Concepts
of
Mathematics
21-127

CMU

November 8, 2022

1 Proof and Logic

1.1 Propositional logic

- **Assumptions** are the propositions which are known to be true, or which we are assuming to be true for the purposes of proving something. They include theorems that have already been proved, prior knowledge which is assumed of the reader, and assumptions which are explicitly made using words like ‘suppose’ or ‘assume’.
- **Goals** are the propositions we are trying to prove in order to complete the proof of a result, or perhaps just a step in the proof.

1.1.1 Symbolic logic

By breaking down a complex proposition into simpler statements which are connected together using logical operators and quantifiers, we can more precisely identify what assumptions we can make at any given stage in a proof of the proposition, and what steps are needed in order to finish the proof.

1.1.2 Propositional formulae

- A **propositional variable** is a symbol that represents a proposition. Propositional variables may be assigned truth values (‘true’ or ‘false’).

- A **propositional formula** is an expression that is either a propositional variable, or is built up from simpler propositional formulae ('subformulae') using a logical operator. In the latter case, the truth value of the propositional formula is determined by the truth values of the subformulae according to the rules of the logical operator.

1.1.3 Terminology

- A **theorem** is typically reserved for major results whose proof may require considerable effort.
- A **proposition** is typically not as significant as a theorem and usually takes less effort to prove.
- A **lemma** is a theorem whose main purpose is to help prove another theorem.
- A **corollary** is a result that is an immediate consequence of a theorem or proposition

1.2 Logical operator

1.2.1 Conjunction

The conjunction operator is the logical operator $\wedge$, defined according to the following rules:

- if p is true and q is true, then $p \wedge q$ is true
- if $p \wedge q$ is true, then p is true
- if $p \wedge q$ is true, then q is true

1.2.2 Disjunction

- if p is true,then $p \vee q$ is true
- if q is true, then $p \vee q$ is true
- if $p \vee q$ is true, and if r can be derived from p and q, then r is true

1.2.3 Negation

The **negation operator** is the logical operator $\neg$, defined according to the following rules:

- if p is true, then$\neg p$ is false.
- If $\neg p$ and p are both true, then a contradiction may be derived.

1.2.4 Implication

The implication operator is the logical operator $\Rightarrow$ defined according to the following rules:

- If q can be derived from the assumption that p is true, then $p \Rightarrow q$ is true;
- if $p \Rightarrow q$ is true, and p is true, then q is true.

P.S. The **converse** of a proposition of the form $p \Rightarrow q$ is the proposition $q \Rightarrow p$

1.2.5 Bidirectional Operator

The **biconditional operator** is the logical operator $\Leftrightarrow$, defined by declaring $p \Leftrightarrow q$ to mean $(p \Rightarrow q) \wedge (q \Rightarrow p)$.

1.2.6 Contrapositive

$p \rightarrow q \equiv \neg q \rightarrow \neg p$

1.2.7 Contradiction

A **contradiction** is a proposition that is known or assumed to be false.

1.3 Quantifiers

1.3.1 Logical Formula

A **logical formula** is an expression that is built from predicates using logical operators and quantifiers; it may have both free and bound variables. The truth value of a logical formula depends on its free variables according to the rules for logical operators and quantifiers

1.3.2 Universal quantifier

The universal quantifier is the quantifier $\forall$; if $p\left(x\right)$ is a logical formula with free variable x with range X, then $\forall x \in X$, $p\left(x\right)$ is the logical formula defined according to the following rules:

- If $p\left(x\right)$ can be derived from the assumption that x is an arbitrary element of x, then $\forall x \in X, p(x)$;
- If $(a \in X)$ and $(\forall x \in X, p\left(x\right))$ is true, then $(p\left(a\right))$ is true.

1.3.3 Existential quantifier

The existential quantifier is the quantifier $\exists$ if $p\left(x\right)$ is a logical formula with free variable x with range X, then $\exists x \in X$, $p\left(x\right)$is the logical formula defined according to the following rules:

- If $a \in X$ and $p\left(a\right)$ is true, then $\exists x \in X$, $p\left(x\right)$;

- If $\exists x \in X,\ p\left(x\right)$ is true, and$q$ can be derived from the assumption that $p\left(a\right)$ is true for some fixed $a \in X$, then q is true.

1.3.4 Unique existential quantifier

The unique existential quantifier is the quantifier $\exists!$ defined such that $\exists x \in X$, $p\left(x\right)$ is shorthand for:

$$\left(\exists x \in X, p\left(x\right)\right) \wedge \left(\forall a \in X, \forall b \in X, p\left(a\right) \wedge p\left(b\right) \Rightarrow a = b\right)$$

1.3.5 Quantifier alternation

Let$p\left(x, y\right)$ be a logical formula with free variables $x \in X$ and $y \in Y$,Then:

$$\exists y \in Y, \forall x \in X, p\left(x, y\right) \Rightarrow \forall x \in X, \exists y \in Y, p\left(x, y\right)$$

1.4 Proof in Mathematics

1.4.1 Proof by cases

Sometimes a direct argument is made simpler by breaking into smaller cases.

1.4.2 Proof by contradiction

In this way, we assume that the negation of the argument is true, if the assumption leads to a false statement, then the original argument is true

1.4.3 Proof by Contrapositive

Let p and q be propositional variables. Then $p \Rightarrow q \equiv \neg q \Rightarrow \neg p$

1.4.4 Tautologies

Every logical formula is logically equivalent to a maximally negated logical formula. A **tautology** is a proposition or logical formula that is true, no matter how truth values are assigned to its component propositional variables and predicates.

Let p and q be logical formulae:

1. q can be be derived from p if and only if $p \Rightarrow q$ is a tautology
2. $p \equiv q$ if and only if p $p \iff q$ is a tautology

1.5 Logical Axioms

Aximos are additional logical rules that are utilized in the proofs:

1.5.1 Logical Equivalences

- Idempotence
  - $(p \vee p) \Leftrightarrow p$
  - $(p \wedge p) \Leftrightarrow p$
- Commutativity
  - $(p \vee q) \Leftrightarrow (q \vee p)$
  - $(p \wedge q) \Leftrightarrow (q \wedge p)$
- Associativity
  - $((p \vee q) \vee r) \iff (p \vee (q \vee r))$
  - $((p \wedge q) \wedge r) \iff (p \wedge (q \wedge r))$
- Distributivity
  - $(p \vee (q \vee r)) \Leftrightarrow ((p \vee q) \wedge (q \vee r))$
  - $(p \wedge (q \wedge r)) \Leftrightarrow ((p \wedge q) \vee (q \wedge r))$
- Double Negation
  - $p = \neg\neg p$
- Implication Related
  - $(p \leftrightarrow q) \Leftrightarrow [(\neg q \leftrightarrow \neg p)]$
  - $(p \leftrightarrow q) \Leftrightarrow [(\neg p \vee q)]$
  - $(p \leftrightarrow q) \Leftrightarrow [((p \to q) \wedge (q \to p))]$

1.5.2 De Morgan's Law

- for logical operators
  - $\neg (p \wedge q) \equiv (\neg p) \vee (\neg q)$
  - $\neg (p \vee q) \equiv (\neg p) \wedge (\neg q)$
- for quantifiers
  - $\neg \forall x \in X, p(x) \equiv \exists x \in X, \neg p(x)$
  - $\neg \exists x \in X, p(x) \equiv \forall x \in X, \neg p(x)$

1.6 Inference

1. Modus ponens
2. Modus tollens
3. Disjunctive syllogism
4. Chain Rule
5. Resolution

2 Number sets

A **set** is a collection of **elements** from a specified **universe of discourse**. The collection of everything in the universe of discourse is called the universal set, denoted by U

2.1 Specifying a set

2.1.1 Lists

One way is simply to provide a list of the elements of the set. To specify that the list denotes a set, we enclose the list with {curly brackets}

2.1.2 Implied lists

Sometimes a list might be too long to write out—maybe even infinite—or the length of the list might depend on a variable. In these cases it will be convenient to use an implied list, in which some elements of the list are written, and the rest are left implicit by writing an ellipsis '...'

2.1.3 Set-builder notation

Given a set X, the set of elements of X satisfying some property p(x) is denoted:

$$\{x \in X \mid p\left(x\right)\}$$

2.1.4 Definition of $[n]$

Let $n \in N$. The set $[n]$ is defined by $[n] = \{k \in N \mid 1 \leq k \leq n\}$

2.1.5 Intervals of the real line

The open interval (a, b), the closed interval $[a, b]$, and the half-open intervals $[a, b)$ and $(a, b]$ from a to b are defined by:

$$\begin{aligned} (a,b) &= \{x \in X \mid a < x < b\}, \quad & (a,b] &= \{x \in X \mid a < x \leq b\} \\ [a,b) &= \{x \in X \mid a \leq x < b\}, \quad & [a,b] &= \{x \in X \mid a \leq x \leq b\} \end{aligned}$$

2.1.6 Subset

Let X be a set. A subset of X is a set U such that:

$$\forall a, (a \in U \Rightarrow a \in X)$$

we write $U \subseteq C$ for assertion that U is a subset of X

2.2 Set Attributes

2.2.1 Set extensionality

Let X and Y be sets. Then $X = Y$ if and only if $\forall a, (a \in X \Leftrightarrow a \in Y)$

2.2.2 Proof by double containment

In order to prove that $[x] = [y]$:

- Prove $X \subseteq Y$
- Prove $X \supseteq Y$

2.2.3 Inhabitation and emptiness

A set X is **inhabited** (or nonempty) if it has at least one element; otherwise, it is **empty**.

The **empty set** (also known as the null set) is the set with no elements, and is denoted by Ø

2.2.4 Theroem of emptiness

Let E and E' be sets. If E and E' are empty, then $E = E'$.

2.2.5 Power sets

Let X be a set. The power set of X, written $P(x)$ is the set of all subset of X

2.3 Set operations

2.3.1 Intersection

Let X and Y be sets. The (pairwise) intersection of X and$Y$,denoted $X \bigcap Y$

2.3.2 Disjoint

Let X and Y be sets. We say X and Y are disjoint if $X \bigcap Y$ is empty

2.3.3 Union

Let X and Y be sets. The union of X and Y is defined as:

$$X \cup Y = \{a|a \in X \vee a \in Y\}$$

2.3.4 Index related operation

An (indexed) family of sets is a specification of a set X_i for each element of i in some indexing set I.

Indexed intersection of an indexed family The (indexed) intersection of an indexed family$\{X_i|i \in I\}$is defined by:

$$\bigcap_{i \in I} X_i = \{a|\forall i \in X \vee a \in X_i\}$$

2.3.5 Indexed Union of an indexed family

The (indexed) union of$\{X_i|i \in I\}$ is defined by:

$$\bigcup_{i \in I} X_i = \{a|\exists i \in X \vee a \in X_i\}$$

2.3.6 Relative complement/Set difference

Let X and Y be sets.The relative complement of Y in $X(X \setminus Y)$ is defined by:

$$X \setminus Y = \{x \in X|x \notin Y\}$$

2.3.7 Cartesian product

Let$X$ and Y be sets. The (pairwise) cartesian product of X and Y is the set $X \times Y$:

$$X \times Y = \{(a,b)\,|a \in X \wedge B \in Y\}$$

The elements are called **ordered pairs**.

2.3.8 N-fold cartesian product

The (n-fold) cartesian product of $X_1, X_2, \cdots, X_n$ is set $\prod\limits_{k=1}^{n} X_k$:

$$\prod_{k=1}^{n} X_k = \{(a_1, a_2, \cdots, a_n)\,|a_k \in X_k \text{for all } 1 \leq k \leq n\}$$

The elements are called **ordered k-tuples.**

2.3.9 De Morgan's laws for sets

1. $A \setminus (X \cup Y) = (A \setminus X) \cap (A \setminus Y)$
2. $A \setminus (X \cap Y) = (A \setminus X) \cup (A \setminus Y)$
3. $A \setminus \bigcup_{i \in I} X_i = \bigcap_{i \in I} (A \setminus X_i)$
4. $A \setminus \bigcap_{i \in I} X_i = \bigcup_{i \in I} (A \setminus X_i)$

2.4 Binary Relations

Let X and Y be sets. A (binary) relation from X to Y is a logical formula $R(x, y)$ with two free variables $x \in X$ and $y \in Y$. X is the domain of R and Y is the co-domain of R. The relation R is **homogenous** if the domain and the codomain are the same. Give $x \in X$ and $y \in Y$. if $R(x, y)$ is true, then "x is **related** to y by R" (xRy)

2.4.1 Types of Relations

- The relation is **reflective** if for all $x = y$, the pair (x, y) is related
- The relation is **symmetric** if both(x, y) and (y, x) is related
- The relation is **transitive** if $xRy \vee yRz \rightarrow xRz$
- The relation is **anti-symmetric** if (x, y)xor(y, x) is true

2.5 Equivalence Relation

For a relation R to be a equivalence relation, we have to prove that a relation is:

- Reflective
- Symmetric
- Transitive

2.5.1 Equivalance Class

The equivlalence class of an element $a \in A$ is the set$\{x \in A \mid x \sim a\}$of all elements equivalent to A/

2.5.2 quotient set

The set $\overline{a} = \{x \in A \mid x \sim a\}$ of all elements equivalence to a. The set of all equivlence classes is called the quotient set of A.

2.6 Partial order

For a relation R to be a Partial order, we have to prove that a relation is:

- Reflective
- Anti-symmetric
- Transitive

2.6.1 Comparable

If $(A, \preceq)$ is partially order set elements of a and b of A is said to be comparable if and only if either $a \preceq b$ or $b \preceq a$

2.6.2 Total Order

If $\preceq$ is the partial order on a set A and every two elements of A are comparable, then $\preceq$ is a **total order**,and the pair $(A, \preceq)$ is called totally ordered set

2.6.3 Maxmium/Minimum

An element a of poset is:

- Maximum if and only if $b \preceq a$ for every $b \in A$
- Minimum if and only if $a \preceq b$ for every $a \in A$

Thus, the maximum/minimum are the extreme value (in the sense of $\preceq$)

2.6.4 Maximal/Minimal

An element a of poset is:

- Maximal if and only if $b \in A$ and $a \preceq b$, then $b = a$
- Minimal if and only if $b \in A$ and $b \preceq a$, then $b = a$

The maximal element is the one that is not less than the other.

2.6.5 Greatest lower Bound

An element g is a **greatest lower bound of element** $a, b \in a$ if and only if

1. $g \preceq a, g \preceq b$ and
2. if $c \preceq a$ and $c \preceq b$ for some $c \in A$, then $c \preceq g$

2.6.6 Least upper bound

An element g is a **least upper bound of element** if and only if

1. $a \preceq l$, $b \preceq l$
2. if $a \preceq c$ and $b \preceq c$ for some $c \in A$, then $l \preceq c$

2.6.7 Lattice

A poset in which every two element have both a **Greatest lower Bound** and a **Least upper bound** is called a **latice.**

3 Functions

A function f from a set X to a set Y is a specification of elements $f\left(x\right) \in Y$ for $x \in X$ such that:

$$\forall x \in X!y \in Y, y = f\left(x\right)$$

3.1 Functions

A function f from a set X (called the domain) to a set Y (called the codomain) assigns to each $x \in X$ a unique element $f\left(x\right) \in y$; we write $f : x \to y$ to mean that f is a function from X to Y.

3.1.1 Equality

Two functions are equal if and only if they have the same domain and co-domain and the same values at all arguments.

3.1.2 Compositions

The composite of $f : x \to y$ and $g : y \to z$ is the function $g \circ f : X \to Z$ defined by $\left(\left(g \circ f\right)\left(x\right) = g\left(f\left(x\right)\right)\right)$ for all $x \in X$.

3.1.3 Characteristic functions

The characteristic function of a subset $U \subseteq X$ is the function $\chi U : X \to \{0, 1\}$ defined by, for each $a \in X$, letting $\chi U\left(a\right) = 1$ if $a \in U$, and $\chi U\left(a\right) = 0$ otherwise.

3.1.4 Image and preimage

- The image of a subset $U \subseteq X$ under a function $f : x \to y$ is the subset $f\left[U\right] = \{f\left(x\right) \mid x \in U\} \subseteq Y$. The image of f is the subset $f\left[x\right] \subseteq Y$.
- The preimage of a subset $V \subseteq Y$ under a function $f : x \to y$ is the subset $f^{-1}\left[V\right] = \{x \in X \mid f\left(x\right) \in Y\} \subseteq X$

3.2 Injection and Surjections

3.2.1 injectivity

A function $f : x \to y$ is injective if

$$\forall a, b \in X, f(a) = f(b) \Rightarrow a = b$$

3.2.2 Surjectivity

A function $f : x \to y$ is surjective if:

$$\forall y \in Y, \exists x \in X \Rightarrow f(x) = y$$

3.2.3 Bijectivity

A function $f : x \to y$ is **bijective** if it is injective and surjective.

3.2.4 Inverse

- A left inverse : $Y \to X$ exists only if f is injective. It looks at each element $y \in Y$ and, if it is in the image of f , returns the (unique) value $x \in X$ for which $f(x) = y$.
- A right inverse r : $Y \to X$ exists only if f is surjective. It looks at each element $y \in Y$and picks out one of the (possibly many) values $x \in X$ for which $f(x) = y$.
- If a function has both left and right inverses, the function is bijective.

3.3 Finite set

A set X is finite if their exists a bijection $f : [n] \to X$ for some $n \in \mathbb{N}$. The function is called an enumeratiuon of X. If X is not finite we say it is infinite.

3.3.1 Thereom

- If there exists an injection $f : [m] \to [n]$, then $m \leq n$
- If there exists a surjection $g : [m] \to [n]$,then $m \geq n$
- If there exists a bijection $h : [m] \to [n]$,then $m = n$
- Let X be a finite set and let $f : [m] \to X$ and $g : [n] \to X$ be enumerations of X, where $m, n \in \mathbb{N}$. Then $m = n$.

3.3.2 Size

The size (or **cardinality**) of X, written $|X|$, is the unique natural number n for which there exists a bijection $[n] \to X$. Let X and Y be sets:

- If Y is finite and there is an injection $f : X \to Y$, then X is finite and $[X] \leq [Y]$

- If X is finite and there is an surjection $f : X \to Y$, then Y is finite and $[X] \geq [Y]$
- If one of X or Y is finite and there is a bijection $f : X \to Y$, then both X and Y is finite.

3.4 Countable and uncountable sets

A set X is countably infinite if there exists a bijection $f : \mathbb{N} \to X$. The bijection is called an **enumeration** of X. We say X is **countable** if it is finite or countably infinite.

3.4.1 Propositions

- Let $f : X \to Y$ be a bijection.Then X is countably infinite if and only if Y is countably infinite.
- Let $n \geq 1$ and let $X_1, \cdots X_n$ be countably infinite sets. Then the product $\prod\limits_{i=1}^{n}$ X_i is countably infinite.
- Let $\{X_n \mid n \in \mathbb{N}\}$ be a family of countable sets. Then the set X defined by $X = \bigcup\limits_{n \in \mathbb{N}} X_n$

3.4.2 Uncountable

Let X be a set, and assume that for every function $f : \mathbb{N} \to X$ there is:

1. A family of logical formulae $p_n(x)$ with $x \in X$, one for each $n \in \mathbb{N}$ and
2. An element $b \in X$

such that $\forall n \in \mathbb{N}, [p_n(b) \leftrightarrow \neg p_n(f(n))]$. Then X is **uncountable**

3.4.3 Detecting countability

Let Σ be a set. A word over Σ is an expression of the form$a_1, a_2, \cdots a_n$, where $n \in N$ and $a_i \in \Sigma$ for all $i \in [n]$. The natural number n is called the length of the word. The unique word of length 0 is called the empty word, and is denoted by ε

4 Induction

To prove a statement of the form $\forall n \geq a,\ P(n)$ using mathematical induction, we do the following:

1. prove $P(n)$ is true
2. prove $p(n) \to p(n+1)$ using any method

4.1 Principle of Weak Induction

Let $P(n)$ be a proposition about n. Let $a \in N$. Suppose that:

- $P(n)$ is true
- for all $n \geq a$, $p(n)$ is true $\rightarrow$ $p(n+1)$ is true

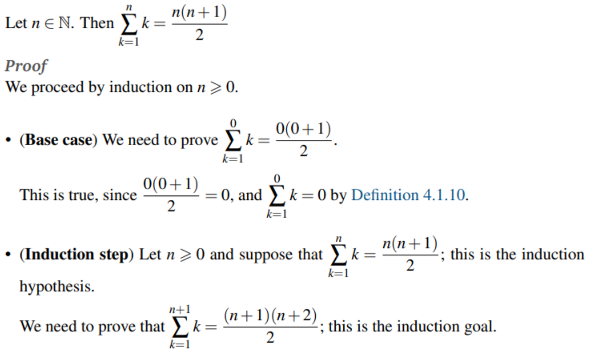
Then $P(n)$ is true for all $n \geq a$,

4.1.1 Proof by weak induction

In order to prove a proposition of the form $\forall n \geq n_0, p(n)$, it suffices to prove that:

- $p(n_0)$is true; and
- for all $n \geq n_0$, if $p(n)$ is true then $p(n+1)$ is also true

4.1.2 Example



Let $n \in \mathbb{N}$. Then $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$

Proof
We proceed by induction on $n \geqslant 0$.

- (**Base case**) We need to prove $\sum_{k=1}^{0} k = \frac{0(0+1)}{2}$.

  This is true, since $\frac{0(0+1)}{2} = 0$, and $\sum_{k=1}^{0} k = 0$ by Definition 4.1.10.

- (**Induction step**) Let $n \geqslant 0$ and suppose that $\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$; this is the induction hypothesis.

  We need to prove that $\sum_{k=1}^{n+1} k = \frac{(n+1)(n+2)}{2}$; this is the induction goal.

4.2 Principle of Strong Induction

Let $P(n)$ be a proposition about n. Let $a \in N$. Suppose that:

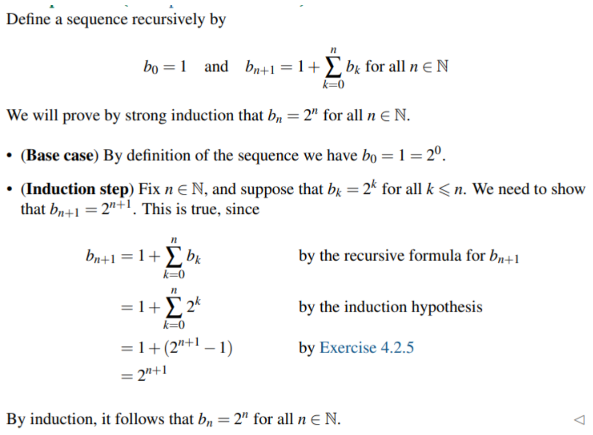
- $P(n)$ is true
- for all $n \geq a$, if $p(k)$ is true for all $a \leq k \leq n$, then $p(n+1)$ is also true.

4.2.1 Proof by Strong induction

In order to prove a proposition of the form $\forall n \geq n_0, p(n)$, it suffices to prove that:

- $p(n_0)$is true; and
- for all $n \geq n_0$, if $p(n)$ is true then $p(n+1)$ is also true

4.2.2 Example



Define a sequence recursively by

$$b_0 = 1 \quad \text{and} \quad b_{n+1} = 1 + \sum_{k=0}^{n} b_k \text{ for all } n \in \mathbb{N}$$

We will prove by strong induction that $b_n = 2^n$ for all $n \in \mathbb{N}$.

- (**Base case**) By definition of the sequence we have $b_0 = 1 = 2^0$.
- (**Induction step**) Fix $n \in \mathbb{N}$, and suppose that $b_k = 2^k$ for all $k \leqslant n$. We need to show that $b_{n+1} = 2^{n+1}$. This is true, since

$$\begin{aligned} b_{n+1} &= 1 + \sum_{k=0}^{n} b_k && \text{by the recursive formula for } b_{n+1} \\ &= 1 + \sum_{k=0}^{n} 2^k && \text{by the induction hypothesis} \\ &= 1 + (2^{n+1} - 1) && \text{by Exercise 4.2.5} \\ &= 2^{n+1} \end{aligned}$$

By induction, it follows that $b_n = 2^n$ for all $n \in \mathbb{N}$. ◁

5 Number Theory

5.1 Division Theory

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. There exist unique $q, r \in \mathbb{Z}$ such that:

$$a = qb + b \text{ and } 0 \leq r \leq |b|$$

We say that q is the **quotient** and **r** is the remainder of a divided by b

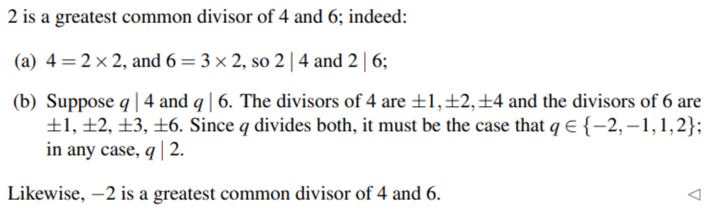
5.1.1 Divides

Let $a, b \in \mathbb{Z}$, b **divides** a if there exists a $q \in \mathbb{Z}$ such that $a = qb$

5.1.2 GCD

Let $a, b \in \mathbb{Z}$ An integer is a GCD of a and b if:

1. $d \mid a$ and $d \mid b$
2. $\exists q, q \mid a, \ q \mid b \ , q \mid c$



2 is a greatest common divisor of 4 and 6; indeed:

(a) $4 = 2 \times 2$, and $6 = 3 \times 2$, so $2 \mid 4$ and $2 \mid 6$;

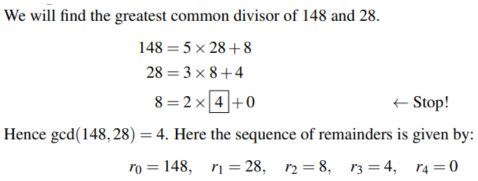
(b) Suppose $q \mid 4$ and $q \mid 6$. The divisors of 4 are $\pm 1, \pm 2, \pm 4$ and the divisors of 6 are ± 1, ± 2, ± 3, ± 6. Since q divides both, it must be the case that $q \in \{-2, -1, 1, 2\}$; in any case, $q \mid 2$.

Likewise, -2 is a greatest common divisor of 4 and 6. ◁

5.1.3 Euclidean algorithm

Let $a, b \in Z$:

1. set $r_0 = |a|$ and $r_1 = |b|$
2. Given r_{n-2} and r_{n-1}, define r_n to be the remainder of r_{n-2} divided by r_{n-1}.
3. Stop when $r_n = 0$, $r_{n-1} = gcd\,(a, b)$



We will find the greatest common divisor of 148 and 28.

$$148 = 5 \times 28 + 8$$
$$28 = 3 \times 8 + 4$$
$$8 = 2 \times \boxed{4} + 0 \qquad \leftarrow \text{Stop!}$$

Hence $\gcd(148, 28) = 4$. Here the sequence of remainders is given by:

$$r_0 = 148, \quad r_1 = 28, \quad r_2 = 8, \quad r_3 = 4, \quad r_4 = 0$$

5.1.4 Bezout's lemma

Let $a, b, c \in Z$, and let $d = gcd\,(a, b)$ .The equation:

$$ax + by = c$$

has a solution $(x, y) \in Z \times Z \leftrightarrow d \mid c$.

5.1.5 Least Common Multiple

Let $a, b \in \mathbb{Z}$ An integer m is a GCD of a and b if:

1. $m \mid a$ and $m \mid b$
2. $\exists c, a \mid c,\ b \mid c\ , m \mid c$

5.2 Prime Numbers

- There are infinitely many prime
- If a natrual number $n > 1$ is not prime, then n is divisible by some prime number $p \leq \sqrt{n}$
- Every natrual number $n \geq 2$ can be written as $n = p_1, p_2, \cdots, p_r$as a product of prime numbers.
- For any integer $n > 2$, the equation $a^n + b^n = c^n$ has no nonzero integer solution.
- Every even integer greater than 2 is the sum of two primes.

5.3 Congruence

5.3.1 Congruence class

The congruence class mod n of an integer is the set of all integers to which a is contruent mod n. Thus:

$$\bar{a} = \{b \in z \mid a \equiv b \pmod{n}\}$$

5.3.2 Equivlant Expression

- $n \mid (a - b)$
- $a \equiv b \pmod{n}$
- $a \in \bar{b}$
- $\bar{a} = \bar{b}$

5.3.3 Propositions

- If $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$:
  1. $a + b \equiv x + y \pmod{n}$
  2. $ab \equiv xy \pmod{n}$
- if $ac \equiv bc \pmod{n}$ and $gcd\,(c, n) = 1$, then $a \equiv b \pmod{n}$or $ax + by = 1$
- Let $n > 1$ be a natrual number and let a be a integer with $gcd\,(a, n) = 1$
  1. There exists an integer such that $sa = 1 \pmod{n}$
  2. For any integer b, the congruence $ax \equiv b \pmod{n}$
  3. The solution to $ax \equiv b \pmod{n}$ is unique mod n in the snese that if $ax_1 \pmod{n}$ and $ax_2 \pmod{n}$, then $x_1 \equiv x_2 \pmod{n}$
  4. If p is prime and $p \not| c$, $c^{p-1} \equiv 1 \pmod{p}$

5.3.4 Chinese Remainder Theorem

$$S: \begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad\cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

1. Let $M = m_1 m_2 \cdots m_n$, $M_i = \frac{M}{M_i}$
2. $t_i M_i = 1 \pmod{m_i}, \forall i \in \{1, 2, \cdots, n\}$
3. $x = kM + \sum\limits_{i=1}^{n} a_i t_i M_i$

6 Counting

6.1 Inclusion Exclusion

6.1.1 Set properties

- $A \cup B = A + B - A \cap B$
- $A \cap B \leq \min\{A, B\}$
- $A \setminus B = A - A \cup B$
- $A^c = U - A$
- $A \oplus B = A \cup B - A \cap B$

6.1.2 Inclusion Exclusion

Given a finie number of finite set, the number of elemeny in the union is:

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = \sum_i A_i - \sum_{i<j} A_i \cap A_j + \sum A_i \cap A_j \cap A_k - \cdots + (-1)^{n+1} \sum A_1 \cap A_2 \cap \cdots \cap A_n$$

6.2 Addition and Multiplication Rules

6.2.1 Addition Rules

The number of ways in which precisely one of a collection of mutually exclusive events can occur is the sum of the numbers of ways in which each event can occur.

6.2.2 Muliplication Rules

The number of ways in which a sequence of events can occur is the product of the numbers of ways in which each event can occur.

6.3 The Pigeonhole Principle

If n object are put into m boxes and $n > m$, then at least some box contains $\lceil \frac{n}{m} \rceil$ objects.

7 Permutation and Combination

7.1 Permutation

A permutation of a ser of distinct symbols is an arrangement of them in a line in some order. It is calculated through :

$$n! = n(n-1)(n-2)(n-3)\cdots 2 \times 1$$

$$P\left(n,r\right)=\frac{n!}{\left(n-r\right)!}$$

7.2 Combination

Let n and r be integers with $n \geq 0$ and $0 \leq r \leq n$, the number of ways to choose r objecys from n, namely the number of combination is:

$$\left(\begin{array}{c} n \\ r \end{array}\right)=\frac{n!}{r!\left(n-r\right)!}$$