overline{AB} = \frac{a}{b}bd = ad$ .

<sup>7</sup>Compare the triangles  $BAE$  and  $BDE$  which are respectively right in  $A$  and  $D$  with common hypotenuse and  $\overline{AB} = \overline{DB}$ , so, by the Pythagorean theorem,  $\overline{AE} = \overline{ED}$ . Besides the triangle  $CDE$  is isosceles right in  $D$  by angle considerations, thus  $\overline{ED} = \overline{DC}$ .

Before leaving  $\sqrt{2}$ , I would like to show you a funny proof relying on the *tertium non datur*.

**Proposition 6.64.** *There exist  $a, b > 0$  irrational numbers such that  $a^b \in \mathbb{Q}$ .*

*Proof.*

- Assume that  $\sqrt{2}^{\sqrt{2}} \in \mathbb{Q}$ . Then we can take  $a = b = \sqrt{2}$ .
- Assume that  $\sqrt{2}^{\sqrt{2}} \notin \mathbb{Q}$ . Then we can take  $a = \sqrt{2}^{\sqrt{2}}$  and  $b = \sqrt{2}$ . Indeed,  $\left(\sqrt{2}^{\sqrt{2}}\right)^{\sqrt{2}} = \sqrt{2}^2 = 2$ . ■

**Remark 6.65.** Note that in the above proof it is not necessary to know whether  $\sqrt{2}^{\sqrt{2}}$  is rational or not in order to conclude! That's really cool! By the way, it is not rational using Gelfond–Schneider Theorem.

## 6.7 $e$ is irrational

You know from your first year calculus that  $e = \sum_{n=0}^{+\infty} \frac{1}{n!}$ .

**Theorem 6.66.**  $e \notin \mathbb{Q}$

*Proof 1.* Assume by contradiction that  $e = \frac{a}{b}$  where  $a, b \in \mathbb{N} \setminus \{0\}$ . Note that  $b > 1$  since  $e \notin \mathbb{N}$ . Besides

$$b! \left( e - \sum_{n=0}^b \frac{1}{n!} \right) = b! \left( \sum_{n \geq b+1} \frac{1}{n!} \right)$$

Note that the LHS is an integer. We are going to derive a contradiction by proving that the RHS is not an integer. Indeed

$$0 < b! \left( \sum_{n \geq b+1} \frac{1}{n!} \right) \leq \sum_{n \geq 1} \frac{1}{(b+1)^n} = \frac{1}{b} < 1$$

■

It is also possible to use an approach similar to the eighth proof for the irrationality of  $\sqrt{2}$ :

*Proof 2.* For  $n \in \mathbb{N}$ , set  $u_n = \int_0^1 x^n e^x dx$ .

Using an induction and integration by part, we can prove that for  $n \in \mathbb{N}$ , there exist  $a_n, b_n \in \mathbb{Z}$  such that  $u_n = a_n + eb_n$ .

Assume by contradiction that  $e = \frac{p}{q}$  where  $p, q \in \mathbb{N} \setminus \{0\}$ . Then  $0 < u_n = a_n + b_n \frac{p}{q} = \frac{qa_n + pb_n}{q}$ .

Since  $u_n > 0$  we get that  $qa_n + pb_n \geq 1$  and that  $u_n \geq \frac{1}{q}$ .

Therefore  $\forall n \in \mathbb{N}$ ,  $0 < \frac{1}{q} \leq u_n \leq \int_0^1 x^n e^x dx = \frac{e}{n+1}$ .

Which is impossible. ■

## Exercises

### Exercise 1.

Prove that  $\sqrt{7+4\sqrt{3}} + \sqrt{7-4\sqrt{3}} \in \mathbb{N}$ .

### Exercise 2.

1. Prove that  $\forall a, b \in \mathbb{R}, ab \leq \frac{a^2 + b^2}{2}$ .
2. Prove that  $\forall a, b, c \in \mathbb{R}, ab + bc + ac \leq a^2 + b^2 + c^2$ .
3. Prove that  $\forall a, b, c \in \mathbb{R}, 3ab + 3bc + 3ac \leq (a + b + c)^2$ .

### Exercise 3.

Prove that  $\forall x \in \mathbb{R}, |x - 1| \leq x^2 - x + 1$ .

### Exercise 4.

1. Prove that  $\forall x, y \in \mathbb{R}, |x| + |y| \leq |x + y| + |x - y|$ .
2. Prove that  $\forall x, y \in \mathbb{R}, \frac{|x + y|}{1 + |x + y|} \leq \frac{|x|}{1 + |x|} + \frac{|y|}{1 + |y|}$ .

### Exercise 5.

Let  $A \subset \mathbb{R}$  be non-empty and bounded. We set  $B = \{|x - y| : x, y \in A\}$ .

1. Prove that  $B$  admits a supremum.
2. Prove that  $\sup B = \sup A - \inf A$ .

### Exercise 6.

Prove that if  $f : [0, 1] \rightarrow [0, 1]$  is non-decreasing then  $f$  admits a fixed point, i.e.  $\exists a \in [0, 1], f(a) = a$ .

*Hint: study  $\{x \in [0, 1] : f(x) \geq x\}$ .*

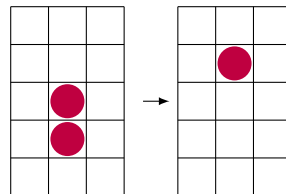
### Exercise 7.

Let  $A \subset \mathbb{R}$  be non-empty and bounded from above. Set  $M = \sup(A)$ .

Prove that if  $M \notin A$  then for all  $\varepsilon > 0$  the set  $(M - \varepsilon, M) \cap A$  contains infinitely many elements.

### Exercise 8. *Conway's Soldiers, or why geometric series are useful*

We consider an infinite checkerboard represented by  $\mathbb{Z} \times \mathbb{Z}$  with pieces on it. The pieces are allowed to move using the peg solitaire rules: a move consists of one piece jumping over another piece into an empty cell (either horizontally or vertically), the piece which was jumped over is then removed.



The goal of this exercise is to show that there is no initial configuration with finitely many pieces located on  $\mathbb{Z} \times \mathbb{Z}_{\leq 0}$  allowing to reach cells with  $y$ -coordinate 5.

1. Prove that there exists initial configurations allowing to reach cells with  $y$ -coordinate 1, 2, 3 and 4.
2. We denote by  $\sigma$  the positive root of  $x^2 + x - 1 = 0$  and we fix a target cell on  $\mathbb{Z} \times \mathbb{Z}$ . We label each cell of  $\mathbb{Z} \times \mathbb{Z}$  with  $\sigma^n$  where  $n$  is the Manhattan distance from the target to the cell.

$\sigma^4$	$\sigma^3$	$\sigma^2$	$\sigma^3$
$\sigma^3$	$\sigma^2$	$\sigma^1$	$\sigma^2$
$\sigma^2$	$\sigma^1$	$\sigma^0$	$\sigma^1$
$\sigma^3$	$\sigma^2$	$\sigma^1$	$\sigma^2$
$\sigma^4$	$\sigma^3$	$\sigma^2$	$\sigma^3$

Given a finite configuration  $C$  (i.e. finitely pieces on the checkerboard), we define  $F(C) = \sum_{i \in C} \sigma^{n_i}$  where  $n_i$  is the Manhattan from the target cell to the cell  $i$ .

Prove that if  $C'$  is a configuration obtained after one move then  $F(C') - F(C) \leq 0$ .

3. Compute  $\sum_{n=2}^{+\infty} \sigma^n$ .
4. Assume that the target cell is  $(0, 5)$ . Compute  $F(C)$  where  $C$  contains all the cells with non-positive  $y$ -coordinates (hence  $C$  contains infinitely many cells).
5. Conclude that there is no finite initial configuration in  $\mathbb{Z} \times \mathbb{Z}_{\leq 0}$  allowing to reach  $(0, 5)$ .

#### Exercise 9.

1. Prove that  $\forall x, y \in \mathbb{R}, \lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$ .
2. Prove that  $\forall n \in \mathbb{N} \setminus \{0\}, \forall x \in \mathbb{R}, \left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor = \lfloor x \rfloor$ .

#### Exercise 10.

1. Prove that  $\forall n \in \mathbb{N}, (2 + \sqrt{3})^n + (2 - \sqrt{3})^n \in 2\mathbb{N}$ .
2. Prove that for every  $n \in \mathbb{N}, \left\lfloor (2 + \sqrt{3})^n \right\rfloor$  is odd.

#### Exercise 11.

Let  $I$  and  $J$  be two open intervals of  $\mathbb{R}$ . Prove that  $(I \cap \mathbb{Q}) \cap (J \cap \mathbb{Q}) = \emptyset \implies I \cap J = \emptyset$ .

#### Exercise 12.

1. Is the sum of two irrational numbers always an irrational number?
2. Is the product of two irrational numbers always an irrational number?
3. Prove that  $\forall x \in \mathbb{R} \setminus \mathbb{Q}, \forall y \in \mathbb{Q}, x + y \notin \mathbb{Q}$ .
4. Prove that  $\forall x \in \mathbb{R} \setminus \mathbb{Q}, \forall y \in \mathbb{Q} \setminus \{0\}, xy \notin \mathbb{Q}$ .

#### Exercise 13.

Prove that the following numbers are irrational

1.  $\sqrt{3}$
2.  $\sqrt{6}$
3.  $\sqrt{11}$
4.  $\sqrt[3]{3 + \sqrt{11}} \notin \mathbb{Q}$
5.  $\sqrt{2} + \sqrt{3}$
6.  $(\sqrt{2} + \sqrt{3})^2$
7.  $\sqrt{2} + \sqrt{3} + \sqrt{6}$
8.  $(3\sqrt{2} + 2\sqrt{3} + \sqrt{6})^2$
9.  $\sqrt{7} + \sqrt{3}$ .

**Exercise 14.**

Prove that  $\forall n \in \mathbb{N}, \sqrt{n} \in \mathbb{Q} \Leftrightarrow \sqrt{n} \in \mathbb{N} \Leftrightarrow \exists m \in \mathbb{N}, n = m^2$ .

**Exercise 15.**

Is  $\sum_{n=1}^{+\infty} 10^{-\frac{n(n+1)}{2}} = 0.101001000100001000001 \dots$  a rational number?

**Exercise 16.**

1. We fix  $r > 0$  and  $n \in \mathbb{N}$ . We define  $f : \mathbb{R} \rightarrow \mathbb{R}$  by  $f(x) = \frac{1}{n!} x^n (1-x)^n$  and we set

$$F(x) = \sum_{k \geq 0} (-1)^k r^{2n-2k} f^{(2k+1)}(x)$$

(note that the sum is finite since  $f$  is a polynomial).

- (a) Prove that  $\forall k \in \mathbb{N}, f^{(k)}(0) \in \mathbb{Z}$ .
- (b) Prove that  $\forall k \in \mathbb{N}, f^{(k)}(1) \in \mathbb{Z}$ .
- (c) Prove that  $F''(x) = -r^2 F(x) + r^{2n+2} f(x)$ .
- (d) Compute  $\frac{d}{dx} (F'(x) \sin(rx) - rF(x) \cos(rx))$ .
- (e) Compute  $\int_0^1 f(x) \sin(rx) dx$ .

2. Prove that  $\forall r \in (0, \pi], r \in \mathbb{Q} \implies (\sin(r) \notin \mathbb{Q} \text{ or } \cos(r) \notin \mathbb{Q})$ .

3. Prove that  $\pi \notin \mathbb{Q}$ .

## Chapter 7

# Cardinality

Let's start with a short story.

A conference about singularity theory is going to take place in the lovely village of Tarski, and participants start to arrive. Most of them decided to be hosted at the Aleph Nought Hotel. It is a huge hotel, built especially for this occasion, with infinitely many rooms numbered using  $\mathbb{N}$ : 0, 1, 2, 3... Despite this large number of rooms, the sign *FULL* lights up over the front door indicating that there is no vacancy!

A group of 42 late mathematicians from Nice show up at the front desk and are received by the receptionist David H. who exclaims *"For Cantor's sake! I thought that we were not expecting new guests! No worries, I will find a solution"*. Then he uses the intercom of the hotel to send the following message to all the current guests: *"Sorry for the inconvenience, but I would need your cooperation in order to accomodate new guests. Please, if your current room is labeled  $n$  then could you move to the room  $n + 42$ ? Thank you so much and once again, sorry of the inconvenience"*. Therefore the rooms 0, 1, 2, ..., 41 are now available for the latecomers and the already hosted guests still have individual rooms.

Later a bus containing the canadian delegation reaches the hotel. The driver meets David H. and says *"Sorry for the delay, I got lost on the way. I have a bus full with infinitely many canadian mathematicians! We booked infinitely rooms at your hotel and for your conveniency we gave to each of our member a card with a natural number: 0, 1, 2..."*. Then David H. desperates *"Holy Dedekind! What a night! No worries, I will handle the situation!"*.

And once again, he uses the intercom of the hotel to send the following message: *"If you are currently in the room  $n$ , please could you move to the room  $2n + 1$ ? Sorry for the inconvenience."* This way the guests already in the hotel still have individual rooms and now there are infinitely many empty rooms (the even numbered ones) for the canadian participants. Next David H. asks the newcomers *"If your card shows the number  $m$ , please go to the room  $2m$ "*, and everyone gets an individual room<sup>1</sup>.

Our friendly receptionist is later awakened by a terrible loudly noise outside. He shouts *"In Gödel's name, what's happening now?"* and then he reaches the front door to see infinitely many flying saucers<sup>2</sup> (numbered 0, 1, 2, ...). An extraterrestrial mathematician goes to meet David H. and tells *"Sorry for the delay, we come from Proxima Centauri and we got stuck in traffic jams. Each of our ships contains infinitely countably many participants!"*.

David H. doesn't seem particularly concerned and send the following message to the current guests using his intercom: *"Dear guest, if you are currently in the room  $n$ , please could you move to the room  $2n$ ?"*. Therefore the odd-numbered rooms are now free. Then David H. asks the  $k^{\text{th}}$  passenger of the  $l^{\text{th}}$  ship to go to the room  $3^k 5^l$ , so that everyone gets an individual room<sup>3</sup>.

---

<sup>1</sup>The function  $\mathbb{N} \ni n \mapsto 2n + 1 \in \mathbb{N}$  is one-to-one so the current guests keep individual rooms. Then  $\mathbb{N} \ni m \mapsto 2m \in \mathbb{N}$  is also one-to-one, so two different newcomers are sent to two different rooms (and these rooms are empty since even numbered).

<sup>2</sup>Until now, the story was quite realistic...

<sup>3</sup>By uniqueness of the prime factorization,  $\mathbb{N} \ni (k, l) \mapsto 3^k 5^l \in \mathbb{N}$  is injective, so the newcomers are sent to different rooms, and these rooms are free since odd-numbered.

This story highlights something interesting about the behaviour of infinite sets such as  $\mathbb{N}$ . First we were able to add 42 elements to  $\mathbb{N}$  without changing its *size*. Even less intuitively, then we added a copy of  $\mathbb{N}$  to  $\mathbb{N}$  without changing its *size*. And finally, we were even able to add  $\mathbb{N} \times \mathbb{N}$  (i.e. infinitely many copies of  $\mathbb{N}$ ) to  $\mathbb{N}$  without changing its *size*.

The goal of this chapter is to formally define the notion of *size* of a set (it will be called *cardinality*) and to study its properties (which may be counter-intuitive, as above, for infinite sets).

## 7.1 Reviews about functions

**Definition 7.1** (Informal<sup>4</sup> definition of a function). A *function* (or *map*) is the data of two sets  $A$  and  $B$  together with a "process" which assigns to each  $x \in A$  a unique  $f(x) \in B$ :

$$f : \begin{cases} A & \rightarrow & B \\ x & \mapsto & f(x) \end{cases}$$

Here,  $f$  is the name of the function,  $A$  is the *domain* of  $f$ , and  $B$  is the *codomain* of  $f$ .

**Remark 7.2.** This process can be:

- A formula: define  $f : \mathbb{R} \rightarrow \mathbb{R}$  by  $f(x) = e^{x^2 - \pi} + 42$ .
- An exhaustive list: define  $f : \{1, 2, 3\} \rightarrow \mathbb{R}$  by  $f(1) = \pi$ ,  $f(2) = \sqrt{2}$ ,  $f(3) = e$ .
- A property characterizing  $f$  uniquely:  $\log$  is the unique antiderivative of  $g : (0, +\infty) \rightarrow \mathbb{R}$  defined by  $g(x) = \frac{1}{x}$  such that  $\log(1) = 0$ .
- By induction: we define the sequence  $u_n : \mathbb{N} \rightarrow \mathbb{R}$  by  $u_0 = 1$  and  $\forall n \in \mathbb{N}$ ,  $u_{n+1} = u_n^2 + 1$ .
- The solution of a differential equation: the exponential function  $\exp : \mathbb{R} \rightarrow \mathbb{R}$  is the unique differentiable function such that  $\exp' = \exp$  and  $\exp(0) = 1$ .
- The solution of a functional equation: the exponential function with base  $a \in \mathbb{R}$  denoted by  $\exp_a : \mathbb{R} \rightarrow \mathbb{R}$  is the unique monotonic function such that  $\exp_a(x + y) = \exp_a(x) \exp_a(y)$  and  $\exp_a(1) = a$ .
- ...

**Remark 7.3.** The domain and codomain are part of the definition of a function. For instance:

- $f : \begin{cases} \mathbb{R} & \rightarrow & (0, +\infty) \\ x & \mapsto & e^x \end{cases}$  and  $g : \begin{cases} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & e^x \end{cases}$  are not the same function (the first one is surjective but not the second one, see below).
- $f : \begin{cases} [0, +\infty) & \rightarrow & \mathbb{R} \\ x & \mapsto & x^2 + 1 \end{cases}$  and  $g : \begin{cases} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & x^2 + 1 \end{cases}$  are not the same function (the first one is injective but not the second one, see below).

A function is not simply a "formula", you need to specify the domain and the codomain.

**Definitions 7.4.** Given a function  $f : A \rightarrow B$ .

- The *image* of  $E \subset A$  by  $f$  is  $f(E) := \{f(x) : x \in E\} \subset B$ .
- The *image* of  $f$  (or *range* of  $f$ ) is  $\text{Range}(f) := f(A)$ .
- The *preimage* of  $F \subset B$  by  $f$  is  $f^{-1}(F) := \{x \in A : f(x) \in F\}$ .
- The *graph* of  $f$  is the set  $\Gamma_f := \{(x, y) \in A \times B : y = f(x)\}$ .
- We say that  $f$  is *injective* (or *one-to-one*) if  $\forall x_1, x_2 \in A$ ,  $x_1 \neq x_2 \implies f(x_1) \neq f(x_2)$  or equivalently by taking the contrapositive  $\forall x_1, x_2 \in A$ ,  $f(x_1) = f(x_2) \implies x_1 = x_2$ .
- We say that  $f$  is *surjective* (or *onto*) if  $\forall y \in B$ ,  $\exists x \in A$ ,  $y = f(x)$ .
- We say that  $f$  is *bijective* if it is injective and surjective, i.e.  $\forall y \in B$ ,  $\exists! x \in A$ ,  $y = f(x)$ .

<sup>4</sup>Formally, a function  $f : A \rightarrow B$  is characterized by its graph  $\Gamma_f \subset A \times B$  which needs to satisfy  $\forall x \in A$ ,  $\exists! y \in B$ ,  $(x, y) \in \Gamma_f$ .

**Proposition 7.5.** Let  $f : E \rightarrow F$  and  $g : F \rightarrow G$  be two functions.

1. If  $f$  and  $g$  are injective then so is  $g \circ f$ .
2. If  $f$  and  $g$  are surjective then so is  $g \circ f$ .
3. If  $g \circ f$  is injective then  $f$  is injective too.
4. If  $g \circ f$  is surjective then  $g$  is surjective too.

*Proof.*

1. Let  $x, y \in E$  be such that  $g(f(x)) = g(f(y))$ . Then  $f(x) = f(y)$  since  $g$  is injective. Thus  $x = y$  since  $f$  is injective.
2. Let  $z \in G$ . Since  $g$  is surjective, it exists  $y \in F$  such that  $z = g(y)$ . Since  $f$  is surjective, it exists  $x \in E$  such that  $y = f(x)$ . Therefore  $z = g(f(x))$ .
3. Let  $x, y \in E$  such that  $f(x) = f(y)$ . Then  $g(f(x)) = g(f(y))$  and thus  $x = y$  since  $g \circ f$  is injective.
4. Let  $z \in G$ . Since  $g \circ f$  is surjective, there exists  $x \in E$  such that  $z = g(f(x))$ . Then  $y = f(x) \in F$  satisfies  $g(y) = z$ . ■

**Proposition 7.6.**  $f : A \rightarrow B$  is bijective if and only if there exists  $g : B \rightarrow A$  such that  $\begin{cases} \forall x \in A, g(f(x)) = x \\ \forall y \in B, f(g(y)) = y \end{cases}$ .

Then  $g$  is unique, it is called the inverse of  $f$  and denoted by  $f^{-1} : B \rightarrow A$ .

*Proof.*  $\Rightarrow$  Assume that  $f$  is bijective, then  $\forall y \in B, \exists! x_y \in A, f(x_y) = y$ . We define  $g : B \rightarrow A$  by  $g(y) = x_y$ . Then  $g$  satisfies the required properties.

$\Leftarrow$  Assume that there exists  $g$  as in the statement. Then  $g \circ f = id_A$  is injective, so  $f$  is too by Proposition 7.5. And  $f \circ g = id_B$  is surjective, thus  $f$  is too, still by Proposition 7.5. Therefore  $f$  is bijective.

For the uniqueness: assume there exist two such functions  $g_1, g_2 : B \rightarrow A$ . Let  $y \in B$ . Then  $f(g_1(y)) = y = f(g_2(y))$ . So  $g_1(y) = g_2(y)$  since  $f$  is injective. ■

## 7.2 Finite sets

**Definition 7.7.** We say that a set  $E$  is finite if there exists  $n \in \mathbb{N}$  and a bijection  $f : \{k \in \mathbb{N} : k < n\} \rightarrow E$ . Then we write  $|E| = n$ .

**Remark 7.8.** Note that  $\{k \in \mathbb{N} : k < n\} = \{0, 1, 2, \dots, n-1\}$ .

We are first going to prove that if such a  $n$  exists, then it is unique.

**Lemma 7.9.** Let  $n, p \in \mathbb{N}$ . If there exists an injective function  $f : \{k \in \mathbb{N} : k < n\} \rightarrow \{k \in \mathbb{N} : k < p\}$  then  $n \leq p$ .

*Proof.* We prove the statement by induction on  $n$ .

- *Base case at  $n = 0$ :* for any  $p \in \mathbb{N}$  we have  $n \leq p$ .
- *Induction step.* Assume that the statement holds for some  $n \in \mathbb{N}$ .  
Let  $p \in \mathbb{N}$ . Assume that there exists an injective function  $f : \{k \in \mathbb{N} : k < n+1\} \rightarrow \{k \in \mathbb{N} : k < p\}$ .  
Define  $g : \{k \in \mathbb{N} : k < n\} \rightarrow \{k \in \mathbb{N} : k < p-1\}$  as follows:

$$g(x) = \begin{cases} f(x) & \text{if } f(x) < f(n) \\ f(x) - 1 & \text{if } f(x) > f(n) \end{cases}$$

Note that  $f(x) \neq f(n)$  since  $f$  is injective.



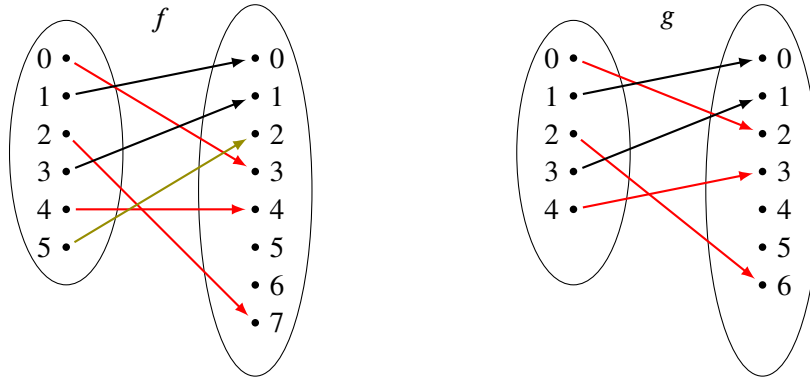


FIGURE: an example.

- Claim 1:  $g$  is well-defined, i.e.  $\forall x \in \{k \in \mathbb{N} : k < n\}, g(x) \in \{k \in \mathbb{N} : k < p - 1\}$ .  
 Let  $x \in \{k \in \mathbb{N} : k < n\}$ .  
 So either  $f(x) < f(n)$ , and then  $g(x) = f(x) < f(n) < p$ , therefore  $0 \leq g(x) < p - 1$ .  
 Or  $f(x) > f(n)$ , and then  $g(x) = f(x) - 1 < p - 1$ , therefore  $0 \leq g(x) < p - 1$ .
- Claim 2:  $g$  is injective.  
 Let  $x, y \in \{k \in \mathbb{N} : k < n\}$  be such that  $g(x) = g(y)$ .
  - \* First case:  $f(x), f(y) < f(n)$ .  
 Then  $g(x) = f(x)$  and  $g(y) = f(y)$ . So  $f(x) = f(y)$  and thus  $x = y$  since  $f$  is injective.
  - \* Second case:  $f(x), f(y) \geq f(n)$ .  
 Then  $g(x) = f(x) - 1$  and  $g(y) = f(y) - 1$ . So  $f(x) = f(y)$  and thus  $x = y$  since  $f$  is injective.
  - \* Third case:  $f(x) < f(n)$  and  $f(y) > f(n)$ .  
 Then  $g(x) = f(x) < f(n)$  and  $g(y) = f(y) - 1 > f(n) - 1 \geq f(n)$ . Therefore, this case is impossible.
  - \* Fourth case:  $f(y) < f(n)$  and  $f(x) > f(n)$ . Similar to the previous one.

Therefore, by the induction hypothesis,  $n \leq p - 1$ , i.e.  $n + 1 \leq p$ . ■

**Corollary 7.10.** *Let  $E$  be a finite set. If  $|E| = n$  and  $|E| = m$ , then  $m = n$ .  
 Then we say that  $|E|$  is the cardinal of  $E$ , which is uniquely defined.*

*Proof.* Assume there exists a bijection  $f_1 : \{k \in \mathbb{N} : k < n\} \rightarrow E$  and a bijection  $f_2 : \{k \in \mathbb{N} : k < m\} \rightarrow E$ .  
 Then  $f_2^{-1} \circ f_1 : \{k \in \mathbb{N} : k < n\} \rightarrow \{k \in \mathbb{N} : k < m\}$  is a bijection, so by the above lemma,  $n \leq m$ .  
 Similarly,  $f_1^{-1} \circ f_2 : \{k \in \mathbb{N} : k < m\} \rightarrow \{k \in \mathbb{N} : k < n\}$  is a bijection and thus  $m \leq n$ .  
 Therefore  $n = m$ . ■

**Remark 7.11.** Informally, the cardinal of a finite set is its size, i.e. the number of elements it contains.

**Remark 7.12.**  $|E| = 0 \Leftrightarrow E = \emptyset$

Indeed, if  $E = \emptyset$  then  $f : \{k \in \mathbb{N} : k < 0\} \rightarrow E$  is always bijective: injectiveness and surjectiveness are vacuously true. So  $|E| = 0$ .

Otherwise, if  $E \neq \emptyset$  then  $f : \{k \in \mathbb{N} : k < 0\} \rightarrow E$  is never surjective, so  $|E| \neq 0$ .

**Proposition 7.13.** *If  $E \subset F$  and  $F$  is finite then  $E$  is finite too, besides,  $|E| \leq |F|$ .*

*Proof.* Let's prove by induction on  $n = |F|$  that if  $E \subset F$  then  $E$  is finite and  $|E| \leq n$ .

- Base case at  $n = 0$ : then  $F = \emptyset$ , so the only possible subset is  $E = \emptyset$  and then  $|E| = 0$ .
- Induction step. Assume that the statement holds for some  $n \in \mathbb{N}$ .  
 Let  $F$  be a set such that  $|F| = n + 1$ .
  - First case:  $E = F$ . Then the statement is obvious.

- *Second case:  $E \neq F$ .* Then there exists  $x \in F \setminus E$ .

There exists a bijection  $f : \{k \in \mathbb{N} : k < n+1\} \rightarrow F$ .

Since  $f$  is bijective, there exists a unique  $m \in \{0, 1, \dots, n\}$  such that  $f(m) = x$ .

Define  $g : \{k \in \mathbb{N} : k < n\} \rightarrow F \setminus \{x\}$  by  $g(k) = f(k)$  for  $k \neq m$  and, if  $m \neq n$ ,  $g(m) = f(n)$ .

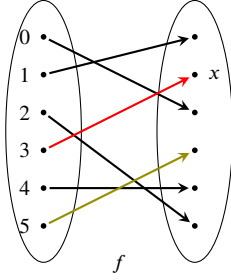


Figure 7.1: If  $m \neq n$ , i.e.  $f(n) \neq x$

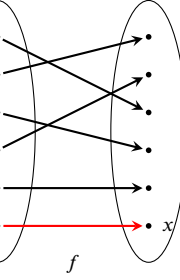
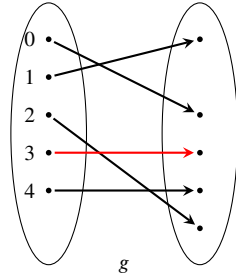
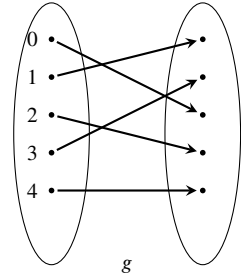


Figure 7.2: If  $m = n$ , i.e.  $f(n) = x$



Then  $g$  is a bijection (*check it*), so  $F \setminus \{x\}$  is finite and  $|F \setminus \{x\}| = n$ .

Since  $E \subset F \setminus \{x\}$ , by the induction hypothesis,  $E$  is finite and  $|E| \leq n < n+1$ . ■

**Proposition 7.14.** Let  $E \subset F$  with  $F$  finite. Then  $|F| = |E| + |F \setminus E|$ .

*Proof.* Since  $F \setminus E \subset F$  and  $E \subset F$ , we know that  $E$  and  $F \setminus E$  are finite. Denote  $r = |E|$  and  $s = |F \setminus E|$ . There exist bijections  $f : \{k \in \mathbb{N} : k < r\} \rightarrow E$  and  $g : \{k \in \mathbb{N} : k < s\} \rightarrow F \setminus E$ .

Define  $h : \{k \in \mathbb{N} : k < r+s\} \rightarrow F$  by  $h(k) = \begin{cases} f(k) & \text{if } k < r \\ g(k-r) & \text{if } k \geq r \end{cases}$ .

- $h$  is well-defined:

Indeed, if  $0 \leq k < r$  then  $f(k)$  is well-defined and  $f(k) \in E \subset F$ .

If  $r \leq k < r+s$  then  $0 \leq k-r < s$  so that  $g(k-r)$  is well-defined and  $g(k-r) \in F \setminus E \subset F$ .

- $h$  is a bijection:

- $h$  is injective: let  $x, y \in \{0, 1, \dots, r+s-1\}$  be such that  $h(x) = h(y)$ .

Either  $h(x) = h(y) \in E$  and then  $f(x) = h(x) = h(y) = f(y)$  thus  $x = y$  since  $f$  is injective.

Or  $h(x) = h(y) \in F \setminus E$  and then  $g(x-r) = h(x) = h(y) = g(y-r)$  thus  $x-r = y-r$  since  $g$  is injective, hence  $x = y$ .

- $h$  is surjective: let  $y \in F$ .

Either  $y \in E$ , and then there exists  $x \in \{0, 1, \dots, r-1\}$  such that  $f(x) = y$ , since  $f$  is surjective. Then  $h(x) = f(x) = y$ .

Or  $y \in F \setminus E$ , and then there exists  $x \in \{0, 1, \dots, s-1\}$  such that  $g(x) = y$  since  $g$  is surjective. Then  $h(x+r) = g(x) = y$ .

Therefore  $|F| = r+s = |E| + |F \setminus E|$ . ■

**Proposition 7.15.** Let  $E$  and  $F$  be two finite sets. Then

1.  $|E \cup F| = |E| + |F| - |E \cap F|$
2.  $|E \times F| = |E| \times |F|$

*Proof.*

1. Using Proposition 7.14 twice, we get

$$|E \cup F| = |E \sqcup (F \setminus (E \cap F))| = |E| + |F \setminus (E \cap F)| = |E| + |F| - |E \cap F|$$

2. We prove this proposition by induction on  $n = |F| \in \mathbb{N}$ .

- *Base case at  $n = 0$ :* then  $F = \emptyset$  so  $E \times F = \emptyset$  too and  $|E \times F| = 0 = |E| \times 0 = |E| \times |F|$ .

- *Case  $n = 1$ :* we will use this special case later in the proof.

Assume that  $F = \{*\}$  and that  $|E| = p$ . Then there exists a bijection  $f : \{k \in \mathbb{N} : k < p\} \rightarrow E$ .

Note that  $g : \{k \in \mathbb{N} : k < p\} \rightarrow E \times F$  defined by  $g(k) = (f(k), *)$  is a bijection.

Therefore  $|E \times F| = p = p \times 1 = |E| \times |F|$ .

- *Induction step.* Assume that the statement holds for some  $n \in \mathbb{N}$ .

Let  $F$  be a set such that  $|F| = n + 1$ .

Since  $|F| > 0$ , there exists  $x \in F$  and  $|F \setminus \{x\}| = |F| - |\{x\}| = n + 1 - 1 = n$ . Then

$$\begin{aligned} |E \times F| &= |(E \times (F \setminus \{x\})) \sqcup (E \times \{x\})| \\ &= |E \times (F \setminus \{x\})| + |E \times \{x\}| \\ &= |E| \times |F \setminus \{x\}| + |E| \text{ using the induction hypothesis and the case } n = 1 \\ &= |E| \times (|F| - 1) + |E| \\ &= |E| \times |F| \end{aligned}$$

■

**Proposition 7.16.** Assume that  $E \subset F$  with  $F$  finite. Then  $E = F \Leftrightarrow |E| = |F|$ .

*Proof.*

$\Rightarrow$  It is obvious.

$\Leftarrow$  Assume that  $|E| = |F|$ . Then  $|F \setminus E| = |F| - |E| = 0$ . Thus  $F \setminus E = \emptyset$ , i.e.  $E = F$ .

■

**Proposition 7.17.** Let  $E$  a finite set. Then  $F$  is finite and  $|E| = |F|$  if and only if there exists a bijection  $f : E \rightarrow F$ .

*Proof.*

$\Rightarrow$  Assume that  $F$  is finite and that  $|E| = |F| = n$ .

Then there exist bijections  $\varphi : \{k \in \mathbb{N} : k < n\} \rightarrow E$  and  $\psi : \{k \in \mathbb{N} : k < n\} \rightarrow F$ .

Therefore  $f = \psi \circ \varphi^{-1} : E \rightarrow F$  is a bijection.

$\Leftarrow$  Assume that there exists a bijection  $f : E \rightarrow F$ .

Since  $E$  is finite there exists a bijection  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$ .

Thus  $f \circ \varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow F$  is a bijection. Therefore  $F$  is finite and  $|F| = |E|$ .

■

**Proposition 7.18.** Let  $E, F$  be two finite sets such that  $|E| = |F|$ . Let  $f : E \rightarrow F$ . Then TFAE:

1.  $f$  is injective,
2.  $f$  is surjective,
3.  $f$  is bijective.

*Proof.*

Assume that  $f$  is injective.

There exists a bijection  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$ .

Then  $f \circ \varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow f(E)$  is a bijection. Thus  $|f(E)| = |E| = |F|$ .

Since  $f(E) \subset F$  and  $|f(E)| = |F|$ , we get  $f(E) = F$ , i.e.  $f$  is surjective.

Assume that  $f$  is surjective.

Then for every  $y \in F$ ,  $f^{-1}(y) \subset E$  is finite and non-empty, i.e.  $|f^{-1}(y)| \geq 1$ .

Assume by contradiction that there exists  $y \in F$  such that  $|f^{-1}(y)| > 1$ .

$$\text{Thus } |E| = \left| \bigsqcup_{y \in F} f^{-1}(y) \right| = \sum_{y \in F} |f^{-1}(y)| > |F| = |E|.$$

Hence a contradiction.

■

**Proposition 7.19.** Let  $E$  and  $F$  be two finite sets. Then  $|E| \leq |F|$  if and only if there exists an injection  $f : E \rightarrow F$ .

*Proof.*

$\Rightarrow$  Assume that  $|E| \leq |F|$ .

There exist bijections  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$  and  $\psi : \{k \in \mathbb{N} : k < |F|\} \rightarrow F$ .

Since  $|E| \leq |F|$ ,  $f = \psi \circ \varphi^{-1} : E \rightarrow F$  is well-defined and injective.

$\Rightarrow$  Assume that there exists an injection  $f : E \rightarrow F$ .

Then  $f$  induces a bijection  $f : E \rightarrow f(E)$ , so that  $|E| = |f(E)|$ .

And since  $f(E) \subset F$ , we have  $|f(E)| \leq |F|$ . ■

**Corollary 7.20** (The pigeonhole principle or Dirichlet's drawer principle).

Let  $E$  and  $F$  be two finite sets. If  $|E| > |F|$  then there is no injective function  $E \rightarrow F$ .

**Example 7.21.** There are two non-bald people in Toronto with the exact same number of hairs on their heads.

**Example 7.22.** During a post-covid party with  $n > 1$  participants, we may always find two people who shook hands to the same number of people.

**Remark 7.23.** Since the cardinal of a finite set is a natural number, we deduce that given two finite sets  $E$  and  $F$ , exactly one of the followings occurs:

- either  $|E| < |F|$  (i.e. there is an injection  $E \rightarrow F$  but no bijection  $E \rightarrow F$ ),
- or  $|E| = |F|$  (i.e. there is a bijection  $E \rightarrow F$ ),
- or  $|E| > |F|$  (i.e. there is an injection  $F \rightarrow E$  but no bijection  $E \rightarrow F$ ).

### 7.3 Generalization to infinite sets

**Definition 7.24.** We say that a set is *infinite* if it is not finite.

**Theorem 7.25.**  $\mathbb{N}$  is infinite.

*Proof.* Assume by contradiction that  $\mathbb{N}$  is finite. Then  $\mathbb{N} \setminus \{0\} \subset \mathbb{N}$  so  $\mathbb{N} \setminus \{0\}$  is finite too.

We define  $f : \mathbb{N} \rightarrow \mathbb{N} \setminus \{0\}$  by  $f(n) = n + 1$ . Note that  $f$  is bijective with inverse  $f^{-1} : \mathbb{N} \setminus \{0\} \rightarrow \mathbb{N}$  defined by  $f^{-1}(n) = n - 1$ .

Thus  $|\mathbb{N}| = |\mathbb{N} \setminus \{0\}| = |\mathbb{N}| - |\{0\}| = |\mathbb{N}| - 1$ , i.e.  $0 = 1$ .

Hence a contradiction. ■

So, we need to find a way in order to generalize the notion of cardinal from finite sets to all sets.

**Definition 7.26.** We say that two sets  $E$  and  $F$  have same *cardinality*, denoted by  $|E| = |F|$ , if there exists a bijection  $f : E \rightarrow F$ .

We also say that  $E$  and  $F$  are *equinumerous* or *equipotent*.

**Proposition 7.27.**

1. If  $E$  is a set then  $|E| = |E|$ .
2. Given two sets  $E$  and  $F$ , if  $|E| = |F|$  then  $|F| = |E|$ .
3. Given three sets  $E$ ,  $F$  and  $G$ , if  $|E| = |F|$  and  $|F| = |G|$  then  $|E| = |G|$ .

*Proof.*

1.  $id : E \rightarrow E$  is a bijection.
2. Assume that  $|E| = |F|$ , i.e. that there exists a bijection  $f : E \rightarrow F$ .  
Then  $f^{-1} : F \rightarrow E$  is a bijection, so  $|F| = |E|$ .
3. Assume that  $|E| = |F|$  and  $|F| = |G|$ , i.e. that there exist bijections  $f : E \rightarrow F$  and  $g : F \rightarrow G$ .  
Then  $g \circ f : E \rightarrow G$  is a bijection, thus  $|E| = |G|$ . ■

**Remark 7.28.** At first glance, it seems that equipotence is an equivalence relation since it satisfies reflexivity, symmetry and transitivity. Nonetheless, recall that an equivalence relation is a binary relation on a set. If equipotence were an equivalence relation, then it would be a binary relation on the set of all sets, which doesn't exist (See Theorem 7.54).

**Theorem 7.29.** A set  $E$  is infinite if and only if for every  $n \in \mathbb{N}$  there exists  $S \subset E$  such that  $|S| = n$ .

*Proof.*

$\Rightarrow$  Assume that  $E$  is infinite.

We are going to prove by induction that for every  $n \in \mathbb{N}$  there exists  $S \in \mathcal{P}(E)$  such that  $|S| = n$ .

- *Base case at  $n = 0$ :*  $\emptyset \subset E$  satisfies  $|\emptyset| = 0$ .
- *Induction step.* Assume that for some  $n \in \mathbb{N}$  there exists  $T \subset E$  such that  $|T| = n$ .  
Note that  $E \setminus T \neq \emptyset$  (otherwise  $E = T$ , which is impossible since  $E$  is infinite).  
Therefore there exists  $x \in E \setminus T$ . Define  $S := T \sqcup \{x\}$ , then  $S \subset E$  is finite and  $|S| = |T| + 1 = n + 1$ .  
Which ends the induction step.

$\Leftarrow$  Let  $E$  be a set such that for every  $n \in \mathbb{N}$  there exists  $S \subset E$  such that  $|S| = n$ .

Assume by contradiction that  $E$  is finite. Then there exists  $k \in \mathbb{N}$  such that  $|E| = k$ .

Since  $k + 1 \in \mathbb{N}$ , there exists  $S \subset E$  such that  $|S| = k + 1$ .

Since  $S \subset E$ , we get  $k + 1 = |S| \leq |E| = k$ . Hence a contradiction.  $\blacksquare$

**Corollary 7.30.** A set  $E$  is infinite if and only if for all  $n \in \mathbb{N}$  there exists an injective function  $\{k \in \mathbb{N} : k < n\} \rightarrow E$ .

**Definition 7.31.** Given two sets  $E$  and  $F$ , we write  $|E| \leq |F|$  if there exists an injective function  $f : E \rightarrow F$ .

**Theorem 7.32** (Cantor–Schröder–Bernstein theorem).

Given two sets  $E$  and  $F$ , if  $|E| \leq |F|$  and  $|F| \leq |E|$  then  $|E| = |F|$ .

**Remark 7.33.** The above theorem states that if there exist injections  $E \rightarrow F$  and  $F \rightarrow E$  then there exists a bijection  $E \rightarrow F$ . It is less trivial than it seems at first glance when you look at the above statement.

It was first stated in 1887 by Cantor who didn't provide a proof. The first known proof is due to Dedekind on the same year, but he did not publish his proof (which was only found after he passed away). In 1895 Cantor published a proof relying on the trichotomy principle (see Theorem 7.56), but Tarski later proved that the latter is actually equivalent to the axiom of choice.

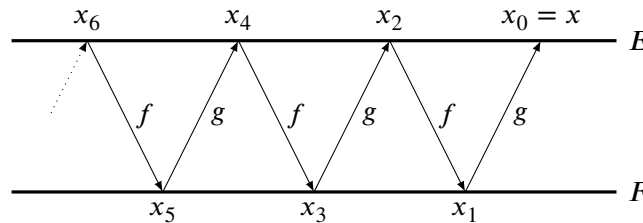
Around 1897, Bernstein, Schröder and Dedekind independently found proofs of the theorem (another one for Dedekind). But Schröder's proof later appeared to be incorrect. Several mathematicians subsequently gave alternative proofs, including Zermelo (1901, 1908) and König (1906).

Cantor–Schröder–Bernstein theorem is a little bit tricky to prove, so first I would like to informally explain the strategy of the proof before actually proving it.

We are given two injective functions  $f : E \rightarrow F$  and  $g : F \rightarrow E$ .

Let's fix  $x \in E$ . We construct a *chain*  $x_0, x_1, x_2, \dots$  of elements which are alternatively in  $E$  and  $F$  as follows. First we set  $x_0 = x \in E$  and then we define the next terms inductively by

- if  $x_n \in E$  then we define  $x_{n+1} \in F$  as the unique antecedant of  $x_n$  by  $g$  (if it exists, otherwise we stop the construction at  $x_n$ ),
- if  $x_n \in F$  then we define  $x_{n+1} \in E$  as the unique antecedant of  $x_n$  by  $f$  (if it exists, otherwise we stop the construction at  $x_n$ ).

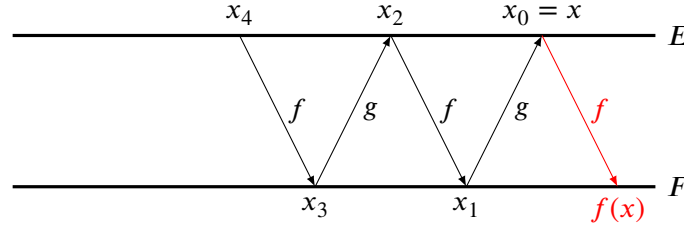


Then we face three possible cases:

1. Either the chain ends with an element in  $E$ , and then we put  $x$  in  $E_E$ ,
2. or the chain ends with an element in  $F$ , and then we put  $x$  in  $E_F$ ,
3. or the inductive definition of the chain doesn't stop, and then we put  $x$  in  $E_\infty$ .

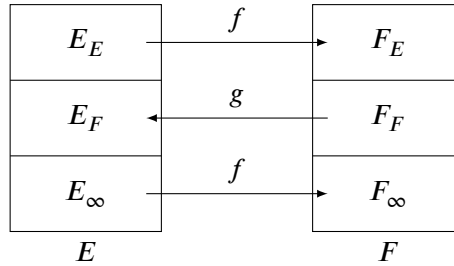
We have a partition  $E = E_E \sqcup E_F \sqcup E_\infty$ . We perform the same construction with  $x_0 = x \in F$  in order to obtain  $F = F_E \sqcup F_F \sqcup F_\infty$ .

Now assume that  $x \in E_E$ , for instance the chain stops at  $x_4$  as below. Then  $f(x) \in F_E$ , since its chain continues at  $x_0$  and stops at  $x_4 \in E$ .



Therefore the function  $f|_{E_E} : E_E \rightarrow F_E$  is well-defined. Besides, it is injective since  $f$  is, and it is surjective by definition of  $F_E$ . Therefore  $f|_{E_E} : E_E \rightarrow F_E$  is a bijection.

Similarly  $g|_{F_F} : F_F \rightarrow E_F$  and  $f|_{E_\infty} : E_\infty \rightarrow F_\infty$  are bijections. Finally, we glue them in order to obtain a bijection  $h : E \rightarrow F$ .



*Proof of Cantor–Schröder–Bernstein theorem.*

Let  $f : E \rightarrow F$  and  $g : F \rightarrow E$  be two injective functions. Set

- $E_E = \{x \in E : \exists n \in \mathbb{N}, \exists r \in E \setminus \text{Im}(g), x = (g \circ f)^n(r)\}$
- $E_F = \{x \in E : \exists n \in \mathbb{N}, \exists s \in F \setminus \text{Im}(f), x = g((f \circ g)^n(s))\}$
- $E_\infty = E \setminus (E_E \sqcup E_F)$
- $F_E = \{y \in F : \exists n \in \mathbb{N}, \exists r \in E \setminus \text{Im}(g), y = f((g \circ f)^n(r))\}$
- $F_F = \{y \in F : \exists n \in \mathbb{N}, \exists s \in F \setminus \text{Im}(f), y = (f \circ g)^n(s)\}$
- $F_\infty = F \setminus (F_E \sqcup F_F)$

Note that if  $x \in E_E$  then  $f(x) \in F_E$ . So  $f|_{E_E} : E_E \rightarrow F_E$  is well-defined. It is injective since  $f$  is injective. And it is surjective by definition of the sets. Thus it is bijective.

Similarly,  $g|_{F_F} : F_F \rightarrow E_F$  is well-defined and bijective and  $f|_{E_\infty} : E_\infty \rightarrow F_\infty$  is well-defined and bijective.

We define  $h : E \rightarrow F$  by  $h(x) = \begin{cases} f(x) & \text{if } x \in E_E \\ g^{-1}(x) & \text{if } x \in E_F \\ f(x) & \text{if } x \in E_\infty \end{cases}$ .

Then  $h$  is clearly a bijection (*I can use "clear", but you can't, and the same holds for "trivial" and "obvious" :-p*). ■

### Proposition 7.34.

1. If  $E$  is a set then  $|E| \leq |E|$ .
2. Given two sets  $E$  and  $F$ , if  $|E| \leq |F|$  and  $|F| \leq |E|$  then  $|E| = |F|$ .
3. Given three sets  $E$ ,  $F$  and  $G$ , if  $|E| \leq |F|$  and  $|F| \leq |G|$  then  $|E| \leq |G|$ .

*Proof.*

1.  $id : E \rightarrow E$  is an injective function.
2. It is Cantor–Bernstein–Schröder theorem.
3. Assume that  $|E| \leq |F|$  and  $|F| \leq |G|$ , i.e. that there exist injections  $f : E \rightarrow F$  and  $g : F \rightarrow G$ . Then  $g \circ f : E \rightarrow G$  is injective, thus  $|E| \leq |G|$ . ■

**Remark 7.35.** Comparison of cardinals shares the characteristic properties of an order. Nonetheless, it is not an order since it is not a binary relation on a set (as for equipotence).

**Proposition 7.36.** *If  $E \subset F$  then  $|E| \leq |F|$ .*

*Proof.* Indeed,  $f : E \rightarrow F$  defined by  $f(x) = x$  is injective. ■

**Proposition 7.37.** *If  $|E_1| = |E_2|$  and  $|F_1| = |F_2|$  then  $|E_1 \times F_1| = |E_2 \times F_2|$ .*

*Proof.* Assume that  $|E_1| = |E_2|$  and  $|F_1| = |F_2|$  then there exist bijections  $f : E_1 \rightarrow E_2$  and  $g : F_1 \rightarrow F_2$ . We define  $h : E_1 \times F_1 \rightarrow E_2 \times F_2$  by  $h(x, y) = (f(x), g(y))$ . Let's check that  $h$  is a bijection.

- $h$  is injective.

Let  $(x, y), (x', y') \in E_1 \times F_1$  be such that  $h(x, y) = h(x', y')$ .

Then  $f(x) = f(x')$  and  $g(y) = g(y')$ , thus  $x = x'$  and  $y = y'$  since  $f$  and  $g$  are injectives.

We proved that  $(x, y) = (x', y')$ .

- $h$  is surjective.

Let  $(z, w) \in E_2 \times F_2$ . Since  $f$  is surjective, there exists  $x \in E_1$  such that  $z = f(x)$ .

Since  $g$  is surjective, there exists  $y \in F_1$  such that  $w = g(y)$ .

Then  $h(x, y) = (f(x), g(y)) = (z, w)$ . ■

**Theorem 7.38.** *Given two sets  $E$  and  $F$ ,  $|E| \leq |F|$  if and only if there exists a surjective function  $g : F \rightarrow E$ .*

*Proof.*

$\Rightarrow$  Assume that there exists an injective function  $f : E \rightarrow F$ , then  $\tilde{f} : E \rightarrow f(E)$  is bijective.

If  $E = \emptyset$ , then there is nothing to prove. So we may assume that there exists  $u \in E$ .

Define  $g : F \rightarrow E$  by  $g(y) = \begin{cases} \tilde{f}^{-1}(y) & \text{if } y \in f(E) \\ u & \text{otherwise} \end{cases}$

Let  $x \in E$ , then  $g(f(x)) = \tilde{f}^{-1}(f(x)) = x$ . Thus  $g$  is surjective.

$\Leftarrow$  Assume that there exists a surjective function  $g : F \rightarrow E$ , then<sup>5</sup>  $\forall x \in E, \exists y_x \in g^{-1}(x)$ .

Define  $f : E \rightarrow F$  by  $f(x) = y_x$ . Then  $f$  is injective, so  $|E| \leq |F|$ .

Indeed, assume that  $f(x) = f(x')$  then  $g(f(x)) = g(f(x'))$ .

But  $g(f(x)) = g(y_x) = x$  and similarly  $g(f(x')) = x'$ . Thus  $x = x'$ . ■

**Theorem 7.39.** *Given two sets  $E$  and  $F$ , if  $|E| = |F|$  then  $|\mathcal{P}(E)| = |\mathcal{P}(F)|$ .*

*Proof.* Let  $E$  and  $F$  be such that  $|E| = |F|$ . Then there exists a bijection  $f : E \rightarrow F$ .

Note that  $\tilde{f} : \mathcal{P}(E) \rightarrow \mathcal{P}(F)$  defined by  $\tilde{f}(A) = f(A)$  is bijective too (*prove it!*).

Therefore  $|\mathcal{P}(E)| = |\mathcal{P}(F)|$ . ■

## 7.4 Countable sets

In what follows, we set  $\aleph_0 := |\mathbb{N}|$  (pronounced *aleph nought*).

**Definition 7.40.** A set  $E$  is countable if either  $E$  is finite or  $|E| = \aleph_0$ .

**Proposition 7.41.** *If  $S \subset \mathbb{N}$  is infinite then  $|S| = \aleph_0$ .*

*Proof.* Let's define the function  $f : \mathbb{N} \rightarrow S$  by induction as follows.

Set  $f(0) = \min S$  (which is well-defined by the well-ordering principle since  $S \neq \emptyset$  as it is infinite).

And then, assuming that  $f(n)$  is already defined, we set  $f(n+1) = \min\{k \in S : k > f(n)\}$  (which is well-defined by the well-ordering principle: the involved set is non-empty since otherwise  $S$  would be finite).

It is easy to check that  $f$  is injective (note that  $\forall n \in \mathbb{N}, f(n+1) > f(n)$ ), therefore  $\aleph_0 \leq |S|$ .

But since  $S \subset \mathbb{N}$ , we also have  $|S| \leq \aleph_0$ .

Thus, by Cantor–Schröder–Bernstein theorem,  $|S| = \aleph_0$ . ■

<sup>5</sup>(AC) See Remark 7.57.

**Proposition 7.42.** *A set  $E$  is countable if and only if  $|E| \leq \aleph_0$  (i.e. there exists an injection  $f : E \rightarrow \mathbb{N}$ ), otherwise stated  $E$  is countable if and only if there exists a bijection between  $E$  and a subset of  $\mathbb{N}$ .*

*Proof.*

$\Rightarrow$  Assume that  $E$  is countable.

- Either  $E$  is finite and then there exists  $n \in \mathbb{N}$  together with a bijection  $g : \{k \in \mathbb{N} : k < n\} \rightarrow E$ . We define  $f : E \rightarrow \mathbb{N}$  by  $f(x) = g^{-1}(x)$  (which is well-defined since  $\{k \in \mathbb{N} : k < n\} \subset \mathbb{N}$ ). And  $f$  is an injection since  $g^{-1}$  is.
- Or  $|E| = \aleph_0$ , i.e. there exists a bijection  $f : E \rightarrow \mathbb{N}$ .

$\Leftarrow$  Assume there exists an injection  $f : E \rightarrow \mathbb{N}$ .

Assume that  $E$  is infinite. Then  $|E| = |f(E)| = \aleph_0$  by Proposition 7.41.

Thus either  $E$  is finite or  $|E| = \aleph_0$ . In both cases  $E$  is countable. ■

**Proposition 7.43.** *The set of finite subsets of  $\mathbb{N}$  is countably infinite, i.e.  $|\{S \in \mathcal{P}(\mathbb{N}) : \exists n \in \mathbb{N}, |S| = n\}| = \aleph_0$ .*

*Proof.* Define  $f : \{S \in \mathcal{P}(\mathbb{N}) : \exists n \in \mathbb{N}, |S| = n\} \rightarrow \mathbb{N}$  by  $f(S) = \sum_{k \in S} 2^k$ .

Then  $f$  is bijective by existence and uniqueness of the binary positional numeral system. ■

**Proposition 7.44.**  $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

*Proof.* Define  $f : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$  by  $f(a, b) = 2^a 3^b$ . Then  $f$  is injective by uniqueness of the prime decomposition. Thus  $|\mathbb{N} \times \mathbb{N}| \leq \aleph_0$ .

Besides  $\{0\} \times \mathbb{N} \subset \mathbb{N} \times \mathbb{N}$ , thus  $\aleph_0 = |\{0\} \times \mathbb{N}| \leq |\mathbb{N} \times \mathbb{N}|$ .

Hence  $|\mathbb{N} \times \mathbb{N}| = \aleph_0$  by Cantor–Schröder–Bernstein theorem. ■

**Theorem 7.45.** *A countable union of countable sets is countable, i.e. if  $I$  is countable and if for every  $i \in I$ ,  $E_i$  is countable then  $\bigcup_{i \in I} E_i$  is countable.*

*Proof.* WLOG we may now assume that  $I \subset \mathbb{N}$ .

Let  $i \in I$ . Since  $E_i$  is countable, there exists an injection  $f_i : E_i \rightarrow \mathbb{N}^6$ .

We define  $\varphi : \bigcup_{i \in I} E_i \rightarrow \mathbb{N} \times \mathbb{N}$  by  $\varphi(x) = (n, f_n(x))$  where  $n = \min\{i \in I : x \in E_i\}$  (well-ordering principle).

It is not difficult to check that  $\varphi$  is injective. Therefore  $\bigcup_{i \in I} E_i$  is countable. ■

**Theorem 7.46.** *If  $E$  is an infinite set then there exists  $T \subset E$  such that  $|T| = \aleph_0$ , i.e.  $\aleph_0$  is the least infinite cardinal.*

*Proof.* For  $n \in \mathbb{N}$ , set  $E_n = \{S \in \mathcal{P}(E) : |S| = n\}$ . By Theorem 7.29,  $E_n \neq \emptyset$ .

So for every  $n \in \mathbb{N}$ , we can pick  $S_n \in E_n$ <sup>7</sup>.

Then  $T := \bigcup_{n \in \mathbb{N}} S_n$  is countable by Theorem 7.45.

Besides,  $\forall n \in \mathbb{N}$ ,  $S_n \subset T$  and  $|S_n| = n$ . Therefore  $T$  is infinite by Theorem 7.29.

Thus  $|T| = \aleph_0$  as an infinite countable set. ■

**Theorem 7.47.**  $|\mathbb{Z}| = \aleph_0$

*Proof 1.* Since  $\mathbb{N} \subset \mathbb{Z}$ , we have  $|\mathbb{N}| \leq |\mathbb{Z}|$ .

Define  $f : \mathbb{Z} \rightarrow \mathbb{N}$  by  $f(n) = \begin{cases} 2^n & \text{if } n \geq 0 \\ 3^{-n} & \text{if } n < 0 \end{cases}$ .

Then  $f$  is injective by uniqueness of the prime factorization. Therefore  $|\mathbb{Z}| \leq |\mathbb{N}|$ .

Hence  $|\mathbb{Z}| = |\mathbb{N}|$  by Cantor–Schröder–Bernstein theorem. ■

*Proof 2.*

Define  $f : \mathbb{Z} \rightarrow \mathbb{N}$  by  $f(n) = \begin{cases} 2n & \text{if } n \geq 0 \\ -(2n+1) & \text{if } n < 0 \end{cases}$ .

Then  $f$  is bijective with inverse  $f^{-1}(m) = \begin{cases} k & \text{if } \exists k \in \mathbb{N}, m = 2k \\ -k-1 & \text{if } \exists k \in \mathbb{N}, m = 2k+1 \end{cases}$ .

Therefore  $|\mathbb{Z}| = |\mathbb{N}|$ . ■

<sup>6</sup>(ACC) See Remark 7.58.

<sup>7</sup>(ACC) See Remark 7.59.



**Theorem 7.48.**  $|\mathbb{Q}| = \aleph_0$

**Remark 7.49.** This theorem asserts that there are as many rational numbers than natural numbers. Which seems counter-intuitive. Since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ , we could expect that  $\mathbb{R}$  is also countable. That's not the case as we will see in the next section.

*Proof 1.* Note that  $\mathbb{N} \subset \mathbb{Q}$ , therefore  $\aleph_0 \leq |\mathbb{Q}|$ .

Define  $f : \mathbb{Q} \rightarrow \mathbb{Z} \times \mathbb{Z}$  by  $f\left(\frac{a}{b}\right) = (a, b)$  where  $\frac{a}{b}$  is in lowest form.

By uniqueness of the lowest form expression of a rational number,  $f$  is well-defined and injective.

Thus  $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{Z}|$ . Since  $|\mathbb{Z}| = |\mathbb{N}|$ , we get  $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

We conclude using Cantor–Schröder–Bernstein theorem. ■

*Proof 2.* Note that  $\mathbb{N} \subset \mathbb{Q}$ , therefore  $\aleph_0 \leq |\mathbb{Q}|$ .

The function  $f : \mathbb{Z} \times \mathbb{N} \setminus \{0\} \rightarrow \mathbb{Q}$  defined by  $f(a, b) = \frac{a}{b}$  is surjective.

Thus, by Proposition 7.38<sup>8</sup>,  $|\mathbb{Q}| \leq |\mathbb{Z} \times \mathbb{N} \setminus \{0\}|$ .

Since  $|\mathbb{Z}| = |\mathbb{N}|$  and  $|\mathbb{N} \setminus \{0\}| = |\mathbb{N}|$ , we get  $|\mathbb{Z} \times \mathbb{N} \setminus \{0\}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

We conclude using Cantor–Schröder–Bernstein theorem. ■

*Proof 3.*

Note that  $\mathbb{N} \subset \mathbb{Q}$ , therefore  $\aleph_0 \leq |\mathbb{Q}|$ .

Besides  $\mathbb{Q} = \bigcup_{(a,b) \in \mathbb{Z} \times \mathbb{N} \setminus \{0\}} \left\{ \frac{a}{b} \right\}$ , so that  $\mathbb{Q}$  is countable by Theorem 7.45<sup>9</sup>, i.e.  $|\mathbb{Q}| \leq \aleph_0$ .

We conclude using Cantor–Schröder–Bernstein theorem. ■

## 7.5 Cantor's diagonal argument

**Theorem 7.50.**  $\aleph_0 < |\mathbb{R}|$

The following proof relies on Cantor's diagonal argument<sup>10</sup>. That's a very general method that we will use later to prove Cantor's theorem<sup>11</sup>.

*Proof.* We are going to prove that there is no surjection  $\mathbb{N} \rightarrow \mathbb{R}$  (and hence no such bijection).

Let  $f : \mathbb{N} \rightarrow \mathbb{R}$  be a function. Given  $n \in \mathbb{N}$ , we know<sup>12</sup> that  $f(n)$  has a unique proper decimal expansion

$$f(n) = \sum_{k=0}^{+\infty} a_{nk} 10^{-k}$$

where  $a_{n0} \in \mathbb{Z}$  and  $a_{nk} \in \{0, 1, \dots, 9\}$  for  $k \geq 1$ , i.e.

$$\begin{aligned} f(0) &= a_{00} . a_{01} a_{02} a_{03} a_{04} a_{05} \dots \\ f(1) &= a_{10} . a_{11} a_{12} a_{13} a_{14} a_{15} \dots \\ f(2) &= a_{20} . a_{21} a_{22} a_{23} a_{24} a_{25} \dots \\ f(3) &= a_{30} . a_{31} a_{32} a_{33} a_{34} a_{35} \dots \\ f(4) &= a_{40} . a_{41} a_{42} a_{43} a_{44} a_{45} \dots \\ &\vdots \qquad \qquad \qquad \vdots \end{aligned}$$

<sup>8</sup>Actually we only need a weak version of Proposition 7.38 which doesn't involve the axiom of choice: using the well-ordering principle, we can prove that a surjective function whose domain is  $\mathbb{N}$  admits a right inverse.

<sup>9</sup>The axiom of countable choice is not necessary here: the sets are singletons, so there is no choice.

<sup>10</sup>This elegant argument was published by Cantor in 1891, but he gave a previous proof of the uncountability of  $\mathbb{R}$  in 1874 (with a modified version in 1879).

<sup>11</sup>It can also be used to prove that the box topology on  $\mathbb{R}^{\mathbb{N}}$  is not first-countable, or to derive from Erdős–Kaplansky's theorem (if  $E$  is an infinite dimensional vector space then  $\dim E^* = |E^*|$ ) that if  $E$  is an infinite dimensional vector space then  $E$  is not isomorphic to its dual  $E^*$ .

<sup>12</sup>Chapter 6, Theorem 56.

Given  $k \in \mathbb{N}$ , we set  $b_k = \begin{cases} 1 & \text{if } a_{kk} = 0 \\ 0 & \text{otherwise} \end{cases}$ .

Then  $b = \sum_{k=0}^{+\infty} b_k 10^{-k}$  is a real number written with its unique proper decimal expansion.

Note that for every  $n \in \mathbb{N}$ ,  $b \neq f(n)$  since  $b_n \neq a_{nn}$  (we use the uniqueness of the proper decimal expansion). Therefore  $b \notin \text{Im}(f)$  and  $f$  is not surjective. ■

**Theorem 7.51** (Cantor's theorem). *Given a set  $E$ ,  $|E| < |\mathcal{P}(E)|$ .*

**Remark 7.52.** As a consequence, we get that there is no greatest cardinal.

*Proof of Cantor's theorem.*

First, note that  $g : E \rightarrow \mathcal{P}(E)$  defined by  $g(x) = \{x\}$  is injective, therefore  $|E| \leq |\mathcal{P}(E)|$ .

We are going to prove that there is no surjection  $E \rightarrow \mathcal{P}(E)$  (and hence no such bijection).

Let  $f : E \rightarrow \mathcal{P}(E)$  be a function. Define  $S = \{x \in E : x \notin f(x)\}$ .

Let  $x \in E$ . If  $x \in f(x)$  then  $x \notin S$ . Otherwise, if  $x \notin f(x)$  then  $x \in S$ . Therefore  $f(x) \neq S$  (since one contains  $x$  but not the other one).

Thus  $S \notin \text{Im}(f)$  and  $f$  is not surjective. ■

We already know that  $|\mathbb{N}| < |\mathbb{R}|$  and that  $|\mathbb{N}| < |\mathcal{P}(\mathbb{N})|$ .

The following theorem asserts that actually  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ .

**Theorem 7.53.**  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

*Proof.*

Define  $f : \mathcal{P}(\mathbb{N}) \rightarrow \mathbb{R}$  by  $f(S) = \sum_{n \in S} 10^{-n}$ .

Then  $f$  is injective by uniqueness of the proper decimal expansion. Thus  $|\mathcal{P}(\mathbb{N})| \leq |\mathbb{R}|$ .

Define  $g : \mathbb{R} \rightarrow \mathcal{P}(\mathbb{Q})$  by  $g(x) = \{q \in \mathbb{Q} : q < x\}$ .

Then  $g$  is injective. Indeed, let  $x, y \in \mathbb{R}$  be such that  $x < y$ . Since  $\mathbb{Q}$  is dense in  $\mathbb{R}$ , there exists  $q \in \mathbb{Q}$  such that  $x < q < y$ . So  $q \notin g(x)$  but  $q \in g(y)$ . Therefore  $g(x) \neq g(y)$ .

Hence  $|\mathbb{R}| \leq |\mathcal{P}(\mathbb{Q})| = |\mathcal{P}(\mathbb{N})|$  using Theorem 7.39 since  $|\mathbb{Q}| = |\mathbb{N}|$ .

We conclude thanks to Cantor–Schröder–Bernstein theorem. ■

## Appendix 7.A What is a set?

The notion of *set* turned out to be necessary in order to handle rigorous definitions of  $\mathbb{R}$  as the ones provided by Dedekind and later by Cantor. It is worth noting that set theory first observed a great resistance<sup>13</sup>, probably because of the influence of Gauss and Kronecker who shared the *horror of the infinite* from ancient Greek philosophers.

Originally Cantor defined a set as “a gathering together into a whole of distinguishable objects (which are called the elements of the set)”<sup>14</sup>. According to current standards, it is a very informal definition. This *naive set theory* was governed by two principles: the *comprehension principle* from which any predicate (i.e. statement) defines a set (i.e. we can define the set of all elements satisfying a given property) and the *extension principle* asserting that two sets are equal if and only if they contain the same elements.

Such an intuitive approach is enough to manipulate sets in everyday mathematics (that's what you did in your courses about calculus, multivariable calculus, linear algebra...). Nonetheless it is not satisfactory

<sup>13</sup>To which Hilbert later replied with the following wonderful and well-known sentence: *Aus dem Paradies, das Cantor uns geschaffen, soll uns niemand vertreiben können* [No one should be able to expel us out of the paradise that Cantor has created for us.].

<sup>14</sup>“Unter einer ‘Menge’ verstehen wir jede Zusammenfassung  $M$  von bestimmten wohlunterscheidbaren Objekten  $M$  unserer Anschauung oder unseres Denkens (welche die ‘Elemente’ von  $M$  genannt werden) zu einem Ganzen”, in *Beiträge zur Begründung der transfiniten Mengenlehre* by Cantor (1895).

since it leads to several paradoxes such as Russell's paradox<sup>15</sup> that we can state as follows using modern notations (and particularly Peano's notation for set membership  $\in$ ).

Since any statement defines a set (*comprehension principle*),  $S = \{x : x \notin x\}$  must be a set. Therefore either  $S \in S$  but then  $S \notin S$  by definition of  $S$ , or  $S \notin S$  but then  $S \in S$  by definition of  $S$ . Which leads to a contradiction.

Zermelo (1908) was the first to suggest a more careful axiomatic set theory. Particularly the comprehension principle is weakened to the *separation principle*: given a set, we can define its subset of elements satisfying a given predicate (that's the set-builder notation  $\{x \in E : P(x)\}$ ).

This theory has been subsequently refined by Fraenkel, Solem, von Neumann, and others, giving rise to Zermelo–Fraenkel (ZF) set theory. It is a first order theory<sup>16</sup> with equality and the set membership binary predicate symbol  $\in$ .

In such a theory, we don't define what is a set: they are the atomic objects over which we use quantifiers<sup>17</sup>. Instead, we have a list of axioms ensuring the existence of some sets and how to define new sets from already defined ones.

There are several equivalent formulations of ZF, for instance this one:

- **Axiom of extensionality:**

$$\forall x \forall y (\forall z (z \in x \Leftrightarrow z \in y) \Leftrightarrow x = y)$$

*Intuitively, this axiom states that two sets are equal if and only if they contain the same elements. Particularly, order doesn't matter and  $\{a, a\} = \{a\}$ .*

- **Axiom of pairing:**

$$\forall x \forall y \exists z \forall w (w \in z \Leftrightarrow (w = x \vee w = y))$$

*This axiom asserts that given two sets  $x$  and  $y$ , the set  $z = \{x, y\}$  containing  $x$  and  $y$  is well-defined.*

*It is often given as an axiom although it is a consequence of the axiom schema of replacement.*

*Note that for a given set  $x$  the axiom of pairing and the axiom of extensionality allow us to define the singleton  $\{x\} = \{x, x\}$ .*

- **Axiom of union:**

$$\forall x \exists y \forall u (u \in y \Leftrightarrow \exists w \in x (u \in w))$$

*This axiom ensures that given a set  $x$  (of sets, everything is a set here), the set  $\bigcup_{w \in x} w$  is well-defined. We will use the abbreviation  $\cup$  in what follows.*

*By the way, note that we have to be more careful about intersections: what would be  $\bigcap_{w \in \emptyset} w$ ?*

- **Axiom of power set:**

$$\forall x \exists y \forall z [z \subset x \Leftrightarrow z \in y]$$

*Here  $z \subset x$  is an abbreviation for  $\forall u (u \in z \implies u \in x)$ . This axiom asserts that given a set  $x$ , the set  $y = \mathcal{P}(x)$  of its subsets is well-defined.*

- **Axiom of empty set:**

$$\exists x \forall y \neg (y \in x)$$

*This axiom ensures that the empty set exists (and it is unique by extensionality), therefore, in what follows, we introduce the term  $\emptyset$  to denote the empty set.*

<sup>15</sup>It was discovered by Zermelo in 1899, but he did not published it, and then rediscovered by Russell in 1901.

<sup>16</sup>A first order theory generalizes propositional calculus by introducing quantified variables.

<sup>17</sup>Actually, it is possible to work with a theory about more general objects: that's for example the case in von Neumann–Bernays–Gödel theory where atomic objects are classes and where a set is defined as a class which is contained in another class. It is known that the statements about sets that can be proved within vNBG coincides with the statement that can be proved within ZFC. Additionally, it doesn't involve axiom schema, i.e. it is described using only finitely many axioms.

- **Axiom of infinity:**

$$\exists x(\emptyset \in x \wedge \forall y \in x(y \cup \{y\} \in x))$$

*This axiom states that there exists a set containing a copy of  $\mathbb{N}$ .*

*We are going to use it to give a construction of  $\mathbb{N}$ . Set  $0 := \emptyset$  and  $s(y) := y \cup \{y\}$  (that's the successor function), therefore  $1 = \{\emptyset\}$ ,  $2 = \{\emptyset, \{\emptyset\}\}$ ,  $3 = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$ ...*

*By the axiom of infinity, there exists a set  $E$  containing  $0$  which is closed by  $s$ . Then it is not too difficult to prove that the intersection of all the subsets of  $E$  containing  $0$  and closed by  $s$  satisfies the induction principle. It is a nice construction of  $\mathbb{N}$  where the order is given by inclusion.*

- **Axiom schema of replacement:**

$$(\forall x \in a \exists! y P(x, y)) \implies (\exists b \forall y (y \in b \iff \exists x \in a P(x, y)))$$

*This one is an axiom schema and not an axiom (i.e. we need it for all formulae  $P(x, y)$ ).*

*It asserts that if a formula defines a "function" then its "range" is a set.*

*Together with the axiom of empty set, the axiom schema of replacement implies that given a set, we may define a subset of elements satisfying a given property (set-builder notation): that's a weak/restricted version of the comprehension principle called the separation principle.*

- **Axiom of foundation:**

$$\forall x(x \neq \emptyset \Rightarrow \exists y \in x(x \cap y = \emptyset))$$

*This axiom is a little bit special: it doesn't define new sets but it is here to avoid paradoxes by removing circular arguments. Particularly, as a consequence of it, a set can't be an element of itself: if  $x$  satisfies  $x \in x$  then the singleton  $\{x\}$  doesn't satisfy the axiom of foundation since  $x \cap \{x\} = \{x\}$ .*

Note that during the interwar period, the French group Bourbaki started to formalize most of known mathematics within set theory.

It is commonly believed that ZF is very likely to be consistent, i.e. there is no contradiction (like Russell's paradox). In what follows, I assume that ZF is consistent (otherwise every statement would be true). Nonetheless, a consequence of Gödel's second incompleteness theorem is that if ZF is consistent then we can't prove within ZF that it is.

You should keep in mind that such a theory was given in response to the foundational crisis of mathematics in the late 19<sup>th</sup> century in order to free mathematics from contradictions and to add more rigor in it. But most mathematicians work at a higher level, not directly from these axioms, and don't care too much about them (we did mathematics before set theory). So, should a contradiction be found, it probably won't impact that much other fields of mathematics: maybe it would be possible to simply fix the axioms in a way to remove the contradiction, or otherwise to work on new foundations for mathematics... Anyway, some choices were made and they can be changed (and even without finding a contradiction, some mathematicians have objections about using set theory as foundations for mathematics, especially since some fields of mathematics involve proper classes which are too big to be sets, so they are *de facto* excluded from set theory).

**Theorem 7.54.** *There is no set containing all sets.*

*Proof.* Assume that such a set  $V$  exists, then the powerset  $\mathcal{P}(V)$  exists too and  $\mathcal{P}(V) \subset V$  by definition of  $V$ . Therefore  $|\mathcal{P}(V)| \leq |V|$ , but  $|V| < |\mathcal{P}(V)|$  by Cantor's theorem. Hence a contradiction. ■

We may similarly prove that there is no set containing all finite sets, or even containing all singletons.

**Theorem 7.55.** *There is no set containing all singletons.*

*Proof.* Assume that the set  $S$  of all singletons exists.

Define  $f : \mathcal{P}(S) \rightarrow S$  by  $f(x) = \{x\}$  (which is well-defined). Since  $f$  is one-to-one, we get that  $|\mathcal{P}(S)| \leq |S|$ . Which contradicts  $|S| < |\mathcal{P}(S)|$  (Cantor's theorem). ■

## Appendix 7.B *Un morceau de choix*

The following statement is (a formulation of) the *axiom of choice*

$$\forall x((\emptyset \notin x \wedge \forall u, v \in x(u = v \vee u \cap v = \emptyset)) \implies \exists y \forall u \in x \exists w(u \cap y) = \{w\}) \quad (\text{AC})$$

It asserts that given a set  $x$  of non-empty pairwise disjoint sets, there exists a set  $y$  which contains exactly one element for each set in  $x$ . Informally, it means that given infinitely many non-empty sets, we can simultaneously pick an element in each set.

We can also state it in the following way. For  $I$  a set together with  $(X_i)_{i \in I}$  a family of sets indexed by  $I$ , we have

$$(\forall i \in I, X_i \neq \emptyset) \implies \prod_{i \in I} X_i \neq \emptyset$$

i.e. there exists  $(x_i)_{i \in I}$  where  $x_i \in X_i$  (we can simultaneously pick  $x_i \in X_i$  for each  $i \in I$ ).

Gödel and Cohen respectively showed that the axiom of choice is not disprovable in ZF and that it is not provable in ZF (assuming that ZF is consistent)<sup>18</sup>. Therefore the axiom of choice can be added to ZF as an axiom without changing its consistency, in this case the theory is denoted ZFC.

Acceptance of the axiom of choice is a little bit controversial: on the one hand it seems very natural and useful in some areas of mathematics<sup>19</sup> but some consequences are counter intuitive (for instance the well-known Banach–Tarski paradox). For this reason, some mathematicians try to avoid it or to use weaker versions (such as the axiom of countable choice, i.e. only when  $I$  is countable).

Here is a (funny) quote summarizing the situation<sup>20</sup>:

*"The axiom of choice is obviously true, the well-ordering principle obviously false, and who can tell about Zorn's lemma?"*  
– Jerry L. Bona<sup>21</sup>.

A statement equivalent to the axiom of choice and which is related to the content of this chapter is the following one (which generalizes Remark 7.23 to infinite sets):

**Theorem 7.56** (Trichotomy principle for cardinality).

Given two sets  $A$  and  $B$ , exactly one of the following occurs:

- $|A| < |B|$
- $|A| = |B|$
- $|A| > |B|$

When Tarski submitted to the *Comptes Rendus de l'Académie des Sciences* his proof that the trichotomy principle is equivalent to the axiom of choice, both Fréchet and Lebesgue refused it: Fréchet because "an implication between two well known propositions is not a new result", and Lebesgue because "an implication between two false propositions is of no interest"<sup>22</sup>.

Below I highlight the places where I used either the axiom of choice or the axiom of countable choice in this chapter.

**Remark 7.57.** In Proposition 7.38, the part that  $|E| \leq |F|$  implies the existence of a surjection  $g : F \rightarrow E$  is true in ZF even without the axiom of choice.

Nonetheless, I used the axiom of choice to prove the converse when I pick  $(y_x)_{x \in E} \in \prod_{x \in E} g^{-1}(x)$ .

Actually the axiom of choice is equivalent to the fact a function is surjective if and only if it admits a right inverse (i.e.  $g : F \rightarrow E$  is surjective if and only if there exists  $f : E \rightarrow F$  such that  $g \circ f = id_E$ ).

<sup>18</sup>According to Gödel's first incompleteness theorem, ZF contains at least one statement which is undecidable, the axiom of choice is such a statement.

<sup>19</sup>For instance, the axiom of choice is equivalent to the fact that every vector space has a basis.

<sup>20</sup>These three statements are equivalent.

<sup>21</sup>STEVEN G. KRANTZ. *Handbook of Logic and Proof Techniques for Computer Science*, p121. Birkhäuser (2002).

<sup>22</sup>JAN MYCIELSKI. *A System of Axioms of Set Theory for the Rationalists*. Notices of the AMS, Volume 53, Number 2.

**Remark 7.58.** Within ZF, Theorem 7.45 is equivalent to the axiom of countable choice.

Nonetheless, using an induction, we can prove within ZF that a finite union of countable sets is countable (see the first part of the proof of Theorem 7.45).

In the proof of Theorem 7.45, I used the axiom of countable choice to pick simultaneously injective functions  $f_i : E_i \rightarrow \mathbb{N}$  for every  $i \in I$ .

**Remark 7.59.** I used the axiom of countable choice in the proof Theorem 7.46 when applying Theorem 7.45. A set is *Dedekind-infinite* if it contains an infinite countable subset<sup>23</sup>. It is true within ZF that a Dedekind-infinite set is infinite. The converse requires the axiom of choice: there exist models of ZF containing amorphous sets, i.e. which are infinite and Dedekind-finite.

## Appendix 7.C Cheatsheet: recollection of some results about cardinality

**Definition.** We say that two sets  $E$  and  $F$  have same *cardinality*, denoted by  $|E| = |F|$ , if there exists a bijection  $f : E \rightarrow F$ .

**Proposition.**

1. If  $E$  is a set then  $|E| = |E|$ .
2. Given two sets  $E$  and  $F$ , if  $|E| = |F|$  then  $|F| = |E|$ .
3. Given three sets  $E$ ,  $F$  and  $G$ , if  $|E| = |F|$  and  $|F| = |G|$  then  $|E| = |G|$ .

**Theorem.** A set  $E$  is infinite if and only if for every  $n \in \mathbb{N}$  there exists  $S \subset E$  such that  $|S| = n$ .

**Definition.** Given two sets  $E$  and  $F$ , we write  $|E| \leq |F|$  if there exists an injective function  $f : E \rightarrow F$ .

**Proposition.**

1. If  $E$  is a set then  $|E| \leq |E|$ .
2. Given two sets  $E$  and  $F$ , if  $|E| \leq |F|$  and  $|F| \leq |E|$  then  $|E| = |F|$  Cantor–Schröder–Bernstein theorem.
3. Given three sets  $E$ ,  $F$  and  $G$ , if  $|E| \leq |F|$  and  $|F| \leq |G|$  then  $|E| \leq |G|$ .

**Proposition.** If  $E \subset F$  then  $|E| \leq |F|$ .

**Proposition.** If  $|E_1| = |E_2|$  and  $|F_1| = |F_2|$  then  $|E_1 \times F_1| = |E_2 \times F_2|$ .

**Theorem.** Given two sets  $E$  and  $F$ ,  $|E| \leq |F|$  if and only if there exists a surjective function  $g : F \rightarrow E$ .

**Theorem.** Given two sets  $E$  and  $F$ , if  $|E| = |F|$  then  $|\mathcal{P}(E)| = |\mathcal{P}(F)|$ .

**Notation.** We set  $\aleph_0 := |\mathbb{N}|$  (pronounced *aleph nought*).

**Definition.** A set  $E$  is countable if either  $E$  is finite or  $|E| = \aleph_0$ .

**Proposition.** If  $S \subset \mathbb{N}$  is infinite then  $|S| = \aleph_0$ .

**Proposition.** A set  $E$  is countable if and only if  $|E| \leq \aleph_0$  (i.e. there exists an injection  $f : E \rightarrow \mathbb{N}$ ), otherwise stated  $E$  is countable if and only if there exists a bijection between  $E$  and a subset of  $\mathbb{N}$ .

**Proposition.**  $|\mathbb{N} \times \mathbb{N}| = \aleph_0$

**Theorem.** A countable union of countable sets is countable, i.e. if  $I$  is countable and if for every  $i \in I$ ,  $E_i$  is countable then  $\bigcup_{i \in I} E_i$  is countable.

**Theorem.** If  $E$  is an infinite set then there exists  $T \subset E$  such that  $|T| = \aleph_0$ , i.e.  $\aleph_0$  is the least infinite cardinal.

**Theorem.**  $|\mathbb{Z}| = \aleph_0$

**Theorem.**  $|\mathbb{Q}| = \aleph_0$

**Theorem.**  $\aleph_0 < |\mathbb{R}|$

**Theorem** (Cantor's theorem). Given a set  $E$ ,  $|E| < |\mathcal{P}(E)|$ .

**Theorem.**  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$

<sup>23</sup> Another equivalent definition is: a set  $E$  is Dedekind-complete if there exists  $A \subsetneq E$  such that  $|A| = |E|$ .



FROM: <https://xkcd.com/982/>

Below are a few other proof methods:

- **Proof by Example/Generalization.** *The statement holds for  $n = 42$  so it holds for any  $n \in \mathbb{N}$ .*
- **Proof by Intimidation.** *Don't be silly, it is trivial.*
- **Proof by Terror.** *When proof by intimidation fails.*
- **Proof by Insignificance.** *Who really cares anyway?*
- **Proof by Homework.** *The proof is left as an exercise to the reader.*
- **Proof by Exhaustion.** *The result is an easy consequence of the following 271 pages.*
- **Proof by Obvious Induction.** *3 is prime, 5 is prime, 7 is prime... hence any odd number greater than 2 is a prime number.*
- **Proof by Omission.** *The reader may easily supply the remaining 314 cases in a similar way.*
- **Proof by the End of the Lecture.** *Since it is already the end of the lecture, I let you finish the proof at home.*  
(Sorry, I might have really used this one)
- **Proof by Lazyness.**
- **Proof by Postponement.** **TODO** :*Finish the proof later.*
- **Proof by General Agreement.** *All in Favor?*
- **Proof by My Agreement.** *Do you believe me? I believe me...*  
(I have been told that I used this one often in MAT237... Can you believe that? I can't believe that!)
- **Proof by Intuition.** *I just have this gut feeling.* (Usually that's how we do research)
- **Proof by Supplication.** *Oh please, let it be true.* (Quite often, research looks like that)
- **Proof by Definition.** *We define it to be true.*
- **Proof by Design.** *We add it as an axiom.*
- **Proof by Authority.** *I've just met Gauss in the elevator, he told me that was true, so it must be!*
- **Proof by Stubbornness.** *The favorite method of a former student of mine.*
- **The Only Valid Proof.** *It is too beautiful to be false.*



## Exercises

### Exercise 1.

Let  $E$  be a set.

1. Prove that  $\forall A, B, C \in \mathcal{P}(E), A \cup B = B \cap C \implies A \subset B \subset C$ .
2. Prove that  $\forall A, B \in \mathcal{P}(E), A \cap B = A \cup B \implies A = B$ .

### Exercise 2.

Let  $f : A \rightarrow B, g : B \rightarrow C$  and  $h : C \rightarrow D$  be three functions.

Prove that  $g \circ f$  and  $h \circ g$  are bijective if and only if  $f, g$  and  $h$  are bijective.

### Exercise 3.

Let  $f : E \rightarrow F$ .

1. Prove that  $\forall A \in \mathcal{P}(E), A \subset f^{-1}(f(A))$ .
2. Prove that  $\forall B \in \mathcal{P}(F), f(f^{-1}(B)) \subset B$ .
3. Can these inclusions be strict?

### Exercise 4.

Let  $f : E \rightarrow F$ .

1. Prove that  $\forall A, B \in \mathcal{P}(F), A \subset B \implies f^{-1}(A) \subset f^{-1}(B)$ .  
Does the converse hold?
2. Prove that  $\forall A, B \in \mathcal{P}(F), f^{-1}(A \cap B) = f^{-1}(A) \cap f^{-1}(B)$ .
3. Prove that  $\forall A, B \in \mathcal{P}(F), f^{-1}(A \cup B) = f^{-1}(A) \cup f^{-1}(B)$ .

### Exercise 5.

Let  $f : E \rightarrow F$ .

1. Prove that  $\forall A, B \in \mathcal{P}(E), A \subset B \implies f(A) \subset f(B)$ .  
Does the converse hold?
2. Prove that  $\forall A, B \in \mathcal{P}(E), f(A \cap B) \subset f(A) \cap f(B)$ .  
Can the inclusion be strict?
3. Prove that  $\forall A, B \in \mathcal{P}(E), f(A \cup B) = f(A) \cup f(B)$ .

### Exercise 6.

Let  $f : E \rightarrow F$ . Prove that  $f$  is injective if and only if  $\forall A, B \in \mathcal{P}(E), f(A \cap B) = f(A) \cap f(B)$ .

### Exercise 7.

Let  $E$  be a finite set. For  $A, B \in \mathcal{P}(E)$  we define the symmetric difference of  $A$  and  $B$  by  $A \Delta B = (A \cup B) \setminus (A \cap B)$ .

Prove that  $\forall A, B \in \mathcal{P}(E), |A \Delta B| = |A| + |B| - 2|A \cap B|$ .

### Exercise 8.

Let  $E$  and  $F$  be two finite sets.

1. Prove that  $F^E$  (the set of functions  $E \rightarrow F$ ) is finite and express  $|F^E|$  in terms of  $|E|$  and  $|F|$ .
2. Prove that the set  $\{f \in F^E : f \text{ is injective}\}$  is finite and express its cardinal in terms of  $|E|$  and  $|F|$ .
3. Prove that the set  $\{f \in F^E : f \text{ is bijective}\}$  is finite and express its cardinal in terms of  $|E|$ .

The case of surjective functions is more tricky.

### Exercise 9.

Let  $E$  be a finite set and  $k \in \{0, 1, \dots, |E|\}$ . What is the cardinal of  $\{A \in \mathcal{P}(E) : |A| = k\}$ ?

### Exercise 10.

Prove that a set  $E$  is finite if and only if  $\mathcal{P}(E)$  is finite.

In this case, give an expression of  $|\mathcal{P}(E)|$  in terms of  $|E|$ .



**Exercise 11.** *The pigeonhole principle or Dirichlet's drawer principle*

I had no enough time to cover this topic in lectures, so here it is :-).

1. Let  $E$  and  $F$  be two finite sets. Prove that  $|E| \leq |F|$  if and only if there exists an injection  $f : E \rightarrow F$ .
2. Let  $E$  and  $F$  be two finite sets. Prove that if  $|E| > |F|$  then there is no injective function  $E \rightarrow F$ .  
*This statement is pigeonhole principle or Dirichlet's drawer principle: if you have  $n$  elements put in  $k < n$  boxes, then at least one box contains two elements.*
3. During a post-covid party with  $n > 1$  participants, we may always find two people who shook hands to the same number of people.
4. Let  $n \in \mathbb{N} \setminus \{0\}$ . Let  $a_1, a_2, \dots, a_n \in \mathbb{Z}$ . Prove that there exists distinct  $i_1, \dots, i_r \in \{1, \dots, n\}$ ,  $r \geq 1$ , so that  $n \mid \sum_{k=1}^r a_{i_k}$ .
5. Prove that among 13 distinct real numbers, there always exist two  $x, y$  satisfying  $0 < \frac{x-y}{1+xy} < 2 - \sqrt{3}$ .  
*Hint: it looks like a trigonometric formula you know!*

**Exercise 12.**

Given three sets  $E, F, G$ , prove that if  $E \subset F \subset G$  and  $|E| = |G|$  then  $|E| = |F|$ .

**Exercise 13.**

Given a set  $S$ , prove that  $|\mathcal{P}(S)| = |\{0, 1\}^S|$  where  $\{0, 1\}^S$  denotes the set of functions  $S \rightarrow \{0, 1\}$ .

*Remark: this formula generalizes the fact that if  $S$  is a finite set with  $n = |S|$  then  $|\mathcal{P}(S)| = 2^n$ .*

*Therefore it is common to denote the powerset of a set  $S$  by  $2^S := \mathcal{P}(S)$ .*

**Exercise 14.**

1. What is  $|\{0, 1\}^{\mathbb{N}}|$ ? i.e. what is the cardinality of the set of functions  $\mathbb{N} \rightarrow \{0, 1\}$ ?
2. What is  $|\mathbb{N}^{\{0,1\}}|$ ? i.e. what is the cardinality of the set of functions  $\{0, 1\} \rightarrow \mathbb{N}$ ?

**Exercise 15.**

1. What is the cardinality of  $S = \{A \in \mathcal{P}(\mathbb{N}) : A \text{ is finite}\}$ .
2. Is  $T = \{A \in \mathcal{P}(\mathbb{N}) : A \text{ is infinite}\}$  countable?

**Exercise 16.**

Prove that any set  $X$  of pairwise disjoint intervals which are non-empty and not reduced to a singleton is countable,

i.e. if  $X \subset \mathcal{P}(\mathbb{R})$  satisfies

- (i)  $\forall I \in X$ ,  $I$  is an interval which is non-empty and not reduced to a singleton
- (ii)  $\forall I, J \in X$ ,  $I \neq J \implies I \cap J = \emptyset$

then  $X$  is countable.

**Exercise 17.**

Prove that a set is infinite if and only if it admits a proper subset of same cardinality.

**Exercise 18.**

1. Prove that  $\mathbb{R} \setminus \mathbb{Q}$  is not countable.
2. Prove that  $|\mathbb{R} \setminus \mathbb{Q}| = |\mathbb{R}|$ .

**Exercise 19.**

Prove that  $|(0, 1)| = |\mathbb{R}|$ .

**Exercise 20.**

1. Prove that  $|\mathbb{R}^2| = |\mathbb{R}|$ .
2. Prove that  $\forall n \in \mathbb{N} \setminus \{0\}, |\mathbb{R}^n| = |\mathbb{R}|$ .
3. Prove that  $|\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$  where  $\mathbb{R}^{\mathbb{N}}$  is the set of sequences/functions  $\mathbb{N} \rightarrow \mathbb{R}$ .

**Exercise 21.**

Set  $S^2 := \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$ . Prove that  $|S^2| = |\mathbb{R}|$ .

**Exercise 22.**

What is the cardinality of the set  $S$  of all circles in the plane?

# Chapter 8

## Sample solutions to the exercises

### 8.1 Chapter 1

#### Sample solutions to Exercise 1.

1. Given  $a \in \mathbb{N}$ , we already know that  $a \times 0 = 0$  by definition of the multiplication. So we only need to prove that  $\forall a \in \mathbb{N}, 0 \times a = 0$ .

Set  $A = \{a \in \mathbb{N} : 0 \times a = 0\}$ , then

- $A \subset \mathbb{N}$
- $0 \in A$  since  $0 \times 0 = 0$  by definition of the multiplication.
- $s(A) \subset A$ . Indeed, let  $m \in s(A)$ , then  $m = s(a)$  for some  $a \in A$ . Then

$$\begin{aligned} 0 \times m &= 0 \times s(a) \\ &= 0 \times a + 0 \text{ by definition of the multiplication} \\ &= 0 + 0 \text{ since } a \in A \\ &= 0 \end{aligned}$$

Thus  $m \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . So  $\forall a \in \mathbb{N}, 0 \times a = 0$ .

2. Let  $a \in \mathbb{N}$ . Then

$$\begin{aligned} a \times 1 &= a \times s(0) \text{ since } 1 = s(0) \\ &= a \times 0 + a \text{ by definition of the multiplication} \\ &= 0 + a \text{ by definition of the multiplication} \\ &= a \end{aligned}$$

#### Sample solutions to Exercise 2.

1. Let  $m \in \mathbb{N}$  then  $m^1 = m^{s(0)} = m^0 \times m = 1 \times m = m$ .

2. Let  $a, b \in \mathbb{N}$ . Set  $A = \{n \in \mathbb{N} : (ab)^n = a^n b^n\}$ .

- $A \subset \mathbb{N}$
- $0 \in A$ : indeed,  $(ab)^0 = 1$  and  $a^0 b^0 = 1 \times 1 = 1$ .

- $s(A) \subset A$ : let  $m \in s(A)$  then  $m = s(n)$  for some  $n \in A$ . Next

$$\begin{aligned}
 (ab)^m &= (ab)^{s(n)} \text{ since } m = s(n) \\
 &= (ab)^n(ab) \text{ by definition of } (ab)^\bullet \\
 &= a^n b^n ab \text{ since } n \in A \\
 &= (a^n a)(b^n b) \text{ by properties of the product} \\
 &= a^{s(n)} b^{s(n)} \text{ by definition of } a^\bullet \text{ and } b^\bullet \\
 &= a^m b^m \text{ since } m = s(n)
 \end{aligned}$$

Hence  $m \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . So for all  $n \in \mathbb{N}$ ,  $(ab)^n = a^n b^n$ .

3. Let  $a, m \in \mathbb{N}$ . Set  $A = \{n \in \mathbb{N} : a^{m+n} = a^m a^n\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$ : indeed,  $a^{m+0} = a^m = a^m \times 1 = a^m \times a^0$
- $s(A) \subset A$ : let  $k \in s(A)$  then  $k = s(n)$  for some  $n \in A$ . Next

$$\begin{aligned}
 a^{m+k} &= a^{m+s(n)} \text{ since } k = s(n) \\
 &= a^{s(m+n)} \text{ by definition of the addition} \\
 &= a^{m+n} \times a \text{ by definition of } a^\bullet \\
 &= a^m a^n a \text{ since } n \in A \\
 &= a^m a^{s(n)} \text{ by definition of } a^\bullet \\
 &= a^m a^k \text{ since } k = s(n)
 \end{aligned}$$

Hence  $k \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . So for all  $n \in \mathbb{N}$ ,  $a^{m+n} = a^m a^n$ .

4. Let  $n \in \mathbb{N} \setminus \{0\}$ . Then there exists  $m \in \mathbb{N}$  such that  $n = s(m)$ . Thus  $0^n = 0^{s(m)} = 0^m \times 0 = 0$ .

5. Set  $A = \{n \in \mathbb{N} : 1^n = 1\}$ . Then

- $A \subset \mathbb{N}$
- $0 \in A$ :  $1^0 = 1$  by definition of  $1^\bullet$ .
- $s(A) \subset A$ : let  $m \in s(A)$  then  $m = s(n)$  for some  $n \in A$ . Next

$$\begin{aligned}
 1^m &= 1^{s(n)} \text{ since } m = s(n) \\
 &= 1^n \times 1 \text{ by definition of } 1^\bullet \\
 &= 1 \times 1 \text{ since } n \in A \\
 &= 1
 \end{aligned}$$

Hence  $m \in A$ .

Therefore, by the induction principle,  $A = \mathbb{N}$ . So for all  $n \in \mathbb{N}$ ,  $1^n = 1$ .

### Sample solutions to Exercise 3.

1. This binary relation is not an order since it is not reflexive.  
Indeed,  $1\mathcal{R}1$  is false since  $1 \neq -1$ .
2. This binary relation is not an order since it is not antisymmetric.  
Indeed,  $0\mathcal{R}(2\pi)$  and  $(2\pi)\mathcal{R}0$  are true but  $0 \neq 2\pi$ .
3. The inclusion is an order on  $\mathcal{P}(S)$ . Indeed

- $\forall A \in \mathcal{P}(S), A \subset A$  (reflexivity).
- $\forall A, B \in \mathcal{P}(S), (A \subset B \text{ and } B \subset A) \implies A = B$  (antisymmetry).
- $\forall A, B, C \in \mathcal{P}(S), (A \subset B \text{ and } B \subset C) \implies A \subset C$  (transitivity).

If  $S = \emptyset$  then  $\mathcal{P}(S) = \{\emptyset\}$ : the order is obviously total.

If  $S = \{*\}$  has only one element then  $\mathcal{P}(S) = \{\emptyset, \{*\}\}$ : the order is obviously total.

If  $S$  contains at least two elements  $a, b$  then the order is not total.

Indeed, set  $A = S \setminus \{a\}$  and  $B = S \setminus \{b\}$ .

Then  $A \not\subset B$  since  $b \in A$  but  $b \notin B$ , and,  $B \not\subset A$  since  $a \in B$  but  $a \notin A$ .

Thus, if  $S$  contains at least two elements, then  $\subset$  is not a total order on  $\mathcal{P}(S)$ .

#### Sample solutions to Exercise 4.

- Reflexivity. Let  $x \in \mathbb{N}$ . Then  $x = 1 \times x^1$ . Hence  $x \mathcal{R} x$ .
  - Antisymmetry. Let  $x, y \in \mathbb{N}$  be such that  $x \mathcal{R} y$  and  $y \mathcal{R} x$ . Then  $x \leq y$  and  $y \leq x$ . Thus  $x = y$ .
  - Transitivity. Let  $x, y, z \in \mathbb{N}$  be such that  $x \mathcal{R} y$  and  $y \mathcal{R} z$ . Then  $y = px^q$  and  $z = ry^s$  for some  $p, q, r, s \in \mathbb{N} \setminus \{0\}$ . Hence  $z = ry^s = rp^s x^{qs}$  with  $rp^s, qs \in \mathbb{N} \setminus \{0\}$ . Thus  $x \mathcal{R} z$ .
- This order is not total since  $0 \mathcal{R} 1$  and  $1 \mathcal{R} 0$  are both false.

#### Sample solutions to Exercise 5.

- Reflexivity. Let  $(x, y) \in \mathbb{N}^2$ , then  $x \leq x$  and  $y \leq y$  hence  $(x, y) < (x, y)$ .
  - Antisymmetry. Assume that  $(x_1, y_1) < (x_2, y_2)$  and that  $(x_2, y_2) < (x_1, y_1)$ . Then  $x_1 \leq x_2, y_1 \leq y_2, x_2 \leq x_1$  and  $y_2 \leq y_1$ . Since  $\leq$  is an order on  $\mathbb{N}$ , we get that  $x_1 = x_2$  and  $y_1 = y_2$ . Thus  $(x_1, y_1) = (x_2, y_2)$ .
  - Transitivity. Assume that  $(x_1, y_1) < (x_2, y_2)$  and that  $(x_2, y_2) < (x_3, y_3)$ . Then  $x_1 \leq x_2, y_1 \leq y_2, x_2 \leq x_3$  and  $y_2 \leq y_3$ . Since  $\leq$  is an order on  $\mathbb{N}$ , we get that  $x_1 \leq x_3$  and  $y_1 \leq y_3$ . Thus  $(x_1, y_1) < (x_3, y_3)$ .
- Note that  $(1, 0) < (0, 1)$  and  $(0, 1) < (1, 0)$  are both false. Hence  $<$  is not a total order on  $\mathbb{N}^2$ .

#### Sample solutions to Exercise 6.

**Method 1:** using the definition.

- Let  $a, b, c, d \in \mathbb{N}$ . Assume that  $a \leq b$  and  $c \leq d$ . Then there exist  $k, l \in \mathbb{N}$  such that  $b = a + k$  and  $d = c + l$ . Hence  $b + d = a + k + c + l = (a + c) + (k + l)$  with  $k + l \in \mathbb{N}$ . Thus  $a + c \leq b + d$ .
- Let  $a, b, c, d \in \mathbb{N}$ . Assume that  $a \leq b$  and  $c \leq d$ . Then there exist  $k, l \in \mathbb{N}$  such that  $b = a + k$  and  $d = c + l$ . Hence  $bd = (a + k)(c + l) = ac + (al + kc + kl)$  with  $al + kc + kl \in \mathbb{N}$ . Thus  $ac \leq bd$ .

**Method 2:** using the properties proved in class.

- Let  $a, b, c, d \in \mathbb{N}$  be such that  $a \leq b$  and  $c \leq d$ . Then  $a \leq b \implies a + c \leq b + c$  and  $c \leq d \implies b + c \leq b + d$ . Finally  $\begin{cases} a + c \leq b + c \\ b + c \leq b + d \end{cases} \implies a + c \leq b + d$ .
- Let  $a, b, c, d \in \mathbb{N}$  be such that  $a \leq b$  and  $c \leq d$ . Then  $a \leq b \implies ac \leq bc$  and  $c \leq d \implies bc \leq bd$ . Finally  $\begin{cases} ac \leq bc \\ bc \leq bd \end{cases} \implies ac \leq bd$ .

**Sample solutions to Exercise 7.**

- The statement is false for  $c = 0$ , indeed,  $2 \times 0 \leq 1 \times 0$  but  $2 \leq 1$  is false.
- The statement is true for  $c \neq 0$ . We are going to prove the contrapositive,  $\forall a, b \in \mathbb{N}, b < a \implies bc < ac$ .  
Let  $a, b \in \mathbb{N}$  be such that  $b < a$ . Then  $b \leq a$  and hence  $bc \leq ac$ .  
Assume by contradiction that  $bc = ac$  then  $b = a$  since  $c \neq 0$ . Hence  $bc < ac$  as expected.

**Sample solutions to Exercise 8.**

Assume by contradiction that the set  $E = \{n \in \mathbb{N} : 0 < n < 1\}$  is not empty.

Then, by the well-ordering principle,  $E$  admits a least element, i.e. there exists  $l \in E$  such that  $\forall n \in \mathbb{N}, l \leq n$ . Since  $l \in E$ , we get that  $l < 1$ . Note that  $0 \notin E$ , so  $l \neq 0$ . Hence  $l < 1 \implies l^2 < l$ .

We know that if  $0 = l^2 = l \times l$  then  $l = 0$ . Hence  $l^2$  is positive.

Finally  $0 < l^2 < l < 1$ . So  $l^2 \in E$  which contradicts the fact that  $l$  is the least element of  $E$ .

**Sample solutions to Exercise 9.**

1. We are going to prove by induction that  $\forall n \in \mathbb{N}, \exists k \in \mathbb{N}, n^3 + 2n = 3k$ .

- *Base case at  $n = 0$ :*  $0^3 + 2 \times 0 = 3 \times 0$ .
- *Induction step:* assume that for some  $n \in \mathbb{N}$  there exists  $k \in \mathbb{N}$  such that  $n^3 + 2n = 3k$ . Then

$$\begin{aligned} (n+1)^3 + 2(n+1) &= n^3 + 3n^2 + 3n + 1 + 2n + 2 \\ &= 3k + 3n^2 + 3n + 3 \quad \text{by the induction hypothesis} \\ &= 3(k + n^2 + n + 1) \end{aligned}$$

The induction step is proved since  $k + n^2 + n + 1 \in \mathbb{N}$ .

2. We are going to prove by induction that  $\forall n \in \mathbb{N}, \sum_{k=0}^n \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$ .

- *Base case at  $n = 0$ :*  $\sum_{k=0}^0 \frac{k}{2^k} = 0$  and  $2 - \frac{0+2}{2^0} = 2 - 2 = 0$ .
- *Induction step:* assume that  $\sum_{k=0}^n \frac{k}{2^k} = 2 - \frac{n+2}{2^n}$  for some  $n \in \mathbb{N}$ .

$$\begin{aligned} \sum_{k=0}^{n+1} \frac{k}{2^k} &= \sum_{k=0}^n \frac{k}{2^k} + \frac{n+1}{2^{n+1}} \\ &= 2 - \frac{n+2}{2^n} + \frac{n+1}{2^{n+1}} \quad \text{by the induction hypothesis} \\ &= 2 - \frac{2n+4-n-1}{2^{n+1}} = 2 - \frac{(n+1)+2}{2^{n+1}} \end{aligned}$$

which ends the induction step.

**Sample solutions to Exercise 10.**

We are going to prove by (strong) induction that  $\forall n \geq 1, u_n = 3n$ .

- *Base case at  $n = 1$ :*  $u_1 = 3 \times 1$ .

- *Induction step*: assume that  $u_k = 3k$  for  $k = 1, \dots, n$  where  $n \geq 1$ . Then

$$\begin{aligned} u_{n+1} &= \frac{2}{n+1} \sum_{k=1}^n u_k \\ &= \frac{2}{n} \sum_{k=1}^n 3k \quad \text{by the induction hypothesis} \\ &= \frac{6}{n} \sum_{k=1}^n k = \frac{6}{n} \frac{n(n+1)}{2} = 3(n+1) \end{aligned}$$

which ends the induction step.

### Sample solutions to Exercise 11.

Let  $x \in [-1, +\infty)$ . We are going to prove by induction that  $\forall n \in \mathbb{N}, (1+x)^n \geq 1+nx$ .

- *Base case at  $n = 0$* :  $(1+x)^0 = 1$  and  $1+0 \times x = 1$ .
- *Induction step*: assume that  $(1+x)^n \geq 1+nx$  for some  $n \in \mathbb{N}$ . Then

$$\begin{aligned} (1+x)^{n+1} &= (1+x)^n(1+x) \\ &\geq (1+nx)(1+x) \quad \text{by the induction hypothesis since } 1+x \geq 0 \\ &= 1+x+nx+nx^2 \\ &\geq 1+x+nx = 1+(n+1)x \end{aligned}$$

which ends the induction step.

### Sample solutions to Exercise 12.

- Let  $n \geq 3$ . Assume that  $P(n)$  is true, i.e.  $2^n > n^2$ , and let's prove  $P(n+1)$ , i.e.  $2^{n+1} > (n+1)^2$ .  
From the assumption, we get that  $2^{n+1} = 2 \times 2^n \geq 2n^2$ . Hence it is enough to prove that  $2n^2 > (n+1)^2$  which is equivalent to  $n^2 - 2n - 1 > 0$ .  
We study the sign of the polynomial  $x^2 - 2x - 1$ . It is a polynomial of degree 2 with positive leading coefficient and its discriminant is  $(-2)^2 - 4 \times (-1) = 8 > 0$ . Therefore

$x$	$-\infty$	$1 - \sqrt{2}$	$1 + \sqrt{2}$	$+\infty$	
$x^2 - 2x - 1$	+	0	-	0	+

Since  $n \geq 3 > 1 + \sqrt{2}$ , we know that  $n^2 - 2n - 1 > 0$ . Hence  $P(n+1)$  holds.

- $P(3)$  and  $P(4)$  are false, but  $P(5)$  is true. So by induction,  $\forall n \geq 5, P(n)$  is true.  
*Beware*: even if the induction step is true for  $n \geq 3$ , we can only start the induction proof at  $n = 5$ ! The base case is very important in a proof by induction.

### Sample solutions to Exercise 13.

The induction step is false when  $n = 2$  (it only holds for  $n \geq 3$ ). Indeed, for  $n = 2$ , we only have that  $A_1, A_2 \in L$  and that  $A_2, A_3 \in L'$ . Which is not enough to get that  $L = L'$  since we only know that they have one point in common (it works if they have at least two points in common).

**Beware**: if you start an induction proof with a base case at  $n_0$ , you have to make sure that the induction step  $P(n) \implies P(n+1)$  holds for every  $n \geq n_0$ . Otherwise, you didn't prove anything...

### Sample solutions to Exercise 14.

**Existence**. We are going to prove the existence of such a couple  $(a, b)$  by a strong induction on  $n$ .

- *Base case at  $n = 1$* :  $1 = 2^0(2 \times 0 + 1)$ .
- *Induction step*. Assume that for  $1, 2, \dots, n$  admit such an expression for some  $n \geq 1$ .

- First case:  $n + 1$  is even, i.e.  $n + 1 = 2k$  for some  $k \in \mathbb{N}$ .  
 Note that  $k \neq 0$  since otherwise  $1 \leq n + 1 = 0$ .  
 Since  $1 < 2$  and  $k \neq 0$ , we get that  $k < 2k = n + 1$ , so that  $k \leq n$ .  
 Hence, by the induction hypothesis,  $k = 2^a(2b + 1)$  for some  $(a, b) \in \mathbb{N}^2$ .  
 Then  $n + 1 = 2k = 2^{a+1}(2b + 1)$ .
  - Second case:  $n + 1$  is odd, i.e.  $n + 1 = 2k + 1$  for some  $k \in \mathbb{N}$ . But then  $n + 1 = 2^0(2 \times k + 1)$ .
- Which ends the induction step.

**Uniqueness.** Assume that  $2^a(2b + 1) = 2^\alpha(2\beta + 1)$  for  $a, b, \alpha, \beta \in \mathbb{N}$ .

If  $a < \alpha$  then, by cancellation, we obtain  $2b + 1 = 2^{\alpha-a}(2\beta + 1)$ . Which is impossible since the LHS is odd whereas the RHS is even.

If  $\alpha < a$  then, by cancellation, we obtain  $2^{a-\alpha}(2b + 1) = 2\beta + 1$ . Which is impossible since the RHS is odd whereas the LHS is even.

Therefore  $a = \alpha$ , and by cancellation we obtain  $2b + 1 = 2\beta + 1$ , hence  $2b = 2\beta$  and finally  $b = \beta$ .

We proved that  $(a, b) = (\alpha, \beta)$ .

### Sample solutions to Exercise 15.

The function  $f : \mathbb{N} \rightarrow \mathbb{N}$  defined by  $f(n) = n$  satisfies the conditions of the question. Actually, as we are going to prove, it is the only one.

From now on, we assume that  $f : \mathbb{N} \rightarrow \mathbb{N}$  satisfies  $f(2) = 2$  and  $\forall p, q \in \mathbb{N}, f(pq) = f(p)f(q)$ , and we want to prove that  $\forall n \in \mathbb{N}, f(n) = n$ .

- We know that  $0 < 1 < 2$  hence  $0 \leq f(0) < f(1) < f(2) = 2$ .  
 Therefore, the only possibility is that  $f(0) = 0$  and  $f(1) = 1$ .
- Let's prove by strong induction that  $\forall n \in \mathbb{N}, f(n) = n$ .
  - Base case at  $n = 0$ :  $f(0) = 0$ .
  - Induction step. Assume that  $f(0) = 0, f(1) = 1, f(2) = 2, f(3) = 3, \dots, f(n) = n$  for some  $n \geq 0$ .
    - \* First case:  $n + 1$  is even, i.e. there exists  $k \in \mathbb{N}$  such that  $n + 1 = 2k$ .  
 Note that  $k \neq 0$  since otherwise  $1 \leq n + 1 = 0$ .  
 Since  $1 < 2$  and  $k \neq 0$ , we get that  $k < 2k = n + 1$ , so that  $k \leq n$ .  
 Then, by the induction hypothesis,  $f(n + 1) = f(2k) = f(2)f(k) = 2k = n + 1$ .
    - \* Second case:  $n + 1$  is odd, i.e. there exists  $k \in \mathbb{N}$  such that  $n + 1 = 2k + 1$ .  
 Either  $k = 0$  and then  $f(n + 1) = f(1) = 1 = n + 1$ .  
 Or  $k \neq 0$  and then  $k + 1 < 2k + 1 = n + 1$ , i.e.  $k \leq n$ .  
 Then  $f(n + 2) = f(2(k + 1)) = f(2)f(k + 1) = n + 2$  by the induction hypothesis.  
 Thus  $n = f(n) < f(n + 1) \leq f(n + 2) = n + 2$ .  
 The only possible value is that  $f(n + 1) = n + 1$ .

### Sample solutions to Exercise 16.

1. Let  $m, m' \in S$  be two greatest elements of  $S$ .  
 Since  $m \in S$  and  $m'$  is a greatest element, we have  $m \leq m'$ .  
 Similarly, since  $m' \in S$  and  $m$  is a greatest element of  $S$ , we have  $m' \leq m$ .  
 Hence  $m = m'$ .

*That's why we say **the** greatest element: if it exists, it is unique (whereas we say **an** upper bound).*

2. Let's prove that a non-empty finite subset  $S \subset \mathbb{Z}$  has a greatest element, by induction on  $n = \#S$ .
  - Base case at  $n = 1$ : if  $S$  is a singleton, then its unique element is its greatest element.
  - Induction step. Assume that the statement holds for sets of cardinal  $n$ , for some  $n \geq 1$ .  
 Let  $S \subset \mathbb{Z}$  be such that  $\#S = n + 1$ .



Particularlry  $S \neq \emptyset$ , so there exists  $a \in S$ .

Set  $T = S \setminus \{a\}$ . Then  $\#T = n$ , so by the induction hypothesis  $T$  admits a greatest element  $m \in T$ .

I claim that  $M = \max(m, a) \in T \cup \{a\} = S$  is the greatest element of  $S$ .

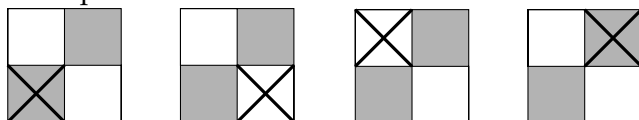
Indeed, let  $n \in S$ , either  $n = a$  and then  $a \leq M$ , or  $n \in T$  and then  $n \leq m \leq M$ .

Which ends the inductive step.

### Sample solutions to Exercise 17.

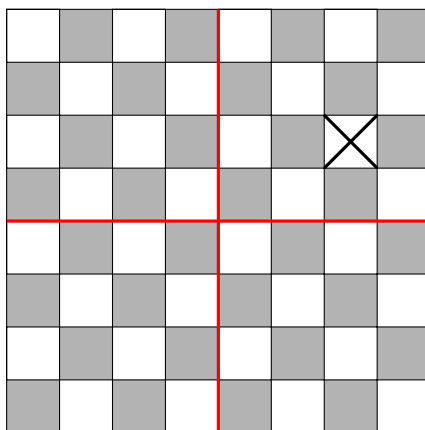
We are going to prove by induction on  $n \geq 1$  that if one square of a  $2^n \times 2^n$  chessboard is removed, then the remaining squares can be covered with L-shaped trominoes.

- *Base case at  $n = 1$ .* There are only four possible cases and for each of them the remaining is exactly one L-shaped tromino:

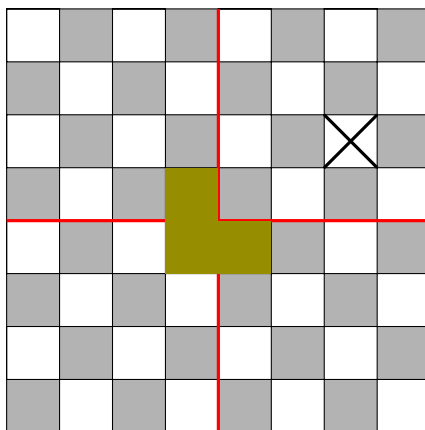


- Assume that the statement holds for some  $n \geq 1$  and consider a  $2^{n+1} \times 2^{n+1}$  chessboard with a removed square.

We may split this chessboard into four  $2^n \times 2^n$  chessboards as follows:



We may place an L-shaped tromino such that it covers the corner situated at the center for each  $2^n \times 2^n$  chessboard without a removed square, see below.



Now, each of the  $2^n \times 2^n$  chessboards has a removed square: we may apply the induction hypothesis in order to cover the remaining squares with L-shaped trominoes.

## 8.2 Chapter 2

### Sample solutions to Exercise 1.

Let  $a, b \in \mathbb{Z}$  such that  $a^2 = b^2$ . Then  $0 = a^2 - b^2 = (a - b)(a + b)$ . Hence either  $a = b$  or  $a = -b$ . In both cases  $|a| = |b|$ .

### Sample solutions to Exercise 2.

Consider  $n$  consecutive integers  $a, a + 1, \dots, a + (n - 1)$ .

By Euclidean division, there exists  $b, q \in \mathbb{Z}$  such that  $a + (n - 1) = bn + r$  and  $0 \leq r < n$ .

Then  $a + (n - 1) - r = bn$  and  $0 \leq (n - 1) - r \leq n - 1$ . Thus  $a + (n - 1) - r$  is an element of the above list which is divisible by  $n$ .

### Sample solutions to Exercise 3.

1. We use Euclid's algorithm:

$$\begin{array}{rclcl} 2260 & = & 816 & \times & 2 & + & 628 \\ 816 & = & 628 & \times & 1 & + & 188 \\ 628 & = & 188 & \times & 3 & + & 64 \\ 188 & = & 64 & \times & 2 & + & 60 \\ 64 & = & 60 & \times & 1 & + & 4 \\ 60 & = & 4 & \times & 15 & + & 0 \end{array}$$

Thus  $\gcd(816, 2260) = 4$ .

2. To find a Bézout's relation for 816 and 2260, we follow Euclid's algorithm backward: at each step we plug the previous remainder starting from the last Euclidean division with non-zero remainder.

$$\begin{aligned} 4 &= 64 - 60 \\ &= 64 - (188 - 64 \times 2) \\ &= -188 + 64 \times 3 \\ &= -188 + (628 - 188 \times 3) \times 3 \\ &= 628 \times 3 + 188 \times (-10) \\ &= 628 \times 3 + (816 - 628) \times (-10) \\ &= 816 \times (-10) + 628 \times 13 \\ &= 816 \times (-10) + (2260 - 816 \times 2) \times 13 \\ 4 &= 2260 \times 13 + 816 \times (-36) \end{aligned}$$

### Sample solutions to Exercise 4.

1. Divisibility doesn't define an order on  $\mathbb{Z}$  since it is not antisymmetric. Indeed  $1 \mid -1$  and  $-1 \mid 1$  but  $-1 \neq 1$ .
2. Divisibility defines an order on  $\mathbb{N}$ :
  - *Reflexivity.* Let  $a \in \mathbb{N}$  then  $a = a \times 1$  so that  $a \mid a$ .
  - *Transitivity.* Let  $a, b, c \in \mathbb{N}$  be such that  $a \mid b$  and  $b \mid c$ . Then  $b = ka$  and  $c = lb$  for some  $k, l \in \mathbb{Z}$ . Thus  $c = lk = lka$ . Hence  $a \mid c$ .
  - *Antisymmetry.* Let  $a, b \in \mathbb{N}$  such that  $a \mid b$  and  $b \mid a$ . Then  $|a| = |b|$ . But since  $a, b \in \mathbb{N}$ ,  $|a| = a$  and  $|b| = b$ . Therefore  $a = b$ .

It is not total since  $2 \nmid 3$  and  $3 \nmid 2$ .

**Sample solutions to Exercise 5.**

Let's prove by induction that  $\forall n \in \mathbb{N}, 7|3^{2n+1} + 2^{4n+2}$ .

Base case at  $n = 0$ :  $3^{2 \times 0 + 1} + 2^{4 \times 0 + 2} = 7$  and  $7|7$ .

Induction step: assume that  $7|3^{2n+1} + 2^{4n+2}$  for some  $n \in \mathbb{N}$ .

Then  $3^{2n+1} + 2^{4n+2} = 7k$  for some  $k \in \mathbb{Z}$  and

$$\begin{aligned} 3^{2(n+1)+1} + 2^{4(n+1)+2} &= 9 \times 3^{2n+1} + 16 \times 2^{4n+2} \\ &= (7 + 2) \times 3^{2n+1} + (7 \times 2 + 2) \times 2^{4n+2} \\ &= 7 \times (3^{2n+1} + 2 \times 2^{4n+2}) + 2 \times (3^{2n+1} + 2^{4n+2}) \\ &= 7 \times (3^{2n+1} + 2^{4n+3}) + 6 \times 7k \\ &= 7 \times (3^{2n+1} + 2^{4n+3} + 6k) \end{aligned}$$

Hence  $7|3^{2(n+1)+1} + 2^{4(n+1)+2}$  which ends the induction step.

**Sample solutions to Exercise 6.**

Since  $ad + bc$  divides  $a, b, c, d$ , there exist  $\alpha, \beta, \delta$  such that  $a = \alpha(ad + bc)$ ,  $b = \beta(ad + bc)$ ,  $c = \gamma(ad + bc)$  and  $d = \delta(ad + bc)$ .

Then  $ad + bc = \alpha(ad + bc)\delta(ad + bc) + \beta(ad + bc)\gamma(ad + bc) = (\alpha\delta + \beta\gamma)(ad + bc)^2$ .

Since  $ad + bc \neq 0$ , we get that  $1 = (\alpha\delta + \beta\gamma)(ad + bc)$ .

Therefore  $(ad + bc)|1$ , and obviously  $1|(ad + bc)$ , hence  $|ad + bc| = |1| = 1$ .

**Sample solutions to Exercise 7.**

Let  $n \in \mathbb{N}$ . Set  $d = \gcd(n^2 + n, 2n + 1)$ . Then  $d | ((2n + 1)^2 - 4(n^2 + n)) = 1$ . Thus  $d = 1$ .

**Sample solutions to Exercise 8.**

Let  $a, b \in \mathbb{Z}$  be such that  $\gcd(a, b) = 1$ .

By Bézout's identity, there exist  $u, v \in \mathbb{Z}$  such that  $au + bv = 1$ .

Hence  $1 = (au + bv)^3 = a^2(au^3 + 3u^2bv) + b^2(bv^3 + 3auv^2)$ .

Thus if  $d|a^2$  and  $d|b^2$  then  $d|a^2(au^3 + 3u^2bv) + b^2(bv^3 + 3auv^2) = 1$ .

Therefore  $\gcd(a^2, b^2) = 1$ .

**Sample solutions to Exercise 9.**

1. Let  $a, b \in \mathbb{Z} \setminus \{0\}$  such that  $a^2|b^2$ .

Set  $d = \gcd(a, b)$ , then  $a = \alpha d$  and  $b = \beta d$  for some  $\alpha, \beta \in \mathbb{Z}$ .

Then  $d = \gcd(a, b) = d \gcd(\alpha, \beta)$ , thus  $\gcd(\alpha, \beta) = 1$ .

And  $\gcd(a^2, b^2) = \gcd(d^2\alpha^2, d^2\beta^2) = d^2 \gcd(\alpha^2, \beta^2) = d^2$  from the previous exercise.

Since  $a^2|b^2$ , we know that  $\gcd(a^2, b^2) = a^2$ .

Hence  $a^2 = d^2$  and thus  $d = \pm a$ .

Therefore  $a = \pm d|b$ .

2. Let  $a, b, c \in \mathbb{Z} \setminus \{0\}$  be such that  $\gcd(a, b) = 1$  and  $c|b$ .

From Bézout's identity, there exist  $u, v \in \mathbb{Z}$  such that  $au + bv = 1$ .

Let  $d \in \mathbb{Z}$  such that  $d|a$  and  $d|c$ . Then,  $d|b$  since  $c|b$ .

Hence  $d|au + bv = 1$ .

Therefore  $\gcd(a, b) = 1$ .

**Sample solutions to Exercise 10.**

1. Let  $a, b \in \mathbb{Z}$  be such that  $\gcd(a, b) = 1$ . From Bézout's identity, there exist  $u, v \in \mathbb{Z}$  such that  $au + bv = 1$ .

Squaring both sides, we get  $a^2u^2 + b^2v^2 + 2abuv = 1$ .

Let  $d = \gcd(a + b, ab)$ . Note that  $a^2 = a(a + b) - ab$ ,  $b^2 = b(a + b) - ab$  hence  $d|a^2$  and  $d|b^2$ . Besides  $d|ab$ .

Therefore  $d|(a^2u^2 + b^2v^2 + 2abuv) = 1$ . Hence  $d = 1$ .

2. Take  $a = b = 1$ . Then  $\gcd(a, b) = 1$  but  $\gcd(a + b, a^2 + b^2) = 2$ . So the statement is false.

**Sample solutions to Exercise 11.**

First, he replaces days with numbers as follows:

- Sunday  $\leftrightarrow 0$
- Monday  $\leftrightarrow 1$
- Tuesday  $\leftrightarrow 2$
- Wednesday  $\leftrightarrow 3$
- Thursday  $\leftrightarrow 4$
- Friday  $\leftrightarrow 5$
- Saturday  $\leftrightarrow 6$

So we can assume that the sticky notes contain a number between 0 and 6 (included).

Then he numbers the participants (including himself) from 0 to 6 (which is possible since there are seven friends).

And then he explains: "each of us will add to the sum of the six days he can see, the unique number of  $\{0, 1, \dots, 6\}$  such that the remainder of the Euclidean division by 7 of the obtained sum corresponds to its assigned number."

Let me explain why it works.

First, by Euclidean division, the actual sum  $N$  of the seven numbers stuck on their foreheads can be uniquely written  $N = 7 \times q + r$  with  $0 \leq r < 7$ , i.e. the possible remainders are  $r \in \{0, 1, \dots, 6\}$ .

I claim that the participant whose assigned number is  $r$  gets the correct answer.

Indeed, if the sum of the six numbers he sees is  $M$ , then there is a unique  $a \in \{0, 1, \dots, 6\}$  such that the Euclidean division of  $M + a$  by 7 is  $r$ , i.e.  $M + a = 7 \times q' + r$ .

Since  $N - M \in \{0, 1, \dots, 6\}$  and since  $N$  and  $M + a$  have same remainder by 7, then necessarily  $N = M + a$ . So  $a$  is exactly the day on the sticky note of the participant whose assigned number is  $r$ . And he gets the good answer.

**Sample solutions to Exercise 12.**

We are going to use the *pigeonhole principle* also called *Dirichlet's drawer principle*.

1. The remainder of an Euclidean division by 41 satisfies  $0 \leq r < 41$ . Hence, there are 41 possible remainders. Therefore, among 42 distinct integers, at least two, say  $a$  and  $b$ , have the same remainder (otherwise the number of remainders will be 42). Then  $a = 41q + r$  and  $b = 41q' + r$  for  $q, q', r \in \mathbb{Z}$  such that  $0 \leq r < 41$ . And finally  $b - a = 41(q' - q)$ .
2. Either we can find 3 of these integers which have the same remainder by Euclidean division by 3, i.e.  $x_1 = 3q_1 + r$ ,  $x_2 = 3q_2 + r$ ,  $x_3 = 3q_3 + r$ . And then  $x_1 + x_2 + x_3 = 3(q_1 + q_2 + q_3 + r)$ .  
Otherwise, we can find one integer for all the possible remainders:  $x_1 = 3q_1 + 0$ ,  $x_2 = 3q_2 + 1$  and  $x_3 = 3q_3 + 2$ . And then  $x_1 + x_2 + x_3 = 3(q_1 + q_2 + q_3 + 1)$ .

**Sample solutions to Exercise 13.**

The positive divisors of 25 are 1, 5 and 25. Hence,  $\gcd(3^{123} - 5, 25)$  has to be equal to one of these numbers. Assume by contradiction that  $\gcd(3^{123} - 5, 25) = 5$  or  $\gcd(3^{123} - 5, 25) = 25$ . In both cases,  $5 \mid 3^{123} - 5$  and so  $5 \mid 3^{123} = (3^{123} - 5) + 5$ . Contradiction.

Therefore  $\gcd(3^{123} - 5, 25) = 1$ .

**Sample solutions to Exercise 14.**

Let  $n \in \mathbb{Z}$ .

Since  $n$ ,  $n + 1$  and  $n + 2$  are three consecutive integers, one is divisible by 2 and one is divisible by 3.

Hence  $n(n + 1)(n + 2) = 2k$  and  $n(n + 1)(n + 2) = 3l$  for some  $k, l \in \mathbb{Z}$ .

Then  $2k = 3l$ , so that  $2 \mid 3l$ . Besides  $\gcd(2, 3) = 1$  thus  $2 \mid l$  by Gauss' lemma, i.e.  $l = 2m$  for some  $m \in \mathbb{Z}$ .

Therefore  $n(n + 1)(n + 2) = 3l = 6m$  and  $6 \mid n(n + 1)(n + 2)$ .

**Sample solutions to Exercise 15.**

In my solutions I use that  $\gcd(a, b) = \gcd(a + kb, b)$  (see Proposition 35 of Chapter 2).

1.  $\gcd(2n, 2n + 2) = \gcd(2n, (2n + 2) - 2n) = \gcd(2n, 2) = \gcd(2n - 2 \times n, 2) = \gcd(0, 2) = 2$ .
2.  $\gcd(2n - 1, 2n + 1) = \gcd(2n - 1, (2n + 1) - (2n - 1)) = \gcd(2n - 1, 2) = \gcd((2n - 1) - 2 \times n, 2) = \gcd(-1, 2) = 1$ .
3. 
$$\begin{aligned} \gcd(5a + 3b, 13a + 8b) &= \gcd(5a + 3b, (13a + 8b) - 2 \times (5a + 3b)) \\ &= \gcd(5a + 3b, 3a + 2b) = \gcd((5a + 3b) - (3a + 2b), 3a + 2b) \\ &= \gcd(2a + b, 3a + 2b) = \gcd(2a + b, (3a + 2b) - (2a + b)) \\ &= \gcd(2a + b, a + b) = \gcd((2a + b) - b, b) \\ &= \gcd(a + b, b) = \gcd(a, b) \end{aligned}$$

**Sample solutions to Exercise 16.**

(a) Let  $x, y \in \mathbb{Z}$ . Then

$$\begin{aligned} xy = 2x + 3y &\Leftrightarrow (x - 3)(y - 2) = 6 \\ &\Leftrightarrow (x - 3, y - 2) \in \{(1, 6), (2, 3), (3, 2), (6, 1), (-1, -6), (-2, -3), (-3, -2), (-6, -1)\} \\ &\Leftrightarrow (x, y) \in \{(4, 8), (5, 5), (6, 4), (9, 3), (2, -4), (1, -1), (0, 0), (-3, 1)\} \end{aligned}$$

(b) Let  $x, y \in \mathbb{Z} \setminus \{0\}$ . Then

$$\begin{aligned} \frac{1}{x} + \frac{1}{y} = \frac{1}{5} &\Leftrightarrow 5y + 5x = xy \\ &\Leftrightarrow (x - 5)(y - 5) = 25 \\ &\Leftrightarrow (x - 5, y - 5) \in \{(1, 25), (5, 5), (25, 1), (-1, -25), (-25, -1)\} \quad \text{since } x, y \neq 0 \\ &\Leftrightarrow (x, y) \in \{(6, 30), (10, 10), (30, 6), (4, -20), (-20, 4)\} \end{aligned}$$

(c) Let  $x, y \in \mathbb{Z}$ . Then

$$\begin{aligned} x + y = xy &\Leftrightarrow x + y - xy + 1 = 1 \\ &\Leftrightarrow (x - 1)(y - 1) = 1 \\ &\Leftrightarrow (x - 1, y - 1) = (-1, -1) \text{ or } (x - 1, y - 1) = (1, 1) \\ &\Leftrightarrow (x, y) = (0, 0) \text{ or } (x, y) = (2, 2) \end{aligned}$$

(d) For the next questions, see Section 2.8.

**Sample solutions to Exercise 17.**

1. Let  $a, b \in \mathbb{Z}$  not both zero. Set  $d = \gcd(a, b)$ .  
Since  $d|a$  and  $d|b$ , we know that  $a = da'$  and that  $b = db'$  for some  $a', b' \in \mathbb{Z}$ .  
Then  $d = \gcd(a, b) = \gcd(da', db') = d \gcd(a', b')$ . Hence  $\gcd(a', b') = 1$ .
2. **Method 1:** Let  $a, b, c \in \mathbb{Z} \setminus \{0\}$  be such that  $c|ab$ .  
Set  $d = \gcd(a, c)$  and  $\delta = \gcd(b, c)$ . Then  $a = da', c = dc', b = \delta b'', c = \delta c''$  where  $\gcd(a', c') = 1$  and  $\gcd(b'', c'') = 1$ .  
Therefore  $c|ab$  becomes  $dc'|da'\delta b''$ , hence  $c'|a'\delta b''$ . Since  $\gcd(a', c') = 1$ , by Gauss' lemma,  $c'|\delta b''$ .  
Hence  $\delta c'' = c = dc'|d\delta b''$ , so that  $c''|db''$ . Since  $\gcd(c'', b'') = 1$ , by Gauss' lemma,  $c''|d$ .  
Finally  $c = \delta c''|\delta d|da'\delta b'' = ab$ .

**Method 2:** Let  $a, b, c \in \mathbb{Z} \setminus \{0\}$  be such that  $c|ab$ .

Write  $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ ,  $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$  and  $c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_r^{\gamma_r}$  where the  $p_i$  are prime numbers and

$\alpha_i, \beta_i, \gamma_i \in \mathbb{N}$ .

Then  $\gcd(a, c) = p_1^{\min(\alpha_1, \gamma_1)} p_2^{\min(\alpha_2, \gamma_2)} \dots p_r^{\min(\alpha_r, \gamma_r)}$  and  $\gcd(b, c) = p_1^{\min(\beta_1, \gamma_1)} p_2^{\min(\beta_2, \gamma_2)} \dots p_r^{\min(\beta_r, \gamma_r)}$ .

Hence  $\gcd(a, c) \gcd(b, c) = p_1^{\min(\alpha_1, \gamma_1) + \min(\beta_1, \gamma_1)} p_2^{\min(\alpha_2, \gamma_2) + \min(\beta_2, \gamma_2)} \dots p_r^{\min(\alpha_r, \gamma_r) + \min(\beta_r, \gamma_r)}$ .

Thus  $c \mid \gcd(a, c) \gcd(b, c)$  if and only if  $\gamma_1 \leq \min(\alpha_1, \gamma_1) + \min(\beta_1, \gamma_1), \dots, \gamma_r \leq \min(\alpha_r, \gamma_r) + \min(\beta_r, \gamma_r)$ .

First case: if  $\min(\alpha_i, \gamma_i) = \gamma_i$  or  $\min(\beta_i, \gamma_i) = \gamma_i$  then  $\gamma_i \leq \min(\alpha_i, \gamma_i) + \min(\beta_i, \gamma_i)$ .

Otherwise:  $\min(\alpha_i, \gamma_i) + \min(\beta_i, \gamma_i) = \alpha_i + \beta_i$  but since  $c \mid ab$ , we know that  $\gamma_1 \leq \alpha_1 + \beta_1, \dots, \gamma_r \leq \alpha_r + \beta_r$ .

### Sample solutions to Exercise 18.

- $$\begin{aligned} ((a+b)^2 + b^2)((a-b)^2 + b^2) &= (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab) \\ &= (a^2 + 2b^2)^2 - (2ab)^2 \\ &= a^4 + 4a^2b^2 + 4b^4 - 4a^2b^2 = a^4 + 4b^4 \end{aligned}$$
- $3^{44} + 4^{29} = (3^{11})^4 + 4 \times (4^7)^4 = \left((3^{11} + 4^7)^2 + 4^{14}\right) \left((3^{11} - 4^7)^2 + 4^{14}\right)$  is non-trivial (i.e. none of the factor is  $\pm 1$ , check it).
- If  $n = 2k$  with  $k \in \mathbb{N} \setminus \{0\}$  then  $n^4 + 4^n$  is even and greater than 2, so it is composite.  
 If  $n = 2k + 1$  with  $k \in \mathbb{N} \setminus \{0\}$  then  $n^4 + 4^n = (2k + 1)^4 + 4 \times (2^k)^4$  which has a non-trivial factorization using Germain's identity (check it), so it is a composite.

### Sample solutions to Exercise 19.

Let  $k \in \mathbb{N} \setminus \{0\}$ . Assume by contradiction that  $(3k + 2)^2 = n^2 + p$  where  $n \in \mathbb{N}$  and  $p$  is a prime number.

Then  $p = (3k + 2)^2 - n^2 = (3k - n + 2)(3k + n + 2)$ .

- If  $3k - n + 2 = 1$  then  $n = 3k + 1$  so  $p = 3k + n + 2 = 6k + 3 = 3(2k + 1)$  is not prime, which leads to a contradiction.
- If  $3k + n + 2 = 1$  then  $3k = -n - 1 < 0$ , which is not possible since  $k > 0$ .

Therefore  $p$  admits a non-trivial factorization. Which is a contradiction.

### Sample solutions to Exercise 20.

Compare with Wilson's theorem from Chapter 4.

We are going to prove the contrapositive:  $\forall n \in \mathbb{N}$ ,  $n$  is not prime  $\implies n \nmid (n-1)! + 1$ .

Let  $n \in \mathbb{N}$ . Assume that  $n$  is not prime. Then there exists  $k \in \mathbb{N}$  such that  $1 < k < n$  and  $k \mid n$ .

Assume by contradiction that  $n \mid (n-1)! + 1$ . Then  $k \mid (n-1)! + 1$ . But  $k \mid (n-1)!$  since  $1 < k < n$ .

Thus  $k \mid (n-1)! + 1 - (n-1)! = 1$ . Which is a contradiction.

Therefore  $n \nmid (n-1)! + 1$ .

### Sample solutions to Exercise 21.

Let  $n \in \mathbb{N} \setminus \{0\}$ . Consider the following  $n$  consecutive natural numbers

$$(n+1)! + 2, (n+1)! + 3, (n+1)! + 4, \dots, (n+1)! + (n+1)$$

Take  $(n+1)! + k$  in the previous list (i.e.  $k = 2, \dots, (n+1)$ ). Then  $k \mid (n+1)! + k$  but  $1 < k < (n+1)! + k$ .

Therefore  $(n+1)! + k$  has a non-trivial divisor.

### Sample solutions to Exercise 22.

- Assume by contradiction that  $\log_{10} 2 = \frac{a}{b} \in \mathbb{Q}$ . Then

$$\frac{\log 2}{\log 10} = \frac{a}{b} \Leftrightarrow b \log 2 = a \log 10 \Leftrightarrow \log(2^a) = \log(10^b) \Leftrightarrow 2^a = 10^b \Leftrightarrow 2^a = 2^b 5^b$$

By uniqueness of the prime factorization,  $a = b = 0$ . Contradiction.

2. Assume by contradiction that  $\sqrt{2} = \frac{a}{b} \in \mathbb{Q}$ . Then  $2b^2 = a^2$ .

The prime factorization of the LHS has an odd number of primes (counted with exponents) whereas the RHS has an even number of primes (counted with exponents). Which is impossible since the prime factorization is unique up to order.

### Sample solutions to Exercise 23.

Assume by contradiction that  $49|n^3 - n^2 - 2n + 1$  for some  $n \in \mathbb{Z}$ .

Note that  $n^3 - n^2 - 2n + 1 = (n+2)^3 - 7n^2 - 14n - 7$ .

Since  $7|49|n^3 - n^2 - 2n + 1$  and  $7|7n^2 + 14n + 7$  then  $7|(n^3 - n^2 - 2n + 1) + 7n^2 + 14n + 7 = (n+2)^3$ .

By Euclid's lemma, since 7 is prime,  $7|(n+2)^2$  and similarly  $7|n+2$ .

Therefore, there exists  $k \in \mathbb{Z}$  such that  $n = 7k - 2$ .

Then  $n^3 - n^2 - 2n + 1 = 49(7k^3 - 7k^2 + 2k) - 7$ .

Therefore  $49|49(7k^3 - 7k^2 + 2k) - (n^3 - n^2 - 2n + 1) = 7$ . Which is a contradiction.

### Sample solutions to Exercise 24.

*It is a special case of Dirichlet's theorem on arithmetic progressions.*

Assume that there are only finitely many primes  $3 = p_1 < p_2 < \dots < p_r$  such that  $p_m = 4k_m + 3$  with  $k_m \in \mathbb{R}$ .

Set  $n = 4p_1p_2 \dots p_r - 1$ . Then  $n = 4(p_1p_2 \dots p_r - 1) + 3$

Write  $n = \prod_{i=1}^s q_i$  as a product of prime numbers.

Note that each  $q_i$  is not one of the  $p_m$  nor 2 (otherwise  $q_i|1$  or  $2|1$ ).

Therefore  $q_i = 4r_i + 1$  (the only possible remainder is 1).

Hence  $n = \prod_{i=1}^s (4r_i + 1) = 4\alpha + 1$  for some  $\alpha \in \mathbb{N}$ .

We obtain a contradiction with the uniqueness of the Euclidean division (the remainder of the Euclidean division of  $n$  by 4 can't be 3 and 1).

### Sample solutions to Exercise 25.

1. Let  $n \in \mathbb{N}$ . We are going to prove by induction on  $k \geq 1$  that

$$\forall k \in \mathbb{N} \setminus \{0\}, 2^{2^{n+k}} - 1 = (2^{2^n} - 1) \times \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1)$$

$$\text{Base case at } k = 1: (2^{2^n} - 1) \times \prod_{i=0}^0 (2^{2^{n+i}} + 1) = (2^{2^n} - 1) \times (2^{2^n} + 1) = (2^{2^n})^2 - 1^2 = 2^{2^{n+1}} - 1.$$

$$\text{Induction step. Assume that } 2^{2^{n+k}} - 1 = (2^{2^n} - 1) \times \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1) \text{ holds for some } k \geq 1. \text{ Then}$$

$$\begin{aligned} (2^{2^n} - 1) \times \prod_{i=0}^{(k+1)-1} (2^{2^{n+i}} + 1) &= (2^{2^n} - 1) \times \prod_{i=0}^k (2^{2^{n+i}} + 1) \\ &= (2^{2^n} - 1) \times \left( \prod_{i=0}^{k-1} (2^{2^{n+i}} + 1) \right) \times (2^{2^{n+k}} + 1) \\ &= (2^{2^{n+k}} - 1) \times (2^{2^{n+k}} + 1) \quad \text{by the induction hypothesis} \\ &= \left( (2^{2^{n+k}})^2 - 1^2 \right) \\ &= (2^{2^{n+k+1}} - 1) \end{aligned}$$

Which ends the induction step.

2. We may assume without loss of generality that  $n < m$ , i.e.  $m = n + k$  for some  $k \in \mathbb{N} \setminus \{0\}$ .

Write  $F_i = 2^{2^i} + 1$  then from the first question we get that

$$F_m + 2 = (2^{2^n} - 1) \times \prod_{i=0}^{k-1} F_{n+i}$$

Let  $g = \gcd(F_m, F_n)$ . Then  $d$  divides  $F_m$  and  $F_n$  thus  $d$  divides  $2 = (2^{2^n} - 1) \times \left(\prod_{i=0}^{k-1} F_{n+i}\right) - F_m$ .

So either  $d = 2$  or  $d = 1$ . Since  $F_m$  is even, we get that  $d = 1$ .

Therefore  $\gcd(F_m, F_n) = 1$ .

### Sample solutions to Exercise 26.

1. Assume that  $a^n - 1$  is prime.

Note that  $a^n - 1 = (a - 1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ .

Since  $a^n - 1$  is prime, then it has no trivial divisor, therefore either  $a - 1 = 1$  or  $a - 1 = a^n - 1$ .

The latter is not possible since  $a, n \geq 2$ , thus  $a - 1 = 1$ , i.e.  $a = 2$ .

Assume that  $n = pq$  with  $p, q \in \mathbb{N}$ . Then  $2^n - 1 = 2^{pq} - 1 = (2^p - 1)((2^p)^{q-1} + (2^p)^{q-2} + \cdots + 2^p + 1)$ .

Since  $2^n - 1$  is a prime number, then either  $2^p - 1 = 1$  or  $2^p - 1 = 2^{pq} - 1$ .

In the first case  $p = 1$  and in the other case  $p = pq = n$ .

Hence the only positive divisors of  $n$  are 1 and itself, i.e.  $n$  is a prime number.

2. No,  $2^{11} - 1 = 2047 = 23 \times 89$ .

### Sample solutions to Exercise 27.

Since  $1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$  must be divisible by 3, either  $3|n$  or  $3|n+1$ . It is easy to check that this necessary condition is also sufficient when  $n > 3$ .

### Sample solutions to Exercise 28.

Note that  $69 = 3 \times 23$ ,  $1150 = 2 \times 5^2 \times 23$  and  $4140 = 2^2 \times 3^2 \times 5 \times 23$ . Note that only positive common divisors are 1 and 23. Assuming the pirate is not alone, the treasure is shared between 23 people so there are 22 sailors.



### 8.3 Chapter 3

#### Sample solutions to Exercise 1.

1. Note that  $2^2 = 4 \equiv -1 \pmod{5}$  and that  $3^2 = 9 \equiv -1 \pmod{5}$ . Therefore, for  $n \in \mathbb{N}$ , we have  
 $2^{2n+1} + 3^{2n+1} = (2^2)^n \times 2 + (3^2)^n \times 3 \equiv (-1)^n \times 2 + (-1)^n \times 3 \pmod{5} \equiv (-1)^n \times 5 \pmod{5} \equiv 0 \pmod{5}$ .
2. Let  $n \in \mathbb{N}$ , then  
 $2^{7n+1} + 3^{2n+1} + 5^{10n+1} + 7^{6n+1} \equiv 9^n \times 2 + 9^n \times 3 + 9^n \times 5 + 9^n \times 7 \pmod{17} \equiv 9^n \times 17 \pmod{17} \equiv 0 \pmod{17}$

#### Sample solutions to Exercise 2.

We first compute  $x^2 + 3 \pmod{7}$  in terms of  $x \pmod{7}$ :

$x \pmod{7}$	0	1	2	3	4	5	6
$x^2 \pmod{7}$	0	1	4	2	2	4	1
$x^2 + 3 \pmod{7}$	3	4	0	5	5	0	4

Let  $x \in \mathbb{Z}$ . Then  $x^2 + 3 \equiv 0 \pmod{7}$  if and only if  $x \equiv 2 \pmod{7}$  or  $x \equiv 5 \pmod{7}$   
if and only if  $x \in \{2 + 7k : k \in \mathbb{Z}\} \cup \{5 + 7k : k \in \mathbb{Z}\}$ .

#### Sample solutions to Exercise 3.

1. We first look for the least  $k \in \mathbb{N} \setminus \{0\}$  such that  $2^k \equiv 1 \pmod{5}$ :

- $2^1 \equiv 2 \pmod{5}$
- $2^2 \equiv 4 \pmod{5}$
- $2^3 \equiv 3 \pmod{5}$
- $2^4 \equiv 1 \pmod{5}$

Hence it is 4.

We perform the Euclidean division of  $n \in \mathbb{N}$  by 4:  $n = 4q + r$  where  $0 \leq r < 4$ .

Then  $2^n = 2^{4q+r} = (2^4)^q 2^r \equiv 1^q 2^r \pmod{5} \equiv 2^r \pmod{5}$ .

Thus

- If  $n \equiv 0 \pmod{4}$  then  $2^n \equiv 2^0 \pmod{5} \equiv 1 \pmod{5}$ , so the remainder is 1.
- If  $n \equiv 1 \pmod{4}$  then  $2^n \equiv 2^1 \pmod{5} \equiv 2 \pmod{5}$ , so the remainder is 2.
- If  $n \equiv 2 \pmod{4}$  then  $2^n \equiv 2^2 \pmod{5} \equiv 4 \pmod{5}$ , so the remainder is 4.
- If  $n \equiv 3 \pmod{4}$  then  $2^n \equiv 2^3 \pmod{5} \equiv 3 \pmod{5}$ , so the remainder is 3.

2. Note that  $1357 = 1355 + 2 \equiv 2 \pmod{5}$ . Therefore  $1357^{2021} \equiv 2^{2021} \pmod{5}$ .

Since  $2021 = 505 \times 4 + 1 \equiv 1 \pmod{4}$  we get that the remainder of  $1357^{2021}$  by 5 is 2.

#### Sample solutions to Exercise 4.

1. Note that  $10 \equiv 0 \pmod{5}$ , hence

$$\begin{aligned}
 5 \mid \overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{5} \\
 &\Leftrightarrow \sum_{k=0}^r a_k 10^k \equiv 0 \pmod{5} \\
 &\Leftrightarrow a_0 \equiv 0 \pmod{5}
 \end{aligned}$$

Therefore  $5 \mid \overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $a_0 = 0$  or  $a_0 = 5$ .

2. Note that  $10^3 = 175 \times 8 \equiv 0 \pmod{8}$ , hence

$$\begin{aligned} 8 \mid \overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{8} \\ &\Leftrightarrow \sum_{k=0}^r a_k 10^k \equiv 0 \pmod{8} \\ &\Leftrightarrow 10^2 a_2 + 10 a_1 + a_0 \equiv 0 \pmod{8} \\ &\Leftrightarrow 4 a_2 + 2 a_1 + a_0 \equiv 0 \pmod{8} \end{aligned}$$

Therefore  $8 \mid \overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $8 \mid (4a_2 + 2a_1 + a_0)$ .

Note that  $8 \mid 958547$  if and only if  $8 \mid 4 \times 5 + 2 \times 4 + 7 = 35 = 8 \times 4 + 3$ . Therefore  $8 \nmid 958547$ .

Note that  $8 \mid 123456789336$  if and only if  $8 \mid 4 \times 3 + 2 \times 3 + 6 = 24 = 8 \times 3$ . Therefore  $8 \mid 123456789336$ .

3. Note that  $10 \equiv -1 \pmod{11}$ , hence

$$\begin{aligned} 11 \mid \overline{a_r a_{r-1} \dots a_0}^{10} &\Leftrightarrow \overline{a_r a_{r-1} \dots a_0}^{10} \equiv 0 \pmod{11} \\ &\Leftrightarrow \sum_{k=0}^r a_k 10^k \equiv 0 \pmod{11} \\ &\Leftrightarrow \sum_{k=0}^r (-1)^k a_k \equiv 0 \pmod{11} \end{aligned}$$

Therefore  $11 \mid \overline{a_r a_{r-1} \dots a_0}^{10}$  if and only if  $11 \mid (-1)^r a_r + (-1)^{r-1} a_{r-1} + \dots + a_2 - a_1 + a_0$ .

Note that  $11 \mid 123456789$  if and only if  $11 \mid 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 = 5$ . Therefore  $11 \nmid 123456789$ .

Note that  $11 \mid 715$  if and only if  $11 \mid 5 - 1 + 7 = 11$ . Therefore  $11 \mid 715$ .

### Sample solutions to Exercise 5.

1. If  $(x, y) \in \mathbb{Z}^2$  is a solution then  $x^2 \equiv 3 \pmod{5}$ . But

- if  $x \equiv 0 \pmod{5}$  then  $x^2 \equiv 0 \pmod{5}$ ,
- if  $x \equiv \pm 1 \pmod{5}$  then  $x^2 \equiv 1 \pmod{5}$ ,
- if  $x \equiv \pm 2 \pmod{5}$  then  $x^2 \equiv 4 \pmod{5}$ .

Thus the equation has no integer solution.

2. Assume that  $(x, y) \in \mathbb{Z}^2$  is a solution, then taking congruences modulo 3, the equation becomes

$$0x^2 - (-1)y^2 \equiv 0 \pmod{3}$$

i.e.  $y^2 \equiv 0 \pmod{3}$ .

$y \pmod{3}$	0	1	2
$y^2 \pmod{3}$	0	1	1

Therefore  $y \equiv 0 \pmod{3}$ , i.e.  $y = 3k$  for some  $k \in \mathbb{Z}$ , and the equation becomes  $15x^2 - 63k^2 = 9$ .

Dividing by 3, we get  $5x^2 - 21k^2 = 3$ . Taking congruences modulo 3, we obtain  $-x^2 \equiv 0 \pmod{3}$ .

As above, the only possibility is that  $x \equiv 0 \pmod{3}$ , i.e.  $x = 3l$  for some  $l \in \mathbb{Z}$ .

Then the equation becomes  $45l^2 - 21k^2 = 3$ , and dividing by 3, we get  $15l^2 - 7k^2 = 1$ .

Modulo 3, we finally get  $-k^2 \equiv 1 \pmod{3}$ , i.e.  $k^2 \equiv -1 \pmod{3} \equiv 2 \pmod{3}$ .

Which is impossible (a square modulo 3 is either congruent to 0 or 1, according to the above array).

Thus the equation has no integer solution.

3. Below are the possible values for  $x^2 \pmod{4}$  depending on  $x \pmod{4}$ .

$x \pmod{4}$	0	1	2	3
$x^2 \pmod{4}$	0	1	0	1

Therefore either  $x^2 \equiv 0 \pmod{4}$  or  $x^2 \equiv 1 \pmod{4}$  and similarly either  $y^2 \equiv 0 \pmod{4}$  or  $y^2 \equiv 1 \pmod{4}$ . Thus either  $x^2 + y^2 \equiv 0 \pmod{4}$ , or  $x^2 + y^2 \equiv 1 \pmod{4}$ , or  $x^2 + y^2 \equiv 2 \pmod{4}$ .

Since  $4003 = 4 \times 1000 + 3 \equiv 3 \pmod{4}$ , there is no integer solutions.

### Sample solutions to Exercise 6.

Note that  $3^3 \equiv 1 \pmod{13}$ . Since  $126 = 3 \times 42$ , we get  $3^{126} \equiv (3^3)^{42} \pmod{13} \equiv 1^{42} \pmod{13} \equiv 1 \pmod{13}$ .

Note that  $5^4 \equiv 1 \pmod{13}$ . Since  $126 = 4 \times 31 + 2$ , we get  $5^{126} \equiv (5^4)^{31} \times 5^2 \pmod{13} \equiv 1^{31} \times 25 \pmod{13} \equiv -1 \pmod{13}$ .

Therefore  $3^{126} + 5^{126} \equiv 0 \pmod{13}$ .

### Sample solutions to Exercise 7.

1. Let  $n \in \mathbb{N}$ .

- If  $n$  is even, i.e.  $n = 2k$ , then  $3^n + 4n + 1 = 9^k + 8k + 1 \equiv 1^k + 0 + 1 \pmod{8} \equiv 2 \pmod{8}$ .
- If  $n$  is odd, i.e.  $n = 2k + 1$ , then  $3^n + 4n + 1 = 9^k \times 3 + 8k + 4 + 1 \equiv 1^k \times 3 + 0 + 4 + 1 \pmod{8} \equiv 0 \pmod{8}$ .

Therefore  $8 \mid 3^n + 4n + 1$  if and only if  $n$  is odd.

2. Let  $n \in \mathbb{N}$ . Note that  $2^6 = 64 = 21 \times 3 + 1 \equiv 1 \pmod{21}$ .

Therefore, if  $n = 6q + r$  with  $0 \leq r < 6$ , we have that  $2^n = (2^6)^q \times 2^r \equiv 2^r \pmod{21}$ .

Thus  $2^n \pmod{21}$  depends only on  $n \pmod{6}$ . Let's study the cases separately.

$n \pmod{6}$	0	1	2	3	4	5
$2^n \pmod{21}$	1	2	4	8	16	11
$2^{2^n} \pmod{21}$	2	4	-5	4	16	-10
$2^{2^n} + 2^n + 1 \pmod{21}$	4	7	0	13	12	2

Therefore  $21 \mid 2^{2^n} + 2^n + 1$  if and only if  $n \equiv 2 \pmod{6}$ .

### Sample solutions to Exercise 8.

1. For  $a, b \in \mathbb{Z}$ , we compute  $a^2 + b^2 \pmod{3}$  depending on  $a \pmod{3}$  and  $b \pmod{3}$ :

$a \pmod{3} \backslash b \pmod{3}$	0	1	2
0	0	1	1
1	1	2	2
2	1	2	2

We see that  $a^2 + b^2 \equiv 0 \pmod{3}$  if and only if  $a \equiv 0 \pmod{3}$  and  $b \equiv 0 \pmod{3}$ .

2. Same as above.

3. Let  $a, b \in \mathbb{Z}$ . Assume that  $21 \mid a^2 + b^2$ . Then  $3 \mid a^2 + b^2$ , thus  $3 \mid a$  and  $3 \mid b$  from the first question. Similarly  $7 \mid a$  and  $7 \mid b$  from the second question.

Therefore the least common divisor of 3 and 7 divides  $a$  and  $b$ , i.e.  $21 \mid a$  and  $21 \mid b$ .

Hence  $a = 21k$  and  $b = 21l$ , so  $a^2 + b^2 = 441(k^2 + l^2)$ .

**Sample solutions to Exercise 9.**

Note that  $2^4 \equiv 1 \pmod{15}$ . Since  $445 = 4 \times 111 + 1$  we get

$$2^{445} + 7 = (2^4)^{111} \times 2 + 7 \equiv 1^{111} \times 2 + 7 \pmod{15} \equiv 9 \pmod{15}$$

Therefore, there exists  $k \in \mathbb{Z}$  such that  $2^{445} + 7 = 15k + 9$ .

Finally  $\gcd(2^{445} + 7, 15) = \gcd(15k + 9, 15) = \gcd(9, 15) = 3$ .

**Sample solutions to Exercise 10.**

Note that 2 doesn't work and that 3 works.

Assume that  $p$  is a prime number greater than 3, then

$$2^p + p^2 \equiv (-1)^p + (\pm 1)^2 \pmod{3} \equiv -1 + 1 \pmod{3} \equiv 0 \pmod{3}$$

so  $3 \mid 2^p + p^2$  and thus  $2^p + p^2$  is not prime.

The only prime number  $p$  such that  $2^p + p^2$  is also prime is  $p = 3$ .

**Sample solutions to Exercise 11.**

Note that  $7^2 \equiv -1 \pmod{10}$  so  $7^4 \equiv 1 \pmod{10}$ .

Therefore if  $n = 4q + r$  with  $0 \leq r < 4$ , we get that  $7^n = (7^4)^q \times 7^r \equiv 1^q \times 7^r \pmod{10} \equiv 7^r \pmod{10}$ .

Hence it is enough to compute  $3^{8^4} \pmod{4}$ . Note that  $3^2 = 9 \equiv 1 \pmod{4}$ , therefore

$$3^{8^4} = 3^{8^3 \times 8} = (3^2)^{8^3 \times 4} \equiv 1^{8^3 \times 4} \pmod{4} \equiv 1 \pmod{4}$$

and  $3^{8^4} = 4q + 1$  for some  $q \in \mathbb{N}$ . Therefore  $7^{3^{8^4}} = 7^{4q+1} \equiv 7 \pmod{10}$ . So the last digit in the decimal expansion of  $7^{3^{8^4}}$  is 7.

**Sample solutions to Exercise 12.**

$$1. \quad 57 \times 60^3 + 42 \times 60^2 + 3 \times 60 + 11 \times 1 = 12463391$$

2. We perform successive Euclidean division by 60:

$$\begin{aligned} 42137 &= 702 \times 60 + 17 \\ &= (11 \times 60 + 42) \times 60 + 17 \\ &= 11 \times 60^2 + 42 \times 60 + 17 \\ &= 42 \times 60 + 17 \end{aligned}$$

$$3. \quad \overline{F42C}^{16} = 15 \times 16^4 + 4 \times 16^3 + 2 \times 16^2 + 0 \times 16 + 12 = 999948$$

4. We perform successive Euclidean division by 16:

$$\begin{aligned} 11211 &= 700 \times 16 + 11 \\ &= (43 \times 16 + 12) \times 16 + 11 \\ &= ((2 \times 16 + 11) \times 16 + 12) \times 16 + 11 \\ &= 2 \times 16^3 + 11 \times 16^2 + 12 \times 16 + 11 \\ &= \overline{2BCB}^{16} \end{aligned}$$

$$\begin{array}{r} \overset{1}{9} \overset{1}{AB} 7 \\ + 3CD \\ \hline = D6C4 \end{array}$$

$$\begin{aligned}
6. \quad \overline{9AB7}^{16} &= 9 \times 16^3 + 10 \times 16^2 + 11 \times 16 + 7 = 39607 \\
\overline{3C0D}^{16} &= 3 \times 16^3 + 12 \times 16^2 + 0 \times 16 + 13 = 15373 \\
39607 + 15373 &= 54980 \\
58820 &= 3436 \times 16 + 4 = (214 \times 16 + 12) \times 16 + 4 = ((13 \times 16 + 6) \times 16 + 12) \times 16 + 4 = 13 \times 16^3 + 6 \times 16^2 + 12 \times 16 + 4 \\
\text{Therefore } \overline{9AB7}^{16} + \overline{3C0D}^{16} &= \overline{D6C4}^{16} \text{ I think it is easier to directly compute in base 16!}
\end{aligned}$$

### Sample solutions to Exercise 13.

Let's denote the number of blue, green, and red chameleons respectively by  $b$ ,  $g$  and  $r$ .

- If a blue and a green chameleons meet, the new repartition becomes  $b' = b - 1$ ,  $g' = g - 1$  and  $r' = r + 2$ .  
Therefore  $b' - g' = b - g$ ,  $b' - r' = b - r - 3$  and  $g' - r' = g - r - 3$ .
- Similarly, if a blue and a red chameleons meet, we have  $b' = b - 1$ ,  $g' = g + 2$  and  $r' = r - 1$ .  
Therefore  $b' - g' = b - g - 3$ ,  $b' - r' = b - r$  and  $g' - r' = g - r + 3$ .
- Finally, if a green and a red chameleons meet, we have  $b' = b + 2$ ,  $g' = g - 1$  and  $r' = r - 1$ .  
Therefore  $b' - g' = b - g + 3$ ,  $b' - r' = b - r + 3$  and  $g' - r' = g - r$ .

Note that in all the cases we have

$$b' - g' \equiv b - g \pmod{3} \quad b' - r' \equiv b - r \pmod{3} \quad g' - r' \equiv g - r \pmod{3}$$

Therefore these three quantities modulo 3 don't change when the chameleons meet, they always stay constant, mathematically we say that they are invariant.

At the beginning, we have

$$b - g \equiv 2 \pmod{3} \quad b - r \equiv 1 \pmod{3} \quad g - r \equiv 2 \pmod{3}$$

Assume by contradiction that all the chameleons become blue after several meetings (i.e.  $b = 45$ ,  $g = 0$  and  $r = 0$ ), then

$$b - g \equiv 0 \pmod{3} \quad b - r \equiv 0 \pmod{3} \quad g - r \equiv 0 \pmod{3}$$

Since these quantities don't change when chameleons meet, we obtain a contradiction. Therefore, it is not possible to obtain an island with only blue chameleons from the initial situation.

We conclude similarly for the other colors. Thus, it is not possible to obtain a monochromatic island!

## 8.4 Chapter 4

### Sample solutions to Exercise 1.

By Fermat's little theorem, we know that  $24^{103} \equiv 24 \pmod{103}$ .

Therefore the remainder of the Euclidean division of  $24^{103}$  by 103 is 24.

### Sample solutions to Exercise 2.

Let  $n \in \mathbb{Z}$ . Set  $A_n = 5n^7 + 7n^5 + 23n$ .

By Fermat's little theorem,  $n^5 \equiv n \pmod{5}$  so  $A_n \equiv 30n \pmod{5} \equiv 0 \pmod{5}$ , i.e.  $5|A_n$ .

Similarly  $n^7 \equiv n \pmod{7}$ , so  $A_n \equiv 28n \pmod{7} \equiv 0 \pmod{7}$ , i.e.  $7|A_n$ .

Therefore  $35 = 5 \times 7|A_n$ , so  $\frac{n^7}{7} + \frac{n^5}{5} + \frac{23n}{35} = \frac{A_n}{35} \in \mathbb{Z}$ .

### Sample solutions to Exercise 3.

Let  $p$  be an odd prime number and  $n \in \mathbb{Z}$ .

- By Fermat's little theorem,  $\begin{cases} (n+1)^p \equiv n+1 \pmod{p} \\ n^p \equiv n \pmod{p} \end{cases}$   
Therefore  $(n+1)^p - (n^p + 1) \equiv 0 \pmod{p}$ , i.e.  $p|(n+1)^p - (n^p + 1)$ .
- Note that  $\forall x \in \mathbb{Z}, \forall k \in \mathbb{N} \setminus \{0\}, x^k \equiv x \pmod{2}$ :

$a \pmod{2}$	0	1
$a^2 \pmod{2}$	0	1

Therefore  $\begin{cases} (n+1)^p \equiv n+1 \pmod{2} \\ n^p \equiv n \pmod{2} \end{cases}$ .

Thus  $(n+1)^p - (n^p + 1) \equiv 0 \pmod{2}$ , i.e.  $2|(n+1)^p - (n^p + 1)$ .

Since 2 and  $p$  are two distinct prime numbers,  $2p|(n+1)^p - (n^p + 1)$ , i.e.  $(n+1)^p - (n^p + 1) \equiv 0 \pmod{2p}$ .

### Sample solutions to Exercise 4.

We are going to prove the statement by induction on  $k \in \mathbb{N}$ .

- *Base case at  $k = 0$ :* it is exactly Fermat's little theorem (v2).
- *Induction step:* assume that the statement hold for some  $k \in \mathbb{N}$ , i.e.

$$\forall n \in \mathbb{Z} \setminus \{0\}, \gcd(n, p) = 1 \implies (n^{p-1})^{p^k} \equiv 1 \pmod{p^{k+1}}$$

Let  $n \in \mathbb{Z}$  be such that  $\gcd(n, p) = 1$ .

By induction hypothesis, there exists  $\lambda \in \mathbb{Z}$  such that  $(n^{p-1})^{p^k} = 1 + \lambda p^{k+1}$ . Then

$$(n^{p-1})^{p^{k+1}} = (n^{p-1})^{p^k \times p} = \left( (n^{p-1})^{p^k} \right)^p = (1 + \lambda p^{k+1})^p = \sum_{i=0}^p \binom{p}{i} \lambda^i p^{i(k+1)} = 1 + \sum_{i=1}^p \binom{p}{i} \lambda^i p^{i(k+1)} \equiv 1 \pmod{p^{k+1}}$$

Which ends the induction step.

### Sample solutions to Exercise 5.

Let  $p$  and  $q$  be two distinct prime numbers.

Since  $\gcd(p, q) = 1$ , by Fermat's little theorem we get that  $p^{q-1} \equiv 1 \pmod{q}$ .

Besides  $q^{p-1} \equiv 0 \pmod{q}$  (since  $p \geq 2$ ).

Therefore  $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$ , i.e.  $p|(p^{q-1} + q^{p-1} - 1)$ .

Similarly, we may prove that  $q|(p^{q-1} + q^{p-1} - 1)$ .

Thus  $pq|(p^{q-1} + q^{p-1} - 1)$ .

**Sample solutions to Exercise 6.**

Let  $x, y \in \mathbb{Z}$ .

By Fermat's little theorem,  $x^4 \equiv 1 \pmod{5}$  (if  $5 \nmid x$ ) or  $x^4 \equiv 0 \pmod{5}$  (if  $5 \mid x$ ).

Therefore  $x^4 + 781 \equiv 1 \pmod{5}$  or  $x^4 + 781 \equiv 2 \pmod{5}$ .

But  $3y^4 \equiv 3 \pmod{5}$  (if  $5 \nmid y$ ) or  $3y^4 \equiv 0 \pmod{5}$  (if  $5 \mid y$ ).

Therefore  $\forall x, y \in \mathbb{Z}$ ,  $x^4 + 781 \not\equiv 3y^4 \pmod{5}$ .

**Sample solutions to Exercise 7.**

Let  $n \geq 5$  be such that  $n + 2$  is prime.

By Wilson's theorem  $(n + 1)! \equiv -1 \pmod{n + 2}$ . Thus  $n + 2 \mid (n + 1)! + 1$ .

Besides  $(n + 1)! + 1 = (n + 2)n! - n! + 1$ .

Thus  $n + 2 \mid n! - 1 = (n + 2)n! - ((n + 1)! + 1)$ .

Since  $n \geq 4$ , we have  $n! > n + 3$  (prove it).

Therefore  $n! - 1$  admits at least three positive divisors:  $1, n + 2, n! - 1$ , so that  $n$  is composite.

**Sample solutions to Exercise 8.**

Let  $p$  be an odd prime number.

By Wilson's theorem  $(p - 1)! \equiv -1 \pmod{p}$ , thus  $2(p - 3)!(p - 2)(p - 1) \equiv -2 \pmod{p}$ .

But we also have that  $2(p - 3)!(p - 2)(p - 1) \equiv 4(p - 3)! \pmod{p}$ .

Thus  $4(p - 3)! \equiv -2 \pmod{p}$ , i.e.  $p \mid 4(p - 3)! + 2 = 2(2(p - 3)! + 1)$ .

Since  $\gcd(2, p) = 1$  (as  $p$  is an odd prime number), by Gauss' lemma we get  $p \mid 2(p - 3)! + 1$ , i.e.  $2(p - 3)! \equiv -1 \pmod{p}$ .

**Sample solutions to Exercise 9.**

$\Rightarrow$  Assume that  $n$  and  $n + 2$  are both prime then,

- By Wilson's theorem,  $(n - 1)! \equiv -1 \pmod{n}$ , so  $4((n - 1)! + 1) + n \equiv 0 \pmod{n}$ , i.e.  $n \mid 4((n - 1)! + 1) + n$ .
- By Wilson's theorem,  $(n + 1)! \equiv -1 \pmod{n + 2}$ .  
Besides  $2 \equiv -n \pmod{n + 2} \equiv (n + 1)n \pmod{n + 2}$ .  
Thus  
 $4((n - 1)! + 1) + n = 2(2(n - 1)! + 1) + 4 + n \equiv 2((n + 1)n(n - 1)! + 2) \pmod{n + 2} \equiv 2((n + 1)! + 1) \equiv 0 \pmod{n + 2}$   
i.e.  $n + 2 \mid 4((n - 1)! + 1) + n$ .

Since  $\gcd(n, n + 2) = 1$ , we get that  $n(n + 2) \mid 4((n - 1)! + 1) + n$ .

**Sample solutions to Exercise 10.**

Let  $p$  be a prime number. Let  $n \in \mathbb{Z}$ .

By Fermat's little theorem  $n^p \equiv n \pmod{p}$  and by Wilson's theorem  $(p - 1)! \equiv -1 \pmod{p}$ .

Therefore  $n^p + (p - 1)!n \equiv n + (-1)n \pmod{p} \equiv 0 \pmod{p}$ .

**Sample solutions to Exercise 11.**

This property is false:  $\varphi(2 \times 2) = 2^2 - 2 = 2$  but  $\varphi(2)\varphi(2) = 1 \times 1$ .

**Sample solutions to Exercise 12.**

$$1 + 2 + 2^2 + 2^3 + \dots + 2^{100} = \sum_{k=0}^{100} 2^k = \frac{1 - 2^{101}}{1 - 2} = 2^{101} - 1 \text{ (geometric sum, Cherge's favorite formula).}$$

Note that  $\varphi(125) = \varphi(5^3) = 5^3 - 5^2 = 100$ .

Therefore, since  $\gcd(2, 101) = 1$ , Euler's theorem gives

$$2^{101} - 1 = 2 \times 2^{100} - 1 \equiv 2 \times 1 - 1 \pmod{125} \equiv 1 \pmod{125}$$

Hence the remainder of the Euclidean division of  $1 + 2 + 2^2 + 2^3 + \dots + 2^{100}$  by 125 is 1.

**Sample solutions to Exercise 13.**

Note that  $\varphi(1000) = \varphi(2^3 5^3) = (2^3 - 2^2)(5^3 - 5^2) = 400$ .

Therefore, since  $\gcd(1000, 3) = 1$ , Euler's theorem gives

$$\begin{aligned} 3^{2021} &= 3^{5 \times 400 + 21} = (3^{400})^5 3^{21} \equiv 1^5 \times 3^{21} \pmod{1000} \\ &\equiv 3^{10} 3^{10} 3 \pmod{1000} \\ &\equiv 59049 \times 59049 \times 3 \pmod{1000} \\ &\equiv 49 \times 49 \times 3 \pmod{1000} \\ &\equiv 7203 \pmod{1000} \\ &\equiv 203 \pmod{1000} \end{aligned}$$

Thus the last 3 digits of  $3^{2021}$  are 203.

**Sample solutions to Exercise 14.**

Let  $n, k \in \mathbb{N} \setminus \{0\}$ .

Write the prime factorization  $n = \prod_{i=1}^r p_i^{\alpha_i}$  where the  $p_i$  are pairwise distinct prime numbers and  $\alpha_i \in \mathbb{N} \setminus \{0\}$ .

$$\text{Then } n^k = \prod_{i=1}^r p_i^{k\alpha_i} \text{ and } \varphi(n^k) = \prod_{i=1}^r (p_i^{k\alpha_i} - p_i^{k\alpha_i-1}) = \prod_{i=1}^r p_i^{(k-1)\alpha_i} \prod_{i=1}^r (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = n^{k-1} \varphi(n).$$

**Sample solutions to Exercise 15.**

Let  $a, b \in \mathbb{N} \setminus \{0\}$ . Assume that  $\gcd(a, b) = 1$ .

Since  $\gcd(a, b) = 1$ , by Euler's theorem  $a^{\varphi(b)} \equiv 1 \pmod{b}$ .

Since  $\varphi(a) \geq 1$ ,  $b^{\varphi(a)} \equiv 0 \pmod{b}$ .

Thus  $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{b}$ , i.e.  $b | a^{\varphi(b)} + b^{\varphi(a)} - 1$ .

Swapping  $a$  and  $b$ , we get similarly that  $a | a^{\varphi(b)} + b^{\varphi(a)} - 1$ .

Since  $\gcd(a, b) = 1$ , we derive from Exercise 1 that  $ab | a^{\varphi(b)} + b^{\varphi(a)} - 1$ , i.e.  $a^{\varphi(b)} + b^{\varphi(a)} \equiv 1 \pmod{ab}$ .

**Sample solutions to Exercise 16.**

Let  $a \in \mathbb{Z}$  and  $n \in \mathbb{N} \setminus \{0\}$ . Assume that  $\gcd(a, n) = \gcd(a-1, n) = 1$ .

Since  $\gcd(a, b) = 1$ , by Euler's theorem we get

$$(a-1) \sum_{k=0}^{\varphi(n)-1} a^k = a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

$$\text{So } n | (a-1) \sum_{k=0}^{\varphi(n)-1} a^k.$$

By Gauss' lemma, since  $\gcd(n, a-1) = 1$ , we get that  $n | \sum_{k=0}^{\varphi(n)-1} a^k$ , i.e.  $\sum_{k=0}^{\varphi(n)-1} a^k \equiv 0 \pmod{n}$ .

**Sample solutions to Exercise 17.**

Let  $a \in \mathbb{N} \setminus \{0, 1\}$  and  $k \in \mathbb{N} \setminus \{0\}$ .

By Euclidean division, there exist  $q, r \in \mathbb{Z}$  such that  $\varphi(a^k - 1) = kq + r$  and  $0 \leq r < k$ .

Since  $\gcd(a^k - 1, a) = \gcd(-1, a) = 1$ , we deduce from Euler's theorem that  $a^{\varphi(a^k - 1)} \equiv 1 \pmod{a^k - 1}$ .

But  $a^{\varphi(a^k - 1)} = a^{kq+r} = (a^k)^q a^r \equiv 1^q a^r \pmod{a^k - 1} \equiv a^r \pmod{a^k - 1}$ .

Therefore  $a^r \equiv 1 \pmod{a^k - 1}$ , i.e.  $a^k - 1 | a^r - 1$ .

But since  $0 \leq r < k$ , we get that  $0 \leq a^r - 1 < a^k - 1$ .

Thence,  $a^r - 1 = 0$ , i.e.  $r = 0$ .

So  $\varphi(a^k - 1) = kq$ , i.e.  $k | \varphi(a^k - 1)$ .



**Sample solutions to Exercise 18.**

First note that if  $n \in \mathbb{N} \setminus \{0\}$  then 
$$\begin{cases} \varphi(n) \leq n - 1 & \text{if } n \geq 2 \\ \varphi(n) = 1 & \text{if } n = 1 \end{cases}.$$

Therefore  $u_{k+1} = \varphi(u_k) \leq u_k$ , so that the sequence is decreasing.

Since it is bounded from below then it is eventually constant.

Assume by contradiction that  $\forall k \geq N, u_{k+1} = u_k > 1$ , then  $u_{k+1} = \varphi(u_k) \leq u_k - 1 < u_k$ . Which is a contradiction.

Therefore the sequence  $(u_k)_k$  is eventually constant equal to 1.

## 8.5 Chapter 5

### Sample solutions to Exercise 1.

$$\begin{aligned}
 \varphi(n) &= (p-1)(q-1) \\
 \Leftrightarrow \varphi(n) &= pq - p - q + 1 \\
 \Leftrightarrow \varphi(n) &= n - p - \frac{n}{p} + 1 \\
 \Leftrightarrow p\varphi(n) &= pn - p^2 - n + p \\
 \Leftrightarrow p^2 - (n - \varphi(n) + 1)p + n &= 0
 \end{aligned}$$

Therefore  $p$  (and similarly for  $q$ ) is a root of the equation  $X^2 - (n - \varphi(n) + 1)X + n = 0$ .

### Sample solutions to Exercise 2.

Let  $l \in \mathbb{N}$  and  $m \in \mathbb{Z}$ .

- Let's prove that  $m^{1+l\varphi(pq)} \equiv m \pmod{p}$ .
  - If  $p|m$  then both sides are congruent to 0 (mod  $p$ ), therefore  $m^{1+l\varphi(pq)} \equiv m \pmod{p}$ .
  - If  $p \nmid m$  then  $\gcd(m^{q-1}, p) = 1$  (check it), therefore, using Fermat's little theorem, we get that

$$(m^{q-1})^{p-1} \equiv 1 \pmod{p}$$

$$\text{Thus } m^{1+l\varphi(pq)} = m \times m^{l(p-1)(q-1)} = m \times \left( (m^{q-1})^{p-1} \right)^l \equiv m \times 1^l \pmod{p} \equiv m \pmod{p}.$$

- We prove similarly that  $m^{1+l\varphi(pq)} \equiv m \pmod{q}$ .

Therefore  $p|m^{1+l\varphi(pq)} - m$  and  $q|m^{1+l\varphi(pq)} - m$ .

Since  $\gcd(p, q) = 1$ , we deduce from Exercise 1 that  $pq|m^{1+l\varphi(pq)} - m$ , i.e.  $m^{1+l\varphi(pq)} \equiv m \pmod{pq}$ .

### Sample solutions to Exercise 3.

- Here  $\varphi(n) = (61-1)(97-1) = 60 \times 96 = 5760$ .  
 Note that  $5760 = 338 \times 17 + 14$ , so  $\gcd(\varphi(n), e) = \gcd(5760, 17) = \gcd(14, 17) = 1$ .  
 Therefore  $e = 17$  is a suitable choice for  $n = 5917$ .  
 Furthermore  $ed = 17 \times 2033 = 34561 = 6 \times 5760 + 1 \equiv 1 \pmod{\varphi(n)}$ .  
 Therefore  $d$  is a suitable choice for  $e = 17$  and  $n = 5917$ .
- $m^e = 42^{17} \equiv 3838 \pmod{5917}$ , so Bob should send  $c = 3838$  to Alice.  
 Then Alice will perform the computation  $c^d = 3838^{2033} \equiv 42 \pmod{5917}$ .
- $c^d = 3141^{2033} \equiv 4630 \pmod{5917}$ , therefore the original message is 4630.

### Sample solutions to Exercise 4.

Using a computer, it is easy to see that  $1003 = 17 \times 59$ .

Therefore  $\varphi(n) = 16 \times 58 = 928$ . Let's look for a multiplicative inverse of  $e = 11$  modulo  $\varphi(n) = 928$ .

We apply Euclid's algorithm:

$$\begin{aligned}
 928 &= 11 \times 84 + 4 \\
 11 &= 4 \times 2 + 3 \\
 4 &= 3 \times 1 + 1
 \end{aligned}$$

Therefore

$$\begin{aligned}
 1 &= 4 - 3 \\
 &= 4 - (11 - 4 \times 2) \\
 &= 4 \times 3 - 11 \\
 &= (928 - 11 \times 84) \times 3 - 11 \\
 &= 928 \times 3 - 11 \times (84 \times 3 + 1) \\
 1 &= 928 \times 3 + 11 \times (-253)
 \end{aligned}$$

Note that we want  $d > 0$ , so we take  $d = -253 + \varphi(n) = 928 - 253 = 675$ .

Therefore we may decipher the message with the private key  $(n, d) = (1003, 675)$ .

Finally  $c^d = 271^{675} \equiv 951 \pmod{1003}$ . So the original message sent by Bob to Alice is 951.

### Sample solutions to Exercise 5.

Alice keys are  $(n, e)$  and  $(n, d)$ .

She wants to send the message  $m \in \{0, 1, \dots, n-1\}$  to Bob in a way that Bob can authenticate her as the sender.

For this purpose she finds the unique  $s \in \{0, \dots, n-1\}$  such that  $s \equiv m^d \pmod{n}$  (using her *private* key), i.e.  $s$  is the remainder of  $m^d$  by  $n$ .

She sends to Bob both the message  $m$  and the signature  $s$ .

Then Bob checks that  $m \equiv s^e \pmod{n}$ . If so, then Alice was the sender (or at least someone knowing Alice's private key).

## 8.6 Chapter 6

### Sample solutions to Exercise 1.

Set  $\alpha = \sqrt{7+4\sqrt{3}} + \sqrt{7-4\sqrt{3}}$  then

$$\alpha^2 = 14 + 2\sqrt{(7+4\sqrt{3})(7-4\sqrt{3})} = 14 + 2\sqrt{7^2 - 4^2 \times 3} = 14 + 2\sqrt{1} = 16$$

So  $\alpha = \pm 4$ , but since  $\alpha > 0$ , we get  $\alpha = 4$ .

### Sample solutions to Exercise 2.

1. Let  $a, b \in \mathbb{R}$ , then  $0 \leq (a-b)^2 = a^2 + b^2 - 2ab$ , so that  $ab \leq \frac{a^2+b^2}{2}$ .
2. Let  $a, b, c \in \mathbb{R}$ . We know from the previous question that  $ab \leq \frac{a^2+b^2}{2}$ ,  $bc \leq \frac{b^2+c^2}{2}$  and  $ac \leq \frac{a^2+c^2}{2}$ .  
By summing these three inequalities, we get  $ab + bc + ac \leq \frac{a^2+b^2+b^2+c^2+a^2+c^2}{2} = a^2 + b^2 + c^2$ .
3. Let  $a, b, c \in \mathbb{R}$ . Then

$$\begin{aligned} (a+b+c)^2 &= a^2 + b^2 + c^2 + 2ab + 2bc + 2ac \\ &\geq ab + bc + ac + 2ab + 2bc + 2ac \quad \text{from the previous question.} \\ &= 3ac + 3bc + 3ac \end{aligned}$$

### Sample solutions to Exercise 3.

Let  $x \in \mathbb{R}$ .

- First case:  $x \leq 1$  then  $x^2 - x + 1 - |x-1| = x^2 - x + 1 + (x-1) = x^2 \geq 0$ , therefore  $|x-1| \leq x^2 - x + 1$ .
- Second case:  $x > 1$  then  $x^2 - x + 1 - |x-1| = x^2 - x + 1 - (x-1) = x^2 - 2x + 2 = (x-1)^2 + 1 > 0$ , therefore  $|x-1| \leq x^2 - x + 1$ .

### Sample solutions to Exercise 4.

1. Let  $x, y \in \mathbb{R}$ . Then  $2|x| = |2x| = |(x+y) + (x-y)| \leq |x+y| + |x-y|$  and similarly  $2|y| \leq |x+y| + |x-y|$ .  
Summing these two inequalities, we obtain  $2(|x| + |y|) \leq 2(|x+y| + |x-y|)$ .
2. Define  $f : [0, +\infty) \rightarrow \mathbb{R}$  by  $f(u) = \frac{u}{1+u}$  then  $f$  is differentiable and  $f'(u) = \frac{1}{(1+u)^2} > 0$ .  
Therefore  $f$  is increasing.  
Let  $x, y \in \mathbb{R}$ . Since  $|x+y| \leq |x| + |y|$ , we obtain

$$\frac{|x+y|}{1+|x+y|} \leq \frac{|x|+|y|}{1+|x|+|y|} = \frac{|x|}{1+|x|+|y|} + \frac{|y|}{1+|x|+|y|} \leq \frac{|x|}{1+|x|} + \frac{|y|}{1+|y|}$$

### Sample solutions to Exercise 5.

1. Since  $A$  is non-empty, there exists  $x \in A$  and then  $0 = |x-x| \in B$ . Therefore  $B$  is non-empty.  
Since  $A$  is bounded, there exists  $M \in \mathbb{R}$  such that  $\forall x \in A, |x| \leq M$ .  
Therefore, if  $x, y \in A$ , then  $|x-y| \leq |x| + |y| \leq 2M$ . Thus  $2M$  is an upper bound of  $B$ .  
Since  $B$  is a non-empty subset of  $\mathbb{R}$  which is bounded from above, it admits a supremum.
2. Since  $A$  is non-empty and bounded from below, there exists  $m = \inf(A)$ .  
Similarly, since  $A$  is non-empty and bounded from above, there exists  $M = \sup(A)$ .  
Let  $x, y \in A$ , then  $m \leq x \leq M$  and  $-M \leq -y \leq -m$ , thus  $-(M-m) \leq x-y \leq M-m$ , i.e.  $|x-y| \leq M-m$ .  
Thus  $M-m$  is an upper bound of  $B$ . Let's check it is the least one.  
Let  $\varepsilon > 0$ . Since  $m = \inf(A)$ , there exists  $y \in A$  such that  $y \leq m + \frac{\varepsilon}{2}$ . Since  $M = \sup(A)$ , there exists

$x \in A$  such that  $M - \frac{\varepsilon}{2} \leq x$ . Therefore  $|x - y| \geq x - y \geq M - m + \varepsilon$ .

We proved that for every  $\varepsilon > 0$ , there exists  $|x - y| \in B$  such that  $|x - y| \geq M - m + \varepsilon$ .

Therefore  $\sup(B) = M - m$ .

### Sample solutions to Exercise 6.

Set  $E = \{x \in [0, 1] : f(x) \geq x\}$ . Since  $f(0) \in [0, 1]$ , we have that  $f(0) \geq 0$ , so  $0 \in E$ .

Besides  $E$  is bounded from above by 1.

Thence, by the least upper bound principle,  $E$  admits a supremum  $a = \sup(E)$ .

Assume by contradiction that  $f(a) \neq a$ , then

- Either  $f(a) < a$ . Since  $a$  is the least upper bound of  $E$ ,  $f(a)$  is not an upper bound, so there exists  $b \in E$  such that  $f(a) < b \leq a$ .  
But then  $b \leq a$  and  $f(a) < b \leq f(b)$  (since  $b \in E$ ), which is impossible since  $f$  is non-decreasing.
- Or  $f(a) > a$ . Then, since  $f$  is non-decreasing, we get  $f(f(a)) \geq f(a)$ . So  $f(a) \in E$ . Which is impossible since for every  $x \in [0, 1]$ ,  $x \leq a < f(a)$  (since  $a$  is an upper bound).

### Sample solutions to Exercise 7.

Let  $\varepsilon > 0$ . Assume by contradiction that  $(M - \varepsilon, M) \cap A$  contains finitely many elements, i.e.

$$(M - \varepsilon, M) \cap A = \{a_1, a_2, \dots, a_p\}.$$

Note that  $a := \max(a_1, \dots, a_p) < M$ .

Set  $\delta = M - a$ . Since  $\delta > 0$ , there exists  $b \in A$  such that  $M - \delta < b \leq M$ .

Since  $M \notin A$ , we have  $b < M$ . Besides  $b > M - \delta = a \geq M - \varepsilon$ .

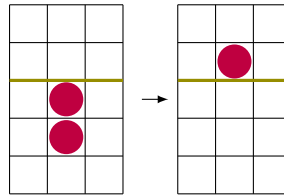
Therefore  $b \in (M - \varepsilon, M) \cap A$ .

But,  $\forall i = 1, \dots, p$ ,  $b > a > a_i$ .

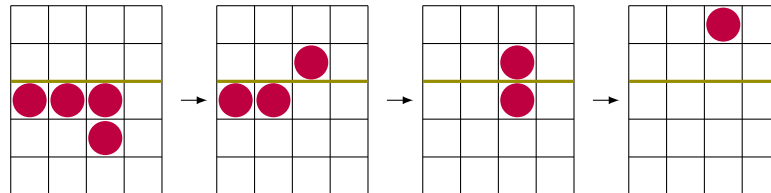
Hence a contradiction

### Sample solutions to Exercise 8.

1. To reach the first row:



To reach the second row:



I let you continue for the third and fourth rows!

2. There are three cases to handle:

- The piece moves towards the target cell: then if the piece is initially located at a cell labeled  $\sigma^n$ , then it jumps over piece in a cell labeled  $\sigma^{n-1}$  to reach a cell labeled  $\sigma^{n-2}$ .  
Therefore  $F(C') - F(C) = -\sigma^n - \sigma^{n-1} + \sigma^{n-2} = \sigma^{n-2}(-\sigma^2 - \sigma + 1) = 0$ .

- The piece remains at the same distance to the target cell: then if the piece is initially located at a cell labeled  $\sigma^n$ , then it jumps over piece in a cell labeled  $\sigma^{n-1}$  to reach a cell labeled  $\sigma^n$ .  
Therefore  $F(C') - F(C) = -\sigma^n - \sigma^{n-1} + \sigma^n = -\sigma^{n-1}$ .
- The piece moves away from the target cell: then if the piece is initially located at a cell labeled  $\sigma^n$ , then it jumps over piece in a cell labeled  $\sigma^{n+1}$  to reach a cell labeled  $\sigma^{n+2}$ .  
Therefore  $F(C') - F(C) = -\sigma^n - \sigma^{n+1} + \sigma^{n+2} = \sigma^n(-1 - \sigma + \sigma^2) = -2\sigma^{n+1}$ .

3. For those who like geometric series, like Cherge: since  $0 < \sigma < 1$ , we have

$$\sum_{n=2}^{+\infty} \sigma^n = \frac{\sigma^2}{1 - \sigma} = 1$$

Otherwise, if you don't like geometric series: since  $\forall n \in \mathbb{N}$ ,  $\sigma^{n+2} = \sigma^n - \sigma^{n+1}$ , we have a telescoping series:

$$\sum_{n=2}^K \sigma^n = \sum_{n=0}^{K-2} \sigma^{n+2} = \sum_{n=0}^{K-2} (\sigma^n - \sigma^{n+1}) = \sigma^0 - \sigma^{K-1} \xrightarrow{K \rightarrow +\infty} 1 - 0 = 1$$

4.

...	$\sigma^{10}$	$\sigma^9$	$\sigma^8$	$\sigma^7$	$\sigma^6$	$\sigma^5$	$\sigma^6$	$\sigma^7$	$\sigma^8$	$\sigma^9$	$\sigma^{10}$	...
...	$\sigma^{11}$	$\sigma^{10}$	$\sigma^9$	$\sigma^8$	$\sigma^7$	$\sigma^6$	$\sigma^7$	$\sigma^8$	$\sigma^9$	$\sigma^{10}$	$\sigma^{11}$	...
...	$\sigma^{12}$	$\sigma^{11}$	$\sigma^{10}$	$\sigma^9$	$\sigma^8$	$\sigma^7$	$\sigma^8$	$\sigma^9$	$\sigma^{10}$	$\sigma^{11}$	$\sigma^{12}$	...

The cells on  $y = 0$  give

$$\sigma^5 + 2\sigma^6 \sum_{k=0}^{+\infty} \sigma^k = \sigma^5 + \frac{2\sigma^6}{1 - \sigma} = \sigma^5 + 2\sigma^4 = \sigma^3(\sigma^2 + 2\sigma) = \sigma^3(1 + \sigma) = \sigma^2(\sigma + \sigma^2) = \sigma^2$$

Therefore, the cells on  $y = n$  give  $\sigma^{2+n}$  and

$$F(C) = \sum_{n=2}^{+\infty} \sigma^n = 1$$

5. Assume that we have a finite initial configuration  $C_0$ , then  $F(C_0) < F(C) = 1$  from the previous question.

If  $C_n$  is a configuration obtained after  $n$  moves then  $(F(C_n))_n$  is decreasing by Question 2.

Assume that we reach 5 after  $n$  moves then  $F(C_n) \geq \sigma^0 = 1$  (since it contains at least a piece located at  $(5, 0)$ ). But  $F(C_n) \leq F(C_0) < 1$ . Hence a contradiction.

**Sample solutions to Exercise 9.**

- Let  $x, y \in \mathbb{R}$ . By definition of the floor function, we know that  $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$  and  $\lfloor y \rfloor \leq y < \lfloor y \rfloor + 1$ .  
Therefore  $\lfloor x \rfloor + \lfloor y \rfloor \leq x + y$ .  
Since  $\lfloor x + y \rfloor$  is the greater integer less than or equal to  $x + y$ , we get that  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$ .  
Finally  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq x + y \leq \lfloor x \rfloor + \lfloor y \rfloor + 2$ .  
So, either  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$  or  $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor + 1$ .  
In both cases we have  $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$ .
- Let  $n \in \mathbb{N} \setminus \{0\}$  and  $x \in \mathbb{R}$ . Since  $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$ , we get  $n\lfloor x \rfloor \leq nx < n\lfloor x \rfloor + n$ .  
Since  $\lfloor nx \rfloor$  is the greatest integer less than or equal to  $nx$ , we obtain  $n\lfloor x \rfloor \leq \lfloor nx \rfloor \leq nx < n\lfloor x \rfloor + n$ .  
Thus  $\lfloor x \rfloor \leq \frac{\lfloor nx \rfloor}{n} < \lfloor x \rfloor + 1$  and hence  $\lfloor x \rfloor = \left\lfloor \frac{\lfloor nx \rfloor}{n} \right\rfloor$ .

**Sample solutions to Exercise 10.**

- Let  $n \in \mathbb{N}$ . Then

$$\begin{aligned} (2 + \sqrt{3})^n + (2 - \sqrt{3})^n &= \sum_{k=0}^n \binom{n}{k} 2^{n-k} \sqrt{3}^k + \sum_{k=0}^n \binom{n}{k} 2^{n-k} (-1)^k \sqrt{3}^k \\ &= \sum_{k=0}^n \binom{n}{k} (1 + (-1)^k) 2^{n-k} \sqrt{3}^k \end{aligned}$$

Note that if  $k$  is odd then  $(1 + (-1)^k) = 0$  and that if  $k = 2l$  is even then

$$\binom{n}{k} (1 + (-1)^k) 2^{n-k} \sqrt{3}^k = \binom{n}{2l} \times 2 \times 2^{n-2l} \times 3^l \in 2\mathbb{N}$$

Therefore  $(2 + \sqrt{3})^n + (2 - \sqrt{3})^n \in 2\mathbb{N}$ .

- Let  $n \in \mathbb{N}$ . Since  $2 - \sqrt{3} \in (0, 1)$ , we have that  $0 < (2 - \sqrt{3})^n < 1$ .  
Therefore, if we set  $S = (2 + \sqrt{3})^n + (2 - \sqrt{3})^n$ , then  $S < (2 + \sqrt{3})^n < S - 1$ , thus

$$S - 1 \leq (2 + \sqrt{3})^n < S$$

i.e.  $\left\lfloor (2 + \sqrt{3})^n \right\rfloor = S - 1$  which is odd according to the previous question.

**Sample solutions to Exercise 11.**

Let's prove the contrapositive, i.e.  $I \cap J \neq \emptyset \implies (I \cap \mathbb{Q}) \cap (J \cap \mathbb{Q}) \neq \emptyset$ .

Assume that  $I \cap J \neq \emptyset$ , then there exists  $a \in I \cap J$ .

Since  $I$  is an open interval, there exists  $\varepsilon > 0$  such that  $(a - \varepsilon, a + \varepsilon) \subset I$ .

Similarly, there exists  $\eta > 0$  such that  $(a - \eta, a + \eta) \subset J$ .

Set  $\delta = \min(\varepsilon, \eta)$ , then  $(a - \delta, a + \delta) \subset I \cap J$ .

Since between two reals there exists a rational, we know that there exists  $q \in \mathbb{Q}$  such that  $a - \delta < q < a + \delta$ .

Therefore  $q \in I \cap \mathbb{Q}$  and  $q \in J \cap \mathbb{Q}$ , so that  $(I \cap \mathbb{Q}) \cap (J \cap \mathbb{Q}) \neq \emptyset$ .

**Sample solutions to Exercise 12.**

- No:  $\sqrt{2}$  and  $-\sqrt{2}$  are both irrational but  $(\sqrt{2}) + (-\sqrt{2}) = 0 \in \mathbb{Q}$ .
- No:  $(\sqrt{2})(\sqrt{2}) = 2 \in \mathbb{Q}$ .
- Let  $x \in \mathbb{R} \setminus \mathbb{Q}$  and  $y \in \mathbb{Q}$ . Assume by contradiction that  $x + y \in \mathbb{Q}$  then  $x = (x + y) - y \in \mathbb{Q}$ .

4. Let  $x \in \mathbb{R} \setminus \mathbb{Q}$  and  $y \in \mathbb{Q} \setminus \{0\}$ . Assume by contradiction that  $xy \in \mathbb{Q}$  then  $x = \frac{xy}{y} \in \mathbb{Q}$ .

### Sample solutions to Exercise 13.

1. Assume by contradiction that  $\sqrt{3} \in \mathbb{Q}$  then  $\sqrt{3} = \frac{a}{b}$  where  $a \in \mathbb{N}$  and  $b \in \mathbb{N} \setminus \{0\}$ . Hence  $a^2 = 3b^2$ .  
The prime factorization of  $a^2$  contains an even number of primes whereas the prime factorization of  $3b^2$  contains an odd number of primes.  
Therefore it contradicts the uniqueness of the prime factorization.
2. Assume by contradiction that  $\sqrt{6} \in \mathbb{Q}$  then  $\sqrt{6} = \frac{a}{b}$  where  $a \in \mathbb{N}$ ,  $b \in \mathbb{N} \setminus \{0\}$  and  $\gcd(a, b) = 1$ .  
Therefore  $6b^2 = a^2$ . So  $2|a^2$ . By Euclid's lemma,  $2|a$ , so there exists  $k \in \mathbb{N}$  such that  $a = 2k$ .  
Hence we may rewrite  $6b^2 = 4k^2$ , which implies  $3b^2 = 2k^2$ . So  $2|3b^2$ .  
Since  $\gcd(2, 3) = 1$ , by Gauss' lemma we get  $2|b^2$  and then by Euclid's lemma, we get  $2|b$ .  
Therefore  $2|\gcd(a, b) = 1$ . Hence a contradiction.
3. Same as for  $\sqrt{3}$ .
4. Assume by contradiction that  $x = \sqrt[3]{3 + \sqrt{11}} \in \mathbb{Q}$ . Then  $x^3 = 3 + \sqrt{11}$ . So  $\sqrt{11} = x^3 - 3 \in \mathbb{Q}$ .
5. Assume by contradiction that  $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$ .  
Then  $(\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{6} \in \mathbb{Q}$ . Therefore  $\sqrt{6} = \frac{(\sqrt{2} + \sqrt{3})^2 - 5}{2} \in \mathbb{Q}$ .
6. Assume by contradiction that  $(\sqrt{2} + \sqrt{3})^2 \in \mathbb{Q}$ .  
Since  $(\sqrt{2} + \sqrt{3})^2 = 2 + 3 + 2\sqrt{6}$ , we get  $\sqrt{6} = \frac{(\sqrt{2} + \sqrt{3})^2 - 5}{2} \in \mathbb{Q}$ .
7. Assume by contradiction that  $x = \sqrt{2} + \sqrt{3} + \sqrt{6} \in \mathbb{Q}$ .  
Then  $\sqrt{2} + \sqrt{3} = x - \sqrt{6}$ . Squaring both sides, we get  $5 + 2\sqrt{6} = x^2 + 6 - 2x\sqrt{6}$ .  
Therefore  $\sqrt{6} = \frac{x^2 + 1}{2 + 2x} \in \mathbb{Q}$ .
8. Assume by contradiction that  $(3\sqrt{2} + 2\sqrt{3} + \sqrt{6})^2 \in \mathbb{Q}$ .  
Since  $(3\sqrt{2} + 2\sqrt{3} + \sqrt{6})^2 = 36 + 12(\sqrt{2} + \sqrt{3} + \sqrt{6})$ , we get  $\sqrt{2} + \sqrt{3} + \sqrt{6} = \frac{(3\sqrt{2} + 2\sqrt{3} + \sqrt{6})^2 - 36}{12} \in \mathbb{Q}$ .
9. There is an elegant method using the complex conjugate.  
Assume by contradiction that  $\sqrt{7} + \sqrt{3} \in \mathbb{Q}$ . Then  $(\sqrt{7} + \sqrt{3})(\sqrt{7} - \sqrt{3}) = 7 - 3 = 4$ . Thus  
 $\sqrt{7} - \sqrt{3} = \frac{4}{\sqrt{7} + \sqrt{3}} \in \mathbb{Q}$ .  
Hence  $\sqrt{3} = \frac{(\sqrt{7} + \sqrt{3}) - (\sqrt{7} - \sqrt{3})}{2} \in \mathbb{Q}$ .

### Sample solutions to Exercise 14.

Let  $n \in \mathbb{N}$ .

- $\sqrt{n} \in \mathbb{Q} \Rightarrow \sqrt{n} \in \mathbb{N}$ :  
Assume that  $\sqrt{n} \in \mathbb{Q}$ , then there exists  $(a, b) \in \mathbb{N} \setminus \{0\}$  such that  $\sqrt{n} = \frac{a}{b}$  and  $\gcd(a, b) = 1$ .  
Then  $a^2 = nb^2$ , thus  $b|a^2$ . By Gauss' lemma applied twice  $b|a$  and then  $b|1$ . Thus  $b = 1$  and  $\sqrt{n} = a \in \mathbb{N}$ .
- $\sqrt{n} \in \mathbb{N} \Rightarrow \exists m \in \mathbb{N}, n = m^2$ : assume that  $\sqrt{n} \in \mathbb{N}$ . Then  $n = (\sqrt{n})^2$ . So we can take  $m = \sqrt{n}$ .
- $\exists m \in \mathbb{N}, n = m^2 \Rightarrow \sqrt{n} \in \mathbb{Q}$ : assume that there exists  $m \in \mathbb{N}$  such that  $n = m^2$ . Then  $\sqrt{n} = m \in \mathbb{N} \subset \mathbb{Q}$ .



**Sample solutions to Exercise 15.**

No,  $\sum_{n=1}^{+\infty} 10^{-\frac{n(n+1)}{2}} = 0.101001000100001000001 \dots$  is not rational since its decimal expansion is not eventually periodic.

We denote the decimals by  $(a_k)_{k \geq 1}$ :  $a_k = 1$  if  $\exists n \in \mathbb{N}$ ,  $k = \frac{n(n+1)}{2}$  and  $a_k = 0$  otherwise.

Let  $r \in \mathbb{N}$  and  $s \in \mathbb{N} \setminus \{0\}$ .

Then there exists  $k \in \mathbb{N}$  such that  $r + k > \frac{s(s+1)}{2}$  and  $a_{r+k} = 1$ , so that  $0 = a_{r+k+s} \neq a_{r+k} = 1$ .

**Sample solutions to Exercise 16.**

$$1. \quad (a) \quad \text{Note that } f(x) = \frac{1}{n!} \sum_{k=0}^n \binom{n}{k} (-1)^k x^{n+k} = \frac{1}{n!} \sum_{k=n}^{2n} \binom{n}{k-n} (-1)^{k-n} x^k.$$

Let  $k \in \mathbb{N}$ . If  $k < n$  or  $k > 2n$  then  $f^{(k)}(0) = 0$ .

Otherwise, if  $n \leq k \leq 2n$  then  $f^{(k)}(0) = (-1)^{k-n} \frac{k!}{n!} \binom{n}{k-n} \in \mathbb{Z}$ .

(b) Let  $k \in \mathbb{N}$ . Since  $f(x) = f(1-x)$ , we get  $f^{(k)}(1) = (-1)^k f^{(k)}(0) \in \mathbb{Z}$ .

$$\begin{aligned} (c) \quad F''(x) &= \sum_{k \geq 0} (-1)^k r^{2n-2k} f^{(2(k+1)+1)}(x) \\ &= -r^2 \sum_{k \geq 0} (-1)^{k+1} r^{2n-2(k+1)} f^{(2(k+1)+1)}(x) \\ &= -r^2 \sum_{k \geq 1} (-1)^k r^{2n-2k} f^{(2k+1)}(x) \\ &= -r^2 (F(x) - r^{2n} f(x)) \\ &= -r^2 F(x) + r^{2n+2} f(x) \end{aligned}$$

$$\begin{aligned} \left( \frac{d}{dx} \right)^d (F'(x) \sin(rx) - rF(x) \cos(rx)) &= F''(x) \sin(rx) + rF'(x) \cos(rx) - rF'(x) \cos(rx) + rF(x) \sin(rx) \\ &= F''(x) \sin(rx) + rF(x) \sin(rx) \\ &= (F''(x) + rF(x)) \sin(rx) \\ &= r^{2n+2} f(x) \sin(rx) \end{aligned}$$

$$\begin{aligned} (e) \quad \int_0^1 f(x) \sin(rx) dx &= \frac{1}{r^{2n+2}} \int_0^1 r^{2n+2} f(x) \sin(rx) dx \\ &= \frac{1}{r^{2n+2}} [F'(x) \sin(rx) - rF(x) \cos(rx)]_0^1 \\ &= \frac{1}{r^{2n+2}} (F'(1) \sin(r) - rF(1) \cos(r) + rF(0)) \end{aligned}$$

2. Let  $r \in (0, \pi] \cap \mathbb{Q}$ . Assume by contradiction that  $\sin(r), \cos(r) \in \mathbb{Q}$ . Then, we may write  $\frac{1}{r} = \frac{a}{d}$ ,  $\sin(r) = \frac{b}{d}$  and  $\cos(r) = \frac{c}{d}$  where  $a, b, c \in \mathbb{Z}$  and  $d \in \mathbb{N} \setminus \{0\}$ .

Let  $n \in \mathbb{N}$ , then using 1.(e), 1.(a) and 1.(b) we get that  $I_n = \frac{A_n}{d^{2n+3}}$  for some  $A_n \in \mathbb{Z}$ .

Since  $I_n > 0$ , we get that  $A_n \geq 1$ , and thus that  $I_n \geq \frac{1}{d^{2n+3}}$ .

But we also have that

$$\begin{aligned} I_n &= \int_0^1 f(x) \sin(rx) dx \\ &\leq \int_0^1 f(x) dx \quad \text{since } \sin > 0 \text{ on } (0, \pi) \\ &\leq \frac{1}{n!} \quad \text{since } f(x) \leq \frac{1}{n!} \text{ on } [0, 1] \end{aligned}$$

Therefore  $\frac{1}{d^{2n+3}} \leq I_n \leq \frac{1}{n!}$  and thus  $n! \leq d^{2n+3}$ . Which leads to a contradiction for  $n$  large enough.

3. We use the contrapositive of the previous question: since  $\pi \in (0, \pi]$  and since  $\sin(\pi) = 0 \in \mathbb{Q}$  and  $\cos(\pi) = -1 \in \mathbb{Q}$ , we get that  $\pi \notin \mathbb{Q}$ .

## 8.7 Chapter 7

### Sample solutions to Exercise 1.

1. Let  $A, B, C \in \mathcal{P}(E)$ . Assume that  $A \cup B = B \cap C$ .  
Let  $x \in A$  then  $x \in A \cup B = B \cap C$ . Therefore  $x \in B$ . So  $A \subset B$ .  
Let  $x \in B$  then  $x \in A \cup B = B \cap C$ . Therefore  $x \in C$ . So  $B \subset C$ .
2. Using the previous question.  
Let  $A, B \in \mathcal{P}(E)$ . Assume that  $A \cap B = A \cup B$ .  
From the previous question we get that  $A \subset B \subset A$ . Hence  $A = B$ .

*Direct proof.*

Let  $A, B \in \mathcal{P}(E)$ . Assume that  $A \cap B = A \cup B$ .  
Let  $x \in A$  then  $x \in A \cup B = A \cap B$ . Thus  $x \in B$ . Therefore  $A \subset B$ .  
Let  $x \in B$  then  $x \in A \cup B = A \cap B$ . Thus  $x \in A$ . Therefore  $B \subset A$ .  
Hence  $A = B$ .

*Proof by contrapositive.*

Let  $A, B \in \mathcal{P}(E)$ . Assume that  $A \neq B$ . Then

- either  $A \setminus B \neq \emptyset$  and then there exists  $x \in E$  such that  $x \in A$  and  $x \notin B$ . Thus  $x \in A \cup B$  but  $x \notin A \cap B$ . Therefore  $A \cap B \neq A \cup B$ .
- or  $B \setminus A \neq \emptyset$  and then there exists  $x \in E$  such that  $x \in B$  and  $x \notin A$ . Thus  $x \in A \cup B$  but  $x \notin A \cap B$ . Therefore  $A \cap B \neq A \cup B$ .

### Sample solutions to Exercise 2.

$\Leftarrow$  Assume that  $f, g$  and  $h$  are bijective then  $g \circ f$  and  $h \circ g$  are too.

$\Rightarrow$  Assume that  $g \circ f$  and  $h \circ g$  are bijective.

Since  $g \circ f$  is surjective,  $g$  is too. Since  $h \circ g$  is injective,  $g$  is too.

Hence  $g$  is bijective, so it admits an inverse  $g^{-1} : C \rightarrow B$ .

Then  $f = g^{-1} \circ (g \circ f)$  and  $h = (h \circ g) \circ g^{-1}$  are bijective as composition of bijective functions.

### Sample solutions to Exercise 3.

1. Let  $A \in \mathcal{P}(E)$ . Let  $x \in A$ . Then  $f(x) \in f(A)$ . Therefore  $x \in f^{-1}(f(A))$ .  
We proved that  $A \subset f^{-1}(f(A))$ .
2. Let  $B \subset \mathcal{P}(F)$ . Let  $y \in f(f^{-1}(B))$ . Then there exists  $x \in f^{-1}(B)$  such that  $y = f(x)$ . But since  $x \in f^{-1}(B)$ ,  $y = f(x) \in B$ .  
We proved that  $f(f^{-1}(B)) \subset B$ .
3. Define

$$f : \begin{cases} \{1, 2\} & \rightarrow & \{1, 2\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 1 \end{cases}$$

Then  $f(f^{-1}(\{1, 2\})) = f(\{1, 2\}) = \{1\} \subsetneq \{1, 2\}$ .

And  $f^{-1}(f(\{1\})) = f^{-1}(\{1\}) = \{1, 2\} \supsetneq \{1\}$ .

### Sample solutions to Exercise 4.

1. Let  $A, B \in \mathcal{P}(F)$  be such that  $A \subset B$ . Take  $x \in f^{-1}(A)$ . Then  $f(x) \in A \subset B$ . Thus  $x \in f^{-1}(B)$ .  
The converse doesn't hold. Indeed, define

$$f : \begin{cases} \{1\} & \rightarrow & \{1, 2\} \\ 1 & \mapsto & 1 \end{cases}$$

then  $f^{-1}(\{2\}) = \emptyset \subset f^{-1}(\{1\})$ . But  $\{2\} \not\subset \{1\}$ .

2. Let  $A, B \in \mathcal{P}(F)$ .

Since  $A \cap B \subset A$  and  $A \cap B \subset B$ , we get that  $f^{-1}(A \cap B) \subset f^{-1}(A)$  and  $f^{-1}(A \cap B) \subset f^{-1}(B)$ . Thus  $f^{-1}(A \cap B) \subset f^{-1}(A) \cap f^{-1}(B)$ .

For the other inclusion, let  $x \in f^{-1}(A) \cap f^{-1}(B)$ . Then  $f(x) \in A$  and  $f(x) \in B$ . Thus  $f(x) \in A \cap B$  so that  $x \in f^{-1}(A \cap B)$ . Thus  $f^{-1}(A) \cap f^{-1}(B) \subset f^{-1}(A \cap B)$ .

3. Let  $A, B \in \mathcal{P}(F)$ .

Since  $A, B \subset A \cup B$ , we get  $f^{-1}(A), f^{-1}(B) \subset f^{-1}(A \cup B)$ . Thus  $f^{-1}(A) \cup f^{-1}(B) \subset f^{-1}(A \cup B)$ .

For the other inclusion, let  $x \in f^{-1}(A \cup B)$ . Then  $f(x) \in A \cup B$ . Either  $f(x) \in A$  and then  $x \in f^{-1}(A) \subset f^{-1}(A) \cup f^{-1}(B)$  or  $f(x) \in B$  and then  $x \in f^{-1}(B) \subset f^{-1}(A) \cup f^{-1}(B)$ . Thus  $x \in f^{-1}(A) \cup f^{-1}(B)$ . We proved that  $f^{-1}(A \cup B) \subset f^{-1}(A) \cup f^{-1}(B)$ .

### Sample solutions to Exercise 5.

1. Let  $A, B \in \mathcal{P}(E)$  be such that  $A \subset B$ . Let  $y \in f(A)$ . Then  $y = f(x)$  for some  $x \in A$ . But  $x \in A \subset B$ . Thus  $y = f(x) \in f(B)$ . We proved that  $f(A) \subset f(B)$ .

The converse doesn't hold. Indeed define

$$f : \begin{cases} \{1, 2\} & \rightarrow & \{1\} \\ 1 & \mapsto & 1 \\ 2 & \mapsto & 1 \end{cases}$$

then  $f(\{1\}) = f(\{2\}) = \{1\}$  but  $\{1\} \not\subset \{2\}$ .

2. Let  $A, B \in \mathcal{P}(E)$ . Since  $A \cap B \subset A, B$  we get  $f(A \cap B) \subset f(A), f(B)$ . Thus  $f(A \cap B) \subset f(A) \cap f(B)$ .

The inclusion can be strict using the same example as above.

3. Let  $A, B \in \mathcal{P}(E)$ . Since  $A, B \subset A \cup B$ , we get  $f(A), f(B) \subset f(A \cup B)$ . Thus  $f(A) \cup f(B) \subset f(A \cup B)$ .

For the other inclusion, let  $y \in f(A \cup B)$ . Then  $y = f(x)$  for some  $x \in A \cup B$ . So either  $x \in A$  and then  $y = f(x) \in f(A) \subset f(A) \cup f(B)$ , or  $x \in B$  and then  $y = f(x) \in f(B) \subset f(A) \cup f(B)$ . In both cases  $y \in f(A) \cup f(B)$ . So we proved that  $f(A \cup B) \subset f(A) \cup f(B)$ .

### Sample solutions to Exercise 6.

$\Rightarrow$  Assume that  $f$  is injective. Let  $A, B \in \mathcal{P}(E)$ .

We already know that  $f(A \cap B) \subset f(A) \cap f(B)$  holds (see the previous exercise).

Let's prove that  $f(A) \cap f(B) \subset f(A \cap B)$ .

Let  $y \in f(A) \cap f(B)$ . Then  $y = f(x_1)$  for some  $x_1 \in A$  and  $y = f(x_2)$  for some  $x_2 \in B$ .

Since  $f(x_1) = f(x_2)$  and  $f$  is injective, we obtain that  $x_1 = x_2 \in A \cap B$ . Therefore  $y = f(x_1) \in f(A \cap B)$ .

We proved that  $f(A) \cap f(B) \subset f(A \cap B)$ . Thus  $f(A) \cap f(B) = f(A \cap B)$ .

$\Leftarrow$  Assume that  $\forall A, B \in \mathcal{P}(E), f(A \cap B) = f(A) \cap f(B)$ .

Let  $x_1, x_2 \in E$  be such that  $f(x_1) = f(x_2)$ . Set  $y := f(x_1) = f(x_2)$ .

Then  $f(\{x_1\} \cap \{x_2\}) = f(\{x_1\}) \cap f(\{x_2\}) = \{y\} \cap \{y\} = \{y\}$ .

Particularly  $\{x_1\} \cap \{x_2\} \neq \emptyset$ , thus  $x_1 = x_2$ .

### Sample solutions to Exercise 7.

$$\begin{aligned} |A \Delta B| &= |(A \cup B) \setminus (A \cap B)| \\ &= |A \cup B| - |A \cap B| \\ &= |A| + |B| - |A \cap B| - |A \cap B| \\ &= |A| + |B| - 2|A \cap B| \end{aligned}$$

**Sample solutions to Exercise 8.**

1. Let  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$ .

Then  $\psi : F^E \rightarrow F^{|E|}$  defined by  $\psi(f) = (f(\varphi(0)), \dots, f(\varphi(|E| - 1)))$  is a bijection (prove it).

Therefore  $|F^E| = |F^{|E|}| = |F|^{|E|}$ .

2. According to the last exercise, there exists an injective function  $E \rightarrow F$  if and only if  $|E| \leq |F|$ .

Next, since  $E$  is finite, there exists a bijection  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$ .

For  $f(\varphi(0))$  we have  $|F|$  possible choices. For  $f(\varphi(1))$  we have  $|F \setminus \{f(\varphi(0))\}| = |F| - 1$  choices. For  $f(\varphi(2))$  we have  $|F \setminus \{f(\varphi(0)), f(\varphi(1))\}| = |F| - 2$  choices. And so on.

Therefore,  $|\{f \in F^E : f \text{ is injective}\}| = |F|(|F| - 1) \cdots (|F| - |E| + 1) = \frac{|F|!}{(|F| - |E|)!}$ .

$$\text{Thus } |\{f \in F^E : f \text{ is injective}\}| = \begin{cases} 0 & \text{if } |E| > |F| \\ \frac{|F|!}{(|F| - |E|)!} & \text{if } |E| \leq |F| \end{cases}.$$

3. It is a special case of the above question when  $|E| = |F|$ :  $|\{f \in E^E : f \text{ is bijective}\}| = \frac{|E|!}{(|E| - |E|)!} = |E|!$ .

**Sample solutions to Exercise 9.**

The number of subsets with cardinality  $k$  included in a set of cardinality  $n$  is denoted  $\binom{n}{k}$  read " $n$  choose  $k$ ".

We are going to prove that  $\binom{n}{k} = \frac{n!}{(n-k)!k!}$ .

Let  $E$  a finite set. Set  $n = |E|$ . Fix  $k \in \{0, 1, \dots, n\}$ .

An ordered list of  $k$  distinct elements is the same as fixing an injection  $\{0, 1, \dots, k-1\} \rightarrow E$ . So, using the previous question there are  $\frac{n!}{(n-k)!}$  such ordered lists.

Two ordered lists of  $k$  elements give the same subset if and only if one is obtained from the other one permuting its elements, which is the same as constructing a bijection  $\{0, 1, \dots, k-1\} \rightarrow \{0, 1, \dots, k-1\}$ . From the previous question there are  $k!$  such bijections.

$$\text{Therefore } \binom{n}{k} = \frac{\frac{n!}{(n-k)!}}{k!} = \frac{n!}{(n-k)!k!}.$$

**Sample solutions to Exercise 10.**

$\Rightarrow$

*Method 1 (by induction):*

Let's prove by induction on  $n = |E|$  that  $\mathcal{P}(E)$  is finite and that  $|\mathcal{P}(E)| = 2^{|E|}$ .

- *Base case at  $n = 0$ :* if  $E = \emptyset$  then  $\mathcal{P}(E) = \{\emptyset\}$  is finite.
- *Induction step:* assume that the statement holds for some  $n \in \mathbb{N}$ , i.e. if  $E$  is a set with  $|E| = n$  then  $\mathcal{P}(E)$  is finite and  $|\mathcal{P}(E)| = 2^n$ .  
Let  $E$  be a set such that  $|E| = n + 1$ . Since  $|E| > 0$ , there exists  $x \in E$ .  
By the induction hypothesis, since  $|E \setminus \{x\}| = n$ , we get that  $\mathcal{P}(E \setminus \{x\})$  is finite and  $|\mathcal{P}(E \setminus \{x\})| = 2^n$ .  
Note that  $\mathcal{P}(E \setminus \{x\}) = \{A \in \mathcal{P}(E) : x \notin A\}$  and that

$$\begin{array}{ccc} \{A \in \mathcal{P}(E) : x \notin A\} & \rightarrow & \{A \in \mathcal{P}(E) : x \in A\} \\ A & \mapsto & A \cup \{x\} \end{array}$$

is a bijection.

Therefore  $\mathcal{P}(E) = \{A \in \mathcal{P}(E) : x \notin A\} \sqcup \{A \in \mathcal{P}(E) : x \in A\}$  is finite and  $|\mathcal{P}(E)| = |\{A \in \mathcal{P}(E) : x \notin A\}| + |\{A \in \mathcal{P}(E) : x \in A\}| = 2^n + 2^n = 2^{n+1}$ .

*Method 2 (using the previous exercise):*

Let  $E$  be a finite set. We know that for  $k = 0, \dots, |E|$ , the number of subsets with  $k$  elements is  $\binom{n}{k}$ .

Therefore the number of subsets included in  $E$  is

$$|\mathcal{P}(E)| = \sum_{k=0}^{|E|} \binom{|E|}{k} = \sum_{k=0}^{|E|} \binom{|E|}{k} 1^k 1^{|E|-k} = (1+1)^{|E|} = 2^{|E|}$$

*Method 3 (which generalizes to infinite sets):*

Let  $E$  be a finite set. We define  $\psi : \mathcal{P}(E) \rightarrow \{0, 1\}^E$  by  $\psi(A)(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$ .

Then  $\psi$  is a bijection thus  $\mathcal{P}(E)$  is finite since  $\{0, 1\}^E$  is and moreover  $|\mathcal{P}(E)| = |\{0, 1\}^E| = 2^{|E|}$ .

$\Leftarrow$  Let  $E$  be a set. Assume that  $\mathcal{P}(E)$  is finite.

Note that  $\Phi : E \rightarrow \mathcal{P}(E)$  defined by  $\Phi(x) = \{x\}$  is injective. Therefore  $E$  is finite too.

### Sample solutions to Exercise 11.

1.  $\Rightarrow$  Assume that  $|E| \leq |F|$ .

There exist bijections  $\varphi : \{k \in \mathbb{N} : k < |E|\} \rightarrow E$  and  $\psi : \{k \in \mathbb{N} : k < |F|\} \rightarrow F$ .

Since  $|E| \leq |F|$ ,  $f = \psi \circ \varphi^{-1} : E \rightarrow F$  is well-defined and injective.

$\Rightarrow$  Assume that there exists an injection  $f : E \rightarrow F$ .

Then  $f$  induces a bijection  $f : E \rightarrow f(E)$ , so that  $|E| = |f(E)|$ .

And since  $f(E) \subset F$ , we have  $|f(E)| \leq |F|$ .

2. It is a consequence of the previous question.

3. A participant shook either 0, 1, ... or  $n-1$  hands. So we have  $n$  "boxes". Not that it is not possible to have at the same time the boxes 0 and  $n-1$  non-empty. Therefore we have only  $n-1$  boxes for  $n$  participants, so two participants must have shaken the same number of boxes.

Formally:

- First case: there is at least one participant who didn't shake any hand. Then  $f : \{\text{participants}\} \rightarrow \{0, 1, \dots, n-2\}$  mapping each participant to the number of hands he shook is well-defined. Since  $|\{\text{participants}\}| = n > n-1 = |\{0, 1, \dots, n-2\}|$ ,  $f$  can't be injective. Therefore at least two participants shook the same number of hands.
- Second case: all participants shook at least one hand. Then  $f : \{\text{participants}\} \rightarrow \{1, \dots, n-1\}$  mapping each participant to the number of hands he shook is well-defined. Since  $|\{\text{participants}\}| = n > n-1 = |\{1, 2, \dots, n-1\}|$ ,  $f$  can't be injective. Therefore at least two participants shook the same number of hands.

4. For  $r = 1, 2, \dots, n$ , set  $s_r = \sum_{k=1}^r a_k$ .

- First case: there exists  $r$  such that  $n|s_r$ . Then we are done.
- Second case: otherwise, we have  $n$  numbers  $s_1, \dots, s_n$  whose remainders for the Euclidean division by  $n$  are among  $1, \dots, n-1$  (i.e.  $n-1$  possible remainders). Hence at least two have the same remainders, let's say  $s_p$  and  $s_q$  with  $q > p$ . Then  $n|s_q - s_p = \sum_{k=p+1}^q a_k$ .

5. First, note that  $\frac{\tan a - \tan b}{1 + \tan a \tan b} = \tan(a - b)$  and that

$$\tan \frac{\pi}{12} = \tan \left( \frac{\pi}{3} - \frac{\pi}{4} \right) = \frac{\tan \frac{\pi}{3} - \tan \frac{\pi}{4}}{1 + \tan \frac{\pi}{3} \tan \frac{\pi}{4}} = \frac{\sqrt{3} - 1}{1 + \sqrt{3}} = \frac{(\sqrt{3} - 1)^2}{2} = 2 - \sqrt{3}$$

Let  $x_1, \dots, x_{13}$  be 13 distinct real numbers. We set  $\alpha_k = \arctan x_k \in \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ . Note that the  $\alpha_k$  are distinct since  $\arctan$  is injective.

Note that  $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right) = I_1 \sqcup I_2 \sqcup I_3 \sqcup \cdots \sqcup I_{12}$  where

$$I_1 = \left(-\frac{\pi}{2}, -\frac{\pi}{2} + \frac{\pi}{12}\right], \quad I_2 = \left(-\frac{\pi}{2} + \frac{\pi}{12}, -\frac{\pi}{2} + 2\frac{\pi}{12}\right], \quad \dots, \quad I_{11} = \left(-\frac{\pi}{2} + 10\frac{\pi}{12}, \frac{\pi}{2} + 11\frac{\pi}{12}\right], \quad I_{12} = \left(-\frac{\pi}{2} + 11\frac{\pi}{12}, \frac{\pi}{2}\right)$$

We define  $f : \{\alpha_1, \dots, \alpha_{13}\} \rightarrow \{1, \dots, 12\}$  by  $f(\alpha_k) = r$  where  $\alpha_k \in I_r$ .

Since  $|\{\alpha_1, \dots, \alpha_{13}\}| = 13 > 12 = |\{1, \dots, 12\}|$ ,  $f$  is not injective. So there exists  $\alpha_k < \alpha_l$  and  $r = 1, \dots, 12$  such that  $\alpha_k, \alpha_l \in I_r$ . Then  $0 < \alpha_l - \alpha_k < \frac{\pi}{12}$ .

Since  $\tan$  is increasing on  $\left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$ , we get that  $\tan 0 < \tan(\alpha_l - \alpha_k) < \tan \frac{\pi}{12} = 2 - \sqrt{3}$ .

Note that  $\tan(\alpha_l - \alpha_k) = \frac{\tan \alpha_l - \tan \alpha_k}{1 + \tan \alpha_l \tan \alpha_k} = \frac{x_l - x_k}{1 + x_l x_k}$ . Thus  $0 < \frac{x_l - x_k}{1 + x_l x_k} < 2 - \sqrt{3}$  as requested.

### Sample solutions to Exercise 12.

Since  $E \subset F$ , we know that  $|E| \leq |F|$ .

Besides, since  $F \subset G$ , we have  $|F| \leq |G| = |E|$ .

By Cantor–Schröder–Bernstein theorem, we have  $|E| = |F|$ .

### Sample solutions to Exercise 13.

We define  $\psi : \mathcal{P}(S) \rightarrow \{0, 1\}^S$  by  $\psi(A)(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{otherwise} \end{cases}$ .

Let's prove that  $\psi$  is a bijection:

- $\psi$  is injective.

Let  $A, B \subset S$  be such that  $A \neq B$ .

WLOG we may assume that there exists  $x \in S$  such that  $x \in A$  and  $x \notin B$ .

Therefore  $\psi(A)(x) = 1$  and  $\psi(B)(x) = 0$ . Thus  $\psi(A) \neq \psi(B)$ .

- $\psi$  is surjective.

Let  $f : S \rightarrow \{0, 1\}$  be a function. Define  $A = \{x \in S : f(x) = 1\}$ . Then  $f = \psi(A)$ .

Therefore  $|\mathcal{P}(S)| = |\{0, 1\}^S|$ .

### Sample solutions to Exercise 14.

$$1. |\{0, 1\}^{\mathbb{N}}| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$$

- The idea here is that a function  $\{0, 1\} \rightarrow \mathbb{N}$  is characterized by the values of 0 and 1.

Define  $\psi : \mathbb{N}^{\{0,1\}} \rightarrow \mathbb{N} \times \mathbb{N}$  by  $\psi(f) = (f(0), f(1))$ .

- $\psi$  is injective: let  $f, g : \mathbb{N} \rightarrow \{0, 1\}$  be such that  $\psi(f) = \psi(g)$ . Then  $(f(0), f(1)) = (g(0), g(1))$  so that  $f(0) = g(0)$  and  $f(1) = g(1)$ . Therefore  $f = g$ .
- $\psi$  is surjective: let  $(a, b) \in \mathbb{N} \times \mathbb{N}$ . Define  $f : \{0, 1\} \rightarrow \mathbb{N}$  by  $f(0) = a$  and  $f(1) = b$ . Then  $\psi(f) = (a, b)$ .

Therefore  $|\mathbb{N}^{\{0,1\}}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

### Sample solutions to Exercise 15.

- Define  $f : S \rightarrow \mathbb{N}$  by  $f(A) = \sum_{k \in A} 2^k$ .

Then  $f$  is bijective by existence and uniqueness of the binary positional representation of a natural number. Therefore  $|S| = |\mathbb{N}| = \aleph_0$ .

- Assume that  $T$  is countable then  $\mathcal{P}(\mathbb{N}) = S \sqcup T$  is countable as the union of countable sets.

Which is a contradiction since  $|\mathcal{P}(\mathbb{N})| = |\mathbb{R}| > \aleph_0$ .

**Sample solutions to Exercise 16.**

Let  $X$  be as in the statement.

For  $I \in X$ , we can find  $q_I \in I \cap \mathbb{Q}$  since  $I$  is an interval which is non-empty and not reduced to a singleton. Define  $f : X \rightarrow \mathbb{Q}$  by  $f(I) = q_I$ . Let's prove that  $f$  is injective.

Let  $I, J \in X$  such that  $q := f(I) = f(J)$ . Then  $q = q_I \in I$  and  $q = q_J \in J$ . Therefore  $q \in I \cap J \neq \emptyset$ . Thus  $I = J$  (use the contrapositive of (ii)).

Hence  $|X| \leq |\mathbb{Q}| = \aleph_0$ . So  $X$  is countable.

**Sample solutions to Exercise 17.**

$\Rightarrow$  Let's prove that any infinite set admits a proper subset of same cardinality.

Let  $X$  be an infinite set. We want to construct  $S \subsetneq X$  satisfying  $|S| = |X|$ .

Since  $X$  is infinite,  $\aleph_0 \leq |X|$ , i.e. there exists an injective function  $f : \mathbb{N} \rightarrow X$ .

We define  $g : \begin{cases} X & \rightarrow & X \\ x & \mapsto & f(n+1) & \text{if } \exists n \in \mathbb{N}, x = f(n) \\ x & \mapsto & x & \text{if } x \notin \text{Im}(f) \end{cases}$ .

- $g$  is well-defined: given  $x \in X$ , if  $\exists n, m \in \mathbb{N}$ ,  $x = f(n) = f(m)$  then  $n = m$  since  $f$  is injective.
- $g$  is injective: let  $x, y \in X$  be such that  $g(x) = g(y)$ .
  - First case:  $g(x) = g(y) \in \text{Im}(f)$  then there exists  $n, m \in \mathbb{N}$  such that  $x = f(n)$  and  $y = f(m)$ . Since  $f(n+1) = g(x) = g(y) = f(m+1)$ , we get that  $n = m$  by injectiveness of  $f$ . Therefore  $x = f(n) = f(m) = y$ .
  - Second case:  $g(x) = g(y) \notin \text{Im}(f)$  then  $x = g(x) = g(y) = y$ .

Note that  $f(0) \notin \text{Im}(g)$ , thus  $f(0) \in X \setminus \text{Im}(g)$ . Besides  $g : X \rightarrow \text{Im}(g)$  is a bijection. Hence  $S = \text{Im}(g)$  satisfies  $S \subsetneq X$  and  $|X| = |S|$ .

$\Leftarrow$  We are going to prove the contrapositive: if a set is finite then it doesn't admit a proper subset of same cardinality.

Let  $X$  be a finite set. Let  $S \subsetneq X$  be a proper subset.

Then there exists  $x_0 \in X \setminus S$  so that  $S \sqcup \{x_0\} \subset X$  and hence  $|S \sqcup \{x_0\}| = |S| + 1 \leq |E|$ , i.e.  $|S| < |E|$ .

**Sample solutions to Exercise 18.**

1. Assume by contradiction that  $\mathbb{R} \setminus \mathbb{Q}$  is countable. Then  $\mathbb{R} = (\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}$  is countable as the union of two countable sets. Hence a contradiction.
2. One way to solve this question is to take an injective function  $\mathbb{R} \rightarrow \mathbb{R}$  whose range is a proper interval of  $\mathbb{R}$  and then to move the rational values in the complement of the range after making them irrational. For instance:

Define  $f : \mathbb{R} \rightarrow \mathbb{R} \setminus \mathbb{Q}$  by

$$f(x) = \begin{cases} e^x & \text{if } e^x \notin \mathbb{Q} \\ -e^x - e & \text{otherwise} \end{cases}$$

- $f$  is well-defined: if  $e^x \in \mathbb{Q}$  then  $-e^x - e \in \mathbb{R} \setminus \mathbb{Q}$  (since  $-e^x \in \mathbb{Q}$  and  $-e \in \mathbb{R} \setminus \mathbb{Q}$ ).
- $f$  is injective: let  $x, y \in \mathbb{R}$  be such that  $f(x) = f(y)$ .
  - First case:  $f(x) = f(y) > 0$  then  $f(x) = e^x$  and  $f(y) = e^y$  thus  $e^x = f(x) = f(y) = e^y$  and then  $x = y$  since  $\exp$  is injective.
  - Second case:  $f(x) = f(y) < 0$  then  $f(x) = -e^x - e$  and  $f(y) = -e^y - e$  thus  $-e^x - e = f(x) = f(y) = -e^y - e$ , so that  $e^x = e^y$  and hence  $x = y$  since  $\exp$  is injective.

Note that  $f(x) = f(y) \neq 0$  since  $0 \in \mathbb{Q}$ .

Thus  $|\mathbb{R}| \leq |\mathbb{R} \setminus \mathbb{Q}|$ . Besides  $|\mathbb{R} \setminus \mathbb{Q}| \leq |\mathbb{R}|$  since  $\mathbb{R} \setminus \mathbb{Q} \subset \mathbb{R}$ .

Hence  $|\mathbb{R}| = |\mathbb{R} \setminus \mathbb{Q}|$  by Cantor–Schröder–Bernstein theorem.



*Comment: (using the axiom of choice) it is true that if  $A$  and  $B$  are infinite sets then  $|A \cup B| = \max(|A|, |B|)$  (but this statement was not proved in class, so you can't use it).*

*Therefore, since  $|\mathbb{Q}| < |\mathbb{R} \setminus \mathbb{Q}|$ ,  $|\mathbb{R}| = |(\mathbb{R} \setminus \mathbb{Q}) \cup \mathbb{Q}| = \max(|\mathbb{R} \setminus \mathbb{Q}|, |\mathbb{Q}|) = |\mathbb{R} \setminus \mathbb{Q}|$ .*

### Sample solutions to Exercise 19.

Define  $f : \mathbb{R} \rightarrow (0, 1)$  by  $f(x) = \frac{\arctan(x) + \frac{\pi}{2}}{\pi}$ . Then

- $f$  is well-defined:

for  $x \in \mathbb{R}$ ,  $-\frac{\pi}{2} < \arctan(x) < \frac{\pi}{2}$  thus  $0 < \arctan(x) + \frac{\pi}{2} < \pi$  and hence  $0 < \frac{\arctan(x) + \frac{\pi}{2}}{\pi} < 1$ , i.e.  $f(x) \in (0, 1)$ .

- $f$  is bijective: *prove it using that  $\arctan : \mathbb{R} \rightarrow \left(-\frac{\pi}{2}, \frac{\pi}{2}\right)$  is bijective.*

Therefore  $|(0, 1)| = |\mathbb{R}|$ .

There are lots of such bijections, for instance:

$$\begin{array}{ccc} (0, 1) & \rightarrow & \mathbb{R} \\ x & \mapsto & \frac{1}{1+e^x} \end{array} \quad \begin{array}{ccc} (0, 1) & \rightarrow & \mathbb{R} \\ x & \mapsto & \frac{2x-1}{x-x^2} \end{array} \quad \begin{array}{ccc} \mathbb{R} & \rightarrow & (0, 1) \\ x & \mapsto & e^{-e^x} \end{array}$$

### Sample solutions to Exercise 20.

#### 1. First method:

We define  $f : (0, 1) \times (0, 1) \rightarrow (0, 1)$  as follows. Let  $(x, y) \in (0, 1) \times (0, 1)$ .

Denote the proper decimal expansions of  $x$  and  $y$  by  $x = \sum_{k=1}^{+\infty} a_k 10^{-k} = 0.a_1 a_2 \dots$  where  $a_k \in \{0, 1, \dots, 9\}$

are not all equal to 0 and  $y = \sum_{k=1}^{+\infty} b_k 10^{-k} = 0.b_1 b_2 \dots$  similarly.

Then we set  $f(x, y) = \sum_{k=0}^{+\infty} a_k 10^{-(2k+1)} + \sum_{k=1}^{+\infty} b_k 10^{-2k} = 0.a_1 b_1 a_2 b_2 \dots = \sum_{k=1}^{+\infty} c_k 10^{-k}$  where

$$c_k = \begin{cases} a_n & \text{if } \exists n \in \mathbb{N} \setminus \{0\}, k = 2n \\ b_n & \text{if } \exists n \in \mathbb{N}, k = 2n + 1 \end{cases}$$

Then  $f$  a bijection by existence and uniqueness of the proper decimal expansion.

Hence  $|(0, 1) \times (0, 1)| = |(0, 1)|$ .

Since  $|(0, 1)| = |\mathbb{R}|$ , we get  $|\mathbb{R} \times \mathbb{R}| = |(0, 1) \times (0, 1)| = |(0, 1)| = |\mathbb{R}|$ .

#### Second method:

Define  $f : \mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N}) \rightarrow \mathcal{P}(\mathbb{N})$  by  $f(A, B) = \{2k : k \in A\} \cup \{2l + 1 : l \in B\}$ .

Then  $f$  is bijective (*prove it*).

Thus  $|\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N})|$ .

Since  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})|$ , we get  $|\mathbb{R} \times \mathbb{R}| = |\mathcal{P}(\mathbb{N}) \times \mathcal{P}(\mathbb{N})| = |\mathcal{P}(\mathbb{N})| = |\mathbb{R}|$ .

#### 2. Let's prove by induction on $n \in \mathbb{N} \setminus \{0\}$ that $|\mathbb{R}^n| = |\mathbb{R}|$ .

- *Base case at  $n = 1$ : then  $\mathbb{R}^1 = \mathbb{R}$  thus  $|\mathbb{R}^1| = |\mathbb{R}|$ .*
- *Inductive step: assume that  $|\mathbb{R}^n| = |\mathbb{R}|$  for some  $n \in \mathbb{N} \setminus \{0\}$ . Then*

$$\begin{aligned} |\mathbb{R}^{n+1}| &= |\mathbb{R}^n \times \mathbb{R}| \\ &= |\mathbb{R} \times \mathbb{R}| \quad \text{since } |\mathbb{R}^n| = |\mathbb{R}| \text{ and } |\mathbb{R}| = |\mathbb{R}| \\ &= |\mathbb{R}| \quad \text{by the previous question} \end{aligned}$$

#### 3. One idea here is to notice that $|\mathbb{R}^{\mathbb{N}}| = \left| \left( \{0, 1\}^{\mathbb{N}} \right)^{\mathbb{N}} \right| = |\{0, 1\}^{\mathbb{N} \times \mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}| = |\mathbb{R}|$ .

Since we have not covered arithmetic of cardinals, we need to prove each equality.

- Since  $|\mathbb{R}| = |\mathcal{P}(\mathbb{N})| = |\{0, 1\}^{\mathbb{N}}|$ , there exists a bijection  $\psi : \mathbb{R} \rightarrow \{0, 1\}^{\mathbb{N}}$ .  
We define  $\varphi : \mathbb{R}^{\mathbb{N}} \rightarrow (\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}$  by  $\varphi(f) = \psi \circ f : \mathbb{N} \rightarrow \{0, 1\}^{\mathbb{N}}$ .  
Then  $\varphi$  is a bijection (*check it*), and thus  $|\mathbb{R}^{\mathbb{N}}| = |(\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}|$ .
- We define  $\xi : \{0, 1\}^{\mathbb{N} \times \mathbb{N}} \rightarrow (\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}$  by  $\xi(f) : \begin{cases} \mathbb{N} & \rightarrow & \{0, 1\}^{\mathbb{N}} \\ n & \mapsto & (m \mapsto f(n, m)) \end{cases}$ .  
Check that  $\xi$  is a bijection. Therefore  $|(\{0, 1\}^{\mathbb{N}})^{\mathbb{N}}| = |\{0, 1\}^{\mathbb{N} \times \mathbb{N}}|$ .
- Since  $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}|$ , there exists a bijection  $\zeta : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ .  
We define  $\gamma : \{0, 1\}^{\mathbb{N}} \rightarrow \{0, 1\}^{\mathbb{N} \times \mathbb{N}}$  by  $\gamma(f) = f \circ \zeta$ .  
Check that  $\gamma$  is a bijection. Therefore  $|\{0, 1\}^{\mathbb{N} \times \mathbb{N}}| = |\{0, 1\}^{\mathbb{N}}|$ .

### Sample solutions to Exercise 21.

Define  $f : (0, 1) \rightarrow S^2$  by  $f(t) = (\cos t, \sin t, 0)$ . Then  $f$  is well-defined and injective.

Thus  $|\mathbb{R}| = |(0, 1)| \leq |S^2|$ .

Besides, since  $S^2 \subset \mathbb{R}^3$ , we have that  $|S^2| \leq |\mathbb{R}^3| = |\mathbb{R}|$ .

By Cantor–Schröder–Bernstein theorem, we get that  $|S^2| = |\mathbb{R}|$ .

### Sample solutions to Exercise 22.

A circle is characterized by its center and its radius. Therefore there is a bijection  $\mathbb{R}^2 \times (0, +\infty) \rightarrow S$  mapping  $(x, y, r)$  to the circle centered at  $(x, y)$  of radius  $r$ .

Thus  $|S| = |\mathbb{R}^2 \times (0, +\infty)|$ .

Since  $\exp : \mathbb{R} \rightarrow (0, +\infty)$  is a bijection, we have  $|(0, +\infty)| = |\mathbb{R}|$ . Hence  $|\mathbb{R}^2 \times (0, +\infty)| = |\mathbb{R}^3| = |\mathbb{R}|$ .

Therefore  $|S| = |\mathbb{R}|$ .

# Chapter 9

## Assessments (with solutions)

### Contents

Problem Set 1	138
Problem Set 2	142
Problem Set 3	145
Problem Set 4	148
Problem Set 5	152
Final exam	155

## Problem Set n°1

Jean-Baptiste Campesato

Due on February 5<sup>th</sup>, 2021

*Except otherwise stated, you can only use the material covered from Jan 12 to Jan 26 (i.e. Chapter 1 & Chapter 2 up to §3).*

### Exercise 1.

We define the binary relation  $<$  on  $\mathbb{N}^2$  by  $(x_1, y_1) < (x_2, y_2) \Leftrightarrow (x_1 < x_2 \text{ or } (x_1 = x_2 \text{ and } y_1 \leq y_2))$ .  
Is it an order? If so, is it total?

### Exercise 2.

Prove that given  $n \in \mathbb{N} \setminus \{0\}$  there exist finitely many  $\alpha_1, \dots, \alpha_m \in \mathbb{N}$  pairwise distinct such that

$$n = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$$

### Exercise 3.

Solve  $4x(x+1) = y(y+1)$  for  $(x, y) \in \mathbb{N}^2$ .

*Your answer can only rely on the properties of  $\mathbb{N}$  proved in Chapter 1.*

*Particularly, your proof should not involve negative integers, rationals, calculus...*

**Hint:** compare  $2x$  and  $y$ .

### Exercise 4.

Prove that for every  $n \geq 3$ , there exist  $x_1, \dots, x_n \in \mathbb{N} \setminus \{0\}$  pairwise distinct such that

$$1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}$$

*In this exercise, you may assume that you already know  $\mathbb{Q}$  or  $\mathbb{R}$  so that  $\frac{1}{x_i}$  is well-defined.*

**Hint:**  $1 = \frac{1}{2} + \frac{1}{2}$ .

**Sample solution to Exercise 1.**

We are going to prove that  $<$  is a total order on  $\mathbb{N}^2$ . It is actually called the *lexicographic order*.

It is the one used in dictionaries: you compare the first letter, if it is the same, then you look at the next one...

- *Reflexivity.* Let  $(x, y) \in \mathbb{N}^2$ . Then  $x = x$  and  $y \leq y$ . Thus  $(x, y) < (x, y)$ .
- *Antisymmetry.* Let  $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$  satisfying  $(x_1, y_1) < (x_2, y_2)$  and  $(x_2, y_2) < (x_1, y_1)$ . Assume by contradiction that  $x_1 < x_2$ , then  $(x_2, y_2) \not< (x_1, y_1)$ . Which is a contradiction. Assume by contradiction that  $x_2 < x_1$ , then  $(x_1, y_1) \not< (x_2, y_2)$ . Which is a contradiction. Thus  $x_1 = x_2$ . Since  $(x_1, y_1) < (x_2, y_2)$ , we know that  $y_1 \leq y_2$ . Since  $(x_2, y_2) < (x_1, y_1)$ , we know that  $y_2 \leq y_1$ . Thus  $y_1 = y_2$ . We proved that  $(x_1, y_1) = (x_2, y_2)$ .
- *Transitivity.* Let  $(x_1, y_1), (x_2, y_2), (x_3, y_3) \in \mathbb{N}^2$  satisfying  $(x_1, y_1) < (x_2, y_2)$  and  $(x_2, y_2) < (x_3, y_3)$ .
  - Case 1:  $x_1 = x_2$  and  $x_2 = x_3$ . Then  $x_1 = x_3$ . Furthermore  $y_1 \leq y_2$  and  $y_2 \leq y_3$ , so  $y_1 \leq y_3$ . Hence  $(x_1, y_1) < (x_3, y_3)$ .
  - Case 2:  $x_1 = x_2$  and  $x_2 < x_3$ . Then  $x_1 < x_3$ . Hence  $(x_1, y_1) < (x_3, y_3)$ .
  - Case 3:  $x_1 < x_2$  and  $x_2 = x_3$ . Then  $x_1 < x_3$ . Hence  $(x_1, y_1) < (x_3, y_3)$ .
  - Case 4:  $x_1 < x_2$  and  $x_2 < x_3$ . Then  $x_1 < x_3$ . Hence  $(x_1, y_1) < (x_3, y_3)$ .
- *$<$  is a total order.* Let  $(x_1, y_1), (x_2, y_2) \in \mathbb{N}^2$ . According to the lectures, exactly one of the follows occurs.
  - Case 1:  $x_1 < x_2$ . Then  $(x_1, y_1) < (x_2, y_2)$ .
  - Case 2:  $x_2 < x_1$ . Then  $(x_2, y_2) < (x_1, y_1)$ .
  - Case 3:  $x_1 = x_2$ . Since  $\leq$  is a total order on  $\mathbb{N}$  then
    - \* either  $y_1 \leq y_2$  and then  $(x_1, y_1) < (x_2, y_2)$
    - \* or  $y_2 \leq y_1$  and then  $(x_2, y_2) < (x_1, y_1)$ .

**Sample solution to Exercise 2.**

That's the existence of the positional numeral system with base 2 (binary numeral system).

**Method 1:**

We are going to prove by strong induction that for every  $n \geq 1$ , there exist finitely many  $\alpha_1, \dots, \alpha_m \in \mathbb{N}$  pairwise distinct such that  $n = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$ .

- *Base case at  $n = 1$ .*  $1 = 2^0$ .
- *Induction step.* Assume that the statement holds for  $1, 2, \dots, n$  where  $n \geq 1$ . By Euclidean division,  $n + 1 = 2q + r$  where  $q \in \mathbb{N}$  and  $r \in \{0, 1\}$ . Note that  $q \neq 0$  since otherwise  $1 < n + 1 = r \leq 1$ . Hence  $1 \leq q < 2q + r = n + 1$ . Thus, by the induction hypothesis,  $q = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$  where  $\alpha_1 > \alpha_2 > \dots > \alpha_m$  are natural numbers. Therefore  $n + 1 = 2q + r = 2^{\alpha_1+1} + 2^{\alpha_2+1} + \dots + 2^{\alpha_m+1} + r2^0$ . Note that  $\alpha_1 + 1 > \alpha_2 + 1 > \dots > \alpha_m + 1 > 0$ . Hence the exponents are pairwise distinct (it is possible for  $2^0$  to not appear if  $r = 0$ ). Which ends the induction step.

**Method 2:**

We are going to prove by strong induction that for every  $n \geq 1$ , there exist finitely many  $\alpha_1, \dots, \alpha_m \in \mathbb{N}$  pairwise distinct such that  $n = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$ .

- *Base case at  $n = 1$ .*  $1 = 2^0$ .
- *Induction step.* Assume that the statement holds for  $1, 2, \dots, n$  where  $n \geq 1$ .
  - (i) First case:  $n + 1$  is even. Then  $n + 1 = 2k$  for some  $k \in \mathbb{N}$ .  
 Note that  $k \neq 0$  since otherwise  $1 \leq n + 1 = 2k = 0$ .  
 Since  $k \neq 0$ , we get that  $k < 2k = n + 1$ , i.e.  $k \leq n$ .  
 Thus, by the induction hypothesis,  $k = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$  where the  $\alpha_1, \dots, \alpha_m \in \mathbb{N}$  are pairwise distinct.  
 So  $n + 1 = 2 \times (2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}) = 2^{\alpha_1+1} + 2^{\alpha_2+1} + \dots + 2^{\alpha_m+1}$ .  
 Assume by contradiction that there exist  $i \neq j$  such that  $\alpha_i + 1 = \alpha_j + 1$ . Then, by the cancellation rule,  $\alpha_i = \alpha_j$ . Which is a contradiction since the  $\alpha_i$  are pairwise distinct.  
 Therefore the  $\alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_m + 1$  are pairwise distinct as requested.
  - (ii) Second case:  $n + 1$  is odd. Then  $n + 1 = 2k + 1$  for some  $k \in \mathbb{N}$ .  
 Note that  $k \neq 0$  since otherwise  $n + 1 = 2 \times 0 + 1 = 1 \implies n = 0$ . Hence, as above,  $k < 2k = n$ .  
 Thus, by the induction hypothesis,  $k = 2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}$  where the  $\alpha_1, \dots, \alpha_m \in \mathbb{N}$  are pairwise distinct.  
 Hence  $n + 1 = 1 + 2k = 2^0 + 2 \times (2^{\alpha_1} + 2^{\alpha_2} + \dots + 2^{\alpha_m}) = 2^0 + 2^{\alpha_1+1} + 2^{\alpha_2+1} + \dots + 2^{\alpha_m+1}$ .  
 As above, the  $\alpha_i + 1$  are pairwise distinct. Moreover  $\alpha_i + 1 > 0$ . Therefore the  $0, \alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_m + 1$  are pairwise distinct, as requested.

Which ends the induction step.

**Sample solution to Exercise 3.**

Let  $(x, y) \in \mathbb{N}^2$  be such that  $4x(x + 1) = y(y + 1)$ .

1. *First case: assume that  $y \leq 2x$ .* Then

$$y(y + 1) \leq 2x(2x + 1) \leq 2x(2x + 2) = 4x(x + 1) = y(y + 1)$$

Hence  $2x(2x + 1) \leq 2x(2x + 2)$  and  $2x(2x + 2) = y(y + 1) \leq 2x(2x + 1)$ .

Thus  $2x(2x + 1) = 2x(2x + 2)$ , from which we get that  $x(2x + 1) = x(2x + 2)$ .

- Either  $x = 0$  and then  $y \leq 0$  so  $y = 0$ .
- Or  $x \neq 0$  and then, by cancellation, we get  $2x + 1 = 2x + 2$ .  
 We derive from the previous equality that  $1 = 2$ , which is impossible.

Thus the only possible solution in this case is  $(x, y) = (0, 0)$ .

2. *Second case: assume that  $2x < y$ , i.e.  $2x + 1 \leq y$ .* Then

$$y(y + 1) \geq (2x + 1)(2x + 2) \geq 2x(2x + 2) = y(y + 1)$$

Hence, as above,  $(2x + 1)(2x + 2) = 2x(2x + 2)$ .

Note that  $2x + 2 \neq 0$  since  $2x + 2 \geq 2 > 0$ .

So, by cancellation,  $2x = 2x + 1$  and hence  $0 = 1$ , which is impossible.

Therefore there is no solution  $(x, y) \in \mathbb{N}^2$  satisfying  $2x < y$ .

We proved that the only possible solution is  $(x, y) = (0, 0)$ .

We have to check that conversely it is a solution, which is the case since then  $4x(x + 1) = 0 = y(y + 1)$ .

So the only solution is  $(x, y) = (0, 0)$ .

**Sample solution to Exercise 4.****Method 1 (using my hint):**

We are going to prove the statement by induction on  $n$ .

- *Base case at  $n = 3$ .* Note that  $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$
- *Induction step.* Assume that the statement holds for some  $n \geq 3$ .  
By the induction hypothesis, there exist  $x_1 < \dots < x_n$  in  $\mathbb{N} \setminus \{0\}$  such that  $1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}$ .  
Note that  $x_1 \neq 1$  since otherwise  $\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = 1 + \frac{1}{x_2} + \dots + \frac{1}{x_n} > 1$ . Thus  $x_1 > 1$ .  
Hence  $1 = \frac{1}{2} + \frac{1}{2} = \frac{1}{2} + \frac{1}{2} \left( \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} \right) = \frac{1}{2} + \frac{1}{2x_1} + \frac{1}{2x_2} + \dots + \frac{1}{2x_n}$ .  
Besides, since  $1 < x_1 < x_2 < \dots < x_n$ , we get that  $2 < 2x_1 < 2x_2 < \dots < 2x_n$ .  
So the  $n + 1$  denominators are pairwise distinct.

**Method 2:**

We are going to prove the following stronger statement by induction on  $n$ : for  $n \geq 3$ , there exist  $1 < x_1 < x_2 < \dots < x_n$  such that  $1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}$  and  $x_n$  is even.

- *Base case at  $n = 3$ .* Note that  $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$
- *Induction step.* Assume that the statement holds for some  $n \geq 3$ .  
By the induction hypothesis, there exist  $1 < x_1 < \dots < x_n$  in  $\mathbb{N}$  such that  $1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}$  and  $x_n$  is even.  
Hence  $x_n = 2k$  for some  $k \in \mathbb{N} \setminus \{0\}$ .  
Note that  $\frac{1}{x_n} = \frac{1}{2k} = \frac{1}{3k} + \frac{1}{6k}$ .  
Hence
$$1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_{n-1}} + \frac{1}{3k} + \frac{1}{6k}$$
  
Besides  $6k$  is even and  $1 < x_1 < x_2 < \dots < x_n = 2k < 3k < 6k$ .  
So the  $n + 1$  denominators are pairwise distinct.

**Method 3:**

We are going to prove the statement by induction on  $n$ .

- *Base case at  $n = 3$ .* Note that  $1 = \frac{1}{2} + \frac{1}{3} + \frac{1}{6}$
- *Induction step.* Assume that the statement holds for some  $n \geq 3$ .  
By the induction hypothesis, there exist  $x_1 < \dots < x_n$  in  $\mathbb{N} \setminus \{0\}$  such that  $1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n}$ .  
Note that  $x_1 \neq 1$  since otherwise  $\frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_n} = 1 + \frac{1}{x_2} + \dots + \frac{1}{x_n} > 1$ . Thus  $x_1 > 1$ .  
Note that for  $x \neq 0$ ,  $\frac{1}{x(x+1)} + \frac{1}{x+1} = \frac{x+1}{x(x+1)} = \frac{1}{x}$ .  
Therefore
$$1 = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_{n-1}} + \frac{1}{x_n} = \frac{1}{x_1} + \frac{1}{x_2} + \dots + \frac{1}{x_{n-1}} + \frac{1}{x_n+1} + \frac{1}{x_n(x_n+1)}$$
  
Since  $1 < x_n$  and  $0 < x_n + 1$ , we get  $x_n + 1 < x_n(x_n + 1)$ .  
Therefore  $1 < x_1 < x_2 < \dots < x_{n-1} < x_n < x_n + 1 < x_n(x_n + 1)$ .  
So the  $n + 1$  denominators are pairwise distinct.

## Problem Set n°2

Jean-Baptiste Campesato

Due on February 26<sup>th</sup>, 2021

*Except otherwise stated, you can only use the material covered in Chapters 1, 2 & 3.*

*You can also use the results proved in the exercise sheets 1, 2, 3 & 4.*

*Write your solutions concisely but without skipping important steps.*

*Make sure that your submission is readable on Crowdmark.*

### Exercise 1.

Find all  $n \in \mathbb{Z}$  such that  $n - 4 \mid 3n - 17$ .

### Exercise 2.

Find the integer solutions of  $x^2 + 6x = y^2 + 12$ .

### Exercise 3.

1. Prove that

$$\forall a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}, (\gcd(a, x_1) = \gcd(a, x_2) = 1) \implies \gcd(a, x_1 x_2) = 1$$

2. Let  $n \geq 2$  be an integer. Prove that

$$\forall a, x_1, \dots, x_n \in \mathbb{Z} \setminus \{0\}, (\gcd(a, x_1) = \gcd(a, x_2) = \dots = \gcd(a, x_n) = 1) \implies \gcd(a, x_1 x_2 \dots x_n) = 1$$

### Exercise 4.

Prove that the equation  $x^3 - x^2 + x + 1 = 0$  has no rational solution.

*For this question, you can assume that  $\mathbb{Q} = \left\{ \frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N} \setminus \{0\}, \gcd(p, q) = 1 \right\}$  with the usual operations.*



**Sample solution to Exercise 1.**

Let  $n \in \mathbb{Z}$  such that  $n - 4 \mid 3n - 17$ .

Since  $n - 4 \mid n - 4$  and  $n - 4 \mid 3n - 17$  then  $n - 4 \mid (3n - 17) - 3(n - 4) = -5$ .

Hence the only possible solutions are  $n - 4 = -5, -1, 1, 5$ , i.e.  $n = -1, 3, 5, 9$ .

Conversely, we need to check which are solutions:

- $n = -1$ : then  $n - 4 = -5$  and  $3n - 17 = -20$ . So it is a solution since  $-5 \mid -20$
- $n = 3$ : then  $n - 4 = -1$ . So it is a solution since  $-1$  divides any integer.
- $n = 5$ : then  $n - 4 = 1$ . So it is a solution since  $1$  divides any integer.
- $n = 9$ : then  $n - 4 = 5$  and  $3n - 17 = 10$ . So it is a solution since  $5 \mid 10$ .

**Sample solution to Exercise 2.**

Let  $x, y \in \mathbb{Z}$ , then

$$x^2 + 6x = y^2 + 12 \Leftrightarrow (x + 3)^2 = y^2 + 21 \Leftrightarrow (x + 3)^2 - y^2 = 21 \Leftrightarrow (x + y + 3)(x - y + 3) = 21$$

Since the divisors of 21 are  $\pm 1, \pm 3, \pm 7$  and  $\pm 21$ , we get the following cases:

1.  $\begin{cases} x + y + 3 = 21 \\ x - y + 3 = 1 \end{cases} \Leftrightarrow (x, y) = (8, 10)$
2.  $\begin{cases} x + y + 3 = -21 \\ x - y + 3 = -1 \end{cases} \Leftrightarrow (x, y) = (-14, -10)$
3.  $\begin{cases} x + y + 3 = 7 \\ x - y + 3 = 3 \end{cases} \Leftrightarrow (x, y) = (2, 2)$
4.  $\begin{cases} x + y + 3 = -7 \\ x - y + 3 = -3 \end{cases} \Leftrightarrow (x, y) = (-8, -2)$
5.  $\begin{cases} x + y + 3 = 3 \\ x - y + 3 = 7 \end{cases} \Leftrightarrow (x, y) = (2, -2)$
6.  $\begin{cases} x + y + 3 = -3 \\ x - y + 3 = -7 \end{cases} \Leftrightarrow (x, y) = (-8, 2)$
7.  $\begin{cases} x + y + 3 = 1 \\ x - y + 3 = 21 \end{cases} \Leftrightarrow (x, y) = (8, -10)$
8.  $\begin{cases} x + y + 3 = -1 \\ x - y + 3 = -21 \end{cases} \Leftrightarrow (x, y) = (-14, 10)$

Hence the integer solutions are  $(8, \pm 10), (-14, \pm 10), (2, \pm 2), (-8, \pm 2)$ .

**Sample solution to Exercise 3.****1. Method 1 (with Bézout's theorem):**

Let  $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$  be such that  $\gcd(a, x_1) = \gcd(a, x_2) = 1$ .

By Bézout's identity, there exist  $u, v, u', v' \in \mathbb{Z}$  such that  $au + x_1v = 1$  and  $au' + x_2v' = 1$ .

Then  $1 = (au + x_1v)(au' + x_2v') = a(auu' + ux_2v' + x_1vu') + x_1x_2(vv')$ .

Therefore  $\gcd(a, x_1x_2) = 1$ .

**Method 2 (with Euclid's lemma):**

Let  $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$  be such that  $\gcd(a, x_1) = \gcd(a, x_2) = 1$ .

Assume by contradiction that  $d = \gcd(a, x_1x_2) > 1$ , then there exists a prime number  $p$  such that  $p|d$ .

Since  $p|d$  and  $d|a$ , we have that  $p|a$ .

Since  $p|d$  and  $d|x_1x_2$ , we have that  $p|x_1x_2$ .

By Euclid's lemma, either  $p|x_1$  or  $p|x_2$ . WLOG, we may assume that  $p|x_1$ .

Then  $p|x_1$  and  $p|a$ , therefore  $p|\gcd(a, x_1) = 1$ . Which is a contradiction.

**Method 3 (with prime factorization):**

Let  $a, x_1, x_2 \in \mathbb{Z} \setminus \{0\}$  be such that  $\gcd(a, x_1) = \gcd(a, x_2) = 1$ .

Write the prime decompositions  $a = \prod_p p^{\alpha_p}$ ,  $x_1 = \prod_p p^{\beta_{1p}}$  and  $x_2 = \prod_p p^{\beta_{2p}}$ .

Since  $\gcd(a, x_i) = 1$ , we know that, for  $p$  prime, we have  $\min(\alpha_p, \beta_{ip}) = 0$ .

Therefore, for  $p$  prime, we have  $\min(\alpha_p, \beta_{1p} + \beta_{2p}) \leq \min(\alpha_p, \beta_{1p}) + \min(\alpha_p, \beta_{2p}) = 0$ .

Note that  $x_1x_2 = \prod_p p^{\beta_{1p} + \beta_{2p}}$ .

Thus  $\gcd(a, x_1x_2) = \prod_p p^{\min(\alpha_p, \beta_{1p} + \beta_{2p})} = 1$ .

**2. Let's prove by induction on  $n \geq 2$  that**

$$\forall a, x_1, \dots, x_n \in \mathbb{Z} \setminus \{0\}, (\gcd(a, x_1) = \gcd(a, x_2) = \dots = \gcd(a, x_n) = 1) \implies \gcd(a, x_1x_2 \dots x_n) = 1$$

- **Base case at  $n = 2$ :** it is exactly the previous question.

- **Induction step.** Assume that the statement holds for some  $n \geq 2$ .

Let  $a, x_1, \dots, x_n, x_{n+1} \in \mathbb{Z} \setminus \{0\}$  such that  $\gcd(a, x_1) = \gcd(a, x_2) = \dots = \gcd(a, x_{n+1}) = 1$ .

By the induction hypothesis,  $\gcd(a, x_1x_2 \dots x_n) = 1$ .

Since

$$\gcd(a, x_1x_2 \dots x_n) = \gcd(a, x_{n+1}) = 1$$

by the previous question, we get that

$$\gcd(a, x_1x_2 \dots x_{n+1}) = 1$$

Which proves the induction step.

**Sample solution to Exercise 4.**

Assume by contradiction that there exists  $x \in \mathbb{Q}$  such that  $x^3 - x^2 + x + 1 = 0$ .

Then  $x = \frac{p}{q}$  where  $p \in \mathbb{Z}$ ,  $q \in \mathbb{N} \setminus \{0\}$  and  $\gcd(p, q) = 1$ .

Therefore  $x^3 - x^2 + x + 1 = 0$  implies  $(p/q)^3 - (p/q)^2 + p/q + 1 = 0$  from which we derive that  $p^3 - p^2q + pq^2 + q^3 = 0$ .

Hence  $p|q^3 = -p^3 + p^2q - pq^2$ .

Since  $\gcd(p, q) = 1$ , by Gauss' lemma,  $p|q^2$  and similarly  $p|q$ .

Hence  $\gcd(p, q) = |p|$ . So either  $p = -1$  or  $p = 1$ .

Similarly  $q|p^3 = p^2q - pq^2 - q^3$  so  $q = 1$ .

Thence the only possible rational solutions are  $-1$  and  $1$ .

But they don't satisfy the equation.

## Problem Set n°3

Jean-Baptiste Campesato

Due on March 12<sup>th</sup>, 2021

*You can only use the material covered in class up to lecture 12 (i.e. Chapters 1, 2, 3 and 4 up to section 5 included). Write your solutions concisely but without skipping important steps. Make sure that your submission is readable on Crowdmark.*

### Exercise 1.

Let  $p$  be a prime number. Prove that

$$\forall s \in \mathbb{N} \setminus \{0\}, \forall n \in \mathbb{N} \setminus \{0\}, \forall x_1, \dots, x_n \in \mathbb{Z}, \left( \sum_{k=1}^n x_k \right)^{p^s} \equiv \sum_{k=1}^n x_k^{p^s} \pmod{p}$$

### Exercise 2.

The following questions are independent.

1. For which  $n \in \mathbb{N}$ , is  $5^n - 3^n$  a prime number?
2. For which  $n \in \mathbb{N}$ , is  $2^{2^n} + 5$  a prime number?

### Exercise 3.

Solve for  $x, y \in \mathbb{N} \setminus \{0\}$ ,  $\sum_{k=1}^x (k!) = y^2$ .

### Exercise 4.

Let  $p$  be a prime number and  $n \in \mathbb{N}$  satisfying  $1 \leq n \leq p-1$ .  
Prove that  $(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$ .

**Sample solution to Exercise 1.****Method 1:**

Let's prove the statement by induction on  $s \geq 1$ .

- *Base case at  $s = 1$ :*

Let  $n \in \mathbb{N} \setminus \{0\}$  and  $x_1, \dots, x_n \in \mathbb{Z}$ .

By Fermat's theorem we have:

- $\left(\sum_{k=1}^n x_k\right)^p \equiv \sum_{k=1}^n x_k \pmod{p}$ , and,
- For  $k = 1, \dots, n$ ,  $x_k^p \equiv x_k \pmod{p}$ .

$$\text{Thus } \left(\sum_{k=1}^n x_k\right)^p \equiv \sum_{k=1}^n x_k \pmod{p} \equiv \sum_{k=1}^n x_k^p \pmod{p}$$

- *Induction step:* assume that the statement of the question holds for some  $s \geq 1$ .

Let  $n \in \mathbb{N} \setminus \{0\}$  and  $x_1, \dots, x_n \in \mathbb{Z}$ .

Then

$$\begin{aligned} \left(\sum_{k=1}^n x_k\right)^{p^{s+1}} &= \left(\left(\sum_{k=1}^n x_k\right)^{p^s}\right)^p \\ &\equiv \left(\sum_{k=1}^n x_k^{p^s}\right)^p \pmod{p} \quad \text{by induction hypothesis} \\ &\equiv \sum_{k=1}^n \left(x_k^{p^s}\right)^p \pmod{p} \quad \text{by the case } s = 1 \\ &\equiv \sum_{k=1}^n x_k^{p^{s+1}} \pmod{p} \end{aligned}$$

**Method 2:**

**Lemma.** Let's first prove by induction on  $s$  that  $\forall s \in \mathbb{N} \setminus \{0\}, \forall x \in \mathbb{Z}, x^{p^s} \equiv x \pmod{p}$ .

- *Base case at  $s = 1$ :* Let  $x \in \mathbb{Z}$  then  $x^p \equiv x \pmod{p}$  by Fermat's theorem.
- *Induction step:* assume that the statement of the question holds for some  $s \geq 1$ .

Let  $x \in \mathbb{Z}$  then

$$\begin{aligned} x^{p^{s+1}} &= \left(x^{p^s}\right)^p \\ &\equiv x^p \pmod{p} \quad \text{by the inductive hypothesis} \\ &\equiv x \pmod{p} \quad \text{by Fermat's theorem} \end{aligned}$$

Which proves the lemma.

Let's prove the statement of the question:

Let  $s \in \mathbb{N} \setminus \{0\}, x_1, \dots, x_n \in \mathbb{Z}$  then

$$\begin{aligned} \left(\sum_{k=1}^n x_k\right)^{p^s} &= \sum_{k=1}^n x_k \quad \text{by the lemma} \\ &= \sum_{k=1}^n x_k^{p^s} \quad \text{by the lemma} \end{aligned}$$

**Sample solution to Exercise 2.**

1. If  $n = 0$  then  $5^0 - 3^0 = 0$  is not prime.

If  $n = 1$  then  $5^1 - 3^1 = 2$  is prime.

If  $n > 1$  then  $5^n - 3^n \equiv 1^n - 1^n \pmod{2} \equiv 0 \pmod{2}$ . Thus  $5^n - 3^n$  is even but  $5^n - 3^n > 2$ , therefore it is not prime.

**Conclusion:**  $5^n - 3^n$  is prime for  $n = 1$  only.

2. If  $n = 0$  then  $2^{2^0} + 5 = 2^1 + 5 = 7$  is prime.

If  $n \geq 1$  then  $2^{2^n} + 5 \equiv (-1)^{2^n} + 2 \pmod{3} \equiv 1 + 2 \pmod{3} \equiv 0 \pmod{3}$  (since  $2^n$  is even as  $n \geq 1$ ).

Therefore  $3 \mid 2^{2^n} + 5$  but  $2^{2^n} + 5 > 3$ . Thus  $2^{2^n} + 5$  is not prime.

**Conclusion:**  $2^{2^n} + 5$  is prime for  $n = 0$  only.

**Sample solution to Exercise 3.**

We first compute  $y^2 \pmod{5}$  in terms of  $y \pmod{5}$ :

$y \pmod{5}$	0	1	2	3	4
$y^2 \pmod{5}$	0	1	4	4	1

We treat several cases.

1. Let  $x = 1$  then  $\sum_{k=1}^x (k!) = 1$ .

The unique  $y \in \mathbb{N} \setminus \{0\}$  such that  $y^2 = 1$  is  $y = 1$ .

2. Let  $x = 2$  then  $\sum_{k=1}^x (k!) = 1! + 2! \equiv 3 \pmod{5}$ .

So there exists no  $y \in \mathbb{Z}$  such that  $\sum_{k=1}^2 (k!) = y^2$  by the above table.

3. Let  $x = 3$  then  $\sum_{k=1}^x (k!) = 1! + 2! + 3! = 9$ .

The unique  $y \in \mathbb{N} \setminus \{0\}$  such that  $y^2 = 9$  is  $y = 3$ .

4. Let  $x \geq 4$ .

Note that for  $k \geq 5$ , we have  $5 \mid k!$ .

Thus  $\sum_{k=1}^x (k!) \equiv 1! + 2! + 3! + 4! \pmod{5} \equiv 33 \pmod{5} \equiv 3 \pmod{5}$ .

So there exists no  $y \in \mathbb{Z}$  such that  $\sum_{k=1}^x (k!) = y^2$  when  $x \geq 4$ , by the above table.

So the solutions are  $(x, y) = (1, 1)$  and  $(x, y) = (3, 3)$ .

**Sample solution to Exercise 4.**

Let  $p$  be a prime number and  $n \in \mathbb{N}$  satisfying  $1 \leq n \leq p-1$ .

Note that

$$\begin{aligned}
 (p-1)! &= (p-n)!(p-(n-1))(p-(n-2)) \cdots (p-1) \\
 &\equiv (p-n)!(- (n-1))(- (n-2)) \cdots (-1) \pmod{p} \\
 &\equiv (p-n)!(-1)^{n-1}(n-1)(n-2) \cdots 1 \pmod{p} \\
 &\equiv (p-n)!(-1)^{n-1}(n-1)! \pmod{p}
 \end{aligned}$$

Since, by Wilson's theorem,  $(p-1)! \equiv -1 \pmod{p}$ , we get that  $(p-n)!(-1)^{n-1}(n-1)! \equiv -1 \pmod{p}$  and thus, multiplying both side by  $(-1)^{n-1}$ , that  $(p-n)!(n-1)! \equiv (-1)^n \pmod{p}$ .

## Problem Set n°4

Jean-Baptiste Campesato

Due on March 28<sup>th</sup>, 2021

*You can only use the material covered in class up to lecture 17 (i.e. up to Chapter 6, §4).*

*Write your solutions concisely but without skipping important steps.*

*Make sure that your submission is readable on Crowdmark.*

### Exercise 1.

Prove that  $\forall a, b \in \mathbb{N} \setminus \{0\}, \varphi(ab)\varphi(\gcd(a, b)) = \varphi(a)\varphi(b) \gcd(a, b)$ .

*Make sure to explain each step.*

### Exercise 2.

Alice posted her RSA public key on her website:  $(n, e) = (4559, 17)$ .

1. Eve wants to spy on Alice: help her to find a suitable private key  $(n, d)$ .
2. Eve intercepts the ciphered message  $c = 2741$  that Bob sent to Alice. What is the original message?

*You may use a computer to compute modular exponentiations, nonetheless, you need to explain your steps.*

*You can use the list of prime numbers less than 100 given in the lecture notes.*

### Exercise 3.

1. Let  $x \in \mathbb{R}$ . Compute  $\lim_{n \rightarrow +\infty} \frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2}$ .
2. Use the above question to prove that any real number is the limit of a sequence of rational numbers.

*For this question, you can use results about sequences from your first year calculus course.*

### Exercise 4.

Let  $A, B \subset \mathbb{R}$  be such that  $\inf(A)$  and  $\sup(B)$  exist.

1. Prove that if  $\inf(A) = \sup(B)$  then  $A \cap B$  contains at most one element.
2. Under the assumption that  $\inf(A) = \sup(B)$ , is it possible for  $A \cap B$  to be empty?  
*You need to justify your answer.*

**Sample solution to Exercise 1.****Method 1:**

Let  $a, b \in \mathbb{N} \setminus \{0\}$ . Write the prime factorization of  $\gcd(a, b)$  as

$$\gcd(a, b) = \prod_{i=1}^r p_i^{\delta_i}$$

where  $r \in \mathbb{N}$ , the  $p_i$  are pairwise distinct prime numbers and  $\delta_i \in \mathbb{N} \setminus \{0\}$ . We set  $r = 0$  when  $\gcd(a, b) = 1$ . Since  $\gcd(a, b) | a$ , we may write

$$a = \prod_{i=1}^r p_i^{\delta_i + \gamma_i} \prod_{j=1}^s q_j^{\alpha_j}$$

where  $s \in \mathbb{N}$ , the  $q_j$  are prime numbers such that the  $p_i, q_j$  are pairwise distinct,  $\gamma_i \in \mathbb{N}$  and  $\alpha_j \in \mathbb{N} \setminus \{0\}$ . We allow  $s = 0$ , with the convention that the product is then equal to 1.

Since  $\gcd(a, b) | b$ , we may write

$$b = \prod_{i=1}^r p_i^{\delta_i + \tilde{\gamma}_i} \prod_{k=1}^t m_k^{\beta_k}$$

where  $t \in \mathbb{N}$ , the  $m_k$  are prime numbers such that the  $p_i, m_k$  are pairwise distinct,  $\tilde{\gamma}_i \in \mathbb{N}$  and  $\beta_k \in \mathbb{N} \setminus \{0\}$ . We allow  $t = 0$ , with the convention that the product is then equal to 1.

Note that  $\{q_1, \dots, q_s\} \cap \{m_1, \dots, m_t\} = \emptyset$  since otherwise a common prime number would divide  $\gcd(a, b)$ . Then the prime factorization of  $ab$  is

$$ab = \prod_{i=1}^r p_i^{\delta_i + \gamma_i + \tilde{\gamma}_i} \prod_{j=1}^s q_j^{\alpha_j} \prod_{k=1}^t m_k^{\beta_k}$$

where the  $p_i, q_j, m_k$  are pairwise distinct prime numbers.

As seen in class, we have

$$\varphi(\gcd(a, b)) = \gcd(a, b) \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right)$$

$$\varphi(a) = a \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right)$$

$$\varphi(b) = b \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{k=1}^t \left(1 - \frac{1}{m_k}\right)$$

$$\varphi(ab) = ab \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right) \prod_{k=1}^t \left(1 - \frac{1}{m_k}\right)$$

Therefore

$$\begin{aligned} \varphi(ab)\varphi(\gcd(a, b)) &= ab \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right) \prod_{k=1}^t \left(1 - \frac{1}{m_k}\right) \gcd(a, b) \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \\ &= \left( a \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{j=1}^s \left(1 - \frac{1}{q_j}\right) \right) \left( b \prod_{i=1}^r \left(1 - \frac{1}{p_i}\right) \prod_{k=1}^t \left(1 - \frac{1}{m_k}\right) \right) \gcd(a, b) \\ &= \varphi(a)\varphi(b) \gcd(a, b) \end{aligned}$$

**Method 2:**

Let  $a, b \in \mathbb{N} \setminus \{0\}$ . Given a prime divisor  $p$  of  $ab$ , by Euclid's lemma, exactly one of the following occurs:

- Either  $p$  divides  $a$  but not  $b$ ,
- Or  $p$  divides  $b$  but not  $a$ ,
- Or  $p$  divides both  $a$  and  $b$ , i.e.  $p \mid \gcd(a, b)$ .

According to the lecture notes,

$$\varphi(ab) = ab \prod_{\substack{p \text{ prime,} \\ p \mid ab}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(a) = a \prod_{\substack{p \text{ prime,} \\ p \mid a}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(b) = b \prod_{\substack{p \text{ prime,} \\ p \mid b}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(\gcd(a, b)) = \gcd(a, b) \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right)$$

Therefore

$$\begin{aligned} \varphi(ab) &= ab \prod_{\substack{p \text{ prime,} \\ p \mid ab}} \left(1 - \frac{1}{p}\right) \\ &= ab \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \nmid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p \nmid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right) \\ &= \frac{\left( a \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \nmid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right) \right) \left( b \prod_{\substack{p \text{ prime,} \\ p \nmid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right) \right)}{\prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right)} \\ &= \frac{\left( a \prod_{\substack{p \text{ prime,} \\ p \mid a}} \left(1 - \frac{1}{p}\right) \right) \left( b \prod_{\substack{p \text{ prime,} \\ p \mid b}} \left(1 - \frac{1}{p}\right) \right)}{\prod_{\substack{p \text{ prime,} \\ p \mid a \text{ and } p \mid b}} \left(1 - \frac{1}{p}\right)} \\ &= \gcd(a, b) \frac{\varphi(a)\varphi(b)}{\varphi(\gcd(a, b))} \end{aligned}$$



**Sample solution to Exercise 2.**

1. Note that  $n = 4559 = 47 \times 97$  where 47 and 97 are prime numbers (see Example 3 of Chapter 3). Therefore  $\varphi(n) = (47 - 1)(97 - 1) = 46 \times 96 = 4416$ .  
Let's find a Bézout's identity for  $\varphi(n) = 4416$  and  $e = 17$ :

$$4416 = 17 \times 259 + 13$$

$$17 = 13 \times 1 + 4$$

$$13 = 4 \times 3 + 1$$

Therefore

$$1 = 13 - 4 \times 3 = 13 - (17 - 13) \times 3 = 17 \times (-3) + 13 \times 4 = 17 \times (-3) + (4416 - 17 \times 259) \times 4 = 17 \times (-1039) + 4416 \times 4$$

Thus, if we set  $d = -1039 + 4416 = 3377$  then  $d > 0$  and  $ed \equiv 1 \pmod{\varphi(n)}$ :

$$ed = 17 \times (-1039 + 4416) \equiv 17 \times (-1039) + 4416 \times 4 \pmod{4416} \equiv 1 \pmod{4416}$$

Thus  $(n, d) = (4559, 3377)$  is a suitable private key.

2.  $c^e = 2741^{3377} \equiv 2718 \pmod{4559}$ , then  $m = 2718$  is the original message since  $m \in \{0, 1, \dots, 4558\}$ .

**Sample solution to Exercise 3.**

1. Since  $\forall k \in \mathbb{N}$ ,  $\lfloor kx \rfloor \leq kx < \lfloor kx \rfloor + 1$ , we get

$$\frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2} \leq \frac{\sum_{k=1}^n kx}{n^2} = x \frac{n(n+1)}{2n^2} = x \frac{n+1}{2n}$$

and

$$\frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2} > \frac{\sum_{k=1}^n (kx - 1)}{n^2} = x \frac{n+1}{2n} - \frac{1}{n}$$

Therefore

$$x \frac{n+1}{2n} - \frac{1}{n} < \frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2} \leq x \frac{n+1}{2n}$$

Since  $\lim_{n \rightarrow +\infty} x \frac{n+1}{2n} - \frac{1}{n} = \lim_{n \rightarrow +\infty} x \frac{n+1}{2n} = \frac{x}{2}$ , we get from the Squeeze Theorem that

$$\lim_{n \rightarrow +\infty} \frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2} = \frac{x}{2}$$

2. Let  $x \in \mathbb{R}$ . For  $n \in \mathbb{N} \setminus \{0\}$ , set  $u_n = 2 \frac{\sum_{k=1}^n \lfloor kx \rfloor}{n^2}$ .  
Then  $\forall n \in \mathbb{N} \setminus \{0\}$ ,  $u_n \in \mathbb{Q}$  and  $x = \lim_{n \rightarrow +\infty} u_n$  from the previous question.

**Sample solution to Exercise 4.**

1. Let  $A, B \subset \mathbb{R}$  be such that  $\inf(A)$  and  $\sup(B)$  exist.  
We are going to prove the contrapositive: if  $A \cap B$  contains at least two elements then  $\inf(A) \neq \sup(B)$ .  
Assume that there exist  $x, y \in A \cap B$  such that  $x < y$ .  
Then, since  $\sup(B)$  is an upper bound of  $B$  and  $y \in B$ , we have  $y \leq \sup(B)$ .  
Since  $\inf(A)$  is a lower bound of  $A$  and  $x \in A$ , we have  $\inf(A) \leq x$ .  
Therefore  $\inf(A) \leq x < y \leq \sup(B)$ , so  $\inf(A) \neq \sup(B)$ .
2. Let  $A = (0, 42)$  and  $B = (-\pi, 0)$ . Then  $\inf(A) = \sup(B) = 0$  and  $A \cap B = \emptyset$ .

## Problem Set n°5

Jean-Baptiste Campesato

Due on April 12<sup>th</sup>, 2021

*Write your solutions concisely but without skipping important steps.  
Make sure that your submission is readable on Crowdmark.*

### Exercise 1.

Prove that  $\forall x \in \mathbb{R} \setminus \mathbb{Q}, \forall a, b, c, d \in \mathbb{Q}, ad - bc \neq 0 \implies \frac{ax+b}{cx+d} \notin \mathbb{Q}$ .

*Remark: note that  $cx + d \neq 0$  under the given assumptions.*

*Either  $c = 0$  but then  $cx + d = d \neq 0$  since  $ad - bc \neq 0$ . Or  $c \neq 0$  but then  $cx \in \mathbb{R} \setminus \mathbb{Q}$  and  $-d \in \mathbb{Q}$  thus  $cx + d \neq 0$ .*

### Exercise 2.

Let  $E$  be a finite set. Express

$$|\{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) : A \cup B = E\}|$$

in terms of  $|E|$ .

*Hint: you may start studying the case where the cardinality of  $A$  is fixed.*

### Exercise 3.

The following questions are independent.

1. Does it exist a set  $E$  such that  $|\mathcal{P}(E)| = \aleph_0$ ?
2. Prove that  $|[0, 1]| = |(0, 1)|$ .

### Exercise 4.

We set

$$S = \{x \in \mathbb{R} : \exists n \in \mathbb{N}, \exists a_0, a_1, \dots, a_n \in \mathbb{Z}, a_n \neq 0 \text{ and } a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0\}$$

What is  $|S|$ ?

*Remark: you can use basic facts concerning polynomials and their roots.*

**Sample solution to Exercise 1.**

Let  $x \in \mathbb{R} \setminus \mathbb{Q}$ . Let  $a, b, c, d \in \mathbb{Q}$  be such that  $ad - bc \neq 0$ .

Assume by contradiction that  $q := \frac{ax+b}{cx+d} \in \mathbb{Q}$ , then

$$\frac{ax+b}{cx+d} = q \Leftrightarrow x(a-qc) = qd-b$$

- First case: if  $a \neq qc$  then  $x = \frac{qd-b}{a-qc} \in \mathbb{Q}$ , so there is a contradiction.
- Second case: if  $a = qc$  then  $qd-b = x(a-qc) = 0$ , i.e.  $b = qd$ .  
Therefore  $ad-bc = qcd - qdc = 0$ , so there is a contradiction.

**Sample solution to Exercise 2.**

Set  $n := |E|$ .

Let  $i = 0, \dots, n$ . Set  $\Omega_i := \{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) : A \cup B = E \text{ and } |A| = i\}$ .

There are  $\binom{n}{i}$  subsets  $A \in \mathcal{P}(E)$  such that  $|A| = i$  (See Q10E09).

For a given  $A$  as above, in order to have  $A \cup B = E$ ,  $B$  must be of the form  $B = A^c \sqcup C$  where  $C \subset A$ .

There are  $2^i = |\mathcal{P}(A)|$  choices for such a subset  $C$ , and hence for  $B$  (See Q10E10).

Therefore  $|\Omega_i| = \binom{n}{i} 2^i$ .

Finally

$$\begin{aligned} |\{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) : A \cup B = E\}| &= \left| \bigsqcup_{i=0}^n \Omega_i \right| = \sum_{i=0}^n |\Omega_i| \\ &= \sum_{i=0}^n \binom{n}{i} 2^i = \sum_{i=0}^n \binom{n}{i} 2^i 1^{n-i} = (2+1)^n = 3^n = 3^{|E|} \end{aligned}$$

**Sample solution to Exercise 3.**

1. Let  $E$  be a set, then:

- Either  $E$  is finite and then  $\mathcal{P}(E)$  is finite too by Q10E10, so that  $|\mathcal{P}(E)| < \aleph_0$ .
- Or  $E$  is infinite and then  $\aleph_0 \leq |E| < |\mathcal{P}(E)|$  by Cantor's theorem.

In both cases  $|\mathcal{P}(E)| \neq \aleph_0$ , so there is no set  $E$  such that  $|\mathcal{P}(E)| = \aleph_0$ .

2. **Method 1.**

Note that  $(0, 1) \subset [0, 1]$ , therefore  $|(0, 1)| \leq |[0, 1]|$ .

Define  $f : [0, 1] \rightarrow (0, 1)$  by  $f(x) = \frac{x+1}{3}$ .

Note that  $f$  is well-defined since if  $0 \leq x \leq 1$  then  $0 < \frac{1}{3} \leq \frac{x+1}{3} \leq \frac{2}{3} < 1$ .

Besides  $f$  is injective since if  $x, y \in [0, 1]$  satisfy  $f(x) = f(y)$ , then  $\frac{x+1}{3} = \frac{y+1}{3}$  which implies  $x = y$ .

Therefore  $|[0, 1]| \leq |(0, 1)|$ .

By Cantor–Schröder–Bernstein theorem, we conclude that  $|[0, 1]| = |(0, 1)|$ .

**Method 2.**

We know that  $(0, 1) \subset [0, 1] \subset \mathbb{R}$  and that  $|(0, 1)| = |\mathbb{R}|$  (see Q11E08).

Therefore  $|[0, 1]| = |(0, 1)|$  (see Q11E01).

**Sample solution to Exercise 4.**

**Comment:** a complex number that is the root of a non-zero polynomial with integers (or rational, it is equivalent) coefficients is said to be an algebraic number. Complex numbers which are not roots of such polynomials are called transcendental numbers.

The field of algebraic real numbers is quite often denoted by

$$\mathbb{R}_{\text{alg}} := \{x \in \mathbb{R} : \exists n \in \mathbb{N}, \exists a_0, a_1, \dots, a_n \in \mathbb{Z}, a_n \neq 0 \text{ and } a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0\}$$

The goal of this exercise was to prove that  $|\mathbb{R}_{\text{alg}}| = \aleph_0$ , i.e. there are infinitely countably many algebraic real numbers, so that almost all real numbers are transcendental (but it is usually quite difficult to prove that a number is transcendental: we still don't know whether  $\pi + e$  or  $\pi e$  are transcendental or not). This was first proved by Cantor in his famous article Ueber eine Eigenschaft des Inbegriffes aller reellen algebraischen Zahlen published 1874.

**Claim.**  $\forall n \in \mathbb{N} \setminus \{0\}, |\mathbb{Z}^n| = \aleph_0$ .

*Proof by induction on  $n \geq 1$ .*

*Base case at  $n = 1$ :*  $|\mathbb{Z}^1| = |\mathbb{Z}| = \aleph_0$  (from the lecture notes).

*Induction step.* Assume that  $|\mathbb{Z}^n| = \aleph_0$  for some  $n \geq 1$ .

Since  $|\mathbb{Z}^n| = |\mathbb{N}|$  and  $|\mathbb{Z}| = |\mathbb{N}|$ , we have  $|\mathbb{Z}^{n+1}| = |\mathbb{Z}^n \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ . □

**Method 1.**

For  $n \in \mathbb{N}$  and  $a_0, a_1, \dots, a_n \in \mathbb{Z}$  with  $a_n \neq 0$ , the set

$$\{x \in \mathbb{R} : a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0\}$$

is finite since a polynomial of degree  $n$  has at most  $n$  roots.

For  $n \in \mathbb{N}$ , we set

$$A_n = \bigcup_{(a_0, a_1, \dots, a_n) \in \mathbb{Z}^n \times (\mathbb{Z} \setminus \{0\})} \{x \in \mathbb{R} : a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0\}$$

Since  $|\mathbb{Z}^n| = |\mathbb{N}|$  and  $|\mathbb{Z} \setminus \{0\}| = |\mathbb{N}|$ , we have that  $|\mathbb{Z}^n \times (\mathbb{Z} \setminus \{0\})| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

Therefore  $A_n$  is countable as a countable union of finite sets.

Hence  $S = \bigcup_{n \in \mathbb{N}} A_n$  is countable as a countable union of countable sets.

Note that  $\mathbb{Z} \subset S$ , since  $m \in \mathbb{Z}$  is a root of  $x - m = 0$ .

Therefore  $S$  is countably infinite, i.e.  $|S| = \aleph_0$ .

**Method 2.**

For  $n \in \mathbb{N}$ , we denote by  $P_n$  the set of polynomials of degree  $n$  with integer coefficients.

Note that  $|P_n| = |\mathbb{Z}^n \times \mathbb{Z} \setminus \{0\}|$  since a polynomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  of degree  $n$  is characterized by its coefficients  $(a_0, a_1, \dots, a_n) \in \mathbb{Z}^n \times (\mathbb{Z} \setminus \{0\})$ .

Since  $|\mathbb{Z}^n| = |\mathbb{N}|$  and  $|\mathbb{Z} \setminus \{0\}| = |\mathbb{N}|$ , we have that  $|P_n| = |\mathbb{Z}^n \times (\mathbb{Z} \setminus \{0\})| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

Hence the set  $P = \bigcup_{n \in \mathbb{N}} P_n$  of non-zero polynomials with integer coefficients is countable as a countable union of countable sets.

Given  $f \in P$ ,  $f^{-1}(\{0\}) = \{x \in \mathbb{R} : f(x) = 0\}$  is finite since a polynomial of degree  $n$  has at most  $n$  roots.

Therefore  $S = \bigcup_{f \in P} f^{-1}(0)$  is countable as a countable union of finite sets.

Note that  $\mathbb{Z} \subset S$ , since  $m \in \mathbb{Z}$  is a root of  $x - m = 0$ .

Therefore  $S$  is countably infinite, i.e.  $|S| = \aleph_0$ .

## Concepts in Abstract Mathematics

## Final Exam

Jean-Baptiste Campesato

April 16<sup>th</sup>, 2021 at 2pm to April 17<sup>th</sup>, 2021 at 2pm

Write your solutions concisely but without skipping important steps.

You can rely on all the material covered in the course (lecture notes, slides, weekly questions and problem sets).

You can use results from other questions of the exam by quoting them properly, even if you did not solve them.

Each question should be submitted in a separate picture on Crowdmark. Make sure that your submission is legible.

**Exercise 1.**

15 P.

Prove that  $\forall n \in \mathbb{N} \setminus \{0, 1\}, 2^n - 1 > n$ .

**Exercise 2.**

20 P.

1. Prove that  $\forall m \in \mathbb{N} \setminus \{0\}, \forall x \in \mathbb{R}, x^m - 1 = (x - 1) \left( \sum_{k=0}^{m-1} x^k \right)$ .
2. Let  $n \in \mathbb{N} \setminus \{0\}$ . Prove that if  $n$  is a composite number then  $2^n - 1$  is composite too.  
Recall that a natural number  $n$  is composite if and only if there exist  $a, b \in \mathbb{N} \setminus \{0, 1\}$  such that  $n = ab$ .
3. We say that  $n \in \mathbb{N} \setminus \{0, 1\}$  is 2-prime if  $2^n \equiv 2 \pmod{n}$ .  
Prove that if  $n$  is 2-prime then  $2^n - 1$  is 2-prime too.
4. Deduce that there are infinitely many composite 2-prime numbers.  
We admit that 341 is 2-prime.

**Exercise 3.**

15 P.

Let  $p$  be a prime number. Prove that  $\forall a, b \in \mathbb{Z}, a^p \equiv b^p \pmod{p} \implies a^p \equiv b^p \pmod{p^2}$ .

**Exercise 4.**

15 P.

We set  $D := \left\{ \frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$ .

Prove that  $D$  is dense in  $\mathbb{R}$ , i.e. prove that  $\forall x, y \in \mathbb{R}, x < y \implies \exists d \in D, x < d < y$ .

**Exercise 5.**

20 P.

Define  $\theta : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{R}$  by  $\theta(a, b) = a + b\sqrt{2}$ .

1. Is  $\theta$  surjective?
2. Prove that  $\theta$  is injective.
3. We set  $\mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ . Prove that  $|\mathbb{Z}[\sqrt{2}]| = \aleph_0$ .

**Exercise 6.**

15 P.

1. Prove that  $|\mathbb{R}^{\mathbb{Q}}| = |\mathbb{R}|$  where  $\mathbb{R}^{\mathbb{Q}}$  is the set of functions  $\mathbb{Q} \rightarrow \mathbb{R}$ .
2. We denote by  $C^0(\mathbb{R})$  the set of continuous functions  $\mathbb{R} \rightarrow \mathbb{R}$ .  
Prove that  $\Phi : \begin{cases} C^0(\mathbb{R}) & \rightarrow & \mathbb{R}^{\mathbb{Q}} \\ f & \mapsto & f|_{\mathbb{Q}} \end{cases}$  is injective, where  $f|_{\mathbb{Q}}$  denotes the restriction of  $f$  to  $\mathbb{Q}$ .

Remark: recall from your calculus course that if  $f \in C^0(\mathbb{R})$  and  $\lim_{n \rightarrow +\infty} x_n = \ell$  then  $\lim_{n \rightarrow +\infty} f(x_n) = f(\ell)$ .

Hint: don't forget you can use results from problem sets.

3. Prove that  $|C^0(\mathbb{R})| = |\mathbb{R}|$ .

**Sample solutions to Exercise 1.**

Let's prove the statement by induction on  $n \geq 2$ .

- *Base case at  $n = 2$ :*  $2^n - 1 = 2^2 - 1 = 3 > 2 = n$ .
- *Induction step.* Assume that  $2^n - 1 > n$  holds for some  $n \geq 2$ . Then

$$\begin{aligned} 2^{n+1} - 1 &= 2 \times 2^n - 1 = 2(2^n - 1) + 1 \\ &> 2n + 1 \quad \text{by the induction hypothesis} \\ &> n + 1 \quad \text{since } n > 0 \end{aligned}$$

Which ends the induction step.

*Comment: I asked this question to evaluate your writings for proof by inductions (since I insisted a lot on it this term) and I picked this statement to prove by induction because it is useful for Exercises 2 and 4.*

**Sample solutions to Exercise 2.**

1. *Comment: Several students complained by e-mail that there is an issue when  $x = 0$  because  $0^0$  is undefined, but you use the convention  $0^0 = 1$  all the time for such formulae, e.g.:*

- *Binomial formula:*  $\forall x, y \in \mathbb{R}, \forall n \in \mathbb{N}, (x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$
- *Geometric sum:*  $\forall x \in \mathbb{R} \setminus \{1\}, \forall n \in \mathbb{N}, \sum_{k=0}^n x^k = \frac{1-x^{n+1}}{1-x}$
- *When defining a polynomial function  $f : \mathbb{R} \rightarrow \mathbb{R}$  by  $f(x) = \sum_{k=0}^n a_k x^k$*
- *When we proved that for finite sets  $|E^F| = |E|^{|F|}$  (including the case  $E = F = \emptyset$ )*
- ...

**Method 1:**

Let  $x \in \mathbb{R}$ .

We are going to prove that  $\forall m \in \mathbb{N} \setminus \{0\}, x^m - 1 = (x - 1) \left( \sum_{k=0}^{m-1} x^k \right)$  by induction on  $m \geq 1$ .

- *Base case at  $m = 1$ :*  $(x - 1) \left( \sum_{k=0}^{1-1} x^k \right) = (x - 1)x^0 = x - 1 = x^1 - 1$ .
- *Induction step.* Assume that  $x^m - 1 = (x - 1) \left( \sum_{k=0}^{m-1} x^k \right)$  for some  $m \geq 1$ . Then

$$\begin{aligned} (x - 1) \left( \sum_{k=0}^m x^k \right) &= (x - 1) \left( \sum_{k=0}^{m-1} x^k + x^m \right) = (x - 1) \sum_{k=0}^{m-1} x^k + (x - 1)x^m \\ &= (x^m - 1) + (x - 1)x^m \quad \text{by induction hypothesis} \\ &= x^m - 1 + x^{m+1} - x^m = x^{m+1} - 1 \end{aligned}$$

which ends the induction step.

**Method 2:**

Let  $m \in \mathbb{N} \setminus \{0\}$  and  $x \in \mathbb{R}$ . Then we have the following telescoping sum:

$$(x - 1) \left( \sum_{k=0}^{m-1} x^k \right) = x \left( \sum_{k=0}^{m-1} x^k \right) - \sum_{k=0}^{m-1} x^k = \sum_{k=0}^{m-1} x^{k+1} - \sum_{k=0}^{m-1} x^k = \sum_{k=1}^m x^k - \sum_{k=0}^{m-1} x^k = x^m - x^0 = x^m - 1$$

2. Let  $n$  be a composite number. Then  $n = ab$  for some  $a, b \in \mathbb{N} \setminus \{0, 1\}$ .

Therefore

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1) \left( \sum_{k=0}^{b-1} 2^{ak} \right) \quad \text{by Question 1 since } b \in \mathbb{N} \setminus \{0\}$$

Since  $a > 1$ , by Exercise 1,  $2^a - 1 > a > 1$ .

Besides  $\sum_{k=0}^{b-1} 2^{ak} \geq 2^0 + 2^a > 1$  since  $b > 1$ .

Therefore  $2^n - 1$  is composite.

**3. Method 1:**

Let  $n \in \mathbb{N} \setminus \{0, 1\}$  be a 2-prime number. Then  $2^n \equiv 2 \pmod{n}$ , so that  $2^n = 2 + \lambda n$  for some  $\lambda \in \mathbb{Z}$ .

Note that, by Exercise 1 as  $n \in \mathbb{N} \setminus \{0, 1\}$ ,  $2^n - 1 > n \geq 2$ . Thus  $2^n - 1 \in \mathbb{N} \setminus \{0, 1\}$  and  $\lambda > 0$ .

Therefore

$$2^{2^n-1} - 2 = 2^{2+\lambda n-1} - 2 = 2^{1+\lambda n} - 2 = 2(2^{\lambda n} - 1) = 2((2^n)^\lambda - 1) = 2(2^n - 1) \left( \sum_{k=0}^{\lambda-1} 2^{nk} \right) \quad \text{by Q1 since } \lambda > 0.$$

So  $2^n - 1 \mid 2^{2^n-1} - 2$ , i.e.  $2^{2^n-1} \equiv 2 \pmod{2^n - 1}$ .

Hence  $2^n - 1$  is 2-prime.

**Method 2:**

Let  $n \in \mathbb{N} \setminus \{0, 1\}$  be a 2-prime number. Then  $2^n \equiv 2 \pmod{n}$ , so that  $2^n = 2 + \lambda n$  for some  $\lambda \in \mathbb{Z}$ .

Note that, by Exercise 1 as  $n \in \mathbb{N} \setminus \{0, 1\}$ ,  $2^n - 1 > n \geq 2$ . Thus  $2^n - 1 \in \mathbb{N} \setminus \{0, 1\}$  and  $\lambda > 0$ .

Therefore  $2^{2^n-1} = 2^{2+\lambda n-1} = 2^{1+\lambda n} = 2 \times (2^n)^\lambda \equiv 2 \times 1^\lambda \pmod{2^n - 1} \equiv 2 \pmod{2^n - 1}$ .

Hence  $2^n - 1$  is 2-prime.

4. Assume by contradiction that the set of composite 2-prime numbers is finite, then it is bounded.

Besides it is non-empty since  $341 = 11 \times 31$  is a composite 2-prime number.

Therefore there exists a greatest composite 2-prime number  $N$  (Chapter 2, Theorem 17).

By Questions 2 and 3,  $2^N - 1$  is a composite 2-prime number too since  $N \geq 341 > 1$ .

Besides  $2^N - 1 > N$  by Exercise 1 since  $N \geq 341 > 1$ .

Hence a contradiction since  $N$  is the greatest composite 2-prime number.

**Sample solutions to Exercise 3.**

Let  $a, b \in \mathbb{Z}$  be such that  $a^p \equiv b^p \pmod{p}$ .

By Fermat's little theorem, since  $p$  is prime, we know that  $a^p \equiv a \pmod{p}$  and that  $b^p \equiv b \pmod{p}$ .

Therefore  $a \equiv b \pmod{p}$ . Thus there exists  $\lambda \in \mathbb{Z}$  such that  $a = b + \lambda p$ .

$$\text{Then } a^p = (b + \lambda p)^p = \sum_{k=0}^p \binom{p}{k} b^{p-k} (\lambda p)^k = b^p + p b^{p-1} \lambda p + \sum_{k=2}^p \binom{p}{k} b^{p-k} \lambda^k p^k \equiv b^p + 0 + \sum_{k=2}^p 0 \pmod{p^2} \equiv b^p \pmod{p^2}$$

(note that  $p^2 \mid p b^{p-1} \lambda p = p^2 b^{p-1} \lambda$  and that  $p^2 \mid p^k$  for  $k \geq 2$ ).

**Sample solutions to Exercise 4.**

We adapt the proof of Theorem 45 from Chapter 6, using  $2^n$  as denominator instead of  $n$ .

Let  $x, y \in \mathbb{R}$  be such that  $x < y$ .

Set  $\varepsilon = y - x > 0$ .

By the archimedean property of  $\mathbb{R}$ , there exists  $n \in \mathbb{N}$  such that  $n\varepsilon > 1$ .

Note that  $n > 0$ , since otherwise  $0 > 1$ . Therefore  $\frac{1}{n} < \varepsilon$ .

Note that  $2^n > n$ . Indeed if  $n > 1$  then  $2^n > n + 1 > n$  by Exercise 1, otherwise if  $n = 1$  then  $2^1 = 2 > 1$ .

Thus  $0 < \frac{1}{2^n} < \frac{1}{n} < \varepsilon$ .

Set  $m = \lfloor 2^n x \rfloor + 1$ , then  $2^n x < m \leq 2^n x + 1$ , so  $x < \frac{m}{2^n} \leq x + \frac{1}{2^n} < x + \varepsilon = y$ .

Hence  $d = \frac{m}{2^n} \in D$  satisfies  $x < d < y$ .

**Sample solutions to Exercise 5.****1. Method 1:**

We are going to prove that  $\sqrt{3} \notin \text{Im}(\theta)$ .

Assume by contradiction that there exists  $(a, b) \in \mathbb{Z}^2$  such that  $\theta(a, b) = \sqrt{3}$ . Then  $\sqrt{3} = a + b\sqrt{2}$ .

- If  $a = 0$ , then  $\sqrt{3} = b\sqrt{2}$ , so that  $3 = 2b^2$  with  $b^2 \in \mathbb{Z}$ . Then  $2|3$  which is impossible.  
(alternatively: if  $a = 0$  then  $\frac{3}{2} = b^2 \in \mathbb{Z}$ , which is impossible).  
Hence  $a \neq 0$ .
- If  $b = 0$ , then  $\sqrt{3} = a \in \mathbb{Q}$ . Which is impossible.  
Hence  $b \neq 0$ .

Squaring  $\sqrt{3} = a + b\sqrt{2}$ , we get  $3 = a^2 + 2b^2 + 2ab\sqrt{2}$ , so that  $\sqrt{2} = \frac{3-a^2-2b^2}{2ab} \in \mathbb{Q}$ .

Which is a contradiction. Hence  $\sqrt{3} \notin \text{Im}(\theta)$  and  $\theta$  is not surjective.

**Method 2:**

We are going to prove that  $\sqrt{3} \notin \text{Im}(\theta)$ .

Assume by contradiction that there exists  $(a, b) \in \mathbb{Z}^2$  such that  $\theta(a, b) = \sqrt{3}$ .

Then  $\sqrt{3} = a + b\sqrt{2}$ , so that  $\sqrt{3} - b\sqrt{2} = a$ .

Squaring the previous equality, we get  $3 + 2b^2 - 2b\sqrt{6} = a^2$ .

Note that  $b \neq 0$  since otherwise  $\sqrt{3} = a \in \mathbb{Q}$  which is impossible.

Therefore  $\sqrt{6} = \frac{3+2b^2-a^2}{2b} \in \mathbb{Q}$  which is a contradiction. Hence  $\sqrt{3} \notin \text{Im}(\theta)$  and  $\theta$  is not surjective.

**Method 3:**

We are going to prove that  $\frac{314}{42} \notin \text{Im}(\theta)$  (or anything in  $\mathbb{Q} \setminus \mathbb{Z}$ ).

Assume by contradiction that there exists  $(a, b) \in \mathbb{Z}^2$  such that  $\theta(a, b) = \frac{314}{42}$ . Then  $\frac{314}{42} = a + b\sqrt{2}$ .

- First case: if  $b = 0$  then  $\frac{314}{42} = a \in \mathbb{Z}$ . Hence a contradiction.
- Second case: if  $b \neq 0$  then  $b\sqrt{2} \notin \mathbb{Q}$  by Week 9, Ex 4.4, since  $\sqrt{2} \notin \mathbb{Q}$  and  $b \in \mathbb{Q} \setminus \{0\}$ .  
But  $b\sqrt{2} = \frac{314}{42} - a \in \mathbb{Q}$ . Hence a contradiction.

Therefore  $\frac{314}{42} \notin \text{Im}(\theta)$  and  $\theta$  is not surjective.

**Method 4:** We are going to prove that  $\frac{1}{2} \notin \text{Im}(\theta)$ .

Assume by contradiction that there exists  $(a, b) \in \mathbb{Z}^2$  such that  $\theta(a, b) = \frac{1}{2}$ .

Then  $\frac{1}{2} = a + b\sqrt{2} \implies b\sqrt{2} = \frac{1}{2} - a \implies 2b^2 = \frac{1}{4} + a^2 - a \implies \frac{1}{4} = 2b^2 - a^2 + a \in \mathbb{Z}$ .

Hence a contradiction.

Therefore  $\frac{1}{2} \notin \text{Im}(\theta)$  and  $\theta$  is not surjective.

**Method 5:** We are going to prove that  $\frac{\sqrt{2}}{2} \notin \text{Im}(\theta)$ .

Assume by contradiction that there exists  $(a, b) \in \mathbb{Z}^2$  such that  $\theta(a, b) = \frac{\sqrt{2}}{2}$ .

Then  $\frac{\sqrt{2}}{2} = a + b\sqrt{2}$ , so that  $\left(\frac{1}{2} - b\right)\sqrt{2} = a$ . Note that  $\frac{1}{2} \notin \mathbb{Z}$  so that  $b \neq \frac{1}{2}$ , hence  $\sqrt{2} = \frac{a}{1/2-b} \in \mathbb{Q}$ .

Hence a contradiction. Therefore  $\frac{\sqrt{2}}{2} \notin \text{Im}(\theta)$  and  $\theta$  is not surjective.

**Method 6:** Since  $|\mathbb{N}| = |\mathbb{Z}|$ , we have  $|\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \aleph_0 < |\mathbb{R}|$ .

Therefore, there is no surjection  $\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{R}$ , so that  $\theta$  can't be surjective.



2. Let  $(a, b), (c, d) \in \mathbb{Z}^2$  be such that  $\theta(a, b) = \theta(c, d)$ .

Then  $a + b\sqrt{2} = c + d\sqrt{2}$ , i.e.  $(a - c) + (b - d)\sqrt{2} = 0$ .

- If  $b \neq d$ , then  $\sqrt{2} = \frac{c-a}{b-d} \in \mathbb{Q}$ , which is impossible.
- If  $b = d$ , then  $a - c = 0$ , so that  $(a, b) = (c, d)$ .

Therefore  $\theta$  is injective.

3. **Method 1:**

Note that  $\text{Im}(\theta) = \mathbb{Z}[\sqrt{2}]$  by definition of  $\mathbb{Z}[\sqrt{2}]$ .

Therefore  $\tilde{\theta} : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}[\sqrt{2}]$  defined by  $\tilde{\theta}(a, b) = \theta(a, b)$  is well-defined and surjective.

Besides, it is injective (and hence bijective) by the previous question.

Hence  $|\mathbb{Z}[\sqrt{2}]| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$  since  $|\mathbb{Z}| = |\mathbb{N}|$ .

**Method 2:**

Since  $|\mathbb{Z}| = |\mathbb{N}|$ , we get  $|\mathbb{Z}^2| = |\mathbb{Z} \times \mathbb{Z}| = |\mathbb{N} \times \mathbb{N}| = \aleph_0$ .

So  $\mathbb{Z}[\sqrt{2}] = \bigcup_{(a,b) \in \mathbb{Z}^2} \{a + b\sqrt{2}\}$  is countable as a countable union of countable sets (singletons).

Thus  $|\mathbb{Z}[\sqrt{2}]| \leq \aleph_0$ .

Besides  $\mathbb{Z} \subset \mathbb{Z}[\sqrt{2}]$ , hence  $\aleph_0 = |\mathbb{Z}| \leq |\mathbb{Z}[\sqrt{2}]|$ .

Finally, by Cantor–Schröder–Bernstein theorem, we get that  $|\mathbb{Z}[\sqrt{2}]| = \aleph_0$  as required.

**Sample solutions to Exercise 6.**

1. Since  $|\mathbb{Q}| = |\mathbb{N}|$ , there exists a bijective function  $\psi : \mathbb{Q} \rightarrow \mathbb{N}$ .  
We define  $\Psi : \mathbb{R}^{\mathbb{N}} \rightarrow \mathbb{R}^{\mathbb{Q}}$  by  $\Psi(f) = f \circ \psi$ . Note that  $\Psi$  is bijective with inverse  $\Psi^{-1}(g) = g \circ \psi^{-1}$ .  
Indeed, for  $f \in \mathbb{R}^{\mathbb{N}}$ ,  $\Psi^{-1}(\Psi(f)) = f \circ \psi \circ \psi^{-1} = f$ , and for  $g \in \mathbb{R}^{\mathbb{Q}}$ ,  $\Psi(\Psi^{-1}(g)) = g \circ \psi^{-1} \circ \psi = g$ .  
Therefore  $|\mathbb{R}^{\mathbb{Q}}| = |\mathbb{R}^{\mathbb{N}}| = |\mathbb{R}|$  by Week 11 Exercise 9.
2. Let  $f, g \in C^0(\mathbb{R})$  be such that  $\Phi(f) = \Phi(g)$ , i.e.  $f|_{\mathbb{Q}} = g|_{\mathbb{Q}}$  (otherwise stated,  $\forall x \in \mathbb{Q}, f(x) = g(x)$ ).  
Let  $x \in \mathbb{R}$ . By PS4, Exercise 3, there exists a sequence  $(q_n)_n$  of rational numbers such that  $\lim_{n \rightarrow +\infty} q_n = x$ .  
Then

$$\begin{aligned} f(x) &= \lim_{n \rightarrow +\infty} f(q_n) \quad \text{since } f \text{ is continuous} \\ &= \lim_{n \rightarrow +\infty} g(q_n) \quad \text{since } \forall n, q_n \in \mathbb{Q} \text{ and } f|_{\mathbb{Q}} = g|_{\mathbb{Q}} \\ &= g(x) \quad \text{since } g \text{ is continuous} \end{aligned}$$

Therefore,  $\forall x \in \mathbb{R}, f(x) = g(x)$ , so that  $f = g$ .

3. Since  $\Phi$  is injective, we know that  $|C^0(\mathbb{R})| \leq |\mathbb{R}^{\mathbb{Q}}| = |\mathbb{R}|$ .  
Note that  $\Gamma : \mathbb{R} \rightarrow C^0(\mathbb{R})$  mapping  $x_0$  to the constant function

$$\Gamma(x_0) : \begin{array}{ccc} \mathbb{R} & \rightarrow & \mathbb{R} \\ x & \mapsto & x_0 \end{array}$$

is well-defined (since a constant function is continuous) and injective.

Therefore  $|\mathbb{R}| \leq |C^0(\mathbb{R})|$ .

From Cantor–Schröder–Bernstein theorem, we get that  $|C^0(\mathbb{R})| = |\mathbb{R}|$ .