M1F Notes

David Burgschweiger

February 19, 2016

Contents

1 Sets

Definition 1.1. A *set* S is a collection of objects (called *elements* of the set). If x is an *element* of S let us write $x \in S$ otherwise $x \notin S$.

Remark. The order of the elements or any repetition is unimportant.

Example 1. $\{1,3\} = \{3,1,1\}$

Definition 1.2. For two sets S and T let us write $S \subseteq T$ (S is a *subset* of in T) if

$$x \in S \Rightarrow x \in T.$$

Definition 1.3. $S = T$ iff $S \subseteq T$ and $T \subseteq S$.

Axiom 1.1. *Foundation Axiom*

$$S \notin S$$

Remark. Nonetheless, elements can be sets.

Definition 1.4. $\emptyset$ is the set with no elements.

Property 4.1. $\emptyset \subseteq S$ and $S \subseteq S$ for all sets S

1.1 Set Operators

Definition 1.5. The *intersection* $S \cap T$ of two sets S and T is

$$\{x |\ x \in S \text{ and } x \in T\}.$$

Definition 1.6. The *union* $S \cup T$ of two sets S and T is

$$\{x |\ x \in S \text{ or } x \in T\}.$$

Definition 1.7. The *difference* $S \backslash T$ of two sets S and T is

$$\{x |\ x \in S \text{ and } x \notin T\}.$$

Definition 1.8. The *symmetric difference* $S \triangle T$ of two sets S and T is

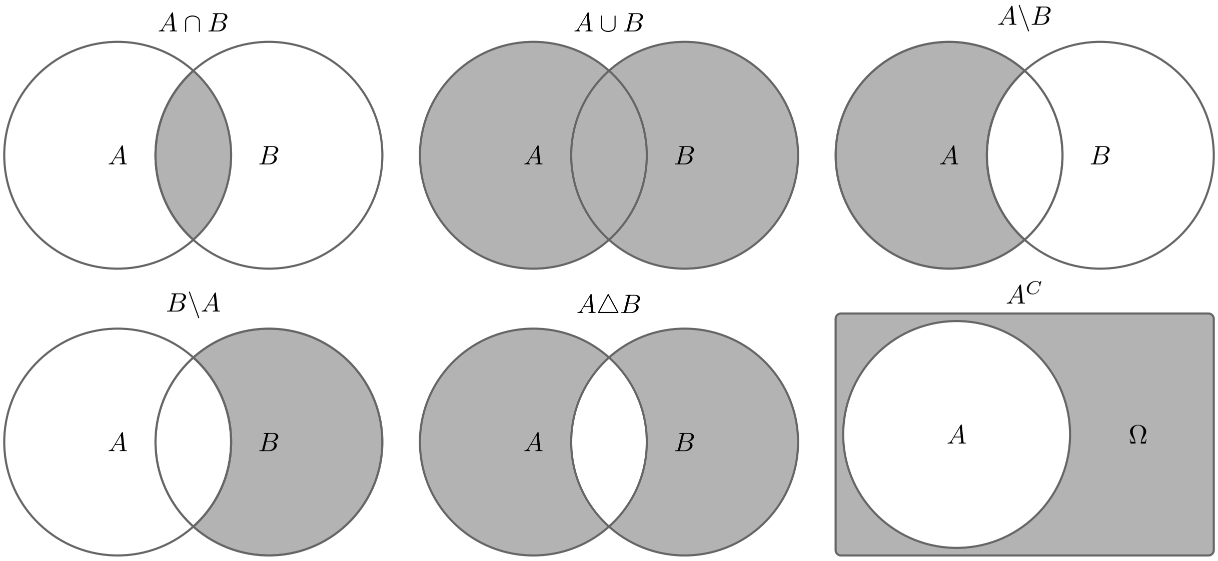
$$\{x |\ x \in S \text{ or } x \in T \text{ but not both}\}.$$

Definition 1.9. The complement A^C of a set A with regard to a set $\Omega, A \subseteq \Omega$ is

$$\{x \in \Omega |\ x \notin A\} = \Omega \backslash A.$$

Remark. The complement is only used when the reference set Ω is clear.

Figure 1: The operations on sets can be visualized by *Venn diagrams.* In order to understand a set-related problem, in some cases it may be helpful to draw a Venn Diagram.



Some sets we will work with in this course are:

$$\mathbb{N} = \{0, 1, 2, \dots\}$$
$$\mathbb{Z} = \{0, 1, -1, 2, -2 \dots\}$$
$$\mathbb{Q} = \left\{ \frac{p}{q} \middle|\ p \in \mathbb{N}, q \in \mathbb{Z} \backslash \{0\} \right\}$$

$\mathbb{R}$ reals

$\mathbb{C}$ complex numbers

1.2 Intervals in $\mathbb{R}$

Definition 1.10. If $a, b \in \mathbb{R},\ a \leq b$, then

$$\begin{aligned}
[a,b] &= \{t \in \mathbb{R} |\ a \leq t \leq b\}\\
(a,b) &= \{t \in \mathbb{R} |\ a < t < b\}\\
[a,b) &= \{t \in \mathbb{R} |\ a \leq t < b\}\\
(a,b] &= \{t \in \mathbb{R} |\ a < t \leq b\}\\
[a,\infty) &= \{t \in \mathbb{R} |\ a < t\}\\
(-\infty,b] &= \{t \in \mathbb{R} |\ t \leq b\}.
\end{aligned}$$

1.3 Infinite Unions and Intersections

Definition 1.11. Suppose that, for all $n \in \mathbb{N}$, we are given a set A_n. Define

$$\begin{aligned}
\bigcup_{n=a}^{\infty} A_n &= \{x |\text{ there exists a } n \in \mathbb{N}, n \geq a \text{ such that } x \in A_n\}\\
\bigcap_{n=a}^{\infty} A_n &= \{x |\text{ for all } n \in \mathbb{N}, n \geq a \text{ such that } x \in A_n\}.
\end{aligned}$$

Example 2.

$$\begin{aligned}
\bigcup_{n=1}^{\infty} \left[0, 1-\frac{1}{n}\right] &= [0,1)\\
\bigcap_{n=1}^{\infty} \left(1-\frac{1}{n}, 1+\frac{1}{n}\right) &= \{1\}
\end{aligned}$$

2 Proofs

2.1 Elements of propositional calculus

Definition 2.1. A *statement* (proposition) is an assertion that can be either true (T) or false (F).

Remark. In maths such an assertion usually takes the form: "If such and such assumptions are made, then we can infer such and such conclusions."

Example 3.
- $n = 3$
- $(A + B)^2 = A^2 + 2AB + B^2$
- If it n^2 is odd, then n is odd too.
- If it rains, then it is cloudy.
- For all real numbers greater than or equal to 0 there exists a square root.

Definition 2.2. A *proof* is a chain of statements linked by logical implications (inferences) that establish the truth of the last statement. In the course of the proof one is allowed to "call up"

- assumptions that are made,
- statements proven previously,
- axioms (statements that are generally accepted and never proven).

"Grammar elements" of mathematical statements are Quantifiers:

Type	Sign	Meaning
Existential	$\exists$ $\exists_1$	there exists there exists a unique
Universal	$\forall$	for all
	:, $\vert$	such that

Ways to form new statements from old ones are:

- If P is a statement then $\overline{P}$ "non-P" is the statement which is true if P is false and false if P is true.
- If P and Q are statements then we can form:

Sign	Meaning
$P \wedge Q$, $P \& Q$	P and Q.
$P \vee Q$	Either P or Q or both.
$P \veebar Q$	Either P or Q but not both.
$P \Rightarrow Q$	If P then Q.
$P \Leftarrow Q$	If Q then P.
$P \Leftrightarrow Q$	P if and only if Q.

Remark. $P \Rightarrow Q$ means any of the following:

- If P then Q.
- Q if P.
- P is true only if Q is true.
- P only if Q.
- P is sufficient for Q.
- Q is necessary for P.
- If Q is false then P is false.
- $\overline{Q} \Rightarrow \overline{P}$

Similarly, $P \Leftrightarrow Q$ means any of the following:

- $(P \Rightarrow Q) \wedge (Q \Rightarrow P)$
- P if and only if Q.
- P is necessary and sufficient for Q.

The rigorous definition of $P \wedge Q$, $P \Rightarrow Q$ can be made through a truth table.

Definition 2.3. $P \wedge Q$ is defined by:

P	Q	$P \wedge Q$
T	T	T
T	F	F
F	T	F
F	F	F

Definition 2.4. Also, $P \Rightarrow Q$ is defined by:

P	Q	$P \Rightarrow Q$
T	T	T
T	F	F
F	T	T
F	F	T

Example 4. The statement "If $x \in \{n \in \mathbb{N} |\ n^2 < 0\}$, then x is a sheep." is true as well as the statement "If $x \in \{n \in \mathbb{N} | n^2 < 0\}$, then x is not a sheep."

2.2 Inference rules

Example 5. *Premise 1.* If it is raining then it is cloudy.
Premise 2. It is raining.
Conclusion. It is cloudy.

We can write this more abstractly as follows:
P: it is raining
Q: it is cloudy
In this form:
Premise 1. $P \Rightarrow Q$
Premise 2. P
Conclusion. Q

This is an example of an inference rule which we write like this:

$$((P \Rightarrow Q) \quad \wedge \quad P) \qquad \Rightarrow \qquad Q$$

There are other inference rules:

$$\begin{array}{rcl}
((P \Rightarrow Q) \quad \wedge \quad (Q \Rightarrow R)) & \Rightarrow & (P \Rightarrow R) \\
\big((P \vee Q) \quad \wedge \quad \overline{P}\big) & \Rightarrow & Q \\
(P \wedge Q) & \Rightarrow & P \\
((P \Rightarrow Q) \quad \vee \quad (P \Rightarrow R)) & \Rightarrow & (P \Rightarrow (Q \vee R)) \\
((P \vee Q) \quad \wedge \quad (P \Rightarrow (P \wedge Q))) & \Rightarrow & (R \Rightarrow R) \\
\big((P \Rightarrow Q) \quad \wedge \quad \big(P \Rightarrow \overline{Q}\big)\big) & \Rightarrow & \overline{P} \\
(P \quad \wedge \quad (Q \vee R)) & \Rightarrow & (P \wedge Q) \quad \vee \quad (P \wedge R)
\end{array}$$

Exercise. Proof that

$$\forall n \in \mathbb{N} \qquad n^2\text{odd} \quad \Rightarrow \quad n \text{ odd.}$$

Example 6. Is the following a valid argument:

1. If a movie is not worth seeing, then it is not made in the UK.
2. A movie is worth seeing only if Prof Corti reviews it.
3. "The Maths Graves" was not not reviewed by Prof Corti.
4. Therefore, "The Maths Graves" is not made in the UK.

In order to determine this, let us rewrite the argument in a more formal way:

Variable	Meaning
M	the set of all movies
$W(x)$	"x is worth seeing."
$UK(x)$	"x is made in the UK."
$C(x)$	"Professor Corti reviews x."
m	"The Maths Games" $\in M$

Now the argument can be expressed as:

$$\forall x \in M : \qquad \overline{W(x)} \Rightarrow \overline{UK(x)} \tag{1}$$

$$\forall x \in M : \qquad W(x) \Rightarrow C(x) \tag{2}$$

$$\overline{C(m)} \tag{3}$$

$$((1) \wedge (2) \wedge (3)) \Rightarrow \qquad \overline{UK(x)}$$

Yes it is a valid argument. Indeed, it is the same as:

$$\begin{array}{lr}
\forall x \in M : & UK(x) \Rightarrow W(x) \\
\forall x \in M : & W(x) \Rightarrow C(x)
\end{array}$$

Then you say:

$$\begin{aligned} \forall x && \in M\overline{C(x)} \Rightarrow \overline{UK(x)} \\ && \overline{C(m)} \\ && \Rightarrow \overline{UK(m)} \end{aligned}$$

Result 2.2.1. What can we learn from this? If we want to be understood, we have to learn to present our arguments better. For instance, try to put everything in the positive. Use "if then" throughout. A better way of writing would be:

1. If x is made in the UK, then x is worth seeing.
2. If x is worth seeing then Prof Corti reviews it.
3. Prof Corti did not review m.
4. Therefore m is not made in the UK.

2.3 Proof-Practice

Theorem 2.1. Let A, B, C, Ω be sets with $A, B \in \Omega$. Then:

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \tag{1}$$
$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \tag{2}$$
$$(A \cup B)^C = A^C \cap B^C \tag{3}$$
$$(A \cap B)^C = A^C \cup B^C \tag{4}$$

Exercise. Draw Venn diagrams of these statements.

Proof. Consider (1). We show first:

$$A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$$

Suppose that $x \in A \cap (B \cup C)$, then $x \in A$ and $x \in B \cup C$. That means:

$$\begin{aligned} && x \in A \quad \wedge \quad (x \in B \vee x \in C) \\ \Leftrightarrow && x \in A \cap B \quad \vee \quad x \in A \cap C \\ \Leftrightarrow && x \in (A \cap B) \cup (A \cap C) \end{aligned}$$

This shows $\subseteq$. Now we show:

$$A \cap (B \cup C) \supseteq (A \cap B) \cup (A \cap C)$$

Suppose $x \in (A \cap B) \cup (A \cap C)$, then $x \in A \cap B$ or $x \in A \cap C$. We now distinguish between two cases:

1. $x \in A \cap B$. Then $x \in A$ and $x \in B$. Therefore, $x \in A$ and $x \in B \cup C$. Hence, $x \in A \cap (B \cup C)$.
2. $x \in A \cap C$. Then $x \in A$ and $x \in C$. Therefore, $x \in A$ and $x \in B \cup C$. Hence, $x \in A \cap (B \cup C)$.

Remark. We split the proof of C in two cases. In doing so we used the inference rule:

$$((P \vee Q) \wedge (P \Rightarrow R) \wedge (Q \Rightarrow R)) \Rightarrow R$$

Please finish the proof of the other statements in your own. □

Axiom 2.1. *Archimedeon Axiom*

$$\forall r \in \mathbb{R}\ \exists n \in \mathbb{N} : \quad n > r$$

Lemma 2.1.

$$\forall a, x \in \mathbb{R} \qquad \left(\forall n \in \mathbb{N}, n \geq 1 \quad x \geq a - \frac{1}{n}\right) \quad \Rightarrow \quad x \geq a$$

Proof. We argue by contradiction. Hence, we want to show

$$\left(\exists n \in \mathbb{N}, n \geq 1 : \quad x < a - \frac{1}{n}\right) \quad \Leftarrow \quad x \leq a.$$

By the Archimedeon Axiom

$$\exists n : \quad n > \frac{1}{a-x}.$$

And then also

$$\frac{1}{n} < a - x.$$

Therefore

$$x < a - \frac{1}{n}.$$

□

Proposition 1.

$$\bigcup_{n=1}^{\infty} \left[0, 1 - \frac{1}{n}\right] = [0, 1) \tag{1}$$

$$\bigcap_{n=1}^{\infty} \left(1 - \frac{1}{n}, 1 + \frac{1}{n}\right) = \{1\} \tag{2}$$

Proof. (2)
By definition

$$\bigcap_{n=1}^{\infty} A_n = \{a | \; \forall n, a \in A_n\}.$$

Then

$$L = \bigcap_{n=1}^{\infty} \left(1 - \frac{1}{n}, 1 + \frac{1}{n}\right) = \left\{x \in \mathbb{R} \;\middle|\; \forall n \in \mathbb{N}, \; 1 - \frac{1}{n} < x < 1 + \frac{1}{n}\right\}.$$

Clearly $1 \in L$. This proofs $\supseteq$.

No we are going to prove $\subseteq$. We need to show

$$\left(\forall n \in \mathbb{N}, \quad 1 - \frac{1}{n} < x < 1 + \frac{1}{n}\right) \quad \Rightarrow \quad x = 1.$$

By the lemma, $x \geq 1$. There is a similar lemma that states

$$\left(\forall n, \quad x \leq 1 + \frac{1}{n}\right) \quad \Rightarrow \quad x \leq 1.$$

So in fact $x \geq 1$ and $x \leq 1$. Thus $x = 1$. This shows $\subseteq$.
(1)
Recall that by definition

$$\bigcup_{n=1}^{\infty} A_n = \{a | \; \exists n : \; a \in A_n\}.$$

It is easy to see

$$\bigcup_{n=1}^{\infty} \left[0, 1 - \frac{1}{n}\right) \subseteq [0, 1)$$

Indeed if

$$\exists n : \quad 0 \leq x \leq 1 - \frac{1}{n},$$

then

$$0 \leq x < 1.$$

This shows $\supseteq$. Next we show $\subseteq$. This means exactly

$$(0 \leq x < 1) \Rightarrow \left(\exists n : \ 0 \leq x \leq 1 - \frac{1}{n} \right).$$

By the Archimedeon axiom

$$\exists n : \quad n > \frac{1}{1-x}.$$

Hence $\frac{1}{n} < 1 - x$ and then $x < 1 - \frac{1}{n}$. □

Theorem 2.2.

$$\forall n \in \mathbb{N} \qquad n^2 \text{ odd} \quad \Rightarrow \quad n \text{ odd}$$

Flawed proof. If n is odd then $n = 2k + 1$ for some $k \in \mathbb{N}$ and then

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2\left(2k^2 + 2k\right) + 1 \end{aligned}$$

So n^2 is odd.

Proof. We need to take the following statement for granted, which will be proven later in the document:

$$\forall n \in \mathbb{N} \qquad \exists k \in \mathbb{N} : \ n = 2k \quad \vee \quad \exists k \in \mathbb{N} : \ n = 2k + 1$$

Assuming that, we argue by contradiction:

$$\begin{array}{ccc} n \, \text{even} & \Rightarrow & n^2 \, \text{even} \\ n = 2k & \Rightarrow & n^2 = 2\left(2k^2\right) \end{array}$$

□

2.4 Dis-Proving

The negation $\overline{P}$ of a statement P can be formed with the help of the two following rules:

1.
$$\begin{aligned} & P = (\forall x \in A \quad Q(x)) \\ \Rightarrow \qquad & \overline{P} = \left(\exists x \in A \quad \overline{Q(x)} \right) \end{aligned}$$

2.
$$\begin{aligned} & P = (\exists x \in A \quad Q(x)) \\ \Rightarrow \qquad & \overline{P} = \left(\forall x \in A \quad \overline{Q(x)} \right) \end{aligned}$$

Exercise. Show that Rule 2 is the same as Rule 1.

Remark. An element $a \in A$ such that $\overline{Q(a)}$ is called a counterexample to the statement

$$(\forall x \in A, \quad Q(x))$$

Indeed the very existence of this example $a \in A$ shows that P is false (it "counters" P).

A typical exam question is:

Question. Prove or disprove the following statement:
If $p \in \mathbb{N}$ is prime then $\exists a, b \in \mathbb{Z}: \; p = a^2 + b^2$

Answer. This statement is false. Counterexample: 3

$$\begin{aligned}
& P = \big(\forall p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad \big(\exists (a,b) \in \mathbb{Z}^2 : p = a^2 + b^2\big)\big) \\
\Leftrightarrow \quad & \overline{P} = \Big(\exists p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad \overline{\big(\exists (a,b) \in \mathbb{Z}^2 : p = a^2 + b^2\big)}\Big) \\
\Leftrightarrow \quad & \overline{P} = \big(\exists p \in \{n \in \mathbb{N} |\; n \,\text{prime}\}: \quad \big(\forall (a,b) \in \mathbb{Z}^2 : p \neq a^2 + b^2\big)\big)
\end{aligned}$$

We prove $\overline{P}$ thus we have to name a particular prime. We choose $p = 3$ and claim

$$\forall a, b \in \mathbb{Z}: \quad a^2 + b^2 \neq 3.$$

Suppose for contradiction that for some $a, b \in \mathbb{Z}$, $a^2 + b^2 = 3$. Note that $a^2, b^3 \geq 0$ so both $a^2, b^2 \leq 3$ This means that $|a|, |b| \leq 1$ but then $a^2, b^2 \leq 1$ and $a^2 + b^2 \leq 2$. □

3 Natural Numbers

$\mathbb{N}$ is defined by three axioms:

Axiom 3.1. $0 = \emptyset \in \mathbb{N}$

Axiom 3.2. If $n \in \mathbb{N}$ then

$$n + 1 \overset{def}{=} n \cup \{n\} \in \mathbb{N}.$$

Axiom 3.3. *Smallest element axiom.*
Let $\emptyset \neq S \subseteq \mathbb{N}$. Then S has a smallest element, i.e.

$$\exists k: \; \forall a \in S \qquad k \leq a.$$

Remark. A smallest element is clearly unique.

Example 7.

$$\begin{aligned}
1 &= 0 + 1 = \emptyset \cup \{\emptyset\} = \{\emptyset\} \\
2 &= 1 + 1 = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}
\end{aligned}$$

Remark. Although this definition may seem simple and wonderful, we will not bother with the first two axioms in the further discussion of $\mathbb{N}$ and assume common properties of $+, -, \cdot$, and : (which we are not going to define rigorously).

Theorem 3.1.

$$\forall n, p \in \mathbb{N}, \; \exists_1 q, r \in \mathbb{N}, \; 0 \leq r < p: \qquad n = pq + r.$$

Special case.
For $p = 2$ this says that there exists a q such that either $n = 2q$ or $n = 2q + 1$ but not both.

Proof. Let

$$S = \{y \in \mathbb{N} |\; \exists k \in \mathbb{N}: \; y = n - pk\}.$$

$S \neq \emptyset$ because $n \in S$ for $k = 0$. Axiom 3.3 says that S has a smallest element. Let this smallest element be $y_0 = n - pk_0$. We claim $0 \leq y_0 < p$.

Assume for contradiction $y_0 \geq p$. Then we can construct y_0' with

$$\begin{aligned}
y_0' &= y - p \\
&= (n - pk_0) - p \\
&= n - p(k_0 + 1) \in S
\end{aligned}$$

Due to our definition $y_0' < y$. Hence y_0 can not be the smallest element of S and we get a contradiction.

Now that we know that $0 \leq y_0 < p$ and obviously $n = y_0 + pk_0$, we can choose $r = y$ and $q = k_0$. It remains to show uniqueness.

To show uniqueness suppose there exists $q_1, q_2, r_1, r_2 \in \mathbb{N}, 0 \leq r_1, r_2 < p$. (1)
Without loss of generality we may assume $r_1 \leq r_2$. (2)
Hence

$$n = pq_1 + r_1 \tag{3.1}$$

$$n = pq_2 + r_2. \tag{3.2}$$

Subtracting (3.2) from (3.1) gives us

$$\begin{aligned} & 0 = p(q_1 - q_2) + r_1 - r_2 \\ \Leftrightarrow \qquad & r_2 - r_1 = p(q_1 - q_2) \end{aligned}$$

Using (1) and (2) we get

$$0 \leq r_2 - r_1 = (q_1 - q_2)p < p.$$

So $0 \leq q_1 - q_2 < 1$ and therefore $q_1 = q_2$ and $r_1 = r_2$. □

3.1 Proof by Induction

Theorem 3.2. The *Principle of Induction* is the following:
Suppose that $\forall n \in \mathbb{N}$ we are given a statement P_n. We assume that:

1. P_0 holds.
2. $\forall n \in \mathbb{N}, (Pn \Rightarrow P_{n+1})$ holds.

Then for all $n \in \mathbb{N}$, P_n holds.

Example 8. Let

$$P_n : \qquad 0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}.$$

Let us show $P_n \Rightarrow P_{n+1}$. Assume that

$$0 + 1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

then

$$0 + 1 + 2 + \cdots + n + (n+1) = (0 + 1 + 2 + \cdots + n) + (n+1) = \frac{n(n+1)}{2} + n + 1 = \frac{(n+1)(n+2)}{2}$$

P_0 is the statement that $0 = 0$. Therefore $\forall n$ the formula is true.

Proof. We argue by contradiction. Suppose that the conclusion is false. That means:

$$\exists n \in \mathbb{N} : \qquad \overline{P_n}$$

In other words:

$$S = \{n \in \mathbb{N} | \ \overline{P_n}\} \neq \emptyset$$

Let k be the smallest element of S. k exists by the smallest element axiom. $k - 1 < k$, therefore $k - 1 \in S$, thus P_{k-1} holds. But:

$$P_{k-1} \Rightarrow P_k$$

□

Example 9. The Fibonacci sequence. $\forall n \in \mathbb{N}$ define F_n inductively by the formula:

$$F_0 = 0, \quad F_1 = 1, \quad \forall n \geq 2 F_n = F_{n+1} + F_{n+2}$$

Let us prove by induction that:

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right) = \frac{\varphi^n - \psi^n}{\sqrt{5}}$$

The really interesting thing would be to understand how one can ”come up” with a formula like this. Another interesting thing would be to ”stare” at the formula and see what we can learn from it about life. Instead wo focus on a ”minor” print of logic.

Wrong proof. To prove by induction you need to declare at the outset, $\forall n$ what is P_n. Your instinct here will be to say

$$P_n : \qquad F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right)$$

Then you will write:

$$\begin{aligned} F_{n+1} &= F_n + F_{n+1} \\ &= (\dots) + (\dots) \end{aligned}$$

Remark. You have used both, P_{n-1} and P_n. However, for induction you can only use P_n.

Proof. We use the principle of induction with:

$$Q_n = (P_n \wedge P_{n+1})$$

We need to show $\forall n : \ Q_n \Rightarrow Q_{n+1}$. Suppose $(P_n \wedge P_{n+1} \Rightarrow P_{n+1}) \Rightarrow ((P_n \wedge P_{n+1}) \wedge (P_{n+1} \wedge P_{n+2}))$. Hence we only need to proof that $P_n \wedge P_{n+1} \Rightarrow P_{n+2}$ Assume $P_n \wedge P_{n+1}$, then:

$$\begin{aligned} F_{n+1} = F_{n+1} + F_n &= \frac{1}{\sqrt{5}} \left(\varphi^{n+1} - \psi^{n+1} \right) + \frac{1}{\sqrt{5}} \left(\varphi^n - \psi^n \right) \\ &= \frac{1}{\sqrt{5}} \varphi^n (\varphi + 1) + \frac{1}{\sqrt{5}} \psi^n (\psi + 1) \end{aligned}$$

Since φ and ψ are solutions of the equation $x^2 - x - 1 = 0$ we can rewrite that as:

$$\begin{aligned} &\frac{1}{\sqrt{5}} \varphi^n \varphi^2 + \frac{1}{\sqrt{5}} \psi^n \psi^2 \\ =&\frac{1}{\sqrt{5}} \varphi^{n+2} + \frac{1}{\sqrt{5}} \psi^{n+2} \end{aligned}$$

So P_{n+2} holds. We have shown that $\forall n : \ Q_n \Rightarrow Q_{n+1}$. To finish the proof we need $Q_0 = (P_0 \wedge P_1)$.

$$\begin{aligned} &P_0 \qquad && F_0 = \frac{1}{\sqrt{5}} \left(\varphi^0 - \psi^0 \right) = 1 \\ &P_1 \qquad && F_1 = \frac{1}{\sqrt{5}} \left(\varphi^1 - \psi^1 \right) = 1 \end{aligned}$$

□

Theorem 3.3. Principle of strong induction.
Suppose that $\forall n \in \mathbb{N}$ we are given a statement Q_n. Assume that:

1. Q_0 holds;
2. $\forall n, \ (\forall k \leq n : \ Q_k) \Rightarrow Q_{n+1}$

Then $\forall n \in \mathbb{N}, \ Q_n$ holds.

Proof. Apply induction with:

$$(Q_0 \wedge Q_1 \wedge \cdots \wedge Q_n)$$

□

3.2 Prime numbers

Definition 3.1. $n \neq 0, 1 \in \mathbb{N}$ is irreducible if:

$$\forall u, v \in \mathbb{N} : \quad n = uv \quad \Rightarrow \quad u = 1 \vee v = 1$$

Theorem 3.4. Every $n \in \mathbb{N}, n \neq 0, 1$ is the product of irreducibles.

Proof. We are going to prove the statement by strong induction. Let Q_n be the statement that n is the product of irreducibles.

Q_0 clearly holds.

Assume Q_n for $k \leq n$. If $n+1$ is irreducible then Q_{n+1}. Otherwise $n+1 = u \cdot v$ where $1 < u < n+1$ and $1 < v < n+1$. By Q_u, u is prod of irreducibles. By Q_v, v is the product if irreducibles. Therefore, Q_{n+1} holds. □

Definition 3.2. For $c, a \in \mathbb{Z}$ we say that c divides A and write $c|A$ if

$$\exists R \in \mathbb{Z} : \quad cR = A$$

Remark.

$$c|A_1 \wedge c|A_2 \Rightarrow c|(A_1 + A_2)$$
$$c|A \Rightarrow \forall B \in \mathbb{Z}, c|AB$$

Definition 3.3.

$$\forall a, b \in \mathbb{Z} : \quad hcf(a, b) = \text{Highest Common Factor} = \max\{t \in \mathbb{Z} | \quad t|a \wedge t|b\}$$

Remark.

$$\text{hcf}(a, b) = \text{hcf}(\pm a, \pm b) \in \mathbb{N} = \text{hcf}(b, a)$$

Let us now consider the *Division Algorithm* to compute the highest common factor.
Suppose $a, b \in \mathbb{N}$ with $a \geq b$. We know from last time:

$$\exists q, r \in \mathbb{N}, \quad 0 \leq r < b : \quad a = bq + r$$

Note that

$$(t|a \wedge t|b) \quad \Leftrightarrow \quad (t|b \wedge t|r)$$

This implies that $\text{hcf}(a, b) = \text{hcf}(b, r)$. $a \geq b > r$ so the pair (b, r) is smaller than the pair (a, b), hence our algorithm will eventually come to an end. And I can assume by induction that I know to compute k and (b, r).

Theorem 3.5. If $c = \text{hcf}(a, b)$ then

$$\exists y, x \in \mathbb{Z} : \quad c = ac + by$$

Proof. Assume $a \geq b > 0$ then write $a = bq + r$. But what we said:

$$\text{hcf}(a, b) = \text{hcf}(q, r) = c$$

(q, r) is smaller than (a, b) so by induction there exist x_0, g_0 such that

$$\begin{aligned} c &= rx_0 + by_0 \\ &= (a - bq)x_0 + by_0 \\ &= ax_0 + b(y_0 - qx_0) \end{aligned}$$

□

Example 10. Compute $\mathrm{hcf}(1734, 371) = c$ and $x, y \in \mathbb{Z}$ such that $1734 + 371y = c$

$$\begin{aligned} && 1734 &= 4 \cdot 371 + 250 \\ \Rightarrow && \mathrm{hcf}(1734, 371) &= \mathrm{hcf}(371, 250) \\ && 371 &= 1 \cdot 250 + 121 \\ \Rightarrow && \mathrm{hcf}(371, 250) &= \mathrm{hcf}(250, 121) \\ && 250 &= 2 \cdot 121 + 8 \\ \Rightarrow && \mathrm{hcf}(250, 121) &= \mathrm{hcf}(121, 8) \\ && 121 &= 15 \cdot 8 + 1 \\ \Rightarrow && \mathrm{hcf}(121, 8) &= \mathrm{hcf}(8, 1) \end{aligned}$$

So $c = 1$.

$$\begin{aligned} 1 &= -15 \cdot 8 + 121 \\ &= -15(-2 \cdot 121 + 250) + 121 \\ &= 31 \cdot 121 - 12 \cdot 250 \\ &= 31 \cdot (-1 \cdot 250 + 371) - 15 \cdot 250 \\ &= -46 \cdot 250 + 31 \cdot 371 \\ &= -44(-4 \cdot 371 + 1734) + 31 \cdot 371 \\ &= 215 \cdot 371 - 46 \cdot 1734 \end{aligned}$$

Definition 3.4. We say that $a, b \in \mathbb{Z}$ are *co-prime* if $\mathrm{hcf}(a, c) = 1$.

Definition 3.5. $p \in \mathbb{N} \backslash \{0, 1\}$ is prime if:

$$\forall A, B \in \mathbb{Z} : \quad p|AB \Rightarrow p|A \vee p|Q$$

Theorem 3.6. $P \in \mathbb{N}$ is irreducible if and only if it is prime.

Proof. Suppose p is prime, i.e.

$$p|uv \quad \Rightarrow \quad (p|u \vee p|v)$$

If $p|u$ then $u = kp$ and

$$p = uv = (kv)p \quad \Rightarrow \quad 1 = kv \quad \Rightarrow \quad v = 1$$

Similarly if $p|v$ then $u = 1$. This shows p is irreducible.

Now suppose p is irreducible. Suppose $p|AB$. Because p is irreducible, the positive divisors of p are just 1 and p. Therefore, either $\mathrm{hcf}(p, A) = 1$ or $\mathrm{hcf}(p, A) = p$.

If $\mathrm{hcf}(p, A) = p$ then $p|A$ and we can close. Suppose $hcf(p, A) = 1$. Then $\exists x, y \in \mathbb{Z}$ such that:

$$xp + yA = 1$$

But then

$$xpB + yAB = B$$

p divides the first part because there is a p there. p divides the second part because we are assuming $p|AB$. So $p|B$. □

Definition 3.6. Let p be prime. Then

$$\forall N \in \mathbb{Z}, \quad \mathrm{ord}_p N = \max \left\{ k \in \mathbb{N} | \quad p^k | N \right\}$$

= exponent of the largest power of p that divides n.

Example 11.

$$\begin{aligned} \mathrm{ord}_2 3 &= 0 \\ \mathrm{ord}_2 24 &= 3 \end{aligned}$$

Property 6.1.

$$\forall N_1, N_2 \in \mathbb{Z} \qquad \operatorname{ord}_p(N_1 + N_2) \geq \min\{\operatorname{ord}_p N_1, \operatorname{ord}_p N2\} \tag{1}$$

$$\operatorname{ord}_p(N_1, N_2) = \operatorname{ord}_p N_1 + \operatorname{ord}_p N_2 \tag{2}$$

Proof. (1) If $p^k|N_1$ and $p^k|N_2$ then $p^k|N_1 + N_2$.

(2)

$$a_1 = \operatorname{ord}_p N_i$$

means

$$p^{a_i}|N_i \quad \wedge \quad p^{a_i+1} \nmid N_i$$

It is clear that

$$(p^{a_i}|N \wedge p^{a_2}|N_2) \quad \Rightarrow \quad p^{a_1+a_2}|N_1N_2$$

What we need to show is:

$$p^{a_1+a_2+1} \nmid N_1N_2$$

Write $N_i = p^{a_i}A_i$ where $p_i \nmid A_i$. Then

$$N_1N_2 = p^{a_1+a_2}A_1A_2$$

and

$$p \nmid A_1, p \nmid A_2 \quad \Rightarrow \quad p \nmid A_1A_2$$

□

Result 3.2.1. If p is a prime then $\sqrt{p}$ is irrational.

Proof. Suppose for contradiction that $r^2 = p$ with $r = \frac{k}{n} \in \mathbb{Q}$.

$$\frac{k^2}{n^2} = p$$

or equivalently:

$$k^2 = pn^2$$
$$2\operatorname{ord}_p k = \operatorname{ord}_p(pn^2) = 1 + 2\operatorname{ord}_p n$$

This is a contradiction. (A number can only be either odd or even but not both.) □

Definition 3.7. $N \in \mathbb{Z}$ is a perfect square if $\exists k \in \mathbb{Z} : N = k^2$.

Exercise. N is a perfect square iff for all primes p, $\operatorname{ord}_p N$ is even.

Example 12. $\sqrt{N} \in \mathbb{Q} \;\Leftrightarrow\; N$ is a perfect square.

Proof. $\Leftarrow$ is obvious.

We need to deal with $\Rightarrow$. Suppose $\exists r = \frac{k}{n} \in \mathbb{Q}$ such that $r^2 = N$.

Suppose for contradiction that N is not a perfect square. i.e. there exists a prime p such that $\operatorname{ord}_p N$ is odd. As before we write:

$$k^2 = n^2N$$
$$2\operatorname{ord}_p k = \operatorname{ord}_p k^2 = 2\operatorname{ord}_p n + \operatorname{ord}_p N$$

This is a contradiction because we have an even number on the left and an odd number on the right hand side. □

Theorem 3.7. The fundamental theorem of arithmetic.
Every $n \in \mathbb{N}$ can be written uniquely in the form:

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

where $p_1 < p_2 < \dots < p_r$ are primes and $a_i \in \mathbb{N} \backslash 0$ for $i \in \mathbb{N} \backslash \{0\}$.

Proof. We already know that n can be written like this. For uniqueness:

$$a_i = \operatorname{ord}_{p_i} n$$

□

Remark. What you are really doing is:

$$\begin{aligned} & n = p_1^{a_1} \dots p_r^{a_r} \\ \Rightarrow \qquad & \operatorname{ord}_{p_i} n = \operatorname{ord}_{p_i} (p_1^{a_1} \dots p_r^{a_r}) \\ & = a_1 \operatorname{ord}_{p_i} p_1 + \dots a_{i-1} \operatorname{ord}_{p_i} p_{i-1} + a_i \operatorname{ord}_{p_i} p_i + a_{a+1} \operatorname{ord}_{p_i} p_{i+1} + \dots + a_r \operatorname{ord}_{p_i} p_r = a_i \end{aligned}$$

because $\operatorname{ord}_{p_i} p_i = 1$ and $\operatorname{ord}_{p_j} p_j = 0$ if $i \neq j$.

Example 13. There are infinitely many primes. Suppose for a contradiction that:

$$\mathbb{P} = \{\text{all primes}\} = \{p_1 < p_2 < \dots < p_r\}$$

Consider $N = p_1 p_2 \dots p_r + 1$. Claim $\operatorname{hcf}(N, p_i) = 1$ for all $i = 1, \dots, r$. Manifestly $\exists x, y \in \mathbb{Z}$ such that $xN + yp_i = 1$. Hence, N contradicts the prime decomposition theorem.

New things about hcf.

Lemma 3.1. Suppose $\operatorname{hcf}(a, b) = 1$. Then for all $C \in \mathbb{N}$

$$(a|C \wedge b|C) \Rightarrow ab|C \tag{1}$$

$$a|bC \Rightarrow a|C \tag{2}$$

Proof.

$$\exists x, y \in \mathbb{Z} : \quad ax + by = C \tag{$*$}$$

For (1) multiply $(*)$ with C. We get

$$axC + byC = C$$

$b|C \Rightarrow ab|aC$ so ab divides axC. $a|C \Rightarrow ab|bC$ so ab divides byC. Therefore, $ab|C$.

For (2) again

$$axC + byC = C$$

a obviously divides axC and byC as well because of our assumption. Thus $a|C$. □

Theorem 3.8. Suppose $c|a$ and $c|b$. Then $c|\operatorname{hcf}(a, b)$.

Proof. Indeed let $d = \operatorname{hcf}(a, b)$. We know $\exists x, y \in \mathbb{Z}$ such that

$$ax + by = d$$

c divides ax as well as bx. Thus, $c|d$ □

It follows easily from unique prime factorization that for all p, $\operatorname{ord}_p \operatorname{hcf}(a, b) = \min\{\operatorname{ord}_p a, \operatorname{ord}_p b\}$. Another way to say this is: if

$$a = \Pi p_i^{r_i}, b = \Pi p_i^{s_i}$$

Then

$$\operatorname{hcf}(a, b) = \Pi p_i^{\min\{r_i, s_i\}}$$

Remark. This is a really bad method for computing the hcf.

Example 14.

- (a Diophantine equation)
  Solve for $x, y \in \mathbb{N}$:

$$4y^2 = x^3 + 1$$

Write this as:

$$x^3 = 4y^2 - 1 = (2y+1)(2y-1)$$

Note that $\text{hcf}(2y+1, 2y-1) = c = 1$:

$$(c|2y+1 \ \wedge \ c|2y-1) \quad \Rightarrow \quad c| \ (2y+1) - (2y+1) = 2$$

but both numbers are odd so $c = 1$.

Suppose $\text{hcf}(A, B) = 1$ and $AB = x^3$ is a perfect cube. Then both A, B are perfect cubes. Indeed, if p prime, $\text{ord}_p AB = 3k$ and at least one of $\text{ord}_p A, \ \text{ord}_p B = 0$.

So $2y-1, 2y+1$ are both perfect cubes. Only small cubes can have such a small distance.

$$\ldots \quad -27 \quad -8 \quad -1 \quad 0 \quad 1 \quad 8 \quad 27 \quad \ldots$$

At the end:

$$\begin{aligned} 2y - 1 &= -1 \\ 2y + 1 &= 1 \\ \Rightarrow \qquad y = 0 \quad &\wedge \quad x = -1 \end{aligned}$$

These are all the solutions!

- Consider the equation

$$3x + 7y = 18, \qquad (x, y) \in \mathbb{Z}^2 \tag{1}$$

Ordinarily, you would use Euklid's algorithm to find one solution. This solution can then help to find the general solution. In this case it is easy to spot one: $(x, y) = (6, 0)$. Write $(x, y) = (x_0, y_0) + (x', y')$ and

$$\begin{aligned} & 3x + 7y = 18 \\ \Leftrightarrow \qquad & 3x' + 7y' = 0 \end{aligned} \tag{2}$$

Thus, finding all solutions of (2) is the same as finding all solutions of (1). Note: $7y' = -3x'$.

$$(\text{hcf}(7,3) = 1 \quad \wedge \quad 7|3x') \qquad \Rightarrow 7|x'$$

Therefore, there exists a $t \in \mathbb{Z} : x' = 7t$. Then $7y' = -3t$ The set of all solutions is precisely:

$$\{(x, y) | \quad (x, y) = (6, 0) + t(7, -3), \quad t \in \mathbb{Z}\}$$

We think of this as a parametrised 'integral line'.

Let us regard the general case of the example above. Suppose $A, B, C \in \mathbb{Z}$. We want to find all solutions $(x, y) \in \mathbb{Z}^2$ of:

$$Ax + By = C \tag{*}$$

Sometimes we may want to look for $(x, y) \in \mathbb{N}^2$. Suppose $\text{hcf}(a, b) = d$. Then we write

$$\begin{aligned} a &= da' \\ b &= db' \end{aligned}$$

with $a', b' \in \mathbb{Z}$ and co-prime.

Remark. $(*)$ has a solutions x_0, y_0 iff $d = \text{hcf}(a, b)|c$.

Proof. Suppose $ax_0 + by_0 = c$ Then $d|a$ and $d|b$ and hence $d|c$. Vice versa suppose that $d|c$, i.e. $c = dc'$. We know that there exists $u, v \in \mathbb{Z}$ such that $au + bv = d$ and then $x_0 = ac'$, $y_0 = vc'$ satisfy

$$ax_0 + by_0 = auc' + bvc' = dc' = c$$

□

Remark. Euklid's algorithm gives us a way to compute a solution x_0, y_0 of $(*)$ if a solution exists. The problem is to find all other solutions.

Suppose that x_0, y_0 is a solution of $(*)$. Write

$$(x, y) = (x_0, y_0) + (x', y')$$

then x, y is a solution of $(*)$ is a solution of the homogeneous equation.

$$ax' + bx' = 0 \tag{1}$$

(1) is equivalent to:

$$a'x' + b'y' = 0 \tag{2}$$

Now $\text{hcf}(a', b') = 1$. Write

$$-b'y' = a'x'$$

and notice $b'|a'x'$. Since $\text{hcf}(b'a') = 1$ then $b'|x'$. Wo we can write $x' = tb'$ for some $t \in \mathbb{Z}$ Then (2) says

$$b'a't + b'y' = 0$$

So

$$a't + y' = 0$$

i.e. $y' = a't$. Conclusion: The set of solutions of (1) is

$$\{(x, y) = t(b' - a')| \quad t \in \mathbb{Z}\}$$

The set of solutions of $(*)$ is

$$\{(x, y) + (x_0 + y_0) = t(b' - a')| \quad t \in \mathbb{Z}\}$$

This is the end of the general theory.

Example 15. Find all $c \in \mathbb{Z}$ such that the equation

$$5x + 11y = c$$

has a solution $(x, y) \in \mathbb{N}^2$ All integer solutions (x, y) are of the form $(x, y) = (x_0, y_0) + t(11, -5)$. (this idea can be obtained by drawing the graph. The slope of the line is $\frac{-11}{5}$)

If c is big enough we can always find a positive solution (x, y) with $x \geq 0$, $y \geq 0$. By adding/subtracting an integer multiple of the vector $(11, -5)$. This will work if:

$$\begin{aligned} & \sqrt{\frac{c^2}{5^2} + \frac{c^2}{11^2}} \geq \sqrt{11^2 + 5^2} \\ \Leftrightarrow \quad & \frac{c}{55}\sqrt{11^2 + 5^2} \geq \sqrt{1^2 + 5^2} \end{aligned}$$

If $c \geq 55$ then a solution $(x, y) \in \mathbb{N}^2$ exists. For every pair $(x, y) \in \mathbb{N}$ we compute $5x + 11y$. We can get the following possible sums smaller than 55

$$\begin{aligned} & 0, 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, \\ & 11, 16, 21, 26, 31, 36, 41, 46, 51, \\ & 22, 27, 32, 37, 42, 47, 52, \\ & 33, 38, 43, 48, 53, \\ & 44, 49, 54 \end{aligned}$$

Conclusion: The equation $5x + 11y = c$ has a solution $(x, y) \in \mathbb{N}^2$ iff

$$c \in \{0, 5, 10, 11, 15, 16, 20, 21, 22, 25, 26, 27, 30, 31, 32, 33, 35, 36, 37, 38\} \quad \vee \quad c \leq 40$$

Relations

Definition 3.8. The *Cartesian Product* of two sets A, B is the set

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

where (a,b) is an ordered pair.

Example 16. Suppose $A = \{1,2,3\}$, $B = \{1,2\}$. Then

$$A \times B = \{(1,1),(1,2),(2,1),(2,2),(3,1),(3,2)\}$$

Definition 3.9. A relation on a set S is a subset $R \subseteq S \times S$. We write

$$aRb \quad \text{or} \quad a \sim_R b \qquad \Leftrightarrow \qquad (a,b) \in R$$

Example 17.

- Let S be this room.

$$R = \{(a,b)| \quad a \text{ is in love with } b\}$$

- Some mathematical examples

$$\begin{aligned} \triangle &= \{(a,a)| \quad a \in S\} \\ R &= S \times S \backslash \triangle \end{aligned}$$

Some relations on $\mathbb{R}$ are

$$\begin{aligned} A &= \{(a,b)| \quad a \leq b\} \subseteq \mathbb{R}^2 \\ B &= \{(a,b)| \quad a < b\} \subseteq \mathbb{R}^2 \\ C &= \{(x,y) \in \mathbb{R}^2| \quad y^2 - x^2 = 1\} \subseteq \mathbb{R}^2 \end{aligned}$$

Example 18. How many relations are there on the set $S = \{1,2\}$? A relation on $S = \{1,2\}$ is precisely a subset of $S \times S = \{(1,1),(1,2),(2,1),(2,2)\}$. Hence, there are $2^4 = 16$ Relations on the set.

Remark. If T is a set with n elements, then T has 2^n subsets. (We will prove that further in these notes.)

Property 9.1.

- R is reflexive if for all $a \in S$, $\quad (a,a) \in \mathbb{R}$.
- R is symmetric if for all $a, b \in S$, $\quad (a,b) \in R \Rightarrow (b,a) \in R$.
- R is transitive if for all $a, b, c \in S$, $\quad (a,b) \in R \wedge (b,c) \in R \Rightarrow (a,b) \in R$.
- R is an equivalence relation if R is reflexive, symmetric and transitive

Now we have the language to speak about modular arithmetic:
Fix $m \in \mathbb{N}$. Then we define a relation R on $\mathbb{Z}$:

$$R = \{(a,b) \in \mathbb{Z} \times \mathbb{Z}| \quad m|(a-b)\}$$

Notation

$$a \sim_R b \qquad \Leftrightarrow \qquad a \equiv b \qquad \text{mod } m$$

read a congruent to B mod n. This is the same as saying:
Dividing m into a or b leaves the same remainder.

Property 9.2.

$$\begin{array}{lrcl} \forall a \in \mathbb{Z} & a \equiv a & & \text{mod } m \\ \forall a,b \in \mathbb{Z} & m|a-b & \Leftrightarrow & m|b-a \\ \forall a,b,c \in \mathbb{Z} & m|a-b \wedge m|b-c & \Rightarrow & m|(a-b)+(b-c)=(a-c) \end{array}$$

Therefore, $\equiv \quad \text{mod } m$ is an equivalence relation.

Definition 3.10. Let $\sim$ be an equivalence relation on a set S. For all $a \in S$ we define

$$[a] = \{b \in S| \quad a \sim b\}$$

Theorem 3.9.

$$a \sim b \qquad \Leftrightarrow \qquad [a] = [b] \qquad (1)$$

$$a \nsim b \qquad \Leftrightarrow \qquad [a] \cap [b] = \emptyset \qquad (2)$$

Proof. (1). first prove $\Rightarrow$. We show first $[a] \subseteq [b]$.

Suppose $a \sim c$ then $c \sim a$ and $a \sim b \Rightarrow c \sim b \Rightarrow b \sim c$. So $c \in [b]$.

Similarly $[b] \subseteq [a]$.

$\Leftarrow$ is pretty obvious.

(2). Suppose $[a] \cap [b] \neq \emptyset$. so let $c \in [a] \cap [b]$. Hence, $a \sim c, b \sim c$. Therefore $a \sim c$ and $c \sim b$ and thus $a \sim b$ So $[a] = [b]$. Please finish the proof by yourself. □

Definition 3.11. The *quotientset* of S by an equivalence relation R is

$$S/R := \{[a] \mid \quad a \in S\} \subseteq P(S)$$

where $P(S) = \{A| \quad A \subseteq S\}$.

Suppose that we know how to choose a unique distinguished element in each equivalence class on a set S: denote by $\overline{a}$ the distinguished element in $[a]$. (So if $b \in [a]$ then $\overline{a} = \overline{b}$. Then we can form a concrete model

$$S/R = \{\overline{a} \mid \quad a \in S\} \subseteq S$$

3.3 Modular Arithmetic

Fix $n \geq 2, m \in \mathbb{N}$

$$a \equiv b \mod n$$

iff $m|a-b$. The quotientset is denoted $\mathbb{Z}/m\mathbb{Z}$.

$$\forall a \quad \exists! r \quad 0 \leq r < m : \qquad a = qm + r$$

We call this r the smallest residue of $a \mod m$, we denote it by $\overline{a}$. So

$$\overline{a} = \overline{b} \quad \Leftrightarrow \quad a \equiv b \mod m$$

Example 19.

$$\overline{7} = 1 = \overline{10} \mod 3$$

Every equivalence class has a unique distinguished representative in $\{0, 1, 2, 3, \ldots, n-1\} \subseteq \mathbb{Z}$. so we can think of $\mathbb{Z}/m\mathbb{Z}$ as 'being' the set $\{0, 1, 2, 3, \ldots, n-1\}$.

Theorem 3.10. Suppose $m \in \mathbb{N}$

$$\begin{aligned} a \equiv b &\mod m \\ c \equiv d &\mod m \\ \Rightarrow \qquad a + c \equiv b + d &\mod m \\ \wedge \qquad a \cdot c \equiv b \cdot d &\mod m \end{aligned}$$

This defines the operations $+, \cdot$ on $\mathbb{Z}/m\mathbb{Z}$.

Property 0.1. These operations have familiar rules:

$$\begin{aligned} a + b \equiv b + a &\qquad \mod m \\ a \cdot b \equiv b \cdot a &\qquad \mod m \\ a \cdot (b + c) \equiv a \cdot b + a \cdot c &\qquad \mod m \end{aligned}$$

Example 20. Addition and multiplication tables in $\mathbb{Z}/m\mathbb{Z}$. Addition table:

	0	**1**	**2**	**3**	**4**	**5**
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Multiplication table:

	0	**1**	**2**	**3**	**4**	**5**
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

The thing to note here is: In $\mathbb{Z}/6\mathbb{Z}$ $\overline{2}, \overline{3} \neq 0$ but $\overline{2} \cdot \overline{3} = 0$.

Example 21. Multiplication table in $\mathbb{Z}/5\mathbb{Z}$:

	0	**1**	**2**	**3**	**4**
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Remark. In $\mathbb{Z}/5\mathbb{Z}$

$$(a \neq 0 \quad \wedge \quad b \neq 0) \qquad \Leftrightarrow \qquad ab \neq 0$$

In $\mathbb{Z}/5$ every $a \neq 0$ has a multiplicative inverse a^{-1}:

$$1^{-1} = 1 \quad 2^{-1} = 3, \quad 3^{-1} = 2, \quad 4^{-1} = 4$$

Theorem 3.11. In $\mathbb{Z}/m\mathbb{Z}$ every nonzero element has a multiplicative inverse iff m is prime.

Proof. Suppose m is prime. Let $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. To find a multiplicative inverse of a is exactly the same as solving

$$ax = 1 \qquad \text{in } \mathbb{Z}/p\mathbb{Z}$$

that is $ax - 1 = py$. That is: Find $x, y \in \mathbb{Z}$ such that $ax - py = 1$. We can do that iff $\operatorname{hcf}(a, p) = 1$. Since p is prime this is the same as $p \nmid a$ and this is the same as saying $a \not\equiv 0 \mod p$.

On the other hand if m is not prime, then there exist m_1, m_2 with $m = m_1 \cdot m_2$ and $1 < m_1, m_2 < m$.

$$\begin{aligned} m_1 &\not\equiv 0 && \mod m \\ m_2 &\not\equiv 0 && \mod m \end{aligned}$$

but

$$m_1 \cdot m_2 \equiv 0 \mod m$$

So neither m_1 nor m_2 have a multiplicative inverse.

Indeed if there was a u_1 such that

$$u_1 m_1 \equiv 1 \mod m$$

then

$$\begin{aligned}(u_1m_1)m_2 &\equiv m_2 \not\equiv 0 && \mod m\\ &= u_1(m_1m_2) \equiv 0 && \mod m\end{aligned}$$

□

Example 22.

- What is $2^{100} \mod 15$?

$$2^4 \equiv 1 \mod 15$$

so $2^{100} = (2^4)^{25} \equiv 1 \mod 15$.

- Compute $5^{67} \mod 14$. We first have to find the binary expansion of 67 which is 1000011. Idea:

$$\begin{aligned}67 &= 64 + 2 + 1\\ &= 2^6 + 4 + 1\\ 5^2 &\equiv 11 && \mod 14\\ 5^4 &\equiv (5^2)^2 = 9 && \mod 14\\ 5^8 &\equiv 9^2 = 11 && \mod 14\\ 5^{16} &\equiv 11^2 = 9 && \mod 14\\ 5^{32} &\equiv 11 && \mod 14\\ 5^{64} &\equiv 9 && \mod 14\\ 5^{67} = 5^{64}\cdot 5^2 \cdot 5 &\equiv 9 \cdot 11 \cdot 5 \equiv 5 && \mod 14\end{aligned}$$

- Prove that

$$\forall n \in \mathbb{N}, \qquad \sqrt{5n+3} \notin \mathbb{Q}$$

All we need to show is that for all $n \in \mathbb{N}, 5n+3$ is not a perfect square, i.e. for all $n \in \mathbb{N}$ the equation

$$5n + 3 = x^2$$

has no interger solution $x \in \mathbb{Z}$. Something stronger is true:

$$x^2 \equiv 3 \qquad \mod 5$$

has no solution in $\mathbb{Z}/5\mathbb{Z}$.

$$\begin{array}{lllll} x \equiv 0 & \mod 5 & \Rightarrow & x^2 \equiv 0 & \mod 5\\ x \equiv 1 & \mod 5 & \Rightarrow & x^2 \equiv 1 & \mod 5\\ x \equiv 2 & \mod 5 & \Rightarrow & x^2 \equiv 4 & \mod 5\\ x \equiv 3 & \mod 5 & \Rightarrow & x^2 \equiv 4 & \mod 5\\ x \equiv 4 & \mod 5 & \Rightarrow & x^2 \equiv 1 & \mod 5\end{array}$$

So no x satisfies $x^2 \equiv 3 \mod 5$.

Remark. The same argument also shows that for all $n \in N, 5n+2$ is not a perfect square

- Show that the only solution of

$$x^2 + 5y^2 = 3z^2$$

for $x, y, z \in \mathbb{Q}$ is the trivial solution $x = 0,\ y = 0\ , z = 0$.

The first thing to note is: If x_0, y_0, z_0 is a solution and $r \in \mathbb{Q}$, then rx_0, ry_0, rz_0 is also a solution. Suppose for contradiction that $x_0, y_0, z_0 \in \mathbb{Q}$ is a nontrivial solution. Multiplying x_0, y_0, z_0 by a common denominator, we may assume that $x_0, y_0, z_0 \in \mathbb{Z}$ and $\text{hcf}(x_0, y_0, z_0) = 1$. In particular then reducing the equation mod 5 we get $x^2 \equiv 3z^2 \mod 5$. If $z \equiv 0 \mod 5$ then also $x \equiv 0 \mod 5$. Assume $z_0 \not\equiv 0 \mod 5$. Then z has a multiplicative inverse mod 5. I.e. there exists a $w_0 \in \mathbb{Z}$ such that

$$z_0 w_0 \equiv 1 \mod 5$$

Multiply by w_0^2:

$$(x_0 w_0)^2 \equiv 3(z_0 w_0)^2 \equiv 3 \mod 5$$

and this is impossible. So x_0, z_0 are both $\equiv 0 \mod 5$

$$x_0 = 5x_0', z_0 = 5z_0'$$

plug back into (*)

$$25x_0'^2 + 5y_0^2 = 75x_0'x_0'^2$$

Divide then by 5:

$$5x_0'^2 + y_0^2 = 15z_0'^2$$
$$y_0^2 = 5(3z_0'^2 - x_0'^2)$$

So $5|y_0^2$ and $5|y_0$ as well. In fact $5|x_0, y_0 z_0$. This is a contradiction because:

$$\text{hcf}(x_0, y_0 z_0) = 1$$

Hence every solution is trivial.

Proposition 2. The equation

$$ax \equiv 1 \mod m$$

is solvable for x if and only if $\text{hcf}(a, m) = 1$. I.e. a has a multiplicative inverse mod m if and only if $\text{hcf}(a, m) = 1$

Proof.

$$ax \equiv 1 \mod \quad \Leftrightarrow \quad \exists y : \quad ax + my = 1$$

The equation is solvable if and only if

$$\exists x, y \in \mathbb{Z} : \quad ac + my = 1$$

We know this is equivalent to $\text{hcf}(a, m) = 1$. □

Remark. $\text{hcf}(a, m)$ only depends on $[a] \mod m$. i.e. for all $k \in \mathbb{Z}$:

$$\text{hcf}(a + kn, m) = \text{hcf}(a, m)$$

Definition 3.12. Let A be a set. Denote the number of elements of A, $|A| = \#A$.

Example 23. $|\mathbb{Z}/m\mathbb{Z}| = m$.

Definition 3.13. Let $(\mathbb{Z}/m\mathbb{Z})^x$ be the set of $[a]$ which have a multiplicative inverse. That means:

$$(\mathbb{Z}/m\mathbb{Z})^x = \{r |\ 0 \leq r < m \wedge \text{hcf}(r, m) = 1\}$$

Furthermore, define Euler's function φ with

$$\varphi(m) := |(\mathbb{Z}/m\mathbb{Z})^x|\,.$$

Example 24. If p is prime then for all $a \in \mathbb{Z}$ either $p|a$ or $\text{hcf}(p, a) = 1$ so $\varphi(p) = p - 1$. We will soon know how to compute $\varphi(m)$ for all $m \in \mathbb{N}$.

Exercise. If $a, b, c \in \mathbb{Z}$, define $\text{hcf}(a, b, c) = \max\{t \in \mathbb{Z} | t|a \wedge t|b \wedge t|c\}$. Prove

- $\text{hcf}(a, b, c) = \text{hcf}(\text{hcf}(a, b), c)$.
- there exist integers $p, q, s \in \mathbb{Z}$ such that

$$\text{hcf}(a, b, c) = ap + bq + cs$$

- Use unique factorization to show:

$$\forall p \text{ prime} \qquad \text{ord}_p \text{hcf}(a, b, c) = \min\{\text{ord}_p a, \text{ord}_p b, \text{ord}_p c\}$$

4 Functions

Definition 4.1. Let A, B be sets. Let C be a subset of $A \times B$ such that

$$\forall a \in A\ \exists_1 b \in B : \qquad (a, b) \in C$$

Then a *function* F from A to B is defined as the triple:

$$F = (A, B, C)$$

If $(a, b) \in C$ we write $b = F(a)$ and say that b is the *value* of F at a. A is called the *domain* of f. B is called the *range* of f.

$$\{b \in B| \quad \exists a \in A : \ f(a) = b\} \subseteq B$$

is called the *image* of f.

Notation: $F : \ A \to B$ for a function F from A to B.

A function is a set of arrows. For a set of arrows to be a function means that for all $a \in A$ there is a unique arrow starting at a.

Remark. In the following, if we talk about a function $F = (A, B, C)$ we will mostly refer to the set C.

Example 25.

$$\begin{aligned} f :\ \mathbb{R} \to \mathbb{R} : &\qquad f(x) = x^2 \\ f = \{(x, y) \in \mathbb{R} \times \mathbb{R}| &\quad y = x^2\} \\ f' :\ \mathbb{R} \to [0, \infty) : &\qquad f'(x) = x^2 \\ f' = \{(x, y) \in \mathbb{R} \times [0, \infty)| &\quad y = x^2\} \end{aligned}$$

Note that $f \neq f'$:

$$\begin{aligned} \text{range}(f) &= \mathbb{R} \\ \text{image}(f) &= \mathbb{R}_{\geq 0} \\ \text{range}(f') &= \mathbb{R}_{\geq 0} \\ \text{image}(f') &= \mathbb{R}_{\geq 0} \end{aligned}$$

Remark. This is true due to the fact that for every $y \in \mathbb{R}_{\geq 0}$ there exists an $x \in \mathbb{R}$ with $x^2 = y$ which will be proven later.

Definition 4.2. A function f is *injective* if

$$\forall a_1, a_2 \in A : \qquad f(a_1) = f(a_2) \quad \Rightarrow \quad a_1 = a_2$$

No two elements of A are mapped to the same element of B.

Definition 4.3. A function f is *surjective* if

$$\text{image}(A) = \text{range}(A)$$

For all $b \in B$ there is some $a \in A$ that is mapped to b by f.

Definition 4.4. A function f is *bijective* if it is both injective and surjective.

Definition 4.5. Let A be a set. Define

$$\text{id}_A = \{(a, a)|\ a \in A\}$$

That means for all $a \in A, \text{id}_A(a) = a$.

Definition 4.6. Suppose $f : A \to B$ is a function and $f : B \to C$ is a function. Then we can form a function:

$$\begin{aligned} h = g \circ f : \quad & A \to C \\ h(a) = g(f(a)) & \end{aligned}$$

The function f is *invertible* if

$$\exists g : B \to A : \qquad g \circ f = \mathrm{id}_A \quad \wedge \quad f \circ g = \mathrm{id}_B$$

Notation: $g = f^{-1}(x)$ is called the *inverse* of f.

f is invertible means that if you reverse the arrows of f, then that is a function.

Example 26.

- The function

$$\begin{aligned} & g : [0, \infty) \to [0, \infty) \\ & g(x) = x^2 \end{aligned}$$

is invertible and the inverse is the function

$$\begin{aligned} & g^{-1} : \ [0, \infty) \to [0, \infty) \\ & g^{-1}(y) = \sqrt{y} \end{aligned}$$

- Let us think of

$$\begin{aligned} & f' : \mathbb{R} \to [0, \infty) \\ & f'(x) = x^2 \end{aligned}$$

Look at

$$\begin{aligned} gf^{-1} : [0, \infty) &\to [0, \infty) \\ f^{-1}(y) &= \sqrt{y} \\ f' \circ f^{-1}(y) &= (\sqrt{y})^2 = y \\ \Rightarrow \qquad f' \circ f^{-1} &= \mathrm{id}_{[0,\infty)} \end{aligned}$$

but

$$\begin{aligned} f^{-1} \circ f'(x) &= \sqrt{x^2} = |x| \\ \Rightarrow \qquad f^{-1} \circ f' &\neq \mathrm{id}_{\mathbb{R}} \end{aligned}$$

Remark. We did not prove that f' is not invertible. We just showed that g is not its inverse.

Proposition 3. f is invertible iff f is bijective.

Proof. $\Rightarrow$
Suppose that f is invertible. We have to show that f is injective and surjective. That means

$$\exists g : B \to A : \qquad g \circ f = \mathrm{id}_A \tag{1}$$
$$f \circ g = \mathrm{id}_B \tag{2}$$

f is injective:

$$f(a_1) = f(a_2) \quad \overset{(1)}{\Rightarrow} \quad g \circ f(a_1) = a_1 = f \circ f(a_2) = a_2$$

f is surjective. By (2) for all $b \in B$, $b = f(g(b))$. So indeed there exists $a \in A$ such that $b = f(a)$, namely $a = g(b)$.
$\Leftarrow$
Suppose that f is injective and surjective. Take

$$g = \{(b, a) \in B \times A | \quad (a, b) \in f\} \subseteq B \times A$$

f is injective and surjective means precisely that g is a function.

It is obvious that $g \circ f = \mathrm{id}_A$ and $f \circ g = \mathrm{id}_B$. □

Theorem 4.1. *Fermat's little theorem.*
If p is prime and $p \nmid a$ then $a^{p-1} \equiv 1 \mod p$.

Proof. Consider the function

$$\begin{aligned} f &: \mathbb{Z}/p\mathbb{Z}^x \to \mathbb{Z}/p\mathbb{Z}^x \\ f &: x \mapsto ax \end{aligned}$$

This is an invertible function. We know that a has a multiplicative inverse $b \in (\mathbb{Z}/p\mathbb{Z}^x)$. Take

$$\begin{aligned} g &: \mathbb{Z}/p\mathbb{Z}^x \to \mathbb{Z}/p\mathbb{Z}^x \\ g &: x \mapsto bx \end{aligned}$$

Then $g = f^{-1}$ because $ab \equiv ba \equiv 1 \mod p$.

$$\begin{aligned} &\left\{\overline{a}, \overline{2a}, \dots, \overline{(p-1)a}\right\} = \{1, 2, \dots p-1\} \\ \Rightarrow \qquad & a^{p-1}(p-1)! \equiv (p-1)! \mod p \end{aligned}$$

Dividing through by $(p-1)!$ gives us

$$a^{p-1} \equiv 1 \mod p$$

□

Theorem 4.2. *Chinese Remainder Theorem*
Suppose $\mathrm{hcf}(n, m) = 1$. Then for all a, b the equation

$$\left.\begin{aligned} x &\equiv a \mod n \\ x &\equiv b \mod m \end{aligned}\right\} \qquad (*)$$

has a solution $x \in \mathbb{Z}$. In fact, x is unique $\mod mn'$.

Proof.

$$\begin{aligned} & x = a + pn = b + qm \\ \Rightarrow \qquad & pn - qm = b - a \end{aligned}$$

$\mathrm{hcf}(n, m) = 1$ implies that p and q exist.
As for uniqueness $\mod nm$, suppose that x_0, x_1 are two solutions of $(*)$. Then

$$\begin{aligned} & x_0 - x_1 \equiv 0 \mod n \\ & \equiv 0 \mod m \\ \Rightarrow \qquad & n, m | x_0 - x_1 \qquad (1) \\ (1) \wedge \mathrm{hcf}(n, m) = 1 \Rightarrow \qquad & nm | x_0 - x_1 \end{aligned}$$

□

Proposition 4. Euler's function φ is multiplicative, that is: If $\mathrm{hcf}(n, m) = 1$ then $\varphi(nm) = \varphi(n)\varphi(m)$.

Proof. The Chinese remainder theorem says the following: We can define a function f with

$$\begin{aligned} f &: \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/nm\mathbb{Z} \\ f &: (a, b) \mapsto \text{solution of } (*) \end{aligned}$$

and f is invertible. In fact, f is the inverse of:

$$\begin{aligned} g &: \mathbb{Z}/nm\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ g &: [c] \mod mn \mapsto ([c] \mod n, [c] \mod m) \end{aligned}$$

This shows that

$$f' : (\mathbb{Z}/n\mathbb{Z})^x \times (\mathbb{Z}/m\mathbb{Z})^x \to (\mathbb{Z}/nm\mathbb{Z})^x$$

is invertible. Hence, the cardinality of both sets is the same. □

Proposition 5. For all $n \in \mathbb{N}$

$$\varphi(n) = n \prod_{p \text{ prime, } p|n} \left(1 - \frac{1}{p}\right)$$

Proof. Suppose that p is prime and that $k = p^a$.

$$\begin{aligned} \varphi(k) &= |\{c \in \{1, 2, \dots, p-1\} | \; p \nmid c\}| \\ &= p^a - p^{a-1} \qquad (1) \end{aligned}$$

Therefore, by multiplicativity of φ, if

$$n = p_1^{a_1} p_2^{a_2} \dots p_r^{a_r}$$

then

$$\begin{aligned} \varphi(n) &= \varphi\left(p_1^{a_1}\right) \varphi\left(p_2^{a_2}\right) \dots \varphi\left(p_r^{a_r}\right) \\ &\overset{(1)}{=} \left(p_1^{a_1} p_1^{a_1-1}\right)\left(p_2^{a_2} - p_2^{a_2-1}\right) \dots \left(p_r^{a_r} - p_r^{a_r-1}\right) \\ &= p_1^{a_1} p_2^{a_2} \dots p_r^{a_r} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right). \end{aligned}$$

□

Example 27.

$$\begin{aligned} \varphi(9) &= 9 - 3 \\ &= \{c \in \{1, 2, \dots, 9\} | \; 3 \nmid c\} \end{aligned}$$

Consider the equation $x^k \equiv a \mod m$ We will discuss 2 cases:

1. $m = p$ prime
2. $m = pq$ product of two distinct primes

Proposition 6. Suppose $\text{hcf}(a, p-1) = 1$. Then

$$x^k \equiv a \mod p \qquad (*)$$

has a unique solution modulo p.

Proof. First, there exist $u, v \in \mathbb{N}$ such that

$$ku - (p-1)v = 1.$$

then $x = a^u$ is a solution of $(*)$. Indeed,

$$\begin{aligned} x^k = a^{ku} &= a^{1+(p-1)v} \\ &= a\left(a^{p-1}\right)^v \\ &\equiv a \mod p. \end{aligned}$$

By Fermat's little theorem. Conversely, suppose that $x^k \equiv a \mod p$. Then by Fermat's little theorem,

$$\begin{aligned} x &\equiv x x^{(p-1)v} = x^{1+(p-1)v} \mod p \\ &= x^{ku} \\ &\equiv a^u \mod p \end{aligned}$$

We have shown that $x = a^u$ is a unique solution of $(*)$ mod p. □

Proposition 7. Suppose p and q are distinct primes $\mathrm{hcf}(a, pq) = 1$. Then

$$a^{(p-1)(q-1)} \equiv 1 \mod pq.$$

Proof. By Fermat's little theorem

$$\begin{aligned} a^{(p-1)(q-1)} &\equiv 1^{q-1} \equiv 1 \mod p \\ a^{(p-1)(q-1)} &\equiv 1 \mod q. \end{aligned}$$

And

$$\begin{aligned} x &\equiv 1 \mod p \\ x &\equiv 1 \mod q \end{aligned}$$

has a unique solution by the Chinese remainder theorem. Therefore, $x = 1$ is the unique solution modulo pq. Another solution is $a^{(p-1)(q-1)}$. So $a^{(p-1)(q-1)} \equiv 1 \mod pq$. □

Corollary 4.1. Suppose that p, q are distinct primes. Then for all a, for all $v \in \mathbb{N}$,

$$a^{1+v(p-1)(q-1)} \equiv a \mod pq.$$

Proof.

$$\begin{aligned} a^{1+v(p-1)(q-1)} &\equiv a \mod p \\ a^{1+v(p-1)(q-1)} &\equiv a \mod q \end{aligned}$$

Because of Proposition 4.7. If $p|a$ or $q|a$ these statements obviously hold as well. By the uniqueness part of the Chinese remainder theorem

$$a^{1+v(p-1)(q-1)} \equiv a \mod pq.$$

□

Proposition 8. Suppose $\mathrm{hcf}(k, (p-1)(q-1)) = 1$. Then

$$x^k \equiv a \mod pq \tag{$*$}$$

has a unique solution modulo pq.

Proof. There exist $u, v \in \mathbb{N}$ such that

$$ka - (p-1)(q-1)v = 1.$$

Therefore, $x = a^u$ is a solution of $(*)$:

$$\begin{aligned} x^u &\equiv a^{vu} \mod pq \\ &= aa^{(p-1)(q-1)r} \\ &\equiv a \mod pq \end{aligned}$$

By Proposition 4.7. Conversely, suppose $x^k \equiv a \mod pq$:

$$\begin{aligned} x &\equiv xx^{(p-1)(q-1)r} \mod pq \\ &= x^{ku} \\ &\equiv a^u \mod pq \end{aligned}$$

Thus, $x = a^k$ is the unique solution of $(*)$ mod pq. □

Example 28. Solve for x :

$$x^{53} \equiv -38 \mod 119$$

We check

$$\begin{aligned} 119 &= 7 \cdot 17 \\ \mathrm{hcf}(38, 119) &= 1 \\ \mathrm{hcf}(53, 96) &= 1. \end{aligned}$$

Hence, we can apply Proposition 4.8 to this. To find x we need to find $n, r \in \mathbb{N}$ such that

$$53u - 96r = 1.$$

Euklid's Algorithm gives us

$$5 \cdot 29 - 96 \cdot 1601.$$

By Proposition 4.8, $x = (-38)^{29} \mod 119$. To calculate this we use the method of successive squares:

$$\begin{aligned} & & 29 &= 16 + 8 + 4 + 1 \\ & & (-38)^2 &= 1444 \equiv 16 \mod 119 \\ \Rightarrow & & (-38)^4 &= 16^2 \equiv 18 \mod 119 \\ \Rightarrow & & (-38)^8 &= 18^2 \equiv -33 \mod 119 \\ \Rightarrow & & (-38)^{16} &= (-33)^2 \equiv 18 \mod 119 \end{aligned}$$

Therefore,

$$(-38)^{29} = 18 \cdot (-33) \cdot 18 \cdot (-38) \equiv 30 \mod 119.$$

The unique solution is

$$x \equiv 30 \mod 119.$$

4.1 RSA encryption

A real-life application of simple mathematical ideas is RSA. It is called "public key cryptography". We publish the means to encrypt messages sent to us. Nevertheless, only we have the information that allows us do decrypt the messages.

Here is what we do:

secret	public
We choose two large primes p and q.	$N = pq$
We choose e such that $\mathrm{hcf}\, e, (p-1(q-1) = 1$.	e

A message is an element $a \in \mathbb{Z}/n\mathbb{Z}$. If now an arbitrary person, let us call this person Assange, wants to send an encrypted message a to us, he has to compute

$$b = a^e \in \mathbb{Z}/N\mathbb{Z}.$$

He keeps a to himself and sends b. In order to decrypt, we do the following: Find d such that

$$de \equiv 1 \mod (p-1)(q-1).$$

Then $a \equiv b^d \mod N$. This works by the Proposition 4.8.

Example 29.

secret	public
$p = 7,\ q = 17$	$N = 119$
$(p-1)(q-1) = 96$ and $e = 53$ such that $\mathrm{hcf}(53, 96) = 1$	$e = 53$

Encryption. Assange wants to send us the message $a = 30$ (don't tell anybody). He sends us the encrypted message:

$$\begin{aligned}
& & b &= 30^{53} \mod 119 \\
& & 53 &= 32 + 16 + 4 + 1 \\
& & 30^2 &= 900 \equiv 67 \mod 119 \\
&\Rightarrow & 30^4 &= 67^2 = 4489 \equiv -33 \mod 119 \\
&\Rightarrow & 30^8 &= (-33)^2 = 1089 \equiv 18 \mod 119 \\
&\Rightarrow & 30^{16} &= 18^2 = 324 \equiv -33 \equiv \quad \mod 119 \\
&\Rightarrow & 30^{32} &= (-33)^2 \equiv 18 \mod 119 \\
& & 30^{53} &\equiv 30 \cdot (-33) \cdot (-33) \cdot 18 \mod 119 \\
& & &\equiv -38 \mod 119
\end{aligned}$$

He sends us the message -38.

Decryption. Find d such that $53d \equiv 1 \mod 96$. Solve for $u, v \in \mathbb{N}$:

$$53u - 96 = 1$$

To solve this we use Euklid's algorithm:

$$53 \cdot 29 - 96 \cdot 16 = 1.$$

So $d = 29$. To decrypt we compute

$$(-38)^{29} \equiv 30 \mod 119$$

4.2 Basic counting techniques

Proposition 9. Let S be a finite set. Define

$$P(S) := \{a |\ a \subseteq S\}.$$

Then

$$|P(S)| = 2^{|S|}.$$

Proof. Let A, B be sets. Write

$$A^B = \{f : B \to A |\ f \text{ a function}\}$$

If A, B are finite then:

$$\left|A^B\right| = |A|^{|B|}$$

Let $\underline{2} = \{0, 1\}$. There is a canonical (i.e. naturally defined) bijection:

$$f : P(S) \to \left(\underline{2}^S = \{f :\ S \to \underline{2}\}\right)$$

This bijection can be defined as follows: Suppose that $A \in P(S)$; that is $a \subseteq S$.

$$f : A \mapsto \left(K_A :\ S \to \{0,1\} : \quad K_A(s) = \begin{cases} 1, & s \in A \\ 0, & s \notin A \end{cases} \right)$$

f is a bijection. In fact, its inverse is

$$|P(S)| = |2^S| = 2^{|S|}.$$

□

Proposition 10. The number of ways of ordering the numbers $1, 2, \dots, n$ is $n!$.

Proposition 11. The number of subsets of order r of $\{1, 2, \dots, n\}$ is

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

Proof. We can order $1, 2, \dots, n$ by choosing r elements first, ordering these elements and the others.

$$n! = \binom{n}{r} r!(n-r)!$$

The proposition follows. □

Theorem 4.3.

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

Proof. Write

$$(x+y)^n = \underbrace{(x+y)(x+y)\dots(x+y)}_{n \text{ times}}$$

You score the term $x^{n+r}y^r$ by choosing r ys out of the n brackets. □

4.2.1 Partitions and multinomial coefficients

Definition 4.7. A partition of a set S is a collection of subsets of S:

$$\forall a \in A, S_a \subseteq S : \qquad a \neq b \Rightarrow S_a \cap S_b = \emptyset \qquad \wedge \qquad S = \bigcup_{a \in A} S_a$$

Remark. A typical example of this is where A is the set of equivalence classes of an equivalence relation. In fact, all examples of partitions arise in this fashion.

Definition 4.8. An ordered partition is a partition where the sets S_a are with a chosen order.

Example 30.

$$S = \{1,2,3,4,5,6,7,8\}$$
$$\{\{1,2,3,4\},\{5,6\},\{7,8\}\} = \{\{1,2,3,4\},\{7,8\},\{5,6\}\}$$

but

$$(\{1,2,3,4\},\{5,6\},\{7,8\}) \neq (\{1,2,3,4\},\{7,8\},\{5,6\}).$$

Proposition 12. The number of ordered partitions of $\{1, 2, \dots, n\}$ into k subsets $S_1, S_2, \dots S_k$ of orders $r_1, r_2, \dots r_k$ is

$$\binom{n}{r_1, r_2, \dots, r_k} = \frac{n}{r_1!r_2! \dots, r_k!}$$

where $r_1 + r_2 + \dots + r_k = n$.

Proof. Order $1, 2, \dots, n$ by choosing $r_1, \dots, r_k$ and ordering the first r_1 then r_2 to r_k. We get:

$$n! = \binom{n}{r_1, r_2, \dots, r_k} r_1!r_2! \dots, r_k!$$

The proposition follows. □

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

Theorem 4.4. *Multinomial theorem*

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{r_1,\ldots,r_k \geq 0,\ r_1+\cdots+r_n=n} \binom{n}{r_1,\ldots,r_n} x_1^{r_1} \ldots x_k^{r_k}$$

Proof. Write

$$(x_1 + x_2 + \cdots + x_k)^n = \underbrace{(x_1 + x_2 + \cdots + x_k) \ldots (x_1 + x_2 + \cdots + x_k)}_{n \text{ times}}$$

We score the term $x_1^{r_1} \ldots x_k^{r_k}$ by choosing r_1 x_1s, r_2 x_2s up to r_k x_ks out of the n brackets. □

Example 31. Find the ”constant” coefficient in the expression of

$$\left(x + y + z + \frac{1}{xyz}\right)^n$$

Expand with the multinomial theorem:

$$\sum_{r_1+r_2+r_3+r_4=n} \binom{n}{r_1, r_2, r_3, r_4} \frac{x^{r_1} y^{r_2} z^{r_3}}{(xyz)^r 4}$$

The fraction is a constant if

$$r_1 = r_2 = r_3 = r_4 = k \quad \wedge \quad n = 4k$$

The answer is:

$$c_n = \begin{cases} 0, & 4 \nmid n \\ \binom{4k}{k,k,k,k} = \frac{(4k)!}{(k!)^4}, & n = 4k \end{cases}$$

Proposition 13. *Inclusion-Exclusion principle*
Let $A_1, A_2, \ldots, A_n$ be finite sets. Then

$$\left| \bigcap_{k=1}^{n} A_k \right| = \sum_{1 \leq i_1 < i_2 < \cdots < i_r \leq n} (-1)^{r-1} \left| A_{i_1} \cap \cdots \cap A_{i_r} \right|.$$

Example 32. Let

$$S = \{k \in \mathbb{N} |\ 0 \leq k < 360,\ \ \mathrm{hcf}(k, 360) = 1\}$$

On the one hand, we know $|S| = \varphi(360)$ and we have a formula for this. Hence, we compute $|S|$ as an application of the inclusion-exclusion formula:

$$360 = 2^3 \cdot 3^2 \cdot 5$$

Define

$$\begin{aligned} \Omega &= \{k \in \mathbb{N} |\ 0 \leq k < 360\} \\ A_2 &= \{k \in \Omega |\ 2|k\} \\ A_3 &= \{k \in \Omega |\ 3|k\} \\ A_5 &= \{k \in \Omega |\ 5|k\}. \end{aligned}$$

Then

$$\begin{aligned} S &= \Omega \backslash (A_2 \cup A_2 \cup A_5) \\ |S| &= |\Omega| - |A_2 \cup A_3 \cup A_5| \end{aligned}$$

If $d|360$ write

$$A_d = \{k \in \Omega |\ d|k\}.$$

Then

$$\begin{aligned} A_2 \cup A_3 &= A_6 \\ A_2 \cup A_5 &= A_{10} \\ A_3 \cup A_3 &= A_{15} \\ A_2 \cup A_3 \cup A_5 &= A_{30} \end{aligned}$$

The inclusion-exclusion principle gives us

$$\begin{aligned} |S| &= |\Omega| - |A_2| - |A_3| - |A_5| + |A_6| + |A_{10}| + |A_{15}| - |A_{30}| \\ &= 360 - 180 - 120 - 72 + 60 + 36 + 24 - 12 \\ &= 96 \end{aligned}$$

5 Number Systems

We spoke a bout $\mathbb{N}$ and $\mathbb{Z}$. From now on we take $\mathbb{N}$ and $\mathbb{Z}$ for granted. Let us now talk about $\mathbb{Q}$, which is much harder to define than $\mathbb{N}$ or $\mathbb{Z}$. The reason for this is that $\mathbb{Q} = S/R$ and this leads to equalitie such as:

$$\frac{2}{3} = \frac{6}{9}$$

In fact, the symbol

$$\frac{2}{3}$$

denotes the equivalence class of a pair $(2, 3)$.

What we are aiming for is to take

$$\begin{aligned} S &= \mathbb{Z} \times (\mathbb{Z}\backslash\{0\}) \\ &= \{(a, b)|\ a \in \mathbb{Z}, b \in \mathbb{Z}\backslash\{0\}\}. \end{aligned}$$

We then want to define an equivalence relation R on S such that

$$S/R = \mathbb{Q}$$

and then we can also write

$$[(a, b)] = \frac{a}{b}.$$

Then it will make sense to say

$$\frac{2}{3} = \frac{4}{6} = \frac{6}{9}$$

because this just means $(2, 3) \sim (4, 6)$. The equivalence relation can be defined as

$$(a_1, b_1) \sim (a_2, b_2) \quad \Leftrightarrow \quad a_1 b_2 = a_2 b_1.$$

Another approach is:

$$\begin{aligned} (a_1, b_1) \sim (a_1, b_2) \quad \Leftrightarrow \quad & \exists u, v \in \mathbb{Z}\backslash\{0\} : \\ & ua_1 = va_2 \\ & ub_1 = vb_2 \end{aligned}$$

Exercise. Show that the two approaches are equivalent.

This is an equivalence relation:

- Evidently,

$$(a, b) \sim (a, b).$$

- Suppose $(a_1, b_1) \sim (a_2, b_2)$, i.e. $a_1 b_2 = a_2 b_1$. Then also $a_2, b_1 = a_1 b_2$ and $(a_2, b_2) \sim (a_1, b_1)$.
- Assume $(a_1, b_1) \sim (a_2, b_2)$, i.e. $a_1 b_2 = a_2 b_1$ and $(a_2, b_2) \sim (a_3, b_3)$, i.e. $a_2 b_3 = a_3 b_2$. Hence

$$\begin{aligned} & a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_2 b_1 \\ \Rightarrow \quad & (a_1 b_3 - a_3 b_1) b_2 = 0 \\ \Rightarrow \quad & a_1 b_3 = a_3 b_1 \end{aligned}$$

  This means $(a_1, b_1) \sim (a_3, b_3)$.

Definition 5.1.

$$\mathbb{Q} = \{\text{rational numbers}\} = S/\sim$$
$$[(a, b)] = \frac{a}{b}$$

5.1 Binary operations on $\mathbb{Q}$

Define operations $\oplus$ and $\odot$ on $S = \mathbb{Z} \times (\mathbb{Z} \backslash \{0\})$

$$\begin{aligned} (a, b) \odot (p, q) &= (ap, bq) \\ (a, b) \oplus (p, q) &= (aq + pq, bq) \end{aligned}$$

Proposition 14. Suppose

$$\begin{aligned} & (a_1, b_1) \sim (a_2, b_2) \\ \wedge \quad & (p_1, q_1) \sim (p_2, q_2). \end{aligned}$$

Then

$$(a_1, b_1) \odot (p_1, q_1) \sim (a_2, b_2) \odot (p_2, q_2) \tag{1}$$
$$(a_1, b_1) \oplus (p_1, q_1) \sim (a_2, b_2) \oplus (p_2, q_2) \tag{2}$$

Result 5.1.1. We can define operations on $\mathbb{Q}$:

$$\begin{aligned} \frac{a}{b} \cdot \frac{p}{q} &= \frac{ap}{bq} \\ \frac{a}{b} + \frac{p}{q} &= \frac{aq + bp}{bq} \end{aligned}$$

Proof. (2)

$$\begin{aligned} & (a_1 q_1 + b_1 p_1,\ b_1 q_1) \sim (a_2 q_2 + b_2 p_2,\ b_2 q_2) \\ \Leftrightarrow \quad & (a_1 q_1 + b_1 p_1) \cdot (b_2 q_2) \sim (a_2 q_2 + b_2 p_2) \cdot (b_1 q_1) \\ \Leftrightarrow \quad & a_1 b_2 q_1 q_2 + p_1 q_2 b_1 b_2 = a_2 b_1 q_1 q_2 + p_2 q_1 b_1 b_2 \end{aligned}$$

Due to our assumption $(a_1, b_1) \sim (a_2, b_2)$ i.e. $a_1 b_2 = a_2 b_1$ and $(p_1 q_1) \sim (p_2, q_2)$, the equation above is true. This shows (2). (1) is left as an exercise. □

Property 0.1. For all $a, b, c \in \mathbb{Q}$ the following holds:

1. Commutativity of addition:

$$a + b = b + a$$

2. Commutativity of multiplication:

$$ab = ba$$

3. Associativity of addition:

$$a + (b + c) = (a + b) + c$$

4. Associativity of multiplication:
$$a(bc) = (ab)c$$

5. Distributivity:
$$a(b + c) = ab + ac$$

6. Existence of a neutral element of addition:
$$\exists 0 \in \mathbb{Q} :\ \forall x \in \mathbb{Q} \qquad x + 0 = x$$

7. Existence of an inverse element of addition:
$$\forall x \in \mathbb{Q}\ \exists y \in \mathbb{Q} : \qquad x + y = 0$$
Notation: $y = -x$ and $x + (-y) = x - y$

8. Existence of a neutral element of multiplication:
$$\exists 1 \in \mathbb{Q} :\ \forall x \in \mathbb{Q} \qquad x \cdot 1 = x$$

9. Existence of an inverse element of multiplication:
$$\forall x \in \mathbb{Q}\ \exists y \in \mathbb{Q} : \qquad xy = 1$$
Notation: $y = x^{-1}$ and $x(y^{-1}) = \frac{x}{y}$.

10. $\mathbb{Q}$ has binary relations $<, >$ such that precisely one of the following alternatives holds:
$$\begin{gathered} a > 0 \\ a = 0 \\ 0 > a \end{gathered}$$

11.
$$\begin{aligned} a > 0 \quad &\Leftrightarrow \quad 0 > -a \\ a > 0 \quad &\Leftrightarrow \quad b + a > b \\ (a > 0 \wedge b > 0) \quad &\Leftrightarrow \quad ab > 0 \end{aligned}$$

12. *Archimedean Axiom*
$$\forall x \in \mathbb{Q}\ \exists N \in \mathbb{N} : \qquad N > x$$

All the properties hold for $\mathbb{R}$ as well and for $\mathbb{C}$ properties 1. to 9. hold.

Everything that we know about $\mathbb{Q}$ follows from these properties.

Example 33.

- Consider the very basic and well known property
$$\forall x \in \mathbb{Q} \qquad 0 \cdot x = 0.$$

Proof. Due to 2, 5, 6, 8 we get
$$\begin{aligned} 1 \cdot x &= (0 + 1) \cdot x \\ &= 0 \cdot x + 1 \cdot x \\ &= 0 \cdot x + x. \end{aligned}$$

So for all $x \in \mathbb{Q}$
$$x = 0 \cdot x + x.$$

We add $-x$ to both sides:
$$\begin{aligned} & x + (-x) = 0 \cdot x + x + (-x) \\ \Leftrightarrow \qquad & 0 = 0 \cdot x + 0 \\ \Leftrightarrow \qquad & 0 = 0 \cdot x. \end{aligned}$$

□

- For all $x \in \mathbb{Q}$ either $x = 0$ or $x^2 > 0$ but not both.

  Proof. There are 3 cases:

  1. $x > 0$
  $$x \cdot x = x^2 > 0$$
  2. $x = 0$
  $$x = 0$$
  3. $0 > x$
  $$-x > x + (-x) = 0$$
     We know
  $$0 = 0 \cdot x = (1 + (-1)) \cdot x = x + (-1)x$$
     So $(-1) \cdot s$ is an additive inverse but since there is only one additive inverse it has to be equal to $-x$ (the proof of the uniqueness of additive inverses is left as an exercise).
     Furthermore, $(-1) \cdot (-1) = 1$ (the proof of that statement is also up to the reader). This finishes the proof:
  $$\begin{aligned}(-x)^2 &= (-1) \cdot (-1) \cdot x \cdot x \\ &= x \cdot x\end{aligned}$$

□

Definition 5.2. Let $a \in \mathbb{R}$, then the *round up* of a is the integer
$$[a] = \min\{k \in \mathbb{Z} |\ a \leq k\}.$$
Similarly, the *round down* of a is
$$[a] = \max\{k \in \mathbb{Z} |\ a \geq k\}.$$

Exercise. Show that the Archimedian axiom and the smallest element axiom ensure that the definitions are valid

Definition 5.3. We define the *fractional part* $\{a\}$ of a as
$$\begin{aligned}a &= [a] + \{a\}, \\ 0 &\leq \{a\} < 1\end{aligned}$$

Definition 5.4. The *absolute value* $|a|$ of a real number a is defined as
$$|a| = \sqrt{a^2} = \begin{cases} a, & a \geq 0 \\ -a, & a < 0 \end{cases}$$

The completeness axiom for $\mathbb{R}$.

Definition 5.5. Let $\emptyset \neq S \subseteq \mathbb{R}$. The largest element of S written $M = \max(S)$ such that
$$M \in S \qquad \wedge \qquad \forall a \in S, \quad a \leq M$$

Example 34.

- $$S = [0, 1] \quad \Rightarrow \quad \max(S) = 1$$
- $$S = [0, 1) \quad \Rightarrow \quad \max(S) \text{ does not exist}$$

  It is clear that we want to be looking at $x = 1$ but unfortunately $1 \notin S = [0, 1)$.

Definition 5.6. Let $\emptyset \neq S \subseteq \mathbb{R}$. A real number $A \in \mathbb{R}$ is an *upper bound* for S if

$$\forall a \in S, \qquad a \leq A$$

We say that S is bounded above is S has an upper bound.

Remark. For $S = [0, 1)$, $A = 1$ is an upper bound but so is $A = 2$. The upper bound is not unique.

Definition 5.7. Let $\emptyset \neq S \subseteq \mathbb{R}$. Suppose S is bounded above. The *supremum* or *least upper bound* of S is

$$\sup(S) = \min(T),$$
$$T = \{A \in \mathbb{R} |\ A \text{ is an upper bound}\}$$

Example 35. Say that we are und $\mathbb{Q}$ instead.

$$S = \{r \in \mathbb{Q} |\ r^2 < 2\}$$

does not have a maximum but neither does it have a supremum in $\mathbb{Q}$ (because this supremum would be $\sqrt{2} \notin \mathbb{Q}$).

Axiom 5.1. *Completeness Axiom*
Let $\emptyset \neq S \subseteq \mathbb{R}$ be bounded above. Then S has a real supremum.

Similarly, you can define *lower bound*, *bounded below*, *infimum* or *highest lower bound.*

Result 5.1.2. If $\emptyset \neq S \subseteq \mathbb{R}$ is bounded below, then S has an infimum.

Proof. Define

$$-S = \{-a |\ a \in S\} \subseteq \mathbb{R}$$

That S is bounded below implies that $-S$ is bounded above and hence

$$\inf S = -\sup(-S)$$

□

Lemma 5.1. Let $\emptyset \neq s \subseteq \mathbb{R}$. Then

$$b = \sup S$$

iff

1. b is an upper bound for S and
2. $$\forall \epsilon \in \mathbb{R}, \epsilon > 0,\ \exists a \in S : \qquad b - \epsilon < a.$$

Proof. For all $0 < \epsilon \in \mathbb{R},\ b - \epsilon$ is not an upper bound for S. 2^*
Obviously 2^* is equivalent to 2.
For all $b' < b,\ b$ is not an upper bound for S. $2\dagger$
Again, $2\dagger$ is evidently equivalent to 2^* and hence 2.
So it is enough to prove Lemma†, which is:
Let $\emptyset \neq S \subseteq \mathbb{R}$. Then

$$b = \sup S$$

iff:

1. b is an upper bound for S.
2. $b' < b$ implies b' is not an upper bound of S.

Let us first prove the left-right-implication ($\Rightarrow$). We know if $b = \sup S$, then B is an upper bound but b is the smallest upper bound. Hence, c is an upper bound implies $b \leq c$, i.e. c is not an upper bound if $c < b$.

The right-to-left implication is much similar. If b is an upper bound and there is no upper bound smaller than b, then b is the smallest upper bound. □

Theorem 5.1.

$$\forall y \in \mathbb{R}, y \geq 0,\ \exists_1 x \in \mathbb{R}, x \geq 0 : \qquad x^2 = y$$

Remark. We will write $x = \sqrt{y}$. With similar ideas you can also construct $\sqrt[n]{y}$ for natural positive $n \in \mathbb{N}$.

Proof. Let

$$L = \{t \geq 0 |\ t^2 \leq y\}.$$

Because $y \geq 0$, $0 \in L$. (1)
For $y < 1$, $t > 1$ implies $t^2 > 1 > y$ and the set is bounded above by 1. (2.1)
For $y \geq 1$, $t > y$ implies $t^2 > y^2 \geq y$, t and the set is bounded above by y. (2.2)
By (2.1) and (2.2), L is bounded above. (2)
By (1) and (2), L has a supremum. Let

$$x = \sup\{t \leq 0 | t^2 \leq y\}. \qquad (*)$$

By lemma 5.1, if $0 \leq x' < x$, then x' is not an upper bound for L. Hence there exists a $t \in L$ with $x' < t$. Because of $t^2 \leq y$, we get $x'^2 < t^2$. Writing x' as $x - \epsilon$ we get

$$\forall \epsilon > 0 \qquad (x - \epsilon)^2 \leq y.$$

Note that always

$$x^2 - 2\epsilon x \leq x^2 - 2\epsilon x + \epsilon^2 = (x - \epsilon)^2 \leq y.$$

Therefore

$$\forall \epsilon > 0, \qquad x^2 - 2\epsilon x \leq y. \qquad (3)$$

Assume for contradiction that $x^2 > y$. Choose

$$\epsilon = \frac{x^2 - y}{3x} < \frac{x^2 - y}{2x}.$$

This can be rewritten as

$$x^2 - 2x\epsilon > y.$$

This contradicts (3). Hence $x^2 \leq y$. (4)

Suppose for contradiction $x^2 < y$. Pick

$$\epsilon < \min\left\{\frac{y - x^2}{2x + 1}, 1\right\}. \qquad (5)$$

Then

$$\begin{aligned} & & \epsilon &< \frac{y - x^2}{2x + 1} \\ &\Leftrightarrow & \epsilon(2x + 1) &< y - x^2 \\ &\Leftrightarrow & x^2 + 2\epsilon x + \epsilon &< y \end{aligned}$$

Due to (5), $\epsilon^2 \leq \epsilon$ and thus

$$\begin{aligned} & & x^2 + 2\epsilon x + \epsilon^2 &< y \\ &\Leftrightarrow & (x + \epsilon)^2 &< y \end{aligned}$$

But then x is no upper bound for L. This contradicts $(*)$. Therefore $x \geq y$. (6)
(5) and (6) implies the theorem. □

Similarly, for all $k \in \mathbb{N}$ there exists one and only one $b \geq 0, b \in \mathbb{R}$ such that

$$b^k = a.$$

Definition 5.8. For $r = \frac{p}{q} \in \mathbb{Q}, r \geq 0, x \in \mathbb{R}, x \geq 0$ define

$$x^r = \left(\sqrt[q]{x}\right)^p .$$

Remark. This power is well defined. If $p' = up, q' = uq$ for some $u \in \mathbb{N}\backslash\{0\}$ we need to show

$$\begin{aligned} \left(\sqrt[q']{x}\right)^{p'} &= \left(\sqrt[q]{x}\right)^p \\ \left(\left(\sqrt[uq]{x}\right)^u\right)^p &= \left(\sqrt[q]{x}\right)^p \\ \left(\sqrt[uq]{x}\right)^u &= \sqrt[q]{x} \end{aligned}$$

by uniqueness of p^{th} roots. By uniqueness of q^{th} roots:

$$\begin{aligned} \left(\left(\sqrt[uq]{x}\right)^u\right)^q &= x \\ \left(\sqrt[uq]{x}\right)^{uq} &= x \end{aligned}$$

This holds by properties of the $(uq)^{th}$ root.

Proposition 15. Suppose $a, b \in \mathbb{Q}, x, y \in \mathbb{R}, a, b, x, y \geq 0$. Then

1. $x^a \cdot y^b = x^{a+b}$
2. $x^a \cdot y^a = (xy)^a$
3. $(x^a)^b = x^{ab}$

Proof. In the proof we take for granted the corresponding properties for integer powers. Prove 1:

$$a = \frac{m}{n}, \qquad b = \frac{p}{q}$$
$$x^a \cdot x^b = (\sqrt[n]{x})^m \cdot (\sqrt[q]{x})^p$$

Because x^a is well defined, this is equal to

$$(\sqrt[nq]{x})^{nq} \cdot (\sqrt[nq]{x})^{np}$$

Now we only have integer powers and can apply their properties. So we get

$$(\sqrt[nq]{x})^{mq+np}.$$

And this is by definition x^{a+b}. Finish 2 and 3 on your own. □

Now that we know about $<, \leq$ and we know that $\sqrt[n]{\ }$ exists, we can go back and have a fresh look at some familiar procedures.

Exercise. Suppose $A, B \geq 0$ then

$$A \geq B \quad \Leftrightarrow \quad A^2 > B^2$$

Example 36.

- Is $\sqrt{6} - \sqrt{2} > 1$?
  Since $\sqrt{6} > \sqrt{2}$ the question is equivalent to:

$$\begin{aligned} & & (\sqrt{6} - \sqrt{2})^2 &> 1 \\ &\Leftrightarrow & 6 - 2\sqrt{6}\sqrt{2} + 2 &> 1 \\ &\Leftrightarrow & 8 &> 1 + 4\sqrt{3} \\ &\Leftrightarrow & 7 &> 4\sqrt{3} \\ &\Leftrightarrow & 49 &> 16 \cdot 3 = 48 \end{aligned}$$

Answer: Yes!

- Solve for $x \in \mathbb{R}$:

  $$x > \frac{2}{x+1}$$

  The question really asks to describe the set

  $$\{x \in \mathbb{R} | \; x > \frac{2}{x+1}\}$$

  We have to discuss two cases

  1. $x + 1 > 0$

     $$\begin{aligned} & & x^2 + x > 2 \\ \Leftrightarrow & & x^2 + x - 2 > 0 \\ \Leftrightarrow & & (x+2)(x-1) > 0 \end{aligned}$$

     Either

     $$(x + 2 > 0 \quad \wedge \quad x - 1 > 0) \qquad \vee \qquad (x + 2 < 0 \quad \wedge \quad x - 1 > 0)$$

     So $x > 1$
  2. $(x + 1) < 0$

     $$\begin{aligned} & & x^2 + x < 2 \\ \Leftrightarrow & & (x+2)(x-1) < 0 \end{aligned}$$

     Hence $-2 < x < -1$. The final answer is

     $$\left\{ x \in \mathbb{R} | \; x > \frac{2}{x+1} \right\} = (-2, -1) \cup (1, \infty)$$

5.2 Decimal expansions of real numbers

We are all familiar with

$$\frac{1}{3} =: 0.333 \dots = 0.\overline{3}.$$

What does this really mean?

$$\begin{aligned} \frac{1}{3} &= 0.3 + 0.03 + 0.003 + \dots \\ &= 3 \cdot 10^{-1} + 3 \cdot 10^{-2} + 3 \cdot 10^{-3} + \dots \\ &= 4 \cdot 10^{-1} \left(1 + 10^{-1} + 10^{-2} + \dots\right) \end{aligned}$$

We all know

$$1 + x + x^2 + \dots x^k = \frac{1 - x^{k+1}}{1 - x}$$

If $0 < x < 1$. Then x^k is getting smaller as k grows. It makes sense sense to define

$$1 + x + x^2 + x^3 + \dots = \sup \left\{ \frac{1 - x^k}{1 - x} \,\middle|\, k \in \mathbb{N} \right\}$$

Exercise. Show that this is equal to $\frac{1}{1-x}$.

If we apply this to $x = \frac{1}{10}$ then

$$= 3 \cdot \frac{1}{10} \cdot \frac{1}{1 - \frac{1}{10}} = \frac{1}{3}$$

Every real number has a decimal expansion and conversely every decimal expansion depicts a real number.

$$a.a_1a_2a_3\dots$$

where $a \in \mathbb{Z}$ and $a_i \in \{0, 1, \dots, 9\}$. Let $x \in \mathbb{R}$.

$$\begin{aligned} x = \lfloor x \rfloor + \{x\} \qquad \lfloor x \rfloor \in \mathbb{Z}, 0 \leq \{x\} < 1 \\ a := x \end{aligned}$$

The idea is to zoom in on $\{x\}$ Devide up $[0, 1)$ into 10 equal intervals.

$$\left[0, \frac{1}{10}\right), \left[\frac{1}{10}, \frac{2}{10}\right), \dots, \left[\frac{9}{10}, 1\right)$$

$\{x\}$ fall in precisely one of those intervals.

$$\begin{aligned} \exists_1 a_1 \in \{0, 1, \dots, 9\} : \qquad f_0 = \{x\} \in \left[\frac{a_1}{10}, \frac{a_1}{10} + \frac{1}{10}\right) \\ 10f_0 \in [a_1, a_1 + 1) \\ 10f_0 = \lfloor 10f_0 \rfloor + \{10f_0\} \\ \{10f_0\} = f_1 \end{aligned}$$

$f_1 \in [0, 1)$. Dividing $[0, 1)$ into 10 equal intervals:

$$\left[0, \frac{1}{10}\right), \left[\frac{1}{10}, \frac{2}{10}\right), \dots, \left[\frac{9}{10}, 1\right)$$

$f_1 = \{10f_0\}$ falls into precisely one of those intervals.

$$\begin{aligned} \exists a_2 \in \{0, 1, \dots 9\} : \qquad f_1 \in \left[\frac{a_2}{10}, \frac{a_2}{10} + \frac{1}{10}\right) \\ 10f_1 \in [a_2, a_2 + 1) \\ 10f_2 = \lfloor 10f_2 \rfloor + \{10f_2\} \end{aligned}$$

We see that

$$x = a.a_1a_2a_3\dots$$

where $a = [x]$ and the digits

$$a_1, a_2, a_3, \dots \in \{0, 1, \dots, 9\}$$

are determined inductively as

$$\begin{aligned} f_0 = \{x\} \qquad a_1 = \lfloor 10f_0 \rfloor \\ f_1 = \{10f_0\} \qquad a_2 = \lfloor 10f_1 \rfloor \\ f_2 = \{10f_1\} \qquad a_3 = \lfloor 10f_2 \rfloor \\ \dots \\ x = a + \frac{a_1}{10} + \frac{a_2}{10^2} + \frac{a_3}{10^3} + \dots \end{aligned}$$

This expansion can be formally made as a supremum.

Remark. By dividing the intervals in two instead of ten equal parts we obtain binary expansions,

$$a_k \in [0, 1).$$

Dividing into n parts to get a n-ary expansion.

Example 37.

$$\frac{2}{7} = 0.\overline{285714}$$

there are several divisions by 7. The remainders that we get are all smaller than 7. Once we get a remainder that we have seen before, the calculation goes on repeatedly. The bar is a notation for periodic digits.

Theorem 5.2. Let $x \in \mathbb{R}$ then $x \in \mathbb{Q}$ iff the decimal expansion of x is eventually periodic. (I.e.

$$x = a.a_1 \dots a_n \overline{a_{n+1} \dots a_{n+m}}$$

Application: We can construct many strange irrationals. For example

$$0.101001000100001 \dots \notin \mathbb{Q}$$

Proof. Suppose $x = \frac{p}{q} \in \mathbb{Q}$.

$$\begin{aligned}
\frac{p}{q} &= \left\lfloor \frac{p}{q} \right\rfloor + \left\{ \frac{p}{q} \right\} \\
p &= aq + r \\
10r &= a_1 q + r_1, \qquad 0 \le r_1 < q \\
10r_1 &= a_2 q + r_2 \\
10r_2 &= a_3 q + r_3 \\
\frac{p}{q} &= a.a_1 a_2 \dots
\end{aligned}$$

$a_1, a_2, \dots$ are determined by the inductive rule. Because all $r_k \in \{0, 1, \dots q\}$. After at most q steps you will see a remainder that you have already seen. That shows $\Leftarrow$. □

Remark. The length of the period is smaller or equal to $q - 1$.

If the decimal expansion is eventually periodic, then the real is rational.

Example 38. Let $x = 0.\overline{b_1 \dots b_k}$, then

$$\begin{aligned}
x &= \underbrace{b_1 b_2 b_3 \dots b_k}_{\text{integer written in decimal}} \left(\frac{1}{10^k} + \frac{1}{10^{2k}} + \dots \right) \\
&= \frac{b_1 \dots b_k}{10^k} \cdot \frac{1}{1 - \frac{1}{10^n}} \in \mathbb{Q}
\end{aligned}$$

Decimal expansions are not unique.

Example 39.

$$\begin{aligned}
0.999 \dots &= 1 \\
&= \frac{9}{10} \left(1 + \frac{1}{10} + \frac{1}{10^2} + \dots \right) \\
&= \frac{9}{10} \cdot \frac{1}{1 - \frac{1}{10}} \\
&= 1
\end{aligned}$$

Proposition 16. Suppose $x \in \mathbb{R}$ has two different decimal expansions.Then these are as follows:

$$\begin{aligned}
x &= a_0.a_1 a_2 \dots a_n \overline{9} \qquad \text{with } a_n \le 8 \\
&= a_0.a_1 a_2 \dots a_{n-1}(a_n + 1)
\end{aligned}$$

Proof. Suppose the two expressions are

$$\begin{aligned}
x &= a_0.a_1 \dots a_n a_{n+1} \dots \\
&= b_0.b_1 \dots b_n b_{n+1} \dots
\end{aligned}$$

where $a_n \ne b_n$ and $a_i = b_i, i < n$. Without loss of generality assume $a_n < b_n$. Then

$$\begin{aligned}
x &= a_0.a_1 a_2 \dots a_n a_{n+1} \dots \\
&\le a_0.a_1 a_2 \dots a_n \overline{9} \\
&= a_0.a_1 a_2 \dots (a_n + 1) \\
&\le a_0.a_1 a_2 \dots a_{n-1} b_n b_{n+1} \dots \\
&= x
\end{aligned}$$

So equality holds everywhere. □

5.3 The Complex Numbers

Definition 5.9. Let the operations $+$ and $\cdot$ be defined on $\mathbb{R}^2$ as follows:

$$\begin{aligned}(a,b)+(x,y)&=(a+x,b+y)\\(a,b)\cdot(x,y)&=(ax-by,ay+bx).\end{aligned}$$

Then we call the triple $(\mathbb{R}^2,+,\cdot)=\mathbb{C}$ the complex numbers.

Remark. The two operations satisfy the same axioms as $\mathbb{Q}$ and $\mathbb{R}$ but there is no meaningful order relation $<$.

We think of $\mathbb{R}$ as a subset of $\mathbb{C}$:

$$\begin{aligned}\mathbb{R}&\to\mathbb{C}\quad\text{injective}\\x&\mapsto(x,0)\end{aligned}$$

The operations on $\mathbb{C}$ are compatible with the ones on $\mathbb{R}$:

$$\forall x,y\in\mathbb{R}\qquad x+y\mapsto(x+y,0)=(x,0)+(y,0)$$

This can be done similarly with multiplication. Furthermore

$$(0,1)\cdot(0,1)=(-1,0)=-1$$

Definition 5.10. We define

$$(0,1)=i.$$

Then we can take any complex number:

$$\begin{aligned}(a,b)&=a(1,0)+b(0,1)\\&=a+bi\end{aligned}$$

This is also called the "Cartesian form" of a complex number.

Example 40.

$$\begin{aligned}(a+bi)(x+yi)&=ax+ayi+bxi+byi^2\\&=(ax-by)+(ay+bx)i\\&=(ax-by,ay+bx)\end{aligned}$$

We like to paint complex numbers on the Cartesian plane.
More terminology and notation: If $z=a+bi\in\mathbb{C},a,b\in\mathbb{R}.$ then

Definition 5.11. Let $z=a+bi\in\mathbb{C}$. Then the *conjugate* of z is defined as

$$\overline{z}=a-bi.$$

Definition 5.12. Let $z=a+bi\in\mathbb{C}$. Then the *imaginary part* of z is defined as

$$\operatorname{Re}z=\frac{z+\overline{z}}{2}\in\mathbb{R}.$$

Definition 5.13. Let $z=a+bi\in\mathbb{C}$. Then the *real part* of z is defined as

$$\operatorname{Im}z=\frac{z-\overline{z}}{2i}\in\mathbb{R}.$$

Definition 5.14. Let $z=a+bi\in\mathbb{C}$. Then the *modulus* of z is defined as

$$|z|=\sqrt{a^2+b^2}=\sqrt{z\overline{z}}\in\mathbb{R}.$$

Proposition 17.

$$\begin{aligned}(|z|\geq 0\wedge|z|=0)\quad&\Leftrightarrow\quad z=0\\|zw|&=|z|\cdot|w|\\|z+w|&\leq|z|+|w|\quad\text{triangle inequality}\end{aligned}$$

Exercise. The proof of these statements is left to the reader.

Addition of complex numbers is the same as addition of vectors in $\mathbb{R}^2$ and it can be pictured as a parallelogram (or triangle). Geometrically, the modulus of a number is then the length of this vector or the distance from the origin to the point z in the complex plane. Hence, the triangle inequality can be interpreted as

$$= \text{distance}(0, z+w) \leq \text{distance}(0, z) + \text{distance}(0, w)$$

Example 41.

Question. Express

$$\frac{1+i}{1-2i}$$

in Cartesian form.
Answer. If $z \neq 0$ then $|z| > 0$ so

$$1 = \frac{|z|^2}{|z|^2} = \frac{z\overline{z}}{|z|^2}$$

i.e.

$$\begin{aligned}
\frac{1}{z} &= \frac{\overline{z}}{|z|^2} \\
\frac{1}{1-2i} &= \frac{1+2i}{5} \\
\frac{1+i}{1-2i} &= \frac{(1+i)(1+2i)}{5} \\
&= -\frac{1}{5} + \frac{3i}{5}
\end{aligned}$$

□

5.4 Polar Form of Complex Numbers

The *polar form* allows one to visualize multiplication of complex numbers. (Whereas the Cartesian form allows to visualize addition.) We encode our complex number by $|z| = r \geq 0$ and an angle θ.

r and θ are then called the polar coordinates of $z \in \mathbb{C}$. If $z \neq 0$, we can choose θ uniquely in $[0, 2\pi)$. We can also choose θ uniquely in the interval $[-\pi, \pi)$. (Allowing $r < 0$ you may restrict further, $\theta \in \left[-\frac{\pi}{2}, \frac{\pi}{2}\right)$).

Sometimes it is better not to choose and take $\theta \in \mathbb{R}/2\pi\mathbb{Z}$.

$$\theta_1 \sim \theta_2 \qquad \Leftrightarrow \qquad \exists k \in \mathbb{Z} \quad \theta_1 = \theta_2 + 2\pi k$$

We can do all these things depending on the context. As we identified $\mathbb{Z}/N\mathbb{Z} = \{k |\ 0 \leq k < N\}$, we identify $\mathbb{R}/2\pi\mathbb{Z} = \{\theta \in \mathbb{R} |\ 0 \leq \theta < 2\pi\}$ (or sometimes $\{\theta \in \mathbb{R} |\ -\pi \leq \theta < \pi\}$.)

Definition 5.15. For $\theta \in \mathbb{R}$ (or $\mathbb{R}/2\pi\mathbb{Z}$) we define

$$e^{i\theta} = \cos\theta + i\sin\theta$$

Remark. For $z = x + iy \in \mathbb{C},\ e^z = e^x e^{iy}$.

Proposition 18. e^x is a group homomorphism:

$$\begin{aligned}
&e^x : && (\mathbb{C}, +) \to (\mathbb{C}\backslash\{0\}, \cdot) \\
&\forall z, w \in \mathbb{C} && e^{z+w} = e^z e^w
\end{aligned}$$

Proof.

$$\begin{aligned}
e^{i\theta_1\theta_2} &= \cos(\theta_1 + \theta_2) + i\sin(\theta_1\theta_2) \\
e^{i\theta_1}e^{i\theta_2} &= (\cos\theta_2 + i\sin\theta_2)(\cos\theta_2 + i\sin\theta_2) \\
&= (\cos\theta_2\cos\theta_2 - \sin\theta_1\sin\theta_2) + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2
\end{aligned}$$

This is exactly the content of the addition formulas for cosine and sine. □

Remark.

$$\begin{aligned} & & e^{i\theta_1} &= e^{i\theta_2} \\ \Leftrightarrow & & cos\theta_1 &= \cos\theta_2 \\ & \wedge & \sin\theta_1 &= \sin\theta_2 \\ \Leftrightarrow & & \theta_1 &= \theta_2 \qquad \mod 2\pi \\ \Leftrightarrow & \exists k \in \mathbb{Z}: & \theta_1 &= \theta_2 + 2\pi \end{aligned}$$

Definition 5.16. θ is called the argument (also arg) of z.

An alternative approach to complex numbers are the conversion formulas.

$$\begin{aligned} x &= r\cos\theta \\ y &= r\sin\theta \qquad (*) \\ r &= \sqrt{x^2+y^2} \\ \theta &= \tan^{-1}\frac{y}{x} \qquad (\dagger) \end{aligned}$$

These conversion formulas define an invertible function

$$\mathbb{R}_{>0} \times \mathbb{R}/2\pi\mathbb{Z} \quad \overset{(*)}{\to} \quad \mathbb{R}^2 \backslash \{(0,0)\}$$

where the inverse function is defined by ($\dagger$).

Theorem 5.3. *De Moivre's formula*
When one multiplies two complex numbers $z_1, z_2 \in \mathbb{C}$, the modulus multiplies and the arguments add:

$$\left(z_1 = r_1 e^{i\theta_1} \quad \wedge \quad z_2 = r_2 e^{i\theta_2}\right) \qquad \Rightarrow \qquad z_1 \cdot z_2 = r_1 r_2 e^{i(\theta_1+\theta_2)}$$

5.5 Roots of Unity

The roots of unity are solutions of the equation

$$z^n = 1 \qquad n \in \mathbb{N}, z \in \mathbb{C}.$$

Writing $z = re^\theta$ in polar form gives us

$$\begin{aligned} & & r^n e^{n\theta} &= 1 \\ \Rightarrow & & r &= 1 \\ & \wedge & n\theta &\equiv 0 \mod 2\pi. \end{aligned}$$

I.e.

$$\exists k \in \mathbb{Z}: \qquad \theta = \frac{2\pi k}{n} \qquad (*)$$

Hence we can define a function f with

$$\begin{aligned} f: \quad \mathbb{Z}/n\mathbb{Z} &\to \mathbb{C} \\ [k] &\mapsto e^{i\frac{2\pi k}{n}}. \end{aligned}$$

f is injective:

$$\begin{aligned} & & e^{i\frac{2\pi k}{n}} &= e^{i\frac{2\pi l}{n}} \\ \Leftrightarrow & & \frac{2\pi k}{n} &\equiv \frac{2\pi l}{n} \mod 2\pi \\ \Leftrightarrow & & k &\equiv l \mod \mathbb{Z}/n\mathbb{Z} \end{aligned}$$

Furthermore, we know

$$\begin{aligned} \forall [k] \in \mathbb{Z}/n\mathbb{Z}: & \qquad (f([k]))^n = \left(e^{i\frac{2\pi k}{n}}\right)^n = 1 \\ \Rightarrow & \qquad \text{image}(f) \subseteq \{z | \; z^n = 1\} \end{aligned}$$

Because of ($*$) equality holds. Thus, f is bijective.

Definition 5.17. For $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/p\mathbb{Z}, p$ prime define

$$k[x]$$

as the set of polynomials in x with coefficients in k. A polynomial $p(x) \in k[x]$ can be written as

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n, \qquad a_0, a_1, \ldots, a_n \in k.$$

We call n the *degree* of $k[x]$.

Compare $\mathbb{Z}$ to $k[x]$:

Division algorithm in $\mathbb{Z}$	Degree of $p(x) \in k(x)$
$\forall a, b \in \mathbb{Z}$ $\exists q, r \in \mathbb{Z}, r < a :$ $\frac{a}{b} = q + \frac{r}{b}$	$\forall A(x), B(x) \in k[x]$ $\exists Q(x), R(x) \in k[x], \text{degree}(R(x)) < \text{degree}(A(x))$ $\frac{A(x)}{B(x)} = Q(x) + \frac{R(x)}{B(x)}$
$c = \text{hcf}(a, b)$ $\Rightarrow \exists y, z \in \mathbb{Z} : \qquad ay + bz = c$ prime is equivalent to irreducible unique prime factorization	$C(x) = \text{hcf}(A(x), B(x))$ $\Rightarrow \exists Y(x), Z(x) \in k[z] : \qquad A(x)Y(x) + B(x)Z(x) = C(x)$ prime is equivalent to irreducible unique prime factorization

Proposition 19. Let $\omega = e^{\frac{2\pi\theta}{n},\ n>1}$. Then

$$1 + \omega + \omega^2 + \cdots + \omega^{n-1} = 0.$$

I.e. the sum of all n^{th} roots of one equals 0.

Proof. Let

$$z = 1 + \omega + \omega^2 + \cdots + \omega^{n-1}.$$

then $\omega z = z$. Hence,

$$\begin{aligned} & & (1-\omega)z = 0 \\ \Rightarrow & & z = 0 \end{aligned}$$

□

Alternatively we could have used the polynomial identity:

$$1 + x + x^2 + \cdots + x^{n-1} = \frac{1 - x^n}{1 - x}$$

and plugged in $x = \omega$.

5.6 Polynomial equations

Theorem 5.4. *Fundamental Theorem of Algebra*
Any polynomial $P(z) \in \mathbb{C}[z]$ of degree $n \geq 1$,

$$P(z) = a_n z^n + a_{n-1} z^{n-1} + \cdots + a_0, \qquad a_n \neq 0$$

has a root $\lambda \in \mathbb{C}$. I.e.

$$\exists \lambda \in \mathbb{C} : \qquad P(\lambda) = 0.$$

Proposition 20. For $P(z)$ as above, there are $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$P(z) = a_n(z - \lambda_1) \ldots (z - \lambda_n).$$

That means that the equation $P(z) = 0$ has n solutions $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ which may appear repeatedly.

We know long division of polynomials

$$\forall A(x), B(x) \in k[x], \exists Q(x), R(x) \in k[x] : \qquad A = BQ + R$$

Remark. We can use long division to

- find $\operatorname{hcf}(A(x), B(x)) \in k[x]$.
- express the hcf in the form $AP + BQ$ for some $P(x), Q(x) \in k[x]$.

Proof. Suppose $P(\lambda) = 0$. Divide $(z - \lambda)$ into P:

$$P(z) = Q(z)(z - \lambda) + R(z) \tag{$*$}$$

The degree of R is strictly smaller than the degree of $z - \lambda$ so R has to be a constant. Evaluating $(*)$ at λ gives us

$$\begin{aligned} & 0 = P(\lambda) = Q(\lambda) \cdot 0 + R \\ \Rightarrow \qquad & R = 0 \end{aligned}$$

So

$$P(z) = Q(z)(z - \lambda)$$

By induction on n

$$Q_{n-1}(z) = \prod_{i=1}^{n-1} (z - x_i).$$

□

The proposition essentially states that the primes in $\mathbb{C}[z]$ are precisely the degree 1 polynomials

$$P(z) = z - \lambda, \qquad \lambda \in \mathbb{C}.$$

Example 42. Split

$$p(z) = z^7 - z^6 - 2z^4 + 2z^3 + z - 1 \in \mathbb{C}[z]$$

into degree one factors.

$$\begin{aligned} p(z) &= (z - 1)(z^6 - 2z^3 + 1) \\ &= (z - 1)(z^3 - 1)^2 \\ &= (z - 1)^3(z^2 + z + 1)^2 \end{aligned}$$

To split $z^2 + z + 1$, we need the cube roots of 1.

$$(z - 1)^3 \left(z + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right)^2 \left(z + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)^2$$

Proposition 21. Suppose

$$P(x) \in \mathbb{R}[x]$$

Then $P(x)$ can be written as a product of degree 1 and degree 2 polynomials.in $\mathbb{R}[x]$. The degree 2 polynomials have each 2 complex conjugate roots and they are prime/irreducible in $\mathbb{R}[x]$.

The proof is based on two ideas:

1. Suppose $\lambda \in \mathbb{C}$ and $P(\lambda) = 0$. Then

$$P\left(\overline{\lambda}\right) = 0$$

2. If $\lambda \in \mathbb{C}$ then

$$(x - \lambda)(x - \overline{\lambda}) = x^2 - \left(\lambda + \overline{\lambda}\right) x + \lambda\overline{\lambda} \quad \in \mathbb{R}[x]$$

5.7 Roots and coefficients of algebraic equations

The coefficients of a polynomial are related to its roots in the following way:

$$(z-\lambda_1)(z-\lambda_2)\dots(z-\lambda_n) = z^n a_{n-1} + z^{n+1} + \dots + a_0$$

where

$$\begin{aligned}
a_{n-1} &= -(\lambda_1 + \dots \lambda_n) \\
a_{n-2} &= \sum_{i<j} \lambda_i \lambda_j \\
a_{n-3} &= \sum_{i<j<n} \lambda_i \lambda_j \lambda_n \\
\dots & \quad .
\end{aligned}$$

Example 43.

- Find a cubic polynomial with roots $\lambda_1 = 1,\ \lambda_2 = 1+i$, and $\lambda_3 = 1-i$.

$$z^3 - 3z^2 + (1+i+1-i+2)z - 2 = z^3 - 3z^2 + 4z - 2$$

- Write λ, μ for the roots of

$$ax^2 + bx + c.$$

Write down an equation with roots λ^2, μ^2.

$$\begin{aligned}
6x^2 + \frac{b}{a}x + \frac{c}{a} &= (x-\lambda)(x-\mu) \\
\lambda + \mu &= -\frac{b}{a} \\
\lambda\mu &= \frac{c}{a}
\end{aligned}$$

We are interested in:

$$(x-\lambda^2)(x-\mu^2) = x^2 - (\lambda^2+\mu^2)x + \lambda^2\mu^2.$$

So we are interested in $\lambda^2+\mu^2, \lambda^2\mu^2$.

$$\begin{aligned}
\lambda^2\mu^2 &= (\lambda\mu)^2 \\
&= \frac{c^2}{a^2} \\
\lambda^2+\mu^2 &= (\lambda+\mu)^2 - 2\lambda\mu \\
&= \frac{b^2}{a^2} - \frac{2c}{a}
\end{aligned}$$

So the equation we are looking for is:

$$x^2 + \left(\frac{2c}{a} - \frac{b^2}{a^2}\right)x + \frac{c^2}{a^2}.$$

or, tidying up

$$x^2x^2 + (2ac - b^2)x + c^2 = 0.$$

5.7.1 Equations of degree 3

Everybody knows the quadratic formula:

$$ax^2 + bx + c = 0.$$

Then

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Now we are going to find a formula to similarly compute roots of equations of degree 3. Let's start with

$$x^3 + Ax^2 + Bx + C = 0. \qquad (*)$$

By taking $y = \alpha = \frac{A}{3}$ we can get rid of the term Ax^2:

$$y^2 = \left(x + \frac{A}{3}\right)^3 = x^3 + Ax^2 + \frac{A^2}{3}x + \frac{A^3}{27}$$

Then we get a simpler equation for $(*)$ in y:

$$\begin{aligned}
(*) \Leftrightarrow && \left(x + \frac{A}{3}\right)^3 + Bx - \frac{A^2}{3}x + C - \frac{A^3}{27} = 0 \\
\Leftrightarrow && \left(x + \frac{A}{3}\right)^3 + \left(B - \frac{A^2}{3}\right)\left(x + \frac{A}{3}\right) - \frac{A}{3}\left(B - \frac{A^2}{3}\right) + C - \frac{A^2}{27} = 0 \\
\Leftrightarrow && y^3 + \left(B - \frac{A^2}{3}\right)y + C - \frac{AB}{3} + \frac{2A^3}{27} = 0
\end{aligned}$$

Therefore, we can write our equation in the form

$$y^3 + 3py + 2q = 0.$$

We look for a solution $y = u + v$. (1)
Then

$$y^3 = 3uv(u+v) + u^3 + v^3$$

We try

$$\begin{aligned}
uv = -p \quad &\Leftrightarrow \quad u^3v^3 = -p \\
u^3 + v^3 = -2q &
\end{aligned}$$

Then u^3, v^3 are the two roots of the quadratic equation:

$$x^2 + 2qx - p^3 = 0$$

The quadratic formula gives:

$$u^3, v^3 = -q \pm \sqrt{p^2 + q^3} \qquad (2)$$

So putting (1) and (2) together:

$$y = \sqrt[3]{-q + \sqrt{q^2 + p^3}} + \sqrt[3]{-q - \sqrt{q^2 + p^3}}$$

Remark. We seem to have 9 roots! But remember $uv = -p$ The tells us how to pair up the cube roots to get just 3 roots. We may also rewrite the formula as:

$$y = \sqrt[3]{-q\sqrt{q^2 + p^3}} - \frac{p}{\sqrt[3]{-q + \sqrt{q^2 + p^3}}}$$

Example 44. • Solve for y:

$$\begin{aligned}
& y^3 - y + 1 = 0 \\
\Leftrightarrow \quad & y = \sqrt[3]{-\frac{1}{2} + \sqrt{\frac{1}{4} - \frac{1}{27}}} + \sqrt[3]{-\frac{1}{2} - \sqrt{\frac{1}{4} - \frac{1}{27}}} \\
& = \sqrt[3]{-\frac{1}{2} + \frac{1}{6}\sqrt{\frac{27}{9}}} + \sqrt[3]{-\frac{1}{2} - \frac{1}{2}\sqrt{\frac{27}{9}}}
\end{aligned}$$

You get one solution by taking real cube roots in this formula. The two other (complex conjugated) solutions are:

$$\rho\sqrt[3]{-\frac{1}{2}+\frac{1}{4}\sqrt{\frac{23}{3}}}+\rho^2\sqrt[3]{-\frac{1}{2}-\frac{1}{6}\sqrt{\frac{23}{3}}}$$

where $\rho = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$.

- Suppose you try to find a decent formula for $\cos\frac{\pi}{9}$.

$$e^{\frac{\pi i}{9}} = x + iy$$

then $x = \cos\frac{\pi}{9}, y = \sin\frac{\pi}{9}$.

$$\begin{aligned}(x+iy)^3 &= x^3 - 3xy + (3x^2y - y^3)i\\ &= e^{\frac{\pi i}{3}} = \frac{1}{2} + \frac{i\sqrt{3}}{2}\\ y^2 &= 1 - x^2\end{aligned}$$

equation $4 - x^3 - 3x - \frac{1}{2} = 0$. The cubic formula:

$$\begin{aligned}x &= \sqrt[3]{\frac{1}{16}+\frac{i}{16}\sqrt{3}}+\sqrt{\frac{1}{16}-\frac{i}{16}\sqrt{3}}\\ &= \frac{1}{2}\left(\sqrt[3]{\frac{1}{2}+\frac{i\sqrt{3}}{2}}+\sqrt[3]{\frac{1}{2}-\frac{i\sqrt{3}}{2}}\right)\end{aligned}$$

The cubic formula tells me to find $\sqrt[3]{\frac{1}{2}+i\frac{\sqrt{3}}{2}}$ but this is what we were trying to find from the start. Conclusion: in this case the cubic formula is useless.

5.8 Infinite Sets

Definition 5.18. A set S is countable iff there exists a bijective function $f : \mathbb{N} \to S$.

Basically this means that we can list all the elements of S:

$$S = \{S_1, S_2, S_3, \dots\}$$

(More formally $S_n = f(n)$.) Any countable set is infinite. We want to learn how to prove that some sets are countable.

Proposition 22. Suppose $S \subseteq \mathbb{N}$ is infinite. Then S is countable.

Proof. Informally speaking: Take $S_1 = \min S$. Take S_2 to be the next element of S:

$$\begin{aligned}&S_2 = \min S\backslash\{S_1\}\\ &S_3 = \min S\backslash\{S_2\}\\ &\dots\end{aligned}$$

Now formally, we define a function $f : \mathbb{N} \to S$ inductively as follows:

$$f(1) = \min S$$

and assume $f(k)$ to be defined for $k < n$. Then define

$$f(n) = \min S\backslash\{f(1), \dots, f(n-1)\}$$

Then we want to show that f is injective and surjective. □

Example 45.

- $\mathbb{Z}$ is countable.

Proof. Define

$$f(n) = \begin{cases} \frac{n}{2}, & n \text{ even} \\ -\frac{n+1}{2}, & n \text{ odd} \end{cases} .$$

Then $f : \mathbb{N} \to S$ is bijective. (Now we have to write down a function g which is the inverse of S.) □

- Suppose A, B are countable sets. Then $A \times B$ is countable.

  Proof. It is enough to show that $\mathbb{N}\times\mathbb{N}$ is countable. I can see that $\mathbb{N}\times\mathbb{N}$ is countable by picture. Note: the picture is quite clear. However it still seems awkward to write an explicit formula for a bijective function $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. There is a slightly slicker way. Define an injective function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Then the proposition shows that $\mathbb{N} \times \mathbb{N}$ is countable. (apply to $S = \text{image}(f)$.)

  $$f(k, n) = 2^k 3^n$$

  f is injective by unique factorization. □

Proposition 23. $\mathbb{Q}$ is countable.

Proof.

$$\mathbb{Q} \subset \mathbb{Z} \times \mathbb{Z}\backslash\{0\}$$

$$\left[\frac{p}{q}\right] \mapsto \frac{m}{n} \sim \frac{p}{q} \text{ in lowest terms with } n > 0$$

and $\mathbb{Z} \times (\mathbb{Z}\backslash\{0\}$ is countable. □

Theorem 5.5. $\mathbb{R}$ is not countable.

Some infinite sets are bigger than others

Proof. Suppose for contradiction that one could make a list of all real numbers. Then it would look like this:

$$\begin{aligned} x_1 &= a_1.a_{11}a_{12}a_{13}\dots \\ x_2 &= a_2.a_{21}a_{22}a_{23}\dots \\ x_3 &= a_3.a_{31}a_{32}a_{33}\dots \\ &\dots \end{aligned}$$

where $a_1, a_2, a_3, \dots \in \mathbb{Z}$ and $a_1 1, \dots, a_{kn} \dots \in \{0, 1, 2 \dots, 9\}$. We produce a real number $x \in \mathbb{R}$ which is not on the list.

Pick $b_1 \in \mathbb{Z} b_1 \neq a_1$
Pick $c_1 \in \{0, 1, 2 \dots, 8\} c_1 \neq a_{21}$
Pick $c_2 \in \{0, 1, 2 \dots, 8\} c_2 \neq a_{32}$
and so on. Take

$$x = b_1.c_1c_2c_3\dots$$

□