Propositional Logic

Proposition: a declarative sentence that is either true or false (not both).

- Conventional letters used for propositional variables are $p, q, r, s, \ldots$
- **Truth value** of a proposition: true, denoted by T; false, denoted by F.

Compound propositions are build using logical connectives:

- Negation ¬
- Conjunction ∧
- Disjunction ∨
- Exclusive or ⊕
- Implication →
- Biconditional ↔

Tautology: A compound proposition that is always true, no matter what the truth values of the propositional variables that occur in it.

Conditional Statement (Implication) $p \to q$

if p then q p implies q p is sufficient for q q is necessary for p q follows from p

q unless $\neg p$ (Or equivalently, if you does not get an A, it cannot be the case that you get 100 on the final.)

p only if q (Or equivalently, only if you get an A, you may get 100 on the final.)

("If" indicates sufficient condition; "only if" indicates necessary condition)

Contradiction: A compound proposition that is always false.

The compound propositions p and q are called logically equivalent, denoted by $p \equiv q$, if $p \leftrightarrow q$ is a tautology.

Operator	Precedence
¬	1
∧	2
∨	3
→	4
↔	5

$(p \vee q) \vee r \equiv p \vee (q \vee r)$ $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	Associative laws
$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$ $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	Distributive laws
$\neg(p \wedge q) \equiv \neg p \vee \neg q$ $\neg(p \vee q) \equiv \neg p \wedge \neg q$	De Morgan's laws
$p \vee (p \wedge q) \equiv p$ $p \wedge (p \vee q) \equiv p$	Absorption laws
$p \vee \neg p \equiv \mathbf{T}$ $p \wedge \neg p \equiv \mathbf{F}$	Negation laws

Predicate Logic and Quantified Statements

Predicate Logic: make statements with variables: $P(x)$.

Propositional function $P(x) \xrightarrow{\text{specify } x}$ Proposition

Quantified Statements: Universal quantifier $\forall x P(x)$; Existential quantifier $\exists x P(x)$

$p \to q \equiv \neg p \vee q$ Useful Law

Propositional function $P(x) \xrightarrow{\text{for all/some } x \text{ in domain}}$ Proposition

A predicate is a statement $P(x_1, x_2, \ldots, x_n)$ that contains n variables $x_1, x_2, \ldots x_n$. It becomes a proposition when specific values are substituted for the variables $x_1, x_2, \ldots x_n$.

The domain (universe) D of the predicate variables $x_1, x_2, \ldots x_n$ is the set of all values that may be substituted in place of the variables.

The truth set of $P(x_1, x_2, \ldots, x_n)$ is the set of all values of the predicate variables $(x_1, x_2, \ldots, x_n)$ such that the proposition $P(x_1, x_2, \ldots, x_n)$ is true.

Argument: A sequence of propositions that end with a conclusion.

Validity of Argument Form:

The argument form with premises $p_1, p_2, \ldots, p_n$ and conclusion q is valid, if

$(p_1 \wedge p_2 \wedge \cdots \wedge p_n) \to q$ is a tautology.

Rule of Inference	Name
p, $p \to q$, $\therefore q$	Modus ponens
$\neg q$, $p \to q$, $\therefore \neg p$	Modus tollens
$p \to q$, $q \to r$, $\therefore p \to r$	Hypothetical syllogism
$p \vee q$, $\neg p$, $\therefore q$	Disjunctive syllogism
p, $\therefore p \vee q$	Addition
$p \wedge q$, $\therefore p$	Simplification
p, q, $\therefore p \wedge q$	Conjunction
$p \vee q$, $\neg p \vee r$, $\therefore q \vee r$	Resolution

Rule of Inference	Name
$\forall x P(x)$, $\therefore P(c)$	Universal instantiation
$P(c)$ for an arbitrary c, $\therefore \forall x P(x)$	Universal generalization
$\exists x P(x)$, $\therefore P(c)$ for some element c	Existential instantiation
$P(c)$ for some element c, $\therefore \exists x P(x)$	Existential generalization

Every student in this class has studied algebra.

Logic Expression 3:

- $A(x)$: "x has studied algebra".
- $C(x)$: "x is in this class"
- $S(x)$: "x is a student"
- Domain: all people
- $\forall x (S(x) \wedge C(x) \to A(x))$

Some student in this class has visited Mexico.

Logic Expression 2:

- $M(x)$: "x has visited Mexico".
- $C(x)$: "x is a student in this class."
- Domain: all people
- $\exists x (C(x) \wedge M(x))$

Prove that

Methods of Proving Theorems

A proof is a valid argument that establishes the truth of a mathematical statement.

Direct proof 直接证明

$p \to q$ is proved by showing that if p is true then q follows

Proof by contrapositive 反证法证明

show the contrapositive $\neg q \to \neg p$

Proof by contradiction 矛盾证明

show that $(p \wedge \neg q)$ contradicts the assumptions

Proof by cases 分类讨论证明

give proofs for all possible cases

Proof of equivalence 等价性证明

$p \leftrightarrow q$ is replaced with $(p \to q) \wedge (q \leftarrow p)$

Question 1: Is $\forall x P(x)$ a proposition?

Yes. Its truth value?

True if $P(x)$ is true for all x in the domain.

False if there is an x in the domain such that $P(x)$ is false. (counterexample)

The converse of $p \to q$ is $q \to p$.

The contrapositive of $p \to q$ is $\neg q \to \neg p$.

The inverse of $p \to q$ is $\neg p \to \neg q$.

Proof Exercise 1

$\sqrt{2}$ is irrational. (Rational numbers are those of the form $\frac{m}{n}$, where m and n are integers.)

Proof: Suppose that $\sqrt{2}$ is rational. Then, there exist integers a and b with $\sqrt{2} = a/b$, where $b \neq 0$ and a and b have no common factors (so that the fraction a/b is in lowest terms.)

Since $\sqrt{2} = a/b$, it follows that $2b^2 = a^2$. By the definition of an even integer, it follows that a^2 is even, so a is even (see Exercise 16).

Since a is even, $a = 2k$ for some integer k. Thus, $b^2 = 2k^2$. This implies that b^2 is even, so b is even.

As a result, a and b have a common factor 2, which contradicts our assumption.

Proof Exercise 2

Show that there exist irrational numbers x and y such that x^y is rational.

Proof: We know that $\sqrt{2}$ is irrational. Consider the number $\sqrt{2}^{\sqrt{2}}$.

Case 1: If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have two irrational numbers $x = \sqrt{2}$ and $y = \sqrt{2}$ with $x^y = \sqrt{2}^{\sqrt{2}}$ rational.

Case 2: If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we let $x = \sqrt{2}^{\sqrt{2}}$ and $y = \sqrt{2}$. We have $x^y = (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = 2$ is rational.

Applying Rules of Inference for Quantified Statements

- $C(x)$: x is in this class.
- $B(x)$: x has read the book.
- $P(x)$: x passed the first exam.
- Domain of x: all students

Premises: $\exists x (C(x) \wedge \neg B(x))$, $\forall x (C(x) \to P(x))$

Conclusion: $\exists x (P(x) \wedge \neg B(x))$

Step	Reason
1. $\exists x (C(x) \wedge \neg B(x))$	Premise
2. $C(a) \wedge \neg B(a)$	Existential instantiation from (1)
3. $C(a)$	Simplification from (2)
4. $\forall x (C(x) \to P(x))$	Premise
5. $C(a) \to P(a)$	Universal instantiation from (4)
6. $P(a)$	Modus ponens from (3) and (5)
7. $\neg B(a)$	Simplification from (2)
8. $P(a) \wedge \neg B(a)$	Conjunction from (6) and (7)
9. $\exists x (P(x) \wedge \neg B(x))$	Existential generalization from (8)

Note that although we do not know which case works, we know that one of the two cases has the desired property.

Sets

A set is an unordered collection of objects. $\{x \mid x \text{ has property } P \text{ or property } P(x))\}$

Proof of Subset:

- Showing $A \subseteq B$: if x belongs to A, then x also belongs to B.
- Showing $A \nsubseteq B$: find a single $x \in A$ such that $x \notin B$.

Prove $A = B$?

Cardinality, Power Set, Tuples, and Cartesian Product

Cardinality: If there are exactly n distinct elements in S, where n is a nonnegative integer, we say that S is a finite set and n is the cardinality of S, denoted by $|S|$.

Power Set: Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Tuples: The ordered n-tuple $(a_1, a_2, \ldots, a_n)$ is the ordered collection that has a_1 as its first element and a_2 as its second element and so on.

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

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

- Two sets A, B are *equal* if and only if $\forall x (x \in A \leftrightarrow x \in B)$.

If $A \subseteq B$, but $A \neq B$, then we say A is a proper subset of B, i.e., $\forall x (x \in A \to x \in B) \wedge \exists x (x \in B \wedge x \notin A)$, denoted by $A \subset B$.

Prove that $\emptyset \subseteq S$.

Proof:
By definition, we need to prove $\forall x (x \in \emptyset \to x \in S)$. Since the empty set does not contain any element, $x \in \emptyset$ is always false. Then the implication is always true.

Prove that $S \subseteq S$.

Proof:
By definition, we need to prove $\forall x (x \in S \to x \in S)$. This is obviously true.

Power Set

Given a set S, the power set of S is the set of all subsets of the set S, denoted by $\mathcal{P}(S)$.

Example: What is the power set of the set $\{0, 1, 2\}$?

$$\mathcal{P}(\{0,1,2\}) = \{\emptyset, \{0\}, \{1\}, \{2\}, \{0,1\}, \{0,2\}, \{1,2\}, \{0,1,2\}\}$$

Cartesian Product

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

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

$A_1 \times A_2 \times \ldots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A_i \text{ for } i = 1, 2, \ldots, n\}$

$$A^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in A \text{ for } i = 1, 2, \ldots, n\}$$

Set Operations

Union: Let A and B be sets. The union of the sets A and B, denoted by $A \cup B$, is the set $\{x \mid x \in A \vee x \in B\}$.

Intersection: The intersection of the sets A and B, denoted by $A \cap B$, is the set $\{x \mid x \in A \wedge x \in B\}$.

Difference: Let A and B be sets. The difference of A and B, denoted by $A - B$, is the set containing the elements of A that are not in B.
$A - B = \{x \mid x \in A \wedge x \notin B\} = A \cap \bar{B}$.

Complement: If A is a set, then the complement of the set A (with respect to U), denoted by $\bar{A}$ is the set $U - A$, $\bar{A} = \{x \in U \mid x \notin A\}$

Two sets A and B are called disjoint if their intersection is empty, i.e., $A \cap B = \emptyset$.

Cardinality of the Union

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

The generalization of this result to unions of an arbitrary number of sets is called the principle of inclusion–exclusion.

Prove that $\overline{A \cap B} = \bar{A} \cup \bar{B}$

Proof 1: Using membership tables. Consider an arbitrary element x: 1, x is in A; 0, x is not in A.

Proof 2: by showing that $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$ and $\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

$\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$:

- Suppose that $x \in \overline{A \cap B}$. By the definition of complement, $x \notin A \cap B$. Using the definition of intersection, $\neg((x \in A) \wedge (x \in B))$ is true.
- By applying De Morgan's law, $\neg(x \in A) \vee \neg(x \in B)$. Thus, $x \notin A$ or $x \notin B$. Using the definition of the complement of a set, $x \in \bar{A}$ or $x \in \bar{B}$.
- By the definition of union, we see that $x \in \bar{A} \cup \bar{B}$. Thus, $\overline{A \cap B} \subseteq \bar{A} \cup \bar{B}$.

$\bar{A} \cup \bar{B} \subseteq \overline{A \cap B}$

Proof 3: Using set builder and logical equivalences

$\overline{A \cap B} = \{x \mid x \notin A \cap B\}$	by definition of complement
$= \{x \mid \neg(x \in (A \cap B))\}$	by definition of does not belong symbol
$= \{x \mid \neg(x \in A \wedge x \in B)\}$	by definition of intersection
$= \{x \mid \neg(x \in A) \vee \neg(x \in B)\}$	by the first De Morgan law for logical equivalences
$= \{x \mid x \notin A \vee x \notin B\}$	by definition of does not belong symbol
$= \{x \mid x \in \bar{A} \vee x \in \bar{B}\}$	by definition of complement
$= \{x \mid x \in \bar{A} \cup \bar{B}\}$	by definition of union
$= \bar{A} \cup \bar{B}$	by meaning of set builder notation

Let f be a function from A to B.
A is the domain of f; B is the codomain of f

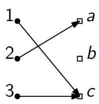
If $f(a) = b$, then b is called the image of a and a is a preimage of b.

The range of f is the set of all images of elements of A, denoted by $f(A)$.

We also say f maps A to B.

Example:

$A = \{1, 2, 3\}$, $B = \{a, b, c\}$



- c is the image of 1
- 2 is a preimage of a
- the domain of f is $\{1, 2, 3\}$
- the codomain of f is $\{a, b, c\}$
- the range of f is $\{a, c\}$

Let A and B be two sets. A function from A to B, denoted by $f : A \to B$, is an assignment of exactly one element of B to each element of A.

One-to-one (injective) function:

- A function f is called one-to-one or injective if and only if $f(x) = f(y)$ implies $x = y$ for all x, y in the domain of f.

Onto (surjective) function:

- A function f is called onto or surjective if and only if for every $b \in B$ there is an element $a \in A$ such that $f(a) = b$.

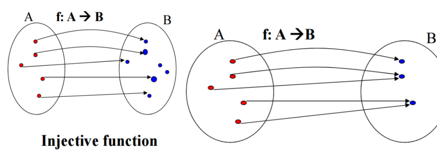
One-to-one (bijective) correspondence

- One-to-one and onto

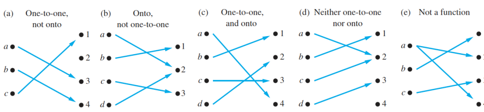
Proof for One-to-One and Onto

Suppose that $f : A \to B$.

To show that f is *injective*	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not *injective*	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective*	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$



Injective function



One-to-One and Onto

Prove that "for a function $f: A \to B$ with $|A| = |B| = n$, f is one-to-one if and only if f is onto."

Proof: Since $|A| = n$, let $\{x_1, x_2, \ldots, x_n\}$ be elements of A.

If f is one-to-one, then f is onto (direct proof): Suppose that f is one-to-one. According to the definition of one-to-one function,
$f(x_i) \neq f(x_j)$ for any $i \neq j$. Thus, $|f(A)| = |\{f(x_1), \ldots, f(x_n)\}| = n$.
Since $|B| = n$ and $f(A) \subseteq B$, we have $f(A) = B$.

If f is onto, then f is one-to-one (contradiction): Suppose that f is onto. Suppose that f is not one-to-one. Thus, $f(x_i) = f(x_j)$ for some $i \neq j$. Then, $|\{f(x_1), \ldots, f(x_n)\}| \leq n - 1$. Note that $|f(A)| = |B| = n$, which leads to a contradiction.

Two Functions on Real Numbers

Let f_1 and f_2 be functions from A to $\boldsymbol{R}$. Then $f_1 + f_2$ and $f_1 f_2$ are also functions from A to $\boldsymbol{R}$ defined for all $x \in A$ by

$$(f_1 + f_2)(x) = f_1(x) + f_2(x)$$
$$(f_1 f_2)(x) = f_1(x) f_2(x)$$

Example:

$f_1 = x - 1$ and $f_2 = x^3 + 1$

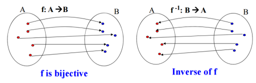
Then

$$(f_1 + f_2)(x) = x^3 + x$$
$$(f_1 f_2)(x) = x^4 - x^3 + x - 1$$

Inverse Functions

Let f be a one-to-one correspondence (bijection) from the set A to the set B. The inverse function of f is the function that assigns to an element b belonging to B the unique element a in A such that $f(a) = b$.

The inverse function of f is denoted by f^{-1}.
Hence, $f^{-1}(b) = a$ when $f(a) = b$.



A bijection is called invertible.

Proof for Inverse Function

1. Prove function f is a bijection: injective, surjective

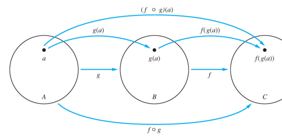
To show that f is *injective*	Show that if $f(x) = f(y)$ for all $x, y \in A$, then $x = y$
To show that f is not *injective*	Find specific elements $x, y \in A$ such that $x \neq y$ and $f(x) = f(y)$
To show that f is *surjective*	Consider an arbitrary element $y \in B$ and find an element $x \in A$ such that $f(x) = y$
To show that f is not *surjective*	Find a specific element $y \in B$ such that $f(x) \neq y$ for all $x \in A$

2. If f is a bijection, then it is invertible
3. Determine the inverse function

Let f be a function from B to C and let g be a function from A to B. The composition of the functions f and g, denoted by $f \circ g$, is defined by $(f \circ g)(x) = f(g(x))$.

The floor function assigns a real number x the largest integer that is $\leq x$, denoted by $\lfloor x \rfloor$. E.g., $\lfloor 3.5 \rfloor = 3$.

The ceiling function assigns a real number x the smallest integer that is $\geq x$, denoted by $\lceil x \rceil$. E.g., $\lceil 3.5 \rceil = 4$.



- Suppose that f is a bijection from A to B. Then $f \circ f^{-1} = I_B$ and $f^{-1} \circ f = I_A$. Since

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(b) = a$$
$$(f \circ f^{-1})(b) = f(f^{-1}(b)) = f(a) = b,$$

where I_A, I_B denote the *identity functions* on the sets A and B, respectively.

Note: Identity function is sometimes denoted by $\iota_A(\cdot)$:

$$\iota_A(x) = x$$

(1a) $\lfloor x \rfloor = n$ if and only if $n \leq x < n + 1$ (1b) $\lceil x \rceil = n$ if and only if $n - 1 < x \leq n$ (1c) $\lfloor x \rfloor = n$ if and only if $x - 1 < n \leq x$ (1d) $\lceil x \rceil = n$ if and only if $x \leq n < x + 1$	
(2) $x - 1 < \lfloor x \rfloor \leq x \leq \lceil x \rceil < x + 1$	
(3a) $\lfloor -x \rfloor = -\lceil x \rceil$ (3b) $\lceil -x \rceil = -\lfloor x \rfloor$	
(4a) $\lfloor x + n \rfloor = \lfloor x \rfloor + n$ (4b) $\lceil x + n \rceil = \lceil x \rceil + n$	

Prove that if x is a real number, then $\lfloor 2x \rfloor = \lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor$.

Proof: Let $x = n + \epsilon$, where n is an integer and $0 \leq \epsilon < 1$.

- $0 \leq \epsilon < \frac{1}{2}$: In this case, $2x = 2n + 2\epsilon$. Since $0 \leq 2\epsilon < 1$, we have $\lfloor 2x \rfloor = 2n$. Similarly, $x + \frac{1}{2} = n + \frac{1}{2} + \epsilon$. Since $0 \leq \frac{1}{2} + \epsilon < 1$, we have $\lfloor x + \frac{1}{2} \rfloor = n$. Thus, $\lfloor 2x \rfloor = 2n$, and $\lfloor x \rfloor + \lfloor x + \frac{1}{2} \rfloor = 2n$.
- $\frac{1}{2} \leq \epsilon < 1$: In this case, $2x = 2n + 2\epsilon = (2n + 1) + (2\epsilon - 1)$. Since $0 \leq 2\epsilon - 1 < 1$, we have $\lfloor 2x \rfloor = 2n + 1$. ....

Prove or disprove that $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$ for all real numbers x and y.

Proof: This statement is false. Consider a counterexample $x = \frac{1}{2}$ and $\frac{1}{2}$. We can find that $\lceil x + y \rceil = 1$, but $\lceil x \rceil + \lceil y \rceil = 2$.

Infinite geometric series can be computed in the closed form for $|x| < 1$.

$$\sum_{k=0}^{\infty} x^k = \lim_{n \to \infty} \sum_{k=0}^{n} x^k = \lim_{n \to \infty} \frac{x^{n+1} - 1}{x - 1} = \frac{1}{1 - x} \qquad \sum_{k=0}^{\infty} k x^{k-1} = \frac{1}{(1 - x)^2}$$

$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$

A set that is either finite or has the same cardinality as the set of positive integers $\mathbf{Z}^+$ is called countable. A set that is not countable is called uncountable. Why are these called countable? The elements of the set can be enumerated and listed.

Countable Sets: Example 1

The set of odd positive integers: $A = \{1, 3, 5, 7, \ldots\}$. Is it countable?

Proof: Using the definition: If there is a one-to-one correspondence from the set of positive integers $\mathbf{Z}^+$ to this set A?

Consider the function

$$f(n) = 2n - 1$$

One-to-one: Suppose $f(n) = f(m)$. Then, $2n - 1 = 2m - 1$, which leads to $n = m$.

Onto: For any arbitrary element in $t \in A$, we have an $n = (t + 1)/2 \in \mathbf{Z}^+$ such that $f(n) = t$.

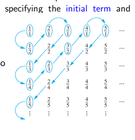
Theorem: The set of positive rational numbers is countable.

Hint: prove by showing that the set of positive rational numbers can be listed in a sequence: specifying the initial term and rule

Solution:

Constructing the list: first list p/q with $p + q = 2$, next list p/q with $p + q = 3$, and so on.

$1, 1/2, 2, 3, 1/3, 1/4, 2/3, \ldots$



Countable Sets: Example 4

Theorem: The set of finite strings S over a finite alphabet A is countably infinite. (Assume an alphabetical ordering of symbols in A)

For example, let $A = \{\text{'a'}, \text{'b'}, \text{'c'}\}$. Then, set $S = \{\text{''}, \text{'a'}, \text{'b'}, \text{'c'}, \text{'ab'} \ldots, \text{'aaaaa'}, \ldots\}$

Solution:

We show that the strings can be listed in a sequence. First list
(i) all the strings of length 0 in alphabetical order.
(ii) then all the strings of length 1 in lexicographic order.
(iii) and so on.
This implies a bijection from $\mathbf{Z}^+$ to S.

The set of all Java programs is countable.

Solution:

Let S be the set of strings constructed from the characters which may appear in a Java program. Use the ordering from the previous example. Take each string in turn

– feed the string into a Java compiler

– if the complier says YES, this is a syntactically correct Java program, we add this program to the list

– we move on to the next string

In this way, we construct a bijection from $\mathbf{Z}^+$ to the set of Java programs.

Theorem: Any subset of a countable set is countable.

Proof: Consider a countable set A and its subset $B \subseteq A$.

- A is a finite set: $|B| \leq |A| < \infty$. Thus, $|B|$ is a finite set and hence countable.
- A is not a finite set: Since A is countable, the elements of A can be listed in a sequence. By removing the elements in the list that are not in B, we can obtain a list for B. Thus, B is countable

Theorem: If A and B are countable sets, then $A \cup B$ is also countable.

A set that is not countable is called uncountable.

Theorem: The set of real numbers $\mathbf{R}$ is uncountable.

$r_1 = 0.d_{11}d_{12}d_{13}d_{14}$
$r_2 = 0.d_{21}d_{22}d_{23}d_{24}$
$r_3 = 0.d_{31}d_{32}d_{33}d_{34}$
where all $d_{ij} \in \{0, 1, 2, \ldots, 9\}$.

Proof by Contradiction: Suppose $\mathbf{R}$ is countable. Then, the interval from 0 to 1 is countable. This implies that the elements of this set can be listed as $r_1, r_2, r_3, \ldots$, where

Uncountable Sets: Example 1

A set that is not countable is called uncountable.

Theorem: The set of real numbers $\mathbf{R}$ is uncountable.

Proof by Contradiction:
We want to show that not all real numbers in the interval between 0 and 1 are in this list. Form a new number called $r = 0.d_1d_2d_3d_4$, where $d_i = 2$ if $d_{ii} \neq 2$, and $d_i = 3$ if $d_{ii} = 2$.

Example: suppose	r1 = 0.75243...	d1 = 2
	r2 = 0.524310...	d2 = 3
	r3 = 0.131257...	d3 = 2
	r4 = 0.9363633...	d4 = 2
	...	...
	rt = 0.23222222...	dt = 3

r and r_i differ in the i-th decimal place for all i.
This leads to a contradiction.

Uncountable Sets: Example 2

Theorem: The set $\mathcal{P}(\mathbf{N})$ is uncountable.

Proof by contradiction:

Assume that $\mathcal{P}(\mathbf{N})$ is countable. This implies that the elements of this set can be listed as $S_0, S_1, S_2, \ldots$, where $S_i \subseteq \mathbb{N}$, and each S_i can be represented uniquely by the bit string $b_{i0}b_{i1}b_{i2}\ldots$, where $b_{ij} = 1$ if $j \in S_i$ and $b_{ij} = 0$ if $j \notin S_i$

- $S_0 = b_{00}b_{01}b_{02}b_{03}\cdots$
- $S_1 = b_{10}b_{11}b_{12}b_{13}\cdots$
- $S_2 = b_{20}b_{21}b_{22}b_{23}\cdots$
- ⋮

all $b_{ij} \in \{0, 1\}$.

Form a new set called $R = b_0b_1b_2b_3\ldots$, where $b_i = 0$ if $b_{ii} = 1$, and $b_i = 1$ if $b_{ii} = 0$. R is different from each set in the list. Each bit string is unique, and R and S_i differ in the i-th bit for all i.

Schröder-Bernstein Theorem

Theorem: If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

In other words, if there are one-to-one functions f from A to B and g from B to A, then there is a one-to-one correspondence between A and B, and hence $|A| = |B|$.

Example: Show that $|(0, 1)| = |(0, 1]|$

$f(x) = x$, $g(x) = x/2$

Cantor's theorem: If S is a set, then $|S| < |P(S)|$.

Countable Sets

Theorem: An infinite set is countable if and only if it is possible to list the elements of the set in a sequence (indexed by the positive integers).

Cardinality of Sets

A set that is either finite or has the same cardinality as the set of positive integers $\mathbf{Z}^+$ is called countable.

If there is a one-to-one function from A to B, the cardinality of A is less than or equal to the cardinality of B, denoted by $|A| \leq |B|$.

Theorem: If there is a one-to-one correspondence between A and B, then the sets A and B have the same cardinality.

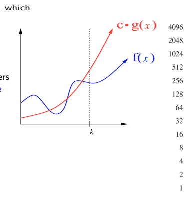
Theorem: If A and B are sets with $|A| \leq |B|$ and $|B| \leq |A|$, then $|A| = |B|$.

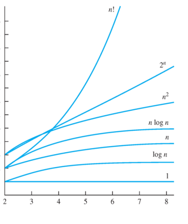
Big-O Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of real numbers. We say that $f(x)$ is $O(g(x))$ if there are constants C and k such that

$$|f(x)| \leq C|g(x)|,$$

whenever $x > k$. [This is read as "$f(x)$ is big-oh of $g(x)$."]





$1+2+\cdots+n = O(n^2)$

$n! = O(n^n)$

$\log n! = O(n\log n)$

$\log_a n = O(n)$ for an integer $a \geq 2$

$n^a = O(n^b)$ for integers $a \leq b$

$n^a = O(2^n)$ for an integer a

Big-O Notation: Example

Show that $f(x) = x^2+2x+1$ is $O(x^2)$.

Proof: We can readily estimate the size of $f(x)$ when $x > 1$:

$$0 \leq x^2+2x+1 \leq x^2+2x^2+x^2 = 4x^2.$$

This is because when $x > 1$, $x < x^2$ and $1 < x^2$. Thus, let $C = 4$, $k = 1$:

$$|f(x)| \leq C|x^2|, \text{ whenever } x > k.$$

Hence, $f(x) = O(x^2)$.

Note that there are multiple ways for proving this. Alternatively, we can estimate the size of $f(x)$ when $x > 2$:

$$0 \leq x^2+2x+1 \leq x^2+x^2+x^2 = 3x^2.$$

It follows that $C = 3$, $k = 2$. ...

Big-Omega Notation

Let f and g be functions from the set of integers or the set of real numbers to the set of integers or the set of real numbers.We say that $f(x)$ is $\Omega(g(x))$ if there are positive constants C and k such that

$$|f(x)| \geq C|g(x)|$$

whenever $x > k$. [This is read as "$f(x)$ is big-Omega of $g(x)$."]

Let f and g be functions from the set of integers or the set of real numbers to the set of integers or the set of real numbers.We say that $f(x)$ is $\Theta(g(x))$ if

- $f(x)$ is $O(g(x))$ and
- $f(x)$ is $\Omega(g(x))$.

When $f(x)$ is $\Theta(g(x))$, we say that $f(x)$ is big-Theta of $g(x)$, that $f(x)$ is of order $g(x)$, and that $f(x)$ and $g(x)$ are of the same order.

If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$, then $(f_1+f_2)(x) = O(\max(|g_1(x)|, |g_2(x)|))$.

If $f_1(x)$ is $O(g_1(x))$ and $f_2(x)$ is $O(g_2(x))$ then $(f_1f_2)(x) = O(g_1(x)g_2(x))$.

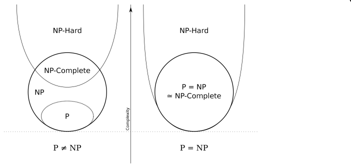
NP-Complete

P: Problems that are solvable using an algorithm with polynomial worst-case complexity

NP: Problems for which a solution can be checked in polynomial time.

NP-Hard: Problems at least as hard as the hardest problems in NP.

NP-Complete: If any of these problems can be solved by a polynomial worst-case time algorithm, then all problems in the class NP can be solved by polynomial worst-case time algorithms.



Functions of the Same Type

Definition: Two positive functions $f(n)$ and $g(n)$ are of the same type if

$$c_1g(n^{a_1})^{b_1} \leq f(n) \leq c_2g(n^{a_2})^{b_2}$$

for all large n, where a_1, b_1, c_1, a_2, b_2, c_2 are some positive constants.

Example:

All polynomials are of the same type

Polynomials and exponentials are of different types.

Number Theory

If a and b are integers with $a \neq 0$,

- we say that a divides b if there is an integer c such that $b = ac$, or equivalently b/a is an integer.

In this case, we say that a is a factor or divisor of b, and b is a multiple of a. (We use the notations $a|b$, $a \nmid b$) $4|24$ $4 \nmid 5$

Divisibility

All integers divisible by $d > 0$ can be enumerated as: $\ldots, -kd, \ldots, -2d, -d, 0, d, 2d, \ldots, kd, \ldots$

Question: Let n and d be two positive integers. How many positive integers not exceeding n are divisible by d?

Answer: Count the number of integers such that $0 < kd \leq n$. Therefore, there are $\lfloor n/d \rfloor$ such positive integers.

Divisibility: Properties

Let a, b, c be integers. Then the following hold:

(i) if $a|b$ and $a|c$, then $a|(b+c)$

(ii) if $a|b$ then $a|bc$ for all integers c

(iii) if $a|b$ and $b|c$, then $a|c$

Proof: Suppose that $a|b$ and $a|c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s+t).$$

Therefore, a divides $b + c$.

Corollary If a, b, c are integers, where $a \neq 0$, such that $a|b$ and $a|c$, then $a|(mb+nc)$ whenever m and n are integers. **Proof:** By part (ii) and part (i) of Properties.

The Division Algorithm

If a is an integer and d a positive integer, then there are unique integers q and r, with $0 \leq r < d$, such that

$$a = dq + r$$

In this case, d is called the divisor, a is called the dividend, q is called the quotient, and r is called the remainder.

In this case, we use the notations $q = a$ **div** d and $r = a$ **mod** d.

Congruence Relation

If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$, denoted $\equiv b$ (**mod** m). This is called congruence and m is its modulus. $15 \equiv 3$ (**mod** 12) $-1 \equiv 11$ (**mod** 6)

Congruence Relation

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that

$$a = b + km$$

- If part: If there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b$ (**mod** m).
- Only if part: If $a \equiv b$ (**mod** m), by the definition of congruence, we know that $m|(a-b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$.

Theorem: Let m be a positive integer. If $a \equiv b$ (**mod** m) and $c \equiv d$ (**mod** m), then

$$a + c \equiv b + d \text{ (mod } m)$$

$$ac \equiv bd \text{ (mod } m)$$

Corollary: Let m be a positive integer and let a and b be integers. Then,

$$(a+b) \text{ mod } m = ((a \text{ mod } m) + (b \text{ mod } m)) \text{ mod } m$$

$$ab \text{ mod } m = ((a \text{ mod } m)(b \text{ mod } m)) \text{ mod } m$$

Let $\mathbf{Z}_m$ be the set of nonnegative integers less than m: $\{0, 1, \ldots, m-1\}$.

$+_m$: $a +_m b = (a+b)$ **mod** m $\cdot_m$: $a \cdot_m b = ab$ **mod** m

Arithmetic Modulo m

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers:

Closure: If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbf{Z}_m$.

Associativity: If a, b, and c belong to $\mathbf{Z}_m$, then $(a +_m b) +_m c = a +_m (b +_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.

Identity elements: $a +_m 0 = a$ and $a \cdot_m 1 = a$.

Additive inverses: If $a \neq 0$ and $a \in \mathbf{Z}_m$, then $m - a$ is an additive inverse of a modulo m. That is, $a +_m (m-a) = 0$ and $0 +_m 0 = 0$.

Commutativity: If $a, b \in \mathbf{Z}_m$, then $a +_m b = b +_m a$.

Distributivity: If $a, b, c \in \mathbf{Z}_m$, then

$$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$$

$$(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$$

Base-b Expansions

```
procedure base b expansion(n, b: positive integers with b > 1)
q := n
k := 0
while (q ≠ 0)
    a_k := q mod b
    q := q div b
    k := k + 1
return(a_{k-1} ,..., a_1,a_0){(a_{k-1} ... a_1a_0)_b is base b expansion of n}
```

Binary Addition of Integers

$$a = (a_{n-1}a_{n-2}\ldots a_1a_0),\ b = (b_{n-1}b_{n-2}\ldots b_1b_0)$$

```
procedure add(a, b: positive integers)
{the binary expansions of a and b are (a_{n-1},a_{n-2},...,a_0)_2 and (b_{n-1},b_{n-2},...,b_0)_2, respectively}
c := 0
for j := 0 to n − 1
    d := ⌊(a_j + b_j + c)/2⌋
    s_j := a_j + b_j + c − 2d
    c := d
s_n := c
return(s_0,s_1,..., s_n){the binary expansion of the sum is (s_n,s_{n-1},...,s_0)_2}
```

Algorithm: Binary Multiplication of Integers

$$a = (a_{n-1}a_{n-2}\ldots a_1a_0)_2,\ b = (b_{n-1}b_{n-2}\ldots b_1b_0)_2$$

$$ab = a(b_02^0 + b_12^1 + + b_{n-1}2^{n-1}) = a(b_02^0) + a(b_12^1) + + a(b_{n-1}2^{n-1})$$

```
procedure multiply(a, b: positive integers)
{the binary expansions of a and b are (a_{n-1},a_{n-2},...,a_0)_2 and (b_{n-1},b_{n-2},...,b_0)_2, respectively}
for j := 0 to n − 1
    if b_j = 1 then c_j = a shifted j places
    else c_j := 0
{c_0,c_1,..., c_{n-1} are the partial products}
p := 0
for j := 0 to n − 1
   p := add(p,c_j)
return p {p is the value of ab}
```

```
    110
  × 101
    110
   000
  110
  11110
```

ALGORITHM 1 The Euclidean Algorithm.

```
procedure gcd(a, b: positive integers)
x := a
y := b
while y ≠ 0
    r := x mod y
    x := y
    y := r
return x{gcd(a, b) is x}
```

Theorem (The Chinese Remainder Theorem): Let m_1, m_2, . . . , m_n be pairwise relatively prime positive integers greater than 1 and a_1, a_2, . . . , a_n arbitrary integers. Then, the system

$$x \equiv a_1 \text{ (mod } m_1)$$
$$x \equiv a_2 \text{ (mod } m_2)$$
$$\ldots$$
$$x \equiv a_n \text{ (mod } m_n)$$

has a unique solution modulo $m = m_1m_2\ldots m_n$.
(That is, there is a solution x with $0 \leq x < m$, and all other solutions are congruent modulo m to this solution.)

How to prove the uniqueness of the solution modulo m?

Proof: Suppose that x and x' are both solutions to all the congruences. As x and x' give the same remainder, when divided by m_k, their difference $x - x'$ is a multiple of each m_k for all $k = 1, 2, \ldots, n$.

As m_1, m_2, . . . , m_n be pairwise relatively prime positive integers, their product m divides $x - x'$, and thus x and x' are congruent modulo m, i.e., $x \equiv x'$ (**mod** m).

This implies that given a solution x with $0 \leq x < m$, all other solutions are congruent modulo m to this solution.

Algorithm: Computing div and mod

Compute $q = a$ **div** d and $r = a$ **mod** d:

```
procedure division algorithm (a: integer, d: positive integer)
q := 0
r := |a|
while r ≥ d
    r := r − d
    q := q + 1
if a < 0 and r > 0 then
    r := d - r
    q := -(q+1)
return (q, r) {q = a div d is the quotient, r = a mod d is the remainder}
```

$O(q\log a)$ bit operations. But there exist more efficient algorithms with complexity $O(n^2)$, where $n = \max(\log a, \log d)$

Algorithm: Binary Modular Exponentiation

Use the algorithm to find 3^{644} mod 645:

```
procedure modular exponentiation(b: integer, n = (a_{k-1}a_{k-2}...a_1a_0)_2 , m: positive integers)
x := 1
power := b mod m
for i := 0 to k − 1
    if a_i = 1 then x := (x·power) mod m
    power := (power·power) mod m
return x {x equals b^n mod m }
```

The algorithm initially sets $x = 1$ and $power = 3$ **mod** $645 = 3$. The binary expansion of 644 is $(1010000100)_2$. Here are the steps used:

$i = 0$: Because $a_0 = 0$, we have $x = 1$ and $power = 3^2$ **mod** $645 = 9$ **mod** $645 = 9$;
$i = 1$: Because $a_1 = 0$, we have $x = 1$ and $power = 9^2$ **mod** $645 = 81$ **mod** $645 = 81$;
$i = 2$: Because $a_2 = 1$, we have $x = 1 \cdot 81$ **mod** $645 = 81$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;
$i = 3$: Because $a_3 = 0$, we have $x = 81$ and $power = 111^2$ **mod** $645 = 12{,}321$ **mod** $645 = 66$;
$i = 4$: Because $a_4 = 0$, we have $x = 81$ and $power = 66^2$ **mod** $645 = 4356$ **mod** $645 = 486$;
$i = 5$: Because $a_5 = 0$, we have $x = 81$ and $power = 486^2$ **mod** $645 = 236{,}196$ **mod** $645 = 126$;
$i = 6$: Because $a_6 = 0$, we have $x = 81$ and $power = 126^2$ **mod** $645 = 15{,}876$ **mod** $645 = 396$;
$i = 7$: Because $a_7 = 1$, we find that $x = (81 \cdot 396)$ **mod** $645 = 471$ and $power = 396^2$ **mod** $645 = 156{,}816$ **mod** $645 = 81$;
$i = 8$: Because $a_8 = 0$, we have $x = 471$ and $power = 81^2$ **mod** $645 = 6561$ **mod** $645 = 111$;
$i = 9$: Because $a_9 = 1$, we find that $x = (471 \cdot 111)$ **mod** $645 = 36$.

Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations can be time consuming since we need to find all factors of the two integers.

For two integers 287 and 91, we want to find $\gcd(287, 91)$.

Step 1: $287 = 91 \cdot 3 + 14$

Step 2: $91 = 14 \cdot 6 + 7$

Step 3: $14 = 7 \cdot 2 + 0$

$$\gcd(287, 91) = \gcd(91, 14) = \gcd(14, 7) = 7$$

Linear Congruences

A congruence of the form $ax \equiv b$ (**mod** m), where m is a positive integer, a and b are integers, and x is a variable, is called a linear congruence.

The solutions to a linear congruence $ax \equiv b$ (**mod** m) are all integers x that satisfy the congruence.

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1$ (**mod** m) is said to be an inverse of a modulo m.

Solve the congruence $ax \equiv b$ (**mod** m) by multiplying both sides by $\bar{a}$.

$$x \equiv \bar{a}b \text{ (mod } m).$$

How to find inverses?

Using extended Euclidean algorithm:

Example: Find an inverse of 101 modulo 4620. That is, find $\bar{a}$ such that $\bar{a} \cdot 101 \equiv 1$ (**mod** 4620).

With extended Euclidean algorithm, we obtain $\gcd(a, b) = sa + tb$, i.e., $1 = -35 \cdot 4620 + 1601 \cdot 101$. It tells us that -35 and 1601 are Bezout coefficients of 4620 and 101. We have

$$1 \text{ mod } 4620 = 1601 \cdot 101 \text{ mod } 4620.$$

Thus, 1601 is an inverse of 101 modulo 4620.

Suppose that a and b are positive integers with $a \geq b$. Let $r_0 = a$ and $r_1 = b$.

$$r_0 = r_1q_1 + r_2 \qquad 0 \leq r_2 < r_1,$$
$$r_1 = r_2q_2 + r_3 \qquad 0 \leq r_3 < r_2,$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_{n-1} + r_n \qquad 0 \leq r_n < r_{n-1},$$
$$r_{n-1} = r_nq_n.$$

$$\gcd(a, b) = \gcd(r_0, r_1) = \ldots = \gcd(r_{n-1}, r_n) = gcd(r_n, 0) = r_n$$

Corollaries of Bezout's Theorem

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof: Since $\gcd(a, b) = 1$, by Bezout's Theorem there exist s and t such that $1 = sa + tb$. This yields $c = sac + tbc$.

Since $a|bc$, we have $a|tbc$. Then, since $a|sac$, we have $a|(sac + tbc)$, i.e., $a|c$.

Lemma: If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_i$ for some i.

(This will be proven in later chapters. Mathematical induction.)

Inverse of a modulo m

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m.

Proof: Since $\gcd(a, m) = 1$, there are integers s and t such that

$$sa + tm = 1.$$

Hence $sa + tm \equiv 1$ (**mod** m). Since $tm \equiv 0$ (**mod** m), it follows that $sa \equiv 1$ (**mod** m). This means that s is an inverse of a modulo m.

How to prove the uniqueness of the inverse?

Suppose that b and c are both inverses of a modulo m. Then $ba \equiv 1$ (**mod** m) and $ca \equiv 1$ (**mod** m). Hence, $ba \equiv ca$ (**mod** m). Because $\gcd(a, m) = 1$ it follows that $b \equiv c$ (**mod** m).

From $ax \equiv b$ (**mod** m), it follows that $\bar{a}ax \equiv \bar{a}b$ (**mod** m).

Note that $\bar{a}ax$ **mod** $m = ((\bar{a}a$ **mod** $m)(x$ **mod** $m))$ **mod** $m = x$ **mod** m.

Thus, x **mod** $m = \bar{a}ax$ **mod** $m = \bar{a}b$ **mod** m, which implies that

$$x \equiv \bar{a}b \text{ (mod } m).$$

Proof: To show such a solution exists: Let $M_k = m/m_k$ for $k = 1, 2, \ldots, n$ and $m = m_1m_2\ldots m_n$. Thus, $M_k = m_1\ldots m_{k-1}m_{k+1}\ldots m_n$.

Since $\gcd(m_k, M_k) = 1$, there is an integer y_k, an inverse of M_k modulo m_k, such that $M_ky_k \equiv 1$ (**mod** m_k). Let

$$x = a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n.$$

It is checked that x is a solution to the n congruences:

$$x \text{ mod } m_k = (a_1M_1y_1 + a_2M_2y_2 + \ldots + a_nM_ny_n) \text{ mod } m_k$$

Since $M_k = m/m_k$, we have x **mod** $m_k = a_kM_ky_k$ **mod** m_k. Since $M_ky_k \equiv 1$ (**mod** m_k), we have $a_kM_ky_k$ **mod** $m_k = a_k$ **mod** m_k. Thus,

$$x \equiv a_k \text{ (mod } m_k).$$

$$x \equiv 2 \text{ (mod } 3)$$
$$x \equiv 3 \text{ (mod } 5)$$
$$x \equiv 2 \text{ (mod } 7)$$

- Let $m = 3 \cdot 5 \cdot 7 = 105$, $M_1 = m/3 = 35$, $M_2 = m/5 = 21$, and $M_3 = m/7 = 15$.
- Compute the inverse of M_k modulo m_k:
  - $35 \cdot 2 \equiv 1$ (**mod** 3) $y_1 = 2$
  - $21 \cdot 1 \equiv 1$ (**mod** 5) $y_2 = 1$
  - $15 \cdot 1 \equiv 1$ (**mod** 7) $y_3 = 1$
- Compute a solution x: $x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \equiv 233 \equiv 23$ (**mod** 105)
- The solutions are all integers x that satisfy $x \equiv 23$ (**mod** 105).

Algorithm: Binary Modular Exponentiation

Compute b^n **mod** m: Let $n = (a_k \ldots a_1a_0)_2$.

$$b^n = b^{a_{k-1}\cdot 2^{k-1}+\ldots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} \cdots b^{a_1\cdot 2} \cdot b^{a_0}$$

Successively finds b **mod** m, b^2 **mod** m, b^4 **mod** m, . . . , $b^{2^{k-1}}$ **mod** m, and multiplies together the terms b^{2^j}, where $a_j = 1$.

```
procedure modular exponentiation(b: integer, n = (a_{k-1}a_{k-2}...a_1a_0)_2 , m: positive integers)
x := 1
power := b mod m
for i := 0 to k − 1
    if a_i = 1 then x := (x·power) mod m
    power := (power·power) mod m
return x {x equals b^n mod m }
```

Recall that

$$ab \equiv ((a \text{ mod } m)(b \text{ mod } m))(\text{mod } m).$$

Primes

A integer p that is greater than 1 is called a prime if the only positive factors of p are 1 and p.

- If n is composite, then n has a prime divisor less than or equal to $\sqrt{n}$.

Let a and b be integers, not both 0. The largest integer d such that $d|a$ and $d|b$ is called the greatest common divisor of a and b, denoted by $\gcd(a, b)$. Let $a = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n}$ and $b = p_1^{b_1}p_2^{b_2}\ldots p_n^{b_n}$. Then,

$$\gcd(a, b) = p^{\min(a_1,b_1)}p^{\min(a_2,b_2)}\ldots p^{\min(a_n,b_n)}$$

The least common multiple of a and b is the smallest positive integer that is divisible by both a and b, denoted by $\mathrm{lcm}(a, b)$.Let $a = p_1^{a_1}p_2^{a_2}\ldots p_n^{a_n}$ and $b = p_1^{b_1}p_2^{b_2}\ldots p_n^{b_n}$. Then,

$$\mathrm{lcm}(a, b) = p^{\max(a_1,b_1)}p^{\max(a_2,b_2)}\ldots p^{\max(a_n,b_n)}.$$

GCD as Linear Combinations

Bezout'S Theorem: If a and b are positive integers, then there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

This equation is called Bezout's identity.

We can use extended Euclidean algorithm to find Bezout's identity.

Lemma: If a, b, c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Lemma: If p is prime and $p|a_1a_2\ldots a_n$, then $p|a_i$ for some i.

Modular Inverse

Modular Inverse: An integer $\bar{a}$ such that $\bar{a}a \equiv 1$ (**mod** m) is said to be an inverse of a modulo m.

When does inverse exist?

Theorem: If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. The inverse is unique modulo m. That is,

- there is a unique positive integer $\bar{a}$ less than m that is an inverse of a modulo m and
- every other inverse of a modulo m is congruent to $\bar{a}$ modulo m.

If we obtain an arbitrary inverse of a modulo m, how to obtain the inverse that is less than m?

GCD as Linear Combinations

We can use extended Euclidean algorithm to find Bezout's identity.

Example: Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

Solution: To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54$$
$$198 = 3 \cdot 54 + 36$$
$$54 = 1 \cdot 36 + 18$$
$$36 = 2 \cdot 18.$$

Substituting the above expressions:

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198.$$

Uniqueness of Prime Factorization

Theorem: A prime factorization of a positive integer, where the primes are in nondecreasing order, is unique.

Proof (by contradiction): Suppose that the positive integer n can be written as a product of primes in two distinct ways:

$$n = p_1p_2\ldots p_s \text{ and } n = q_1q_2\ldots q_t$$

Remove all common primes from the factorizations to get

$$p_{i_1}p_{i_2}\ldots p_{i_u} = q_{j_1}q_{j_2}\ldots q_{j_v}$$

Thus, $p_{i_1}|q_{j_1}q_{j_2}\ldots q_{j_v}$. It then follows that p_{i_1} divides q_{j_k} for some k, contradicting the assumption that p_{i_1} and q_{j_k} are distinct primes.

Theorem*: Let $\gcd(a, m) = d$. Let $m' = m/d$ and $a' = a/d$. The congruence $ax \equiv b$ (**mod** m) has solutions if and only if $d \mid b$.

- If $d \mid b$, then there are exactly d solutions, where by "solution" we mean a congruence class mod m
- If x_0 is a solution, then the other solutions are given by $x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'$.

Proof:

"only if": Let x_0 be a solution, then $ax_0 - b = km$. Thus, $ax_0 - km = b$. Since $d \mid ax_0 - km$, we must have $d \mid b$.

"if": Suppose that $d \mid b$. Let $b = kd$. Since $\gcd(a, m) = d$, there exist integers s and t such that $d = as + mt$. Multiplying both sides by k. Then, $b = ask + mtk$. Let $x_0 = sk$. Then $ax_0 \equiv b$ (**mod** m).

Back Substitution

We may also solve systems of linear congruences with pairwise relatively prime moduli $m_1, m_2, \ldots m_n$ by back substitution.

Example:

(1) $x \equiv 1$ (**mod** 5)
(2) $x \equiv 2$ (**mod** 6)
(3) $x \equiv 3$ (**mod** 7)

According to (1), $x = 5t + 1$, where t is an integer.

Substituting this expression into (2), we have $5t + 1 \equiv 2$ (**mod** 6), which means that $t \equiv 5$ (**mod** 6). Thus, $t = 6u + 5$, where u is an integer.

Substituting $x = 5t + 1$ and $t = 6u + 5$ into (3), we have $30u + 26 \equiv 3$ (**mod** 7), which implies that $u \equiv 6$ (**mod** 7). Thus, $u = 7v + 6$, where v is an integer.

Thus, we must have $x = 210v + 206$. Translating this back into a congruence,

$$x \equiv 206 \text{ (mod } 210).$$