MATH381 Discrete Mathematics

Justin Sawon

Istituto Lorenzo de’ Medici
Florence, 6 July-3 August, 2023
Monday 10th July

- Chapter 1: Logic and Proofs
  - §1.1 Propositional logic
  - §1.3 Propositional equivalences
  - §1.4 Predicates and qualifiers
§1.1 Propositional logic

**Defn:** A proposition is a declarative statement that is either true or false, but not both. Its truth value is T or F, accordingly.

**Defn:** The negation of a proposition p, denoted \( \neg p \), is the statement “it is not the case that p”.
§1.1 Propositional logic - connectives

**Defn:** The conjunction of two propositions \( p \) and \( q \), denoted \( p \land q \), is the proposition “\( p \) and \( q \)”. It is true when \( p \) and \( q \) are both true, false otherwise.

**Defn:** The disjunction of two propositions \( p \) and \( q \), denoted \( p \lor q \), is the proposition “\( p \) or \( q \)”. It is true when \( p \), or \( q \), or both are true, false if both \( p \) and \( q \) are false.
§1.1 Propositional logic

Defn: Let p and q be propositions. The conditional statement $p \rightarrow q$ is the proposition “if p then q”. It is false when p is true and q is false, and true otherwise. We call p the hypothesis and q the conclusion.

Note: We can write $p \rightarrow q$ in many different ways:

“if p then q”  “p implies q”  “p only if q”  “q if p”
“q whenever p”  “q follows from p”  “q unless $\neg p$”
§1.1 Propositional logic

**Defn:** The converse of $p \rightarrow q$ is $q \rightarrow p$. The contrapositive of $p \rightarrow q$ is $\neg q \rightarrow \neg p$. The inverse of $p \rightarrow q$ is $\neg p \rightarrow \neg q$.

**Note:** The contrapositive has the same truth values as (i.e., is equivalent to) the conditional itself.

1. $\neg q \rightarrow \neg p$ is only false if $\neg q$ is $T$ and $\neg p$ is $F$, i.e., if $q$ is $F$ and $p$ is $T$,

2. $p \rightarrow q$ is only false if $p$ is $T$ and $q$ is $F$.

Similarly, the converse has the same truth values as the inverse.
§1.1 Propositional logic

**Defn:** The biconditional statement \( p \iff q \) is the proposition “\( p \) if and only if \( q \)”. It is true when \( p \) and \( q \) are both true or both false, and false otherwise. (Write “\( p \) iff \( q \)”.)

Compound propositions: We can build compound propositions, for example

\[ (q \rightarrow p) \lor ((q \leftrightarrow r) \land \neg p) \]

Order of precedence: We apply \( \neg \) first, then \( \land, \lor, \rightarrow, \leftrightarrow \). (The main thing to remember is that \( \neg \) comes first.)
§1.3 Propositional equivalences

**Defn:** A compound proposition that is always true is called a tautology.

A compound proposition that is always false is called a contradiction.

A compound proposition that is sometimes true and sometimes false is called a contingency.

**Defn:** p and q are logically equivalent, denoted $p \equiv q$, if $p \leftrightarrow q$ is a tautology, i.e., if p and q have the same truth tables.

**Example:** De Morgan’s Laws

$$\neg(p \land q) \equiv \neg p \lor \neg q$$

$$\neg(p \lor q) \equiv \neg p \land \neg q$$
§1.3 Propositional equivalences

Table 6: 19 logical equivalences
Table 7: 9 logical equivalences involving $\rightarrow$
Table 8: 4 logical equivalences involving $\leftrightarrow$
§1.4 Predicates and quantifiers

**Defn:** A predicate $P(x)$ is a statement whose truth value depends on a variable $x$.

When we assign a value to $x$ the predicate becomes a proposition, and thus is either true or false.

Predicates can involve several variables.
Defn: The universal quantification of $P(x)$ is the statement

“$P(x)$ for all $x$ in the domain”.

We write “$\forall x \ P(x)$”.

The domain is important! Sometimes we include it by writing

“$\forall x \ in \ \mathbb{R} \ x^2 \geq 0$”.

(Here $\mathbb{R}$ denotes the real numbers.)
§1.4 Predicates and quantifiers

**Defn:** The existential quantification of \( P(x) \) is the statement

“there exists \( x \) such that \( P(x) \)”.

We write “\( \exists x \ P(x) \)”.

Again, the domain is important!

Even if the domain is given, we can always restrict it further by using the following notation

“\( \exists x > 0 \ (x^2 + 4x + 3 = 0) \)”,

or

“\( \forall x \ \text{in} \ \mathbb{Z} \ x(x + 1) \text{ is even} \)”.

(Here \( \mathbb{Z} \) denotes the integers.)
Bound and free variables:

**Example:** In “∀x (sin x ≥ y)” the variable x is bound and the variable y is free.

We cannot assign a truth value because we don’t know what y is. If we assign a value to y then it becomes true or false.

We do not assign a value to x because it is already “quantified”.
Negating quantified expressions:

**Example:** What is the negation of “everybody had a good time”? It is NOT “nobody had a good time”. Rather, “it is not the case that everybody had a good time”, or equivalently “somebody didn’t have a good time”.

Thus \( \neg (\forall x \ P(x)) \equiv \exists x \ (\neg P(x)) \).

Similarly \( \neg (\exists x \ Q(x)) \equiv \forall x \ (\neg Q(x)) \).

These are De Morgan’s Laws for Quantifiers.
De Morgan’s Laws for Quantifiers:

Suppose the domain is \( \{1, 2\} \).

Then \( \exists x \, P(x) \equiv P(1) \lor P(2) \).
And \( \forall x \, P(x) \equiv P(1) \land P(2) \).

Let’s look at \( \neg (\exists x \, P(x)) \equiv \forall x \, (\neg P(x)) \).

It becomes \( \neg (P(1) \lor P(2)) \equiv \neg P(1) \land \neg P(2) \).

This is just De Morgan’s Law!
Tuesday 11th July

- Chapter 1: Logic and Proofs
  - §1.5 Nested quantifiers
  - §1.6 Rules of inference
§1.5 Nested quantifiers

**Example:** Let the domain be the integers $\mathbb{Z}$. We can combine quantifiers

$$\forall x \ \forall y \ ((x \text{ is even}) \land (y \text{ is odd}) \rightarrow xy \text{ is even})$$

i.e., for every pair of integers $x$ and $y$, if $x$ is even and $y$ is odd then $xy$ is even.

We can change the ordering of $x$ and $y$:

$$\forall x \ \forall y \ P(x,y) \equiv \forall y \ \forall x \ P(x,y)$$
$$\exists x \ \exists y \ P(x,y) \equiv \exists y \ \exists x \ P(x,y)$$

However, order does matter for $\forall x \ \exists y$ and $\exists y \ \forall x$. 
§1.5 Nested quantifiers

**Exercise:** Write “No negative real number has a square root” using quantifiers.

**Exercise:** Write “Every positive real number has two distinct square roots” using quantifiers.

**Exercise:** Write “You can fool some of the people all of the time, and all of the people some of the time, but you can’t fool all of the people all of the time” using quantifiers.
§1.6 Rules of inference

Example: An argument

“If we order more pizza then we will have too much.” premise
“We order more pizza.” premise
Therefore
“We have too much pizza.” conclusion

An argument is valid if:

the premises are true implies the conclusion must be true.
§1.6 Rules of inference

Let $p$ = “we order more pizza” and $q$ = “we have too much pizza”. The argument form is

\[
p \rightarrow q
\]

\[
\begin{array}{c}
p \\
\hline
\therefore q
\end{array}
\]

An argument form is valid if:

the premises are true implies the conclusion must be true.

**Note:** This does not always mean that all the propositional variables must be true. For instance, $p \rightarrow q$ will be true if $q$ is true or $p$ is false.

The above argument form is valid because

\[
(((p \rightarrow q) \land p) \rightarrow q \text{ is a tautology.}
\]
§1.6 Rules of inference

Compare to

“If we order more pizza then we will have too much.”
“We have too much pizza.”
Therefore
“We ordered more pizza.”

This is not a valid argument (form). We call it a fallacy.
Another common argument form is

\[
p \rightarrow q \\
q \rightarrow r \\
\therefore p \rightarrow r
\]

We can use a truth table to verify that this argument form is valid.
§1.6 Rules of inference

We can also build arguments using rules of inference

1. Modus ponens  \( p \)
\[ p \rightarrow q \]
\[ \therefore q \]

5. Addition  \( p \)
\[ \therefore p \lor q \]

2. Modus tollens  \( \neg q \)
\[ p \rightarrow q \]
\[ \therefore \neg p \]

6. Simplification  \( p \land q \)
\[ \therefore p \]

3. Hypothetical syllogism  \( p \rightarrow q \)
\[ q \rightarrow r \]
\[ \therefore p \rightarrow r \]

7. Conjunction  \( p \)
\[ \therefore p \land q \]

4. Disjunctive syllogism  \( p \lor q \)
\[ \neg p \]
\[ \therefore q \]

8. Resolution  \( p \lor q \)
\[ \neg p \lor r \]
\[ \therefore q \lor r \]
§1.6 Rules of inference

Each rule of inference has an associated tautology.

**Example:** Resolution

\[ ((p \lor q) \land (\neg p \lor r)) \to (q \lor r) \]

We can use rules of inference to check whether an argument form is valid.

**Example:**

“It is not raining or Cosimo has his umbrella.”
“Cosimo does not have his umbrella or he does not get wet.”
“It is raining or Cosimo does not get wet.”
Therefore
“Cosimo does not get wet.”
§1.6 Rules of inference

Rules of inference for quantified statements

1. Universal instantiation  \( \forall x \, P(x) \)
   \[ \therefore P(c) \quad \text{for some } c \text{ in the domain} \]

2. Universal generalization  \( P(c) \)
   \[ \therefore \forall x \, P(x) \quad \text{for an arbitrary } c \]

3. Existential instantiation  \( \exists x \, P(x) \)
   \[ \therefore P(c) \quad \text{for some } c \]

4. Existential generalization  \( P(c) \)
   \[ \therefore \exists x \, P(x) \quad \text{for some } c \]
Wednesday 12th July

- Chapter 1: Logic and Proofs
  - §1.7 Introduction to proofs
  - §1.8 Proof methods and strategies
§1.7 Introduction to proofs

**Defn:** A theorem is a statement that can be shown to be true. A proof is an argument showing that a theorem is true. A proposition is a minor theorem. A lemma is a very minor theorem, often a step in a bigger theorem. A corollary is a theorem that follows easily from another theorem. A conjecture is a statement we think is true, but we don’t know how to prove it yet.
§1.7 Introduction to proofs

How to prove a theorem:

Often a theorem is of the form $p \rightarrow q$, or $\forall x \ (P(x) \rightarrow Q(x))$.

We can use a direct proof. We assume $p$ (or $P(x)$) is true and try to show directly that $q$ (or $Q(x)$) is true.

Example: Theorem: The sum of two odd integers is even.
Another way is to **prove the contrapositive**.

\[ p \rightarrow q \equiv \neg q \rightarrow \neg p \]

**Example:** Theorem: If \( x \) is irrational then \( 1/x \) is irrational.
Similar is proof by contradiction.

Suppose we want to prove that statement $p$ is true. Instead, we start by assuming $p$ is false, i.e., $\neg p$ is true. Then we try to show that this leads to a contradiction. Thus we show $\neg p \rightarrow F$ is true. This means that $\neg p$ cannot be true, so $p$ must be true.

In some sense, we are using modus tollens with $q = F$

$$
\neg q = T
\frac{\neg p \rightarrow q = \neg p \rightarrow F}{\therefore p}
$$

Example: Proposition: At least two people in this room were born on the same day of the week.
§ 1.7 Introduction to proofs

To show two statements $p$ and $q$ are equivalent we need to show $p \Rightarrow q$ and $q \Rightarrow p$.

To show that more than two statements, e.g., $p_1, p_2, p_3, p_4,$ and $p_5$, are equivalent we usually show $p_1 \Rightarrow p_2, p_2 \Rightarrow p_3, p_3 \Rightarrow p_4, p_4 \Rightarrow p_5$, and $p_5 \Rightarrow p_1$.

**Example:** Theorem: The following are equivalent:

1. $n$ is even,
2. $n + 5$ is odd,
3. $3n + 2$ is even.
§1.8 Proof methods and strategies

**Exhaustive proof:** Sometimes we only need to check finitely many things.

**Example:** Theorem: No cube less than 200 is the sum of two positive cubes.
§1.8 Proof methods and strategies

**Proof by cases:** Break the proof into several cases.

**Example:** Theorem: \( \max(x,y)+\min(x,y)=x+y \) for all real \( x \) and \( y \).

**Note:** Here we could also use “without loss of generality” (WLOG) to avoid repeating similar cases.

**Example:** Theorem: \( |x| + |y| \geq |x + y| \) for all real \( x \) and \( y \).
Exercise: What is wrong with the following?

Theorem: The geometric mean $\sqrt{xy}$ of two positive numbers $x$ and $y$ lies strictly between the numbers.

Proof: WLOG $x < y$.
Therefore $\sqrt{x} < \sqrt{y}$ (remember that $x$ and $y$ are positive).
Therefore $\sqrt{x}\sqrt{x} < \sqrt{x}\sqrt{y}$ and $\sqrt{x}\sqrt{y} < \sqrt{y}\sqrt{y}$,
i.e., $x < \sqrt{xy}$ and $\sqrt{xy} < y$.
So $x < \sqrt{xy} < y$, i.e., $\sqrt{xy}$ is strictly between $x$ and $y$. 
Existence proofs, constructive: Theorem: There exist 100 consecutive positive integers that are not perfect squares.

Existence proofs, non-constructive: Theorem: There exist infinitely many prime numbers.

(A prime number is a positive integer n whose only factors are 1 and n itself.
Primes: 2, 3, 5, 7, 11, 13, ...
Composites: 4, 6, 8, 9, 10, 12, 14, ...)
§1.8 Proof methods and strategies

Beware! Forward and backward reasoning.

When writing a proof we must start with statements that are true (premises or hypotheses of the theorem) and end with the conclusion of the theorem.

Do not start with the conclusion!

Do not end with a hypothesis or obvious tautology!
Thursday 13th July

- Chapter 2: Sets and Functions
  - §2.1 Sets
  - §2.2 Set operations
  - §2.3 Functions
Defn: A set is an unordered collection of objects. The objects in a set are called its elements.

We write \( a \in A \) to mean \( a \) is an element of the set \( A \).

We write \( a \notin A \) to mean \( a \) is not an element of the set \( A \).
§2.1 Sets

Examples:
1) Set of vowels $V = \{a, e, i, o, u\}$.
2) Set of all letters $A = \{a, b, c, \ldots, x, y, z\}$.
3) Natural numbers $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$.
4) Integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$.
5) Rational numbers $\mathbb{Q} = \left\{ \frac{p}{q} \mid p \in \mathbb{Z}, q \in \mathbb{Z}, q \neq 0 \right\}$.
6) Real numbers $\mathbb{R}$.
7) Positive real numbers $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$.
8) Non-negative real numbers $\mathbb{R}_{\geq 0} = \{x \in \mathbb{R} \mid x \geq 0\}$.
9) Close unit interval $[0, 1] = \{x \mid 0 \leq x \leq 1\}$.
10) Open unit interval $(0, 1) = \{x \mid 0 < x < 1\}$.
11) The empty set $\emptyset = \{\}$, i.e., no elements.
12) $\{\mathbb{R}_{<0}, \mathbb{R}_{>0}\}$ is a set with two elements, $\mathbb{R}_{<0}$ and $\mathbb{R}_{>0}$. It is not the same as the set $\{x \in \mathbb{R} \mid x \neq 0\}$.
§2.1 Sets

**Defn:** Two sets are equal if they have the same elements.

**Examples:**

\[
\{a, b, c\} = \{c, a, b\} \\
\{1, 1, 2, 2, 3, 3\} = \{1, 2, 3\} \\
\{n \in \mathbb{N} \mid n \leq 8 \text{ and } n \text{ is even}\} = \{0, 2, 4, 6, 8\}
\]

**Defn:** We say $A$ is a subset of $B$ if every element of $A$ is also an element of $B$. We write $A \subseteq B$.

We say $A$ is a proper subset of $B$ if $A \subseteq B$ and $A \neq B$.

**Examples:** $\mathbb{N} \subseteq \mathbb{Z}$, $\mathbb{Z} \subseteq \mathbb{R}$, $(0, 1) \subseteq [0, 1]$. 
§2.1 Sets - cardinality

Defn: If a set $A$ has exactly $n$ distinct elements then we say $A$ is a finite set and we write $|A| = n$. Otherwise we say the set is infinite.

Examples: $|\{a, b, c\}| = 3$, $\mathbb{Z}$ is infinite.

Defn: Let $A$ and $B$ be sets. The Cartesian product $A \times B$ is the set of all ordered pairs $(a, b)$ where $a \in A$ and $b \in B$.

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

Example: $A = \{Aydan, Ben, Cynthia, Dino\}$, $B = \{1, 2, 3\}$.

$$A \times B = \{(Aydan, 1), (Aydan, 2), (Aydan, 3), (Ben, 1), \ldots\}$$
§2.2 Set operations

**Defn:** The union $A \cup B$ of two sets is the set containing all elements that are either in $A$ or in $B$ or in both.

$$A \cup B = \{x \mid x \in A \lor x \in B\}$$

**Defn:** The intersection $A \cap B$ of two sets is the set containing all elements that are in $A$ and in $B$.

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

**Defn:** If $A \cap B = \emptyset$ we say $A$ and $B$ are disjoint.
§2.2 Set operations

**Question:** How many elements are in $A \cup B$? (Assume it is finite.)

**Answer:**

$$|A \cup B| = |A| + |B| - |A \cap B|$$

**Defn:** The difference $A - B$ is the set containing all elements of $A$ that are not also in $B$.

$$A - B = \{x \mid x \in A \land x \notin B\}$$

**Defn:** Once a universal set $U$ has been defined, we can define the complement $\overline{A}$ of a set $A$ to be $U - A$.

$$\overline{A} = \{x \mid x \notin A\}$$
§2.2 Set operations

Table 1 - 19 set identities

Example: De Morgan’s Laws

\[ \overline{A \cup B} = \overline{A} \cap \overline{B} \quad \overline{A \cap B} = \overline{A} \cup \overline{B} \]

Four ways to prove set identities:

1. Direct argument, each set contains the other.
2. Set-builder notation.
3. Venn diagrams.
4. Membership tables.
§2.3 Functions

**Defn:** A function from a set $A$ to a set $B$ is an assignment of exactly one element of $B$ to each element of $A$. We write $f(a) = b$ for “$b \in B$ is assigned to $a \in A$” and we write $f : A \rightarrow B$.

We call $A$ the domain of $f$ and $B$ the codomain of $f$.

If $f(a) = b$ we say $b$ is the image of $a$ and $a$ is a preimage of $b$.

The range of $f$ is the set of all images,

\[ \text{i.e., range of } f = \{ b \in B \mid \exists a \in A \ f(a) = b \}. \]
§2.3 Functions

Examples:
1) $A = \mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ and $B = \mathbb{R}$, $f((x, y)) = \max\{x, y\}$.

2) $A = \mathbb{Z}_{>0}$ and $B = \mathbb{N}$, $f(n) = \#$ of distinct digits appearing in $n$.

3) $A = \mathbb{R}$ and $B = \mathbb{R}$, $f(x) = \pm \sqrt{x^2 + 1}$, NOT a function.
Defn: A function $f$ is one-to-one (or injective) if

$$f(a_1) = f(a_2) \text{ implies } a_1 = a_2 \text{ for all } a_1, a_2 \in A.$$ 

Examples:
1) $f : \mathbb{R} \rightarrow \mathbb{R},\ f(x) = x^3$ is one-to-one.
2) $f : \mathbb{R} \rightarrow \mathbb{R},\ f(x) = \sin x$ is NOT one-to-one.
§2.3 Functions

**Defn:** A function \( f : \mathbb{R} \rightarrow \mathbb{R} \) is
increasing if \( f(x) \leq f(y) \) whenever \( x < y \),
strictly increasing if \( f(x) < f(y) \) whenever \( x < y \),
decreasing if \( f(x) \geq f(y) \) whenever \( x < y \),
strictly decreasing if \( f(x) > f(y) \) whenever \( x < y \).

**Note:** The domain could also be a subset of \( \mathbb{R} \).

**Examples:**
1) \( f : \mathbb{R} \rightarrow \mathbb{R}, \ f(x) = x^3 \) is strictly increasing.

**Proposition:** If \( f \) is strictly increasing then \( f \) is one-to-one.
If \( f \) is strictly decreasing then \( f \) is one-to-one.
Defn: A function $f : A \rightarrow B$ is onto (or surjective) if its range and its codomain $B$ are equal.

In other words, for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$,

i.e., $\forall b \in B \ \exists a \in A \ f(a) = b$.

Examples:

1) $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \ f(m, n) = m - n$ is onto.

2) $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}, \ f(m, n) = m^2 + n^2$ is NOT onto.
§2.3 Functions

Defn: A function \( f \) is a one-to-one correspondence (or a bijection) if it is both one-to-one and onto.

Examples: Which of the following are bijections?

1) \( A = \{1, 2, 3\}, B = \{a, b, c\}, f(1) = b, f(2) = c, f(3) = a. \)

2) \( f : \mathbb{Z} \to \mathbb{Z}, f(n) = n + 1. \)

3) \( f : \mathbb{R} \to \mathbb{R}_{>0}, f(x) = e^x. \)

4) \( f : (\frac{-\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}, f(x) = \tan x. \)

5) \( f : [0, 1] \to [0, 1], f(x) = \sin (\frac{\pi}{2} x). \)

6) \( \mathbb{Z} \text{(mod 5)} = \text{“integers modulo 5”} = \{0, 1, 2, 3, 4\}. \)
\( f : \mathbb{Z} \text{(mod 5)} \to \mathbb{Z} \text{(mod 5)}, f(x) = 2x \text{ (mod 5)}. \)
§2.3 Functions

Defn: A function $f$ is a one-to-one correspondence (or a bijection) if it is both one-to-one and onto.

Examples:
1) $A = \{1, 2, 3\}, B = \{a, b, c\}$, $f(1) = b$, $f(2) = c$, $f(3) = a$ is a bijection.

2) $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n + 1$ is a bijection.

3) $f : \mathbb{R} \to \mathbb{R}_{>0}$, $f(x) = e^x$ is a bijection.

4) $f : (\frac{-\pi}{2}, \frac{\pi}{2}) \to \mathbb{R}$, $f(x) = \tan x$ is a bijection.

5) $f : [0, 1] \to [0, 1]$, $f(x) = \sin \left( \frac{\pi}{2} x \right)$ is a bijection.

6) $\mathbb{Z} \pmod{5} = \text{"integers modulo 5"} = \{0, 1, 2, 3, 4\}$. $f : \mathbb{Z} \pmod{5} \to \mathbb{Z} \pmod{5}$, $f(x) = 2x \pmod{5}$ is a bijection.
§2.3 Functions

**Defn:** Let \( f : A \to B \) be a one-to-one correspondence. For each \( b \in B \) there is a unique \( a \in A \) such that \( f(a) = b \). We define the inverse function \( f^{-1} \) of \( f \) by

\[
f^{-1} : B \to A, \quad b \mapsto a.
\]

Thus \( f^{-1}(b) = a \) if and only if \( f(a) = b \).

**Defn:** Given \( g : A \to B \) and \( f : B \to C \), the composition of \( f \) and \( g \) is

\[
f \circ g : A \to C, \quad a \mapsto f(g(a)).
\]

**Proposition:** The inverse of \( f \circ g \) (if it is invertible) is \( g^{-1} \circ f^{-1} \).
Defn: The floor function assigns to a real number $x$ the largest integer less than or equal to $x$. Denote it by $\lfloor x \rfloor$. The ceiling function assigns to a real number $x$ the smallest integer greater than or equal to $x$. Denote it by $\lceil x \rceil$.

Proposition: $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$. 
Tuesday 18th July

- Chapter 4: Number theory
  - §4.1 Divisibility and modular arithmetic
§4.1 Divisibility and modular arithmetic

**Defn:** Let $a$ and $b$ be integers with $a \neq 0$. We say $a$ divides $b$, $a \mid b$, if there is an integer $c$ such that $b = ac$. We say $a$ is a factor of $b$ and $b$ is a multiple of $a$.

“$a$ does not divide $b$” is written $a \nmid b$.

**Theorem:** Let $a$, $b$, and $c$ be integers, $a \neq 0$.

1. If $a \mid b$ and $a \mid c$ then $a \mid (b + c)$.
2. If $a \mid b$ then $a \mid bc$.
3. If $a \mid b$ and $b \mid c$ (and $b \neq 0$) then $a \mid c$.
4. If $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$ for all integers $m$ and $n$. 
§4.1 Divisibility and modular arithmetic

**Theorem**: Let \( a \) and \( d \) be integers, \( d > 0 \). There are unique integers \( q \) and \( r \), \( 0 \leq r < d \), such that

\[
a = dq + r.
\]

**Remark**: \( \frac{a}{d} = \frac{dq+r}{d} = q + \frac{r}{d} \) where \( 0 \leq \frac{r}{d} < 1 \). Thus

\[
q = \left\lfloor \frac{a}{d} \right\rfloor \quad \text{and} \quad r = a - dq.
\]

**Defn**: \( q \) is called the quotient and \( r \) the remainder.
§4.1 Divisibility and modular arithmetic

Defn: Let \( a, b, \) and \( m \) be integers with \( m > 0 \). We say \( a \) is congruent to \( b \) modulo \( m \), written \( a \equiv b \pmod{m} \), if \( m \) divides \( a - b \).

Remark: By the division algorithm applied to \( a/m \), each integer is congruent to its remainder, \( a \equiv r \pmod{m} \), with \( 0 \leq r < m \). These are the \( m \) congruence classes: 0, 1, 2, \ldots, \( m - 1 \pmod{m} \).

Theorem: \( a \equiv b \pmod{m} \) if and only if there exists an integer \( k \) such that \( a = b + km \).
4.1 Divisibility and modular arithmetic

**Theorem:** If \( a \equiv b \pmod{m} \) and \( c \equiv d \pmod{m} \) then:

1. \( a + c \equiv b + d \pmod{m} \),
2. \( a - c \equiv b - d \pmod{m} \),
3. \( ac \equiv bd \pmod{m} \),
4. \( a^2 \equiv b^2 \pmod{m} \).

**Warning:** \( ac \equiv bc \pmod{m} \) does not imply that \( a \equiv b \pmod{m} \).

**Example:** a is even iff \( a^2 \) is even.
a is odd iff \( a^2 \) is odd.

In fact, a is even implies \( a^2 \equiv 0 \pmod{4} \).
And a is odd implies \( a^2 \equiv 1 \pmod{4} \).
Indeed, a is odd implies \( a^2 \equiv 1 \pmod{8} \).
Wednesday 19th July

• Chapter 4: Number theory
  • §4.2 Integer representations and algorithms
  • §4.3 Primes and greatest common divisors
Theorem: Every positive integer $n$ can be expressed uniquely in the form

$$n = a_k 2^k + a_{k-1} 2^{k-1} + \ldots + a_1 2 + a_0,$$

where $k \geq 0$ is an integer, $a_k = 1$, and every other $a_i$ is 0 or 1.

We call $n = a_k a_{k-1} \ldots a_1 a_0$ the binary representation of $n$.

Example: Convert $234_{10}$ to binary.

$$234_{10} = 11101010_2$$

Convert $11010_2$ to decimal.

$$11010_2 = 26_{10}$$
Addition base 2:
Adding $26_{10} = 11010_2$ to $39_{10} = 100111_2$ we get $1000001_2 = 65_{10}$.

Multiplication base 2:
Multiplying $26_{10} = 11010_2$ by $9_{10} = 1001_2$ we get $11101010_2 = 234_{10}$.

Calculating powers in modular arithmetic:
We can calculate $2^{11} \equiv 8 \pmod{15}$.
We can calculate $3^{234} \equiv 81 \pmod{99}$. 
§4.3 Primes and greatest common divisors

**Defn:** An integer \( p > 1 \) is called prime if the only positive factors of \( p \) are 1 and \( p \) itself.
If \( n > 1 \) is not prime then it is called composite.
So \( n \) is composite iff there exists a such that \( 1 < a < n \) and \( a|n \).

**Example:** 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, \ldots are primes.
All even integers greater than 2 are composite.
9 = 3 \times 3, 15 = 3 \times 5, 21 = 3 \times 7, 25 = 5 \times 5, 27 = 3 \times 3 \times 3, \ldots are composite.

**The Fundamental Theorem of Arithmetic:** Every integer \( > 1 \) is either a prime or it can be expressed uniquely as a product of at least two primes, written in order of non-decreasing size.
§4.3 Primes and greatest common divisors

**Theorem:** If \( n \) is composite than \( n \) has a prime divisor \( \leq \sqrt{n} \).

**Example:** To check whether \( n = 151 \) is prime we just need to check whether it has a prime divisor less than \( \sqrt{151} \approx 12.3 \).

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

**Example:** Primes of the form \( 2^p - 1 \) where \( p \) is also a prime are known as Mersenne primes.

**Warning:** Not all numbers of this form, \( 2^p - 1 \), are primes!

**The Prime Number Theorem:** The number of primes less than \( x \) is approximately \( \frac{x}{\ln x} \), i.e.,

\[
\lim_{x \to \infty} \frac{\# \text{ primes} < x}{x/\ln x} = 1.
\]
Goldbach’s Conjecture: Every integer $> 2$ is the sum of two primes.

The Twin Prime Conjecture: There are infinitely many “twin primes”, i.e., primes which differ by 2.
§4.3 Primes and greatest common divisors

**Defn:** The greatest common divisor of two positive integers $a$ and $b$ is the largest integer $d$ such that $d | a$ and $d | b$, written $gcd(a, b)$.

**Defn:** If $gcd(a, b) = 1$ then we say that $a$ and $b$ are relatively prime (or coprime).

**Theorem:** If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ then

$$gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$
**Defn:** The least common multiple of two positive integers $a$ and $b$ is the smallest integer $m$ such that $a|m$ and $b|m$, written $lcm(a, b)$.

**Theorem:** If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$ then

$$gcd(a, b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$ 

**Theorem:** $a \times b = gcd(a, b) \times lcm(a, b)$. 
§4.3 Primes and greatest common divisors

The Euclidean algorithm: This is a quicker way to find gcds.

Lemma: Suppose we divide $a$ by $b$ to get $a = bq + r$ with $0 \leq r < b$. Then $gcd(a, b) = gcd(b, r)$.

To find $gcd(a, b)$ we successively apply the division algorithm

\[
\begin{align*}
a &= bq_1 + r_2 \\
b &= r_2q_2 + r_3 \\
r_2 &= r_3q_3 + r_4 \\
&\quad \vdots \\
r_{n-1} &= r_nq_n + 0.
\end{align*}
\]

Note: $b > r_2 > r_3 > \ldots > r_n$. Eventually we get a remainder of 0.

Then $gcd(a, b) = gcd(b, r_2) = gcd(r_2, r_3) = \ldots = gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$, i.e., $gcd(a, b)$ is the last non-zero remainder $r_n$. 

4.3 Primes and greatest common divisors

**Bezout’s Theorem:** There exist integers s and t (not necessarily positive) such that \( \gcd(a, b) = sa + tb \).

To find s and t we use the “reverse Euclidean algorithm”.

**Corollary:** If a and b are relatively prime then there exist integers s and t such that \( \gcd(a, b) = 1 = sa + tb \).
§4.3 Primes and greatest common divisors

Multiplicative Inverses in Modular Arithmetic:

“\( \frac{1}{3} \equiv 9 \pmod{26} \)”, i.e., \( 3 \times 9 \equiv 27 \equiv 1 \pmod{26} \).

However, “\( \frac{1}{2} \pmod{26} \)” does not exist, as \( 2 \times n \) is not congruent to 1 \( \pmod{26} \) for any integer \( n \).

**Lemma**: If \( a \) and \( m \) are relatively prime then \( a \) has a multiplicative inverse modulo \( m \), i.e., \( \exists \ s \) such that \( as \equiv 1 \pmod{m} \), or “\( \frac{1}{a} \equiv s \pmod{m} \)”.

**Example**: Use the reverse Euclidean algorithm, find “\( \frac{1}{7} \pmod{26} \)”.

Solve \( 7x \equiv 2 \pmod{26} \).
Thursday 20th July

- Chapter 5: Induction
  - §5.1 Mathematical induction
  - §5.2 Strong induction
§5.1 Mathematical induction

To prove $P(n)$ for all positive integers $n$ it suffices to prove:

- **Basis step:** Verify that $P(1)$ is true,
- **Inductive step:** Show $P(k) \rightarrow P(k + 1)$ is true for all $k \geq 1$.

Then $\forall n \geq 1 P(n)$ will follow.

**Remark:** To show $P(k) \rightarrow P(k + 1)$ using a direct proof we assume that $P(k)$ is true and use it to deduce that $P(k + 1)$ is true. Here $P(k)$ is called the inductive hypothesis.

**Note:** This does not mean that we are assuming what we are trying to prove. The inductive step is just showing that $P(k) \rightarrow P(k + 1)$ is true.

To show $p \rightarrow q$ is true we assume $p$ and show that $q$ follows; but at the end, we cannot conclude that $p$ is true or false.
§5.1 Mathematical induction

Summation formulae

1) Show that $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$ for all $n \geq 1$.

2) Show that $1 + 3 + 5 + \ldots + (2n - 1) = n^2$ for all $n \geq 1$.

3) Show that $1^2 + 2^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ for all $n \geq 1$.

4) Show that $1^2 - 2^2 + 3^2 - \ldots + (-1)^{n-1}n^2 = (-1)^{n-1}\frac{n(n+1)}{2}$ for all $n \geq 1$.

5) Show that $a + ar + ar^2 + \ldots + ar^n = \frac{ar^{n+1}-a}{r-1}$ for all $n \geq 0$ (where $a$ and $r$ are fixed real numbers with $r \neq 1$).
5.1 Mathematical induction

Inequalities

1) Show that \(1 + \frac{1}{4} + \frac{1}{9} + \ldots + \frac{1}{n^2} < 2 - \frac{1}{n}\) for all \(n \geq 2\).

2) Show that \(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{2^n} \geq 1 + \frac{n}{2}\) for all \(n \geq 0\).

[This implies \(1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{m} \geq 1 + \frac{\log_2 m}{2}\) for all \(m \geq 1\).]

3) Show that \(n^2 < 2^n\) for all \(n \geq 5\).

Divisibility results

1) Show that \(3 \mid n^3 - n\) for all \(n \geq 0\).
§5.1 Mathematical induction

Template for an inductive proof:

Let $P(n)$ be . . .

**Basis step:** $P(1)$ says . . .
*Verify that it is true!*

**Inductive step:** Assume $P(k)$ is true for some $k \geq 1$. *Use $P(k)$ to deduce $P(k + 1)$.*

Thus $P(k) \rightarrow P(k + 1)$ for all $k \geq 1$.

Therefore $P(n)$ for all $n \geq 1$ by mathematical induction.
§5.2 Strong induction

Induction:
- **Basis step**: $P(1)$ is true,
- **Inductive step**: $P(k) \rightarrow P(k + 1)$ is true for all $k \geq 1$.
Then $\forall n \geq 1 P(n)$ is true.

Strong induction:
- **Basis step**: $P(1)$ is true,
- **Inductive step**: $(P(1) \land P(2) \land \ldots \land P(k)) \rightarrow P(k + 1)$ is true for all $k \geq 1$.
Then $\forall n \geq 1 P(n)$ is true.
§5.2 Strong induction

**Fundamental Theorem of Arithmetic:** Every integer \( n > 1 \) is a prime or can be written as a product of primes.

Let \( P(n) \) : “\( n \) can be written as a product of primes” (possibly just one prime).

**Proof:**

**Basis step:** \( n = 2 \) is a prime, so \( P(2) \) is true.
§5.2 Strong induction

Inductive step: Assume \( P(j) \) is true for all \( j, \ 2 \leq j \leq k \), i.e., assume that 2, 3, 4, . . . , \( k \) can each be written as a product of primes. Now consider \( k + 1 \).

1. If \( k + 1 \) is prime then \( P(k + 1) \) is automatically true.

2. Otherwise we can factor \( k = ab \) with \( 1 < a, b < k + 1 \). By the inductive hypothesis \( P(a) \) and \( P(b) \) are true, i.e., we can write

\[
a = p_1 p_2 \cdots p_s \quad \text{and} \quad b = q_1 q_2 \cdots q_t.
\]

Then

\[
k + 1 = ab = p_1 p_2 \cdots p_s q_1 q_2 \cdots q_t
\]

can also be written as a product of primes, so \( P(k + 1) \) is true.

Thus \( (P(2) \land P(3) \land \ldots \land P(k)) \rightarrow P(k + 1) \) is true for all \( k \geq 2 \).

Thus \( P(n) \) is true for all \( n \geq 2 \) by strong induction. \( \square \)
§5.2 Strong induction

**Question:** What postage can we make from 3 and 5 cent stamps?

Let’s prove that we can make any postage greater than 7.

\[ P(n) : \text{“we can write } n \text{ as a sum of 3s and 5s”} \]

**Basis step:** \( P(8), P(9), P(10) \) are true.

**Inductive step:** Assume \( P(j) \) is true for \( 8 \leq j \leq k \), with \( k \geq 10 \). Let’s show that \( P(k + 1) \) is true. . .

i.e., \( (P(8) \land P(9) \land \ldots \land P(k)) \implies P(k + 1) \) for all \( k \geq 10 \).

Therefore \( P(n) \) is true for all \( n \geq 8 \) by strong induction.
Fibonacci numbers: 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, ... Defined by $f_1 = 1$, $f_2 = 1$, $f_{n+2} = f_{n+1} + f_n$ for $n \geq 1$.

**Proposition:** $P(n) : f_n \geq \left(\frac{3}{2}\right)^{n-2}$ for all $n \geq 1$.

**Proof:** Basis step: $P(1)$ and $P(2)$ are true.

Inductive step: Assume $P(j)$ is true for $1 \leq j \leq k$, with $k \geq 2$. Let’s show that $P(k+1)$ is true. ... i.e., $(P(1) \land P(2) \land \ldots \land P(k)) \rightarrow P(k+1)$ for all $k \geq 2$.

Therefore $P(n)$ is true for all $n \geq 1$ by strong induction. □
Monday 24th July

- Chapter 9: Relations
  - §9.1 Relations and their properties
  - §9.5 Equivalence relations
§9.1 Relations and their properties

**Defn:** Let $A$ and $B$ be sets. A relation from $A$ to $B$ is a subset $R$ of $A \times B$. We write $aRb$ to denote $(a, b) \in R \subseteq A \times B$.

**Example:** $A = \{\text{Alitalia, Delta, United}\}$

$B = \{\text{Florence, Milan, Rome}\}$

$R = \{(a, b) \mid \text{airline a flies to city b}\}$

$= \{\text{(Alitalia, Florence), (Alitalia, Milan), (Alitalia, Roma), (Delta, Rome), (United, Milan),...}\}$
§9.1 Relations and their properties

**Defn:** A relation on a set $A$ is a relation from $A$ to $A$.

**Example:** Let $A = B = \mathbb{Z}_{>0}$ = positive integers.

- $R_1 = \{(a, b) \mid a \neq b\}$
- $R_2 = \{(a, b) \mid a | b\}$
- $R_3 = \{(a, b) \mid a^2 = b\}$
- $R_4 = \{(a, b) \mid a = b^2\}$
- $R_5 = \{(a, b) \mid a \equiv b \pmod{5}\}$

**Defn:** A relation $R$ on $A$ is reflexive if $(a, a) \in R$ for every $a \in A$.

**Defn:** A relation $R$ on $A$ is symmetric if $(a, b) \in R$ iff $(b, a) \in R$, for $a, b \in A$.

**Defn:** A relation $R$ on $A$ is transitive if $(a, b) \in R$ and $(b, c) \in R$ implies $(a, c) \in R$, for $a, b, c \in R$. 
§9.5 Equivalence relations

**Defn:** A relation on set $A$ is called an equivalence relation if it is reflexive, symmetric, and transitive. In other words

1. $aRa$,
2. if $aRb$ then $bRa$,
3. if $aRb$ and $bRc$ then $aRc$.

Two elements that are related by an equivalence relation are called equivalent, written $a \sim b$.

**Example:** $A = \{1, 2, 3, 4\}$
$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$
Example: \( A = \{ f : \mathbb{Z} \to \mathbb{Z} \} \) = set of functions from \( \mathbb{Z} \) to \( \mathbb{Z} \)
\( R = \{ (f, g) \mid f(1) = g(1) \} \)
One can show that \( R \) is reflexive, symmetric, and transitive.

Non-example: \( A = \{ f : \mathbb{Z} \to \mathbb{Z} \} \) = set of functions from \( \mathbb{Z} \) to \( \mathbb{Z} \)
\( R = \{ (f, g) \mid f(1) = g(1) \) or \( f(2) = g(2) \} \)
One can show that \( R \) is reflexive and symmetric, but \textit{not} transitive.

Example - congruence modulo 5: \( A = \mathbb{Z} \)
\( R = \{ (a, b) \mid a \equiv b \mod 5 \} \)
\[
\ldots \equiv -13 \equiv -8 \equiv -3 \equiv 2 \equiv 7 \equiv 12 \equiv 17 \equiv \ldots \mod 5
\]
§9.5 Equivalence relations

**Defn:** Let $R$ be an equivalence relation on $A$. The set of elements equivalent to $a \in A$ is called the equivalence class of $a$, written $[a]$. If $b \in [a]$ (i.e., $b \sim a$) then $b$ is called a representative of the equivalence class $[a]$.

**Example:** For congruence modulo 5 the equivalence classes are all integers congruent to a given integer. For instance

$$[2] = \{ \ldots, -13, -8, -3, 2, 7, 12, 17, \ldots \},$$

$$[4] = \{ \ldots, -11, -6, -1, 4, 9, 14, 19, \ldots \}.$$  

**Theorem:** For $a, b \in A$, either

1. $[a] = [b],$

2. or $[a]$ and $[b]$ are disjoint subsets of $A$, $[a] \cap [b] = \emptyset$. 
Wednesday 26th July

- Chapter 6: Counting
  - §6.1 Basics of counting
§6.1 Basics of counting

The Product Rule: Suppose we have to choose from List A with \( n_1 \) options and List B with \( n_2 \) options. Then altogether there are \( n_1 n_2 \) combinations of choices.

Example: At Trattoria Zaza there are 5 choices for ‘primi’ and 3 choices for ‘secondi’. Altogether there are \( 5 \times 3 = 15 \) choices for a two-course meal.

Example: If there are also 4 choices for dessert then there would be \( 5 \times 3 \times 4 = 60 \) choices for a three-course meal.

Remark: The Product Rule says

\[
|A_1 \times A_2 \times \cdots \times A_k| = |A_1| \cdot |A_2| \cdots |A_k|.
\]
§6.1 Basics of counting

**Exercises:**

1) How many four letter, three number license plates are there (e.g., BOND007)?

2) If there are eight horses in a race, how many possibilities are there for the place-winners (1st/2nd/3rd place)?

3) In how many ways can we choose two finalists from 10 contestants?

4) How many functions \( f : A \to B \) are there if \(|A| = m\) and \(|B| = n\)?
### §6.1 Basics of counting

**The Sum Rule:** Suppose we have to choose from List A with \( n_1 \) options or List B with \( n_2 \) options (and List A and List B are disjoint). Then altogether there are \( n_1 + n_2 \) choices.

**Example:** At Trattoria Zaza there are 5 white wines and 7 red wines. Altogether there are \( 5 + 7 = 12 \) wines to choose from.

**Example:** In how many ways can we choose two different courses if there are 5 ‘primi’, 3 ‘secondi’, and 4 desserts?

**Remark:** The Sum Rule says that for disjoint \( A_i \) we have

\[
|A_1 \cup A_2 \cup \cdots \cup A_k| = |A_1| + |A_2| + \cdots + |A_k|.
\]


§6.1 Basics of counting

Exercises: 1) In how many ways can we choose two different courses if we have either tagliatelle al ragù for primi or bistecca alla fiorentina for secondi or both?

2) How many positive integers less than 1000 are not divisible by 3 or 5?

3) How many ‘words’ (strings of letters) are there of length $\leq 4$ if a ‘word’ must contain at least one vowel and at least one consonent?
Thursday 27th July

- Chapter 6: Counting
  - §6.3 Permutations and combinations
  - §6.4 Binomial coefficients
Example: In how many ways can we order 6 different books on a shelf? (Answer: 720 ways.)

Example: Suppose we have 6 books and we want to select 3 to place on a shelf in order; in how many ways can we do this?

Defn: A permutation is an ordered arrangement of distinct objects. An $r$-permutations is an ordered arrangement of $r$ distinct elements of a set. $P(n, r)$ is the number of $r$-permutations of a set with $n$ elements.

Theorem: $P(n, r) = n(n−1)(n−2)\cdots(n−r+1) = n!/(n−r)!$. In particular, the number of permutations of $n$ objects is $P(n, n) = n(n−1)\cdots2\cdot1 = n!$. 
§6.3 Permutations and combinations

**Exercises:**

1) How many possibilities are there for 1st/2nd/3rd in a race if there are 1000 entrants?

2) How many possibilities for 1st/2nd/last in the same race?

3) A group consists of $n$ women and $n$ men. In how many ways can they line up in a row if women and men must alternate?
Example: Given 7 books, in how many ways can we choose 3 of them to take on a trip? (Answer: 35 ways.)

Defn: An \( r \)-combination of a set of \( n \) elements is an unordered selection of \( r \) elements, i.e., it is just a subset with \( r \) elements. \( C(n, r) \) is the number of \( r \)-combinations of a set with \( n \) elements. \( C(n, r) \) is often written as \( \binom{n}{r} \), and we say “\( n \) choose \( r \)”.

Theorem: \( C(n, r) = \frac{P(n,r)}{P(r,r)} = \frac{n!}{r!(n-r)!} \).

Remark: \( C(n, n - r) = \frac{n!}{(n-r)!(n-(n-r))!} = \frac{n!}{(n-r)!r!} = C(n, r) \).
Exercises: 1) In how many ways can we choose five letters from the alphabet?

2) How many subsets with at least three elements does a set with 30 elements have?

Remark: In general

\[ C(n, 0) + C(n, 1) + C(n, 2) + \ldots + C(n, n) = 2^n. \]

3) In how many ways can eight women and five men stand in a row so that no two men are standing next to each other?
The Binomial Theorem: Let $x$ and $y$ be variables and $n$ a positive integer. Then $(x + y)^n$ is equal to

\[
\binom{n}{0} x^n + \binom{n}{1} x^{n-1}y + \binom{n}{2} x^{n-2}y^2 + \ldots + \binom{n}{n-1} xy^{n-1} + \binom{n}{n} y^n.
\]

Example: For $n = 4$,

\[
(x + y)^4 = \binom{4}{0} x^4 + \binom{4}{1} x^3y + \binom{4}{2} x^2y^2 + \binom{4}{3} xy^3 + \binom{4}{4} y^4
\]

\[
= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4.
\]
§6.4 Binomial coefficients

Corollary:

\[ 2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \ldots + \binom{n}{n-1} + \binom{n}{n} \]

Corollary:

\[ \binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \ldots = \binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \ldots \]

Exercises: 1) What is the coefficient of \(x^5\) in \((2x + 3)^9\)?

2) What is the coefficient of \(x^5\) in \((x^2 - \frac{2}{x})^7\)?

3) What is the coefficient of \(x^k\) in \((x^2 - \frac{2}{x})^{100}\)?
Theorem (Pascal’s Identity): Let \( n \) and \( k \) be positive integers with \( n \geq k \). Then

\[
{n + 1 \choose k} = {n \choose k - 1} + {n \choose k}.
\]

Pascal’s Triangle:
§6.4 Binomial coefficients

Pascal’s Triangle:
Pascal’s Triangle (mod 2):

(Compare to the Sierpiński gasket fractal.)
§6.4 Binomial coefficients

Theorem (Vandermonde’s Identity): Let $m$, $n$, and $r$ be non-negative integers with $r \leq m$ and $r \leq n$. Then

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

Example: $\binom{3+4}{2} = \binom{3}{2} \binom{4}{0} + \binom{3}{1} \binom{4}{1} + \binom{3}{0} \binom{4}{2}$

Corollary:

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

Theorem:

$$
\sum_{k=1}^{n} k \binom{n}{k} = n \cdot 2^{n-1}
$$

Example: $1\binom{4}{1} + 2\binom{4}{2} + 3\binom{4}{3} + 4\binom{4}{4} = 4 \cdot 2^3$
Monday 31st July

- Chapter 6: Counting
  - §6.5 Generalized permutations and combinatorics
§6.5 Generalized permutations and combinatorics

**Remember:** Permutations = ordered, combinations = unordered.

**Permutations with repetition**

**Qu:** How many 8 letter passwords using only letters? (Ans: $26^8$.)

**Combinations with repetition**

**Qu:** How many ways to buy 10 pizzas if the flavor options are Margherita, Napoletana, and Capricciosa?

We use the “stars-and-bars” approach:

```
  * * * * * * | * | * * *
           Margherita  Napoletana  Capricciosa
```

Answer = the number of ways to choose 10 stars (or 2 bars) from 12 symbols, i.e.,

$$\binom{12}{10} = \binom{12}{2} = 66.$$
§6.5 Generalized permutations and combinatorics

**Theorem:** The number of ways to choose $r$ objects from a set with $n$ elements, with repetition allowed, is

$$\binom{n+r-1}{r} = C(n+r-1, r) = C(n+r-1, n-1) = \binom{n+r-1}{n-1}.$$  

**Exercises:**

1) How many solutions are there in non-negative integers $x_1, x_2, x_3$ to the equation

$$x_1 + x_2 + x_3 = 10?$$

(Answer: 66.)

2) How many solutions are there in positive integers $x_1, x_2, x_3$ to the equation

$$x_1 + x_2 + x_3 = 10?$$

(Answer: 36.)
3) How many solutions are there to

\[ x_1 + x_2 + x_3 = 10? \]

if \( x_1 \geq 1, \ x_2 \geq 2, \) and \( x_3 \geq 3? \) (Answer: 15.)

4) How many solutions are there to

\[ x_1 + x_2 + x_3 = 10? \]

if \( x_i \geq 0 \) for all \( i \) and \( x_1 \leq 5? \) (Answer: 66 − 15 = 51.)

5) How many solutions are there to

\[ x_1 + x_2 + x_3 = 10? \]

if \( x_i \geq 0 \) for all \( i, \ x_1 \leq 5, \) and \( x_2 \leq 2? \) (Answer: 66 − 15 − 36 + 3 = 18.)
§6.5 Generalized permutations and combinatorics

**Summary:** Choosing $r$ objects from a set with $n$ elements.

<table>
<thead>
<tr>
<th></th>
<th>ordered?</th>
<th>repetition?</th>
<th>number of ways</th>
</tr>
</thead>
<tbody>
<tr>
<td>$r$-permutations</td>
<td>yes</td>
<td>no</td>
<td>$P(n, r) = \frac{n!}{(n-r)!}$</td>
</tr>
<tr>
<td>$r$-combinations</td>
<td>no</td>
<td>no</td>
<td>$C(n, r) = \binom{n}{r} = \frac{n!}{r!(n-r)!}$</td>
</tr>
<tr>
<td>$r$-permutations</td>
<td>yes</td>
<td>yes</td>
<td>$n^r$</td>
</tr>
<tr>
<td>$r$-combinations</td>
<td>no</td>
<td>yes</td>
<td>$\binom{n+r-1}{r} = \frac{(n+r-1)!}{r!(n-1)!}$</td>
</tr>
</tbody>
</table>