Mathematics 1

Winter Term 2022-23

Jack Maerschand

For errors message:
Nerd#0014

Contents

1 Logic

1.1 Basics

Truth tables are constructed with logical operators each with a different effect on the table. Possible logical operators include: AND, OR, NOR, XOR, etc...

The Logical operator compares two items, a TRUE statment is only returned when both event p and q are TRUE.

p	q	$\overbrace{q \wedge q}^{\textbf{AND}}$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**F**

p	q	$\overbrace{q \vee q}^{\textbf{OR}}$
T	T	**T**
T	F	**T**
F	T	**T**
F	F	**F**

p	q	$\overbrace{q \oplus p}^{\textbf{XOR}}$
T	T	**F**
T	F	**T**
F	T	**T**
F	F	**F**

1.1.1 Implication

An additional logical operator includes implication. This property is denoted by the symbol "$\Rightarrow$" and reads: *P implies Q, if P then Q, Q if P, Q when P*

> If you tidy your room (P), then you will get an ice cream (Q)

p	q	$\overbrace{p \Rightarrow q}^{\textbf{Implication}}$
T	T	**T**
T	F	**F**
F	T	**T**
F	F	**T**

1. If room is cleaned then you will get ice-cream
2. If room is cleaned and you don't get ice-cream it renders the premise FALSE
3. If you room is **not** clean and you have an icecream there is not enough information to disprove that statement
4. When the room is not clean and you dont get any icecream the premise is TRUE

However, the two conditions as shown in the example above **do not have to share causality**. Hence, a logical statement could be *If Rome is in France, 3 is a prime number.*

Different implication conditions for $P \Rightarrow Q$:

$Q \Rightarrow P$	$\neg P \Rightarrow \neg Q$	$\neg Q \Rightarrow \neg P$
Converse	**Inverse**	**Contrapositive**

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\overbrace{P \Rightarrow Q}^{\textbf{converse}}$	$\overbrace{\neg Q \Rightarrow \neg P}^{\textbf{Inverse}}$	$\overbrace{\neg Q \Rightarrow \neg P}^{\textbf{Contrapositive}}$
T	T	F	F	**T**	T	T	T
T	F	F	T	**F**	T	T	F
F	T	T	F	**T**	F	F	T
F	F	T	T	**T**	T	T	T

Hence we can conclude that Implication ≡ Contrapositive. **Logical Equivalence**: when they have the same truth values in all cases.

$$P \Rightarrow Q \equiv \neg Q \Rightarrow \neg P$$

1.1.2 Biconditional Statements

p	q	$\overbrace{p \Leftrightarrow q}^{\textbf{equivalence}}$
T	T	**T**
T	F	**F**
F	T	**F**
F	F	**T**

Output of proposition is only true when both values hold the same value. *Example*:

$$\sqrt{b^2 - 4ac} = 0 \Leftrightarrow \textbf{one real solution}$$

Below Shows how biconditional statements work, it only results in a TRUE value when both conditions are TRUE or FALSE

P	Q	$\neg P$	$\neg Q$	$P \Rightarrow Q$	$\neg Q \Rightarrow \neg P$	$\overbrace{(P \Rightarrow Q) \Leftrightarrow (\neg Q \Rightarrow \neg P)}^{\textbf{Logical equivalence \& tautologies}}$
T	T	F	F	**T**	T	**T**
T	F	F	T	**F**	T	**T**
F	T	T	F	**T**	F	**T**
F	F	T	T	**T**	T	**T**

1.1.3 Laws

1. $\underbrace{P \vee Q \equiv Q \vee P}_{\vee\ =\ \text{OR}}$ and $\underbrace{P \wedge Q \equiv Q \wedge P}_{\wedge\ =\ \text{AND}}$ **(communicative)**
2. $(P \vee Q) \vee R \equiv P \vee (Q \vee R)$ **(associative)** $\vee$ or $\wedge$ possible
3. $P \vee (Q \vee R) \equiv (P \vee Q) \wedge (P \vee R)$ **(distributive)**
4. $P \vee P \equiv P$ **(idempotent)**
5. $\neg\neg P \equiv P$ **(involution)**
6. $\neg(P \vee Q) \equiv \neg P \wedge \neg Q$ **(De Morgan's Law)**
7. $(P \Rightarrow Q) \equiv \neg P \Rightarrow \neg Q$ **(implication/contrapositive)**
8. $P \Rightarrow Q \equiv \neg P \vee Q$ **(implication as disjunction)**
9. $\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$ **(negation of implication)**

2 Sets

2.1 Basics

To **define** a set use **capital letters**: $A, B, ...A_1, A_2$

For elements (objects within a set) you use **lowercase letters**: $a, b, ...x_1, x_2$
Through this we are able to express that an item a is an element of the set A:

$$a \in A$$

Symbols

$\{\}$	**Set:** collection of elements $\{1, 2, 3, 4\}$
$A \cup B$	**Union:** in A or B (or both)
$A \cap B$	**Intersection:** in both A and B
$A \subseteq B$	**Subset:** every element of A in B
$A \subset B$	**Proper Subset:** every element of A is in B but B has more elements
$A \not\subseteq B$	**Not a subset:** A is not a subset of B
$A \supseteq B$	**Superset:** A has same elements as B, or more
$A \supset B$	**Proper superset:** A has B's elements and more
$A \not\supseteq B$	**Not a superset:** A is not a superset of B
A^c	**Complement:** elements not in A
$A - B$	**Difference:** in A but not in B
$\mathbb{N}$	Natural Numbers
$\mathbb{Z}$	Integers
$\mathbb{Q}$	Rational Numbers
$\mathbb{A}$	Algebraic Numbers
$\mathbb{R}$	Real Numbers
$\mathbb{I}$	Imaginary Numbers
$\mathbb{C}$	Complex Numbers
$\mathbb{U}$	Universal Set
$\forall$	For All
$\exists$	There Exists
$\mid$, :	Such that
$\therefore$	Therefore
$\varnothing$	Empty Set
$\in$, $\ni$	Element, Not Element
$\mathcal{P}(A)$	**Power Set:** all subsets of A

2.2 Laws

1. $A \cup B = B \cup A$ and $A \cap B = B \cap A$ **(communicative)**
2. $A \cup (B \cup C) = (A \cup B) \cup C$ **(associative)** also possible: $\cap$
3. $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
   $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ **(distributive)**
4. $A \cup \varnothing = A$ and $A \cap U = A$
5. $A \cup A^c = U$ and $A \cap A^c = \varnothing$
6. $A \cup A = A$ and $A \cap A = A$
7. $A \setminus B = A \cap B^c$
8. $(A \cup B)^c = A^c \cap B^c$
   $(A \cap B)^c = A^c \cup B^c$ **(DeMorgan's rule)**

2.3 Sets I

2.3.1 Breaking Down Sets

A base set A can be broken down into smaller sub sets B:

$$A \coloneqq \{1, 2, 3\}$$

$$\mathcal{P}(A) \text{ or } B \coloneqq \{\varnothing, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

2.3.2 Describing Sets

Say you have a set A shown bellow. To describe this set you can use the symbols shown before: $A \coloneqq \{1, 2, 3\}$

$$A = \{x : x \text{ is integer}, 0 < x \leq 5\} \qquad | \qquad A = \{x \mid x \in \mathbb{N}, x > 0 \text{ and } x \leq 6\}$$

When two sets are the **same** such as the ones shown bellow you can write them as $A_1 = A_2 = A3$. This is because they all **contain the same elements**.

$$A_1 = \{0, 1, 2\} \qquad A_2 = \{2, 0, 1\}$$

$$A_3 = \{0, 0, 1, 1, 2, 2\}$$

2.3.3 Subsets

$$A \subseteq B$$

The statement above implies that A is a subset of B. This means that every element in A is also in B **(possibly)**. This can be written also as:

$$A \subseteq B :\Leftrightarrow \forall x : x \in A \Rightarrow x \in B$$

This reads as:

A is a subset of B such that for all elements x in A, x is an element of B.

However, $\subseteq$ is not the only symbol used. $\subset$ indicates that A is a subset of B and $A \neq B$. This means that there are elements in B that are not an element of A. This can also be denoted with the symbol $\subsetneq$ known as a: **proper subset**.

$$A = \{0, 1, 2\} \qquad B = \{0, 1, 2, 3\}$$
$$\therefore A \subset \textbf{,} \subsetneq B$$

$$\underbrace{A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A}_{\text{Expresses that two sets}A \text{ and } B \text{ are } \textbf{equal}.}$$

Logical Operators

$$A \cup B := \{x \mid x \in A \textbf{ or } x \in B\}$$

$$A \cap B := \{x \mid x \in A \textbf{ and } x \in B\}$$

Examples:

⇝ For $A := \{0, 1, 2, ..., 100\}$ **and** $B := \{50, 51, ..., 149, 150\}$ we get:

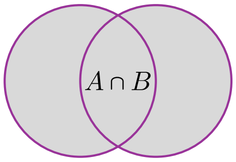
$$A \cup B = \{0, 1, 2, ..., 148, 149, 150\}$$

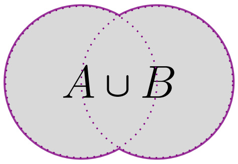
$$A \cap B = \{50, 51, 52, ...98, 99, 100\}$$

⇝ For $A := \{0, 1\}$ **and** $B := \mathcal{P}(A) = \{\varnothing, \{0\}, \{1\}, \{0, 1\}\}$ we get:

$$A \cup B = \{0, 1, \varnothing, \{0\}, \{1\}, \{0, 1\}\}$$

$$A \cap B = \varnothing$$



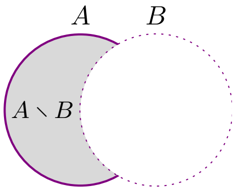


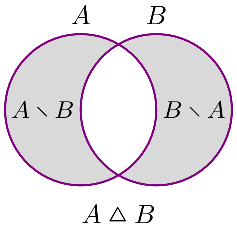
2.4 Set Difference

The set difference is denoted with a back slash. It implies that a new set with only the elements found in A and not in B are included: $A \setminus B$

$$A - B = A \setminus B = \{x \mid x \in A \text{ and } x \notin B\}$$

The **union** set difference of both A and B: $(A \setminus B) \cup (B \setminus A)$. This is symmetric difference denoted as such: $A \triangle B$. This is depicted in the diagrams bellow. It includes everything except $A \cap B$.





2.5 Cartesian Sets

There are two sets A and B, from this we can define the **Cartesian Product** as the **set of ordered pairs**: $A \times B$

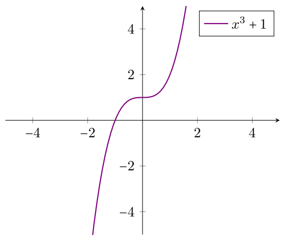
$$A \times B \coloneqq \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Examples:

$$A = \{1, 2, 3\} \quad \text{and} \quad B = \{s, t\}$$

We know this is an ordered element wise mapping. Hence we can combine these to create the Cartesian Product: $A \times B$...

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



We can also apply this element wise mapping to a function: $f(x) : x^3 + 1$

$$\begin{aligned} f :& X \to Y \\ :& x \mapsto f(x) \end{aligned}$$

$$\boxed{G(f) \coloneqq \{(x, f(x)) \ \mid \ x \in X\}}$$

3 Combinatorics

3.1 Basics

3.1.1 Permutations

Permutations are a way of selecting objects in a **definite order**. A **ordered selection** of k objects from a set of n objects is referred to as k-**permutation**. To indicate the use of permutations the mathematical expression bellow is used...

$$^{n}P_k = \frac{n!}{(n-k)!} \qquad \textbf{or} \qquad P(n,k)$$

Example:

Number of permutations that are able to be formed with the set $\{A, B, C\}$

$$n = k = 3 \therefore ABC - ACB - BAC - BCA - CAB - CBA$$

$$^{3}P_3 = \frac{3!}{(3-3)!} = \frac{3!}{(0)!} = \frac{6}{1} = \boxed{6}$$

This means we have 6 possible **permutations** $P(3,3) = 3 \cdot 2 \cdot 1 = 6$. This is because there are 3 possibilities for the 1st position, 2 in the second and 1 in the last position.

3.1.2 Combinations

A combination is the number of possible arrangements where the **order does NOT** matter. In other words its an **unordered** selection of k elements from a set of n elements. The mathematical expression used is...

$$C(n,k) = \frac{P(n,k)}{k!} \qquad \textbf{or} \qquad ^{n}C_k = \frac{n!}{k!(n-k)!}$$

Example:

Number of combinations that are able to be formed with the set $\{A, B, C\}$

$$\begin{aligned} C(3,0) + C(3,1) + C(3,2) + C(3,3) &= \binom{3}{0} + \binom{3}{1} + \binom{3}{2} + \binom{3}{3} \\ &= 1 + 3 + 3 + 1 \\ &= 2^3 = \boxed{8} \end{aligned}$$

3.1.3 Counting with Repetitions

What was described above is without repetitions however, this is not representative. For example, when you create a password you can repeat characters.

	permutations	combinations
without repetition	$\frac{n!}{(n-k)!}$	$\binom{n}{k}$
with repetition	n^k	$\binom{n+k-1}{k}$

3.2 Principles

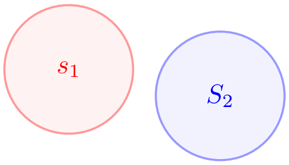
3.2.1 Addition Principle

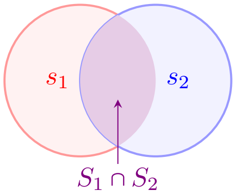
The addition principle states that if an event S_1 can occur in n_1 ways and an event S_2 can occur in n_2 ways. If they are disjoint then S_1 and S_2 can occur in $n_1 + n_2$ different ways.

$$\text{If } S_1 \cap S_2 = \varnothing \quad \Rightarrow \quad |\, S_1 \cup S_2 \,| = |\, S_1 \,| + |\, S_2 \,|$$

However, if $S_1 \cap S_2 \neq \varnothing$ then you have to use:

$$|\, S_1 \cup S_2 \,| = |\, S_1 \,| + |\, S_2 \,| - |\, S_1 \cap S_2 \,|$$





3.2.2 Multiplication Principle

The idea behind this principle is that if there are n_1 ways of doing S_1 and there are n_2 ways of doing S_2 then there are $n_1 \times n_2$ **ways of performing both actions**.

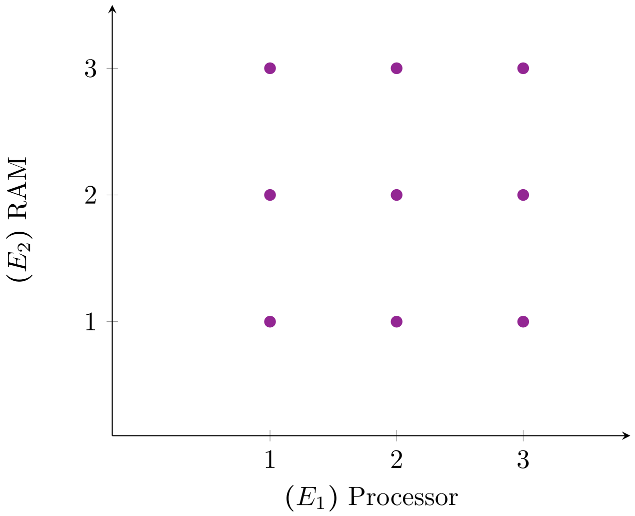
Example: buying a customized Mac Book

- ➠ Processor (E_1): 3 choices n_1
- ➠ RAM (E_2): 3 choices n_2
- ➠ Graphics (E_3): 4 choices n_3
- ➠ SSD (E_4): 5 choices n_4

$$n_1 \times n_2 \times n_3 \times n_4$$
$$= 3 \times 3 \times 4 \times 5 = \boxed{180}$$

The Multiplication Principle in **set-theory** is **comparable** to the cardinality of **Cartesian products**

$$\mid A \times B \mid = \mid A \mid \times \mid B \mid$$



3.3 Binomials

The Binomial Theorem represented by the equation bellow is a method of expanding an expression. By using the equation you are able to find the **binomial coefficient**. Where $n, k \in \mathbb{N}$

$$\textbf{Theorem} \quad (a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\, b^k$$

$$\textbf{Coefficient} \quad \binom{n}{k} = \frac{n}{k! \cdot (n-k)}!$$

When you have an expression such as the one shown bellow, using the binomial theorem will give you the highlighted coefficients of the expanded expression...

$$(x+y)^4 = 1 \cdot x^4 + 4 \cdot x^3 y + 6 \cdot x^2 y^2 + 4 \cdot x y^3 + 1 \cdot y^4$$

The expression holds the form: $(x+y)^n$. Comparing this to **pascals triangle** you will notice that $n = 4$, hence the coefficients are $1, 4, 6, 4, 1$. For small n values using the pascals triangle is possible. **However**, when n is large using the Binomial Theorem is favourable.

3.3.1 Binomial Properties

1. **Intuitive binomial cases:** $\forall n \in \mathbb{N}$

$$\binom{n}{0} = 1 \quad \text{and} \quad \binom{n}{1} = n$$

2. **Symmetry:**

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

3. **Adding Binomial Coefficients:** $\forall k \geq 1$

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

4. **Recursion:**

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

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

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

3.3.2 Pascals Triangle

The pascals triangle is a visual representation of the coefficients depending on their exponent n.

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

4 Number Theory

4.1 Divisibility

4.1.1 Basics

A basic rule is that if an integer a divides an integer b if an integer k exists such that:

$$a \cdot k = b$$

We can further denote this by saying that if an integer a divides and integer b the outcome is $a \mid b$. Or if the two numbers are not divisible we say $a \nmid b$. This can be read as: b is divisible by a.

Additionally, if we have 3 integers a, b, c it can be said that: If $a \mid b$ and $b \mid c$ then $a \mid c$. For example if $a = 12, b = 6, c = 3$. This is shown bellow...

$$a \mid b \ \cap \ b \mid c \ \Rightarrow \ a \mid c$$

4.1.2 Integer Linear Combination

This goes back to the simple rules of division. The two rules shown bellow are referred to as Integer Linear Combinations. The rule is that if $a \mid b$ and $a \mid c$, then...

$$a \mid \ s \cdot b + t \cdot c \quad \forall s, t$$

Hence, if $a \mid b$ and $a \mid c$, then a divides every integer linear combination of b and c. $s, t \in \mathbb{Z}$

4.1.3 Division with Remainder

If an integer b is not divisible by another integer a, we get a quotient and a remainder. To express this remainder we need to establish what the **absolute value** is. The absolute value of a number is denoted as, $\mid x \mid$.

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Essentially the absolute value of a number is the positive equivalent of it. If the number is already positive nothing changes. However, if the number is negative you multiply its by -1. **Examples:** $|5| = 5 \quad |0| = 0 \quad |-5| = 5$

Using the absolute value of a number allows us to find the **range** of the **remainder**. The equation bellow has 4 elements b, a, q, r. b is the number being divided. a is the divisor. q is the quotient, essentially how many times the divisor fits into the number being divided. Lastly, r is the remainder.

$$b = a \cdot q + r \quad \text{and} \quad 0 \leq r < |a|$$

Example: $b = 37$ and $a = 3$

$$\begin{aligned} b &= a \cdot q + r \\ 37 &= 3 \cdot 12 + 1 \end{aligned}$$

4.1.4 Greatest Common Divisor

A **common divisor** is a number that divides two integers a and b. Hence, the greatest common divisor is the number from the set of common divisors that holds the greatest value. This expressed as $\gcd(a, b)$. The two rules for gcd are...

1. $d \mid a$ and $d \mid b$
2. If e is a common divisor of a and b, then $e \mid d$

For the **second condition**, it can be difficult to understand as such the bellow sets show what this property entails. You have two numbers $a = 12$ and $b = 24$, there divisors are listed bellow.

$$\begin{aligned} D_{12} &= \{1, 2, 3, 4, 6, 12\} \\ D_{24} &= \{1, 2, 4, 6, 8, 12, 24\} \\ D_{\text{common}} &= \{1, 2, 4, 6, 12\} \end{aligned}$$

Subsequently, we can conclude that the $\gcd(12, 24) = 12$, as such any number in D_{common} should be able to divide the gcd, 12. This can be written as, $e \mid d$.

4.1.5 Greatest Common Divisor Properties

1. $\gcd(k \cdot a, k \cdot b) = k \cdot \gcd(a, b) \forall k > 0$
2. For two integers a and b, their gcd can be written as a **linear combination**...
$$\gcd(a, b) = s \cdot a + t \cdot b \quad s, t \in \mathbb{Z}$$
3. If $a \mid b \cdot c$ and $\gcd(a, b) = 1$, then $a \mid c$.
4. If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, b \cdot c) = 1$.

4.2 Euclid's Algorithms

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers, a and b. To do this with two integers a, b with $a > b$ and $b > 0$. The gcd occurs with the last remainder as shown bellow. (the remainder cannot be $= 0$, $r_k \neq 0$)

$$b = a \cdot q + r$$

$$\begin{aligned}
2294 &= 1798 \cdot 1 + 496 \quad r_0 = 496 \quad q_0 = 1 \\
1798 &= 496 \cdot 3 + 310 \quad r_1 = 310 \quad q_1 = 3 \\
496 &= 310 \cdot 1 + 186 \quad r_2 = 186 \quad q_2 = 1 \\
310 &= 186 \cdot 1 + 124 \quad r_3 = 124 \quad q_3 = 1 \\
186 &= 124 \cdot 1 + 62 \quad r_4 = 62 \quad q_4 = 1 \\
124 &= \boxed{62} \cdot 2 + 0
\end{aligned}$$

The result is $\gcd(2294, 1798) = 62$

4.2.1 Linear Combination GCD

The Euclidean algorithm can be expressed as a linear combination. Allowing us to find the coefficients s and t.

$$\gcd(a, b) = s \cdot a + t \cdot b$$

(colors above do not apply to 4.2.1)

Example: Find the linear combination of $a = 270$ and $b = 192$

Step 1)

$$\begin{aligned}
270 &= 1 \cdot 192 + 78 \\
192 &= 2 \cdot 78 + 36 \\
78 &= 2 \cdot 36 + 6 \\
36 &= 6 \cdot 6 + 0
\end{aligned}
\quad \xRightarrow[\text{Equations}]{\text{Rewrite}} \quad
\begin{aligned}
78 &= 1(270) - 1(192) \\
36 &= 1(192) - 2(78) \\
6 &= 1(78) - 2(36) \\
&\boxed{s \cdot a + t \cdot b}
\end{aligned}$$

Step 2)

$$\begin{aligned}
6 &= 1(78) - 2(36) \\
&= 1(78) - 2(1(192) - 2(78)) \\
&= -2(192) + 5(78) \\
&= -2(192) + 5(1(270) - 1(192)) \\
&= -2(192) + 5(270) - 5(192) \\
&= 5(270) - 7(192)
\end{aligned}$$

4.3 Prime Numbers

4.3.1 Basics

Prime numbers are numbers that are divisible by **only** themselves and 1. A prime number is a positive integer and is expressed as $\mathbb{P}$. All non-prime numbers are composite numbers. This means they are **composed** of different smaller numbers.

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, \ldots\}$$

4.3.2 Prime Factorization

Every integer can be **uniquely** written as a **product** of a **weakly** increasing sequence of **prime factors:**

$$a = p_1 \cdot p_2 \cdot \ldots \cdot p_r \quad \text{with} \begin{cases} p_1, p_2, \ldots \in \mathbb{P} \\ p_1 \leq p_2 \leq \cdots \leq p_r \end{cases}$$

The meaning of **weakly** is that if you have a sequence of numbers $x_1, x_2, x_3, \ldots$. The weak sequence proposition is $x_i \leq x_j$ for $i < j$. However, a strong sequence is $x_i < x_j$ for $i < j$.

4.4 Modular Arithmetic

4.4.1 Congruence

Congruence is a system of arithmetic for integers, which considers the remainder. The "wrapping point", is how you calculate the remainder, this is referred to as the modulus.

To understand the modulus, you can use a 12- hour clock. If the time is currently $8:00$ then in 9 hours the clock will not show $17:00$ it will show $5:00$. This is because the wrapping point is at 12 so the remainder of $17:00 - 12:00$ is $5:00$. This can be expressed as $\boxed{17 \bmod(12) \equiv 5}$

Generally speaking say you have an expression $a \equiv b(\text{mod}N)$. There are three truth statements:

1. a, b have the same **remainder** when divided by N

$$a \equiv b \bmod m \iff \text{rem}(a, m) = \text{rem}(b, m)$$

2. Converting a congruence statement to an equation, $a - k \cdot n + 6$
3. $n \mid (a - b)$, This means that n divides $(a - b)$ hence its a multiple of N

Example: $10 \equiv 14(\text{mod}4) \begin{cases} 10 \div 4 = & 2 \quad \text{rem: } 2 \\ 14 \div 4 = & 3 \quad \text{rem: } 2 \end{cases}$

4.4.2 Residue Classes

A residue class is a complete set of integers that are congruent modulo for some positive integer.

For two residue classes $\bar{a}$ and $\bar{b} \in \mathbb{Z}_m$ we define their sum and product as the equation bellow. Hence, if we have $N = 3$, this is your modulo and $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ the resulting residue classes are...

$$\bar{a} + \bar{b} = \overline{a + b} \quad \text{and} \quad \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Example: This is from a class exercise, task 4.6

$$\mathbb{Z}_4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

For this example we use the modulo value 4 as that is shown in the subscript $\mathbb{Z}_4$. You calculate by either adding or multiplying the 4 main significant numbers and then applying mod(4), to them.

4.4.3 Multiplicative Inverse

For a given modulo m and an integer a an integer b is called the modulo multiplicative inverse, if

$$a \cdot b \equiv 1 \bmod m$$

Formulated for residue classes: for a residue class $\bar{a} \in \mathbb{Z}_m$ we call $\bar{b} \in \mathbb{Z}_m$ the multiplicative inverse residue class, if

$$\bar{a} \cdot \bar{b} = \bar{1}$$

To know if a given number **has a multiplicative inverse** the greatest common divisor has to be 1. Hence if you have $\bar{a} = \overline{15}$ in $\mathbb{Z}_{23}$, to find if it has a multiplicative inverse calculate $\gcd(15, 23) = 1$.

To know which **residue classes** have multiplicative inverses the same logic from above applies. The gcd has to be equal to 1 (if the two numbers a, m are relatively prime). $a \cdot b = 1 + q \cdot m \quad$ or $\quad 1 = a \cdot b - q \cdot m$

Theorem: If $c \cdot a \equiv c \cdot b \bmod m$ and $\gcd(c, m) = 1$, then $a \equiv b \bmod m$.

Proof: If $c \cdot a \equiv c \cdot b \bmod m$, then $m \mid (ca - cb)$ and $m \mid c \cdot (a - b)$. As $\gcd(c, m) = 1, m$ and c have no common divisors (except 1), so $m \mid (a - b)$ and therefore $a \equiv b \bmod m$.

Example: This is from a class exercise, task 4.6 First step is to calculate the gdc(14, 19) subsequently transforming it into a integer linear combination to find the **coefficient** of 14.

Step 1:

$$\begin{aligned} 19 &= 14 \cdot 1 + 5 & &\Longrightarrow & 5 &= 1(19) - 1(14) \\ 14 &= 5 \cdot 2 + 4 & &\Longrightarrow & 4 &= 1(14) - 2(5) \\ 5 &= 4 \cdot 1 + 1 & &\Longrightarrow & 1 &= 1(5) - 1(4) \\ 4 &= 1 \cdot 4 + 0 & & & & \end{aligned}$$

Step 2:

$$\begin{aligned} 1 &= 1(5) - 1(4) \\ &= 1(5) - (1(14) - 2(5)) \\ &= 3(5) - 1(14) \\ &= 3(1(19) - 1(14)) - 1(14) \\ &= 3(19) - 4(14) \end{aligned}$$

Step 3: The coefficient is shown in blue this is the modular inverse as such we can perform the following, 19 = 4 giving us $\boxed{15}$ which is our modular inverse.

4.5 RSA Encryption

4.5.1 Euler's Totient Function

Also known as the phi function denoted with the φ symbol. It takes a **positive integer** and returns the number of elements that are co prime with that number.

$$\varphi(n) := |\{a \in \mathbb{N} \mid 1 \leq a \leq n \land \gcd(a, n) = 1\}|$$

The statement reads: for any number a that is a Natural number, greater than 1 and smaller than n that has a greatest common divisor of 1 with n.

A number that is **coprime** or **relatively prime** relative to another number, eg. a, b has to have a $\gcd(a, b) = 1$. Hence, their only common divisor is 1.

For **composite numbers** such as the one shown the $\varphi(n)$ has to be calculated as shown... For $n = 6$ the integers $1 \leq a \leq n$ are the set $\{1, 2, 3, 4, 5, 6\}$, of which 1 and 5 are coprime to 6 therefore $\varphi(6) = 2$

However, if $\varphi(\mathbb{P})$, this means that the input value is a **prime number** the output of the function will be $\varphi(\mathbb{P}) = \mathbb{P} - 1$

4.5.2 Totient Multiplication Rule

The multiplication rule can be applied to any number n, where $n = a \cdot b$ with a and b which are **coprime**. This allows us to break down larger numbers within the function, **prime factorization**

$$\varphi(n) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

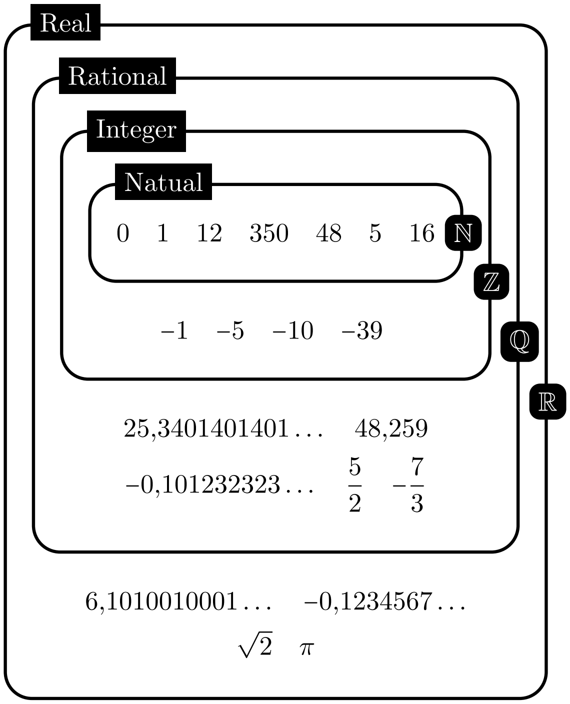
$$\varphi(69) = \varphi(3 \cdot 23) = \varphi(3) \cdot \varphi(23) = (3 - 1) \cdot (23 - 1) = 44$$

4.5.3 Fermat's Little Theorem

5 Numbers

5.1 Basics

As seen in the Sets section, the symbols shown bellow are used to provide information regarding a numbers categorisation. Not included in this diagram are Complex numbers and imaginary numbers.



5.2 Complex Numbers

Complex numbers don't have a solution within the Real number scope. For example, $x^2 = -1$ the value of a square root over a negative number is an imaginary number i. The **set of complex numbers** consists of the sum shown bellow...

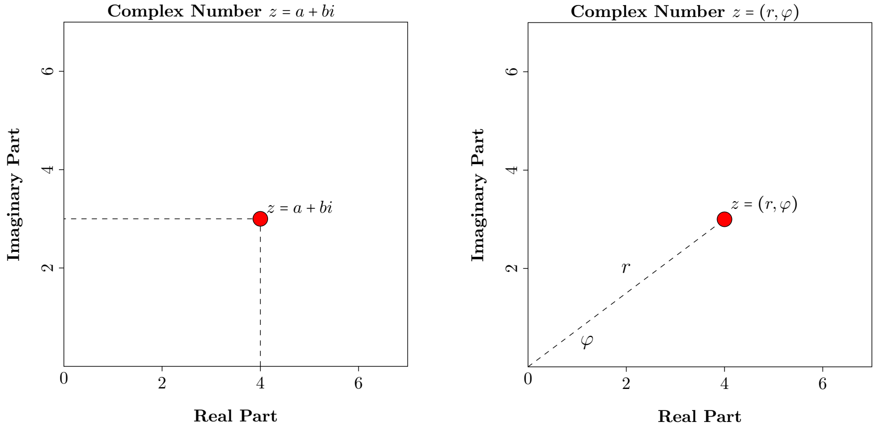
$$z = a + i \cdot b \quad \text{with } a, b \in \mathbb{R}$$

5.2.1 Complex Plane

These complex numbers can be graphed this is done through the use of a complex plain. It makes use of the Cartesian Coordinate system, where the x-axis represents real numbers and the y-axis represents imaginary values.

The output of the equation above, $z = a + i \cdot b$ is in the form (x, y). However, it is easier to plot complex numbers through the use of polar coordinates. The output for plotting them through polar coordinates is shown bellow.

$$(x, y) = (r\cos\vartheta, r\sin\vartheta)$$
$$(r, \vartheta) = (\sqrt{x^2 + y^2}, \arctan\frac{y}{x})$$



5.2.2 Conversions

Furthermore, the conversion table presented bellow can be used to find different values based on the input parameters. The value ϕ is the the only value that is constant, 2π.

$$a = r \cdot \cos\vartheta \qquad b = r \cdot \sin\vartheta$$
$$r^2 = a^2 + b^2 \qquad \tan\vartheta = \frac{b}{a}$$

5.2.3 Addition of Complex Numbers

Say you have two complex numbers, $z_1 = a_1 + b_1 \cdot i$ and $z_2 = a_2 + b_2 \cdot i$. If you want to add or multiply these two numbers you use the **identity**: $i^2 = -1$. Additionally you can only add the real parts with each other and the imaginary parts.

$$z_1 + z_2 = (a_1 + b_1 \cdot i) + (a_2 + b_2 \cdot i) = (a_1 + a_2) + (b_1 + b_2) \cdot i$$
$$(3 + 7 \cdot i) + (8 + 11 \cdot i) = \boxed{11 + 18 \cdot i}$$

5.2.4 Multiplication of Complex Numbers

Distributive property twice or using FOIL to multiply the two binomials, $z_1 = a_1 + b_1 \cdot i$ and $z_2 = a_2 + b_2 \cdot i$

$$\begin{aligned} z_1 \cdot z_2 &= (a_1 + b_1 \cdot i) \cdot (a_2 + b_2 \cdot i) \\ &= (a_1 a_2 - b_1 b_2) + i \cdot (a_1 b_2 + a_2 b_1) \end{aligned}$$

$$\begin{aligned} (1 - 3 \cdot i) \times (2 + 5 \cdot i) =& a(b + c) = ab + ac \\ =& 2(1 - 3 \cdot i) + 5 \cdot i(i - 3 \cdot i) \\ =& 2 - 6 \cdot i + 5 \cdot i - 15i^2 = 2 - 6 \cdot i + 5 \cdot i + 15 \\ =& \boxed{17 - i} \end{aligned}$$

This can also be done in **polar form**, for this to occur you first have to convert the values to polar form as shown bellow.

$$\begin{aligned} z &= a + b \cdot i = r \cdot \cos(\varphi) + i \cdot r \cdot \sin(\varphi) \\ &= r \cdot (\cos(\varphi) + i \cdot \sin(\varphi)) \end{aligned}$$

$$z_1 \cdot z_2 = r_1 r_2 \left[\underbrace{\cos(\varphi_1)\cos(\varphi_2) - \sin(\varphi_1)\sin(\varphi_2)}_{\cos(\varphi_1 + \varphi_2)} + i \cdot \underbrace{(\cos(\varphi_1)\sin(\varphi_2) + \sin(\varphi_1)\cos(\varphi_2))}_{\sin(\varphi_1 + \varphi_2)} \right]$$

When the polar equivalent is calculated the above equation to multiply the two complex numbers can be used. This is a difficult equation to read as such a simplified version of it is shown bellow...

$$z_1 = [r_1, \varphi_1], z_2 = [r_2, \varphi_2]$$
$$z_1 \cdot z_2 = [r_1, \varphi_1] \cdot [r_2, \varphi_2] = [r_1 \cdot r_2, \varphi_1 + \varphi_2]$$

6 Relations and Functions

6.1 Basics

Ordered Pairs also known as the **Cartesian product** or **Tuples**.

The cartesian product of two sets $A \times B$ is the set of all ordered pairs (a, b) where $a \in A$ and $b \in B$.

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\}$$

Similarly we define the product of $A_1 \times A_2 \times \ldots \times A_n$ of a finite number of sets $A_1, \ldots, A_n$ as the set of all n-tuples

$$A_1 \times \ldots \times A_n = \{(a_1, \ldots, a_n) \mid a_j \in A_j\}$$

6.2 Relations

6.2.1 Definition

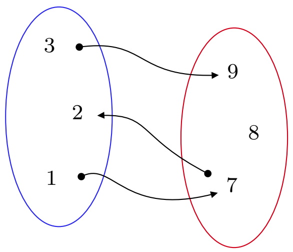
A **relation** is a subset of the Cartesian product of two sets. The sets are called the **domain** and **range** of the relation. The domain is the set of all possible first components of the ordered pairs in the relation. The range is the set of all possible second components of the ordered pairs in the relation.

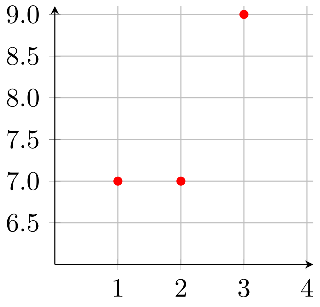
Example: The relation R on the set $\{1, 2, 3\}$ defined by $R = \{(1, 2), (2, 3), (3, 1)\}$ has domain $\{1, 2, 3\}$ and range $\{1, 2, 3\}$.

6.2.2 Visualising Relations

The definition above is crucial as understanding the connection between the domain and range (co-domain). The domain is the first component which is in relation to the range component.

As an example we consider $A = \{1, 2, 3\}$ and $B = \{7, 8, 9\}$ with $1R7, 3R9$ and $7R2$. Which information is missing in one of the plots?





Notes regarding previous figure: As you can see the relations mentioned afore, $1R7, 3R9$ and $7R2$. The first number eg. $1R7 \rightarrow 1$ is the domain and the second number is the rannge.

6.2.3 Visualising Binary Relations

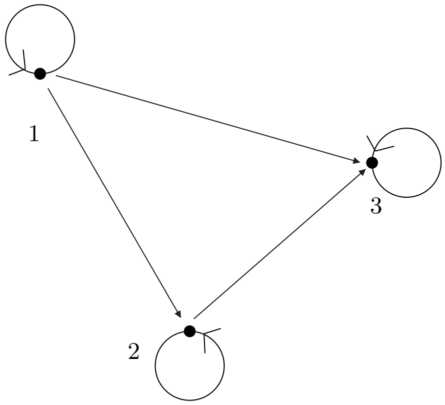
Binary Relations are visualised by using a matrix. The matrix is a table with the domain on the x-axis and the range(co-domain) on the y-axis. The matrix is filled with the elements of the relation. The elements of the relation are marked with a 1 and the elements not in the relation are marked with a 0.

$$M_R = \begin{bmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$A = \{1, 2, 3, 4\}, B = \{0, 2, 4, 6\} \text{ and } R = \{(a, b) \in A \times B \mid a < b\}$$

$$|A| = 4 \text{ and } |B| = 4 \text{ then } M_R = 4 \times 4$$

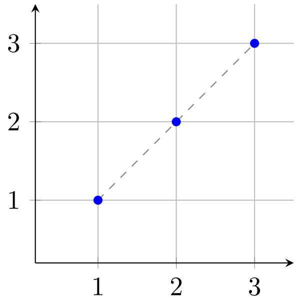
$$R = \{(1, 2), (1, 4), (1, 6), (2, 4), (2, 6), (3, 4), (3, 6), (4, 6)\}$$

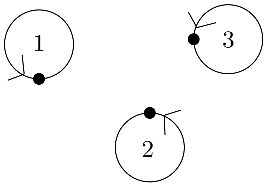


The example depicts the binary relation $1R1, 2R2, 3R3, 1R2, 1R3$ and $2R3$ for $A = \{1, 2, 3\}$. It contains loops or self-loops (which is an edge connecting a vertex with itself)

6.2.4 Properties of Binary Relations

Reflexive Property A binary relation R on a set A is said to be reflexive if aRa for all $a \in A$. In other words, a relation is reflexive if it contains all the elements of the set A in the relation. For example, the relation $R = \{(1,1),(2,2),(3,3)\}$ is reflexive on the set $A = \{1,2,3\}$.

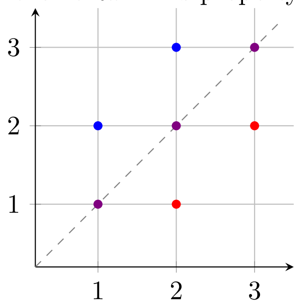


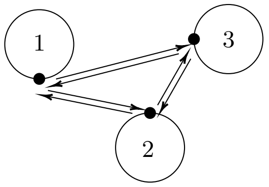


$$\forall a \in A: \quad (a,a) \in R \quad (\forall a \in A : aRa)$$

The cartesian plane diagram shows the reflexiv nature of set A through the diagonal relation R of the sets elements. The second diagram shows the reflexiv property as each vertex has a loop. This implies the relation set $R = \{(1,1),(2,2),(3,3)\}$.

Symmetric Property Symetric property is a relation property that states that if aRb then bRa. This property is denoted by $R \subseteq A \times A$ and $R \subseteq A \times A$.





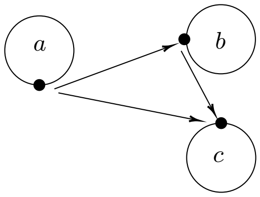
As seen in the diagrams along the cartesian plane, $y = x$ is the line of symetry. Everything is mirrored along this line. So, if you have a point (x,y), then its reflection is (y,x).

The second diagram shows the symetric property through connecting the nodes to eachother with arrows pointing towards eachother.

Transitive Property The transitive property states that if $a \sim b$ and $b \sim c$, then $a \sim c$. The graph bellow presents a connection between a, b and b, c. As such a connection is established between c and a.

$$\forall a, b, c \in A : aRb \wedge bRc \implies aRc$$

$$M_R = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$$



This becomes easier to understand through the use of divisibility.

$aRb \iff a$ divides $b\ldots$ then R is transitive, because $a \mid b$ and $b \mid c$ implies that $a \mid c$.

Equivilance Relations A relation is equivilant if it is reflexive, symmetric, and transitive.

For equivalence relations often one of the symbols $\sim$ or $\sim_R$ is used instead of $R : a \sim b$ or $a \sim_R b$