MATH 240 - Discrete Structures

McGill University
Fall 2011

Last Updated: October 19, 2011

Contents

Course Information

- When/Where: MWF 10:35-11:35, Stewart Bio N2/2
- Instructor: Sergey Norin math.mcgill.ca/ snorin
- Textbook: Discrete Mathematics, Elementary and Beyond by Lovasz, Pelikan and Vesztergombi
- Prerequisites:
- Grading:
  - 20 % assignments 20 % midterm and 60 % final
  - 20 % assignments 80 % final
  - (best of two above)

Introduction

Discrete vs. Continuous structures

- Objects in discrete structures are individual and separable
- An intuitive analogy is that discrete structures focus on individual trees in the forest whereas continuous structures care about the landscape airplane view.
- Discrete structure courses can be called "computer science semantics" in other universities. Mathematics for computer science.
- Naive examples
  - Counting techniques: There are two ice cream shops. One sells 20 different flavours whereas the other offers 1000 different combinations of three flavours. Which one has the most possible combinations of three flavours?
  - Cryptography: Two parties want to communicate securely over an insecure channel. Can they do it? Yes, using number theory. Discrete Structures are used in cryptography (what this question is about), coding theorem (compression of data) and optimization.
  - Graph Theory: Suppose you have 6 cities and you want to connect them with roads joining the least possible number of pairs, so that every pair is connected, perhaps indirectly. In how many ways can we connect these cities using 5 roads?
- Before we address these problems, we must agree upon a language to formalize them.

1 Sets

1.1 Definition

A set is a collection of distinct objects which are called the elements of the set.

Examples: We use a capital letter for sets.

- $A = \{Alice, Bob, Claire, Eve\}$
- $B = \{a, e, i, o, u\} = \{o, i, e, a, u\}$
- $\mathbb{N} = \{1, 2, 3, 4, 5, ...\}$ (natural numbers)
- $\mathbb{Z} = \{.., -2, -1, 0, 1, 2, ..\}$ (integers)
- $\emptyset = \{\}$ (no elements, note: $\{\emptyset\} \neq \emptyset\}$)
- If x is an element of A we write $x \in A$ which is read "belongs", "is an element of" or "is in" e.g. $Alice \in A, Alice \notin \mathbb{N}$
- We say that X is a subset of a set Y if for every $z \in X$ we have $z \in Y$ Notation: $X \subseteq Y$.
- $\emptyset \subseteq \{1, 2, 3, 4, 5\} \subseteq \mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R}$

1.2 Operations on sets

$U = \{1, 2, 3, 4, 5, 6..10\} = \{x \in \mathbb{N} : x \leq 10\}$

$A = \{2, 4, 6, 8, 10\} = \{x \in U : x \text{ is even}\}$

$B = \{2, 3, 5, 7\} = \{x \in U : x \text{ is prime}\}$

An intersection $A \cap B$ is a set of all elements belonging to both A or B: $A \cap B = \{2\}$

A union $A \cup B$ is a set of all elements belonging to either A or B: $A \cap B = \{2, 3, 4, 5, 6, 7, 8, 10\}$

$|A| = 5, |B| = 4, |A \cap B| = 1, |A \cup B| = 8 |\emptyset| = 0, |\mathbb{N}| = \infty$

$A - B$: all elements of A which do not belong to B $\{x : x \in A, x \notin B\}$

$A \oplus B, A \triangle B$: symmetric difference, set of all elements belonging to exactly one of A and B

1.3 Venn Diagrams

A way of depicting all possible relations between a collection of sets. For a set A, $|A|$ denotes the number of elements in it.

Typically, Venn diagrams are useful for 2 or 3 sets.

1.4 Theorems

- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
  - Fact: For any two finites sets $|A| + |B| = |A \cap B| + |A \cup B|$
  - Proof:
    1. $x \in A \cap (B \cup C)$ then $x \in (A \cap B) \cup (A \cap C)$
       * $x \in A$ and ($x \in B$ or $x \in C$)
       * if $x \in B$ then $x \in (A \cap B)$ therefore $x \in (A \cap B) \cup (A \cap C)$
       * if $x \in C$ then $x \in (A \cap C)$ therefore $x \in (A \cap B) \cup (A \cap C)$
    2. $x \in (A \cap B) \cup (A \cap C)$ then $x \in A \cap (B \cup C)$
       * $x \in (A \cap B)$ therefore $x \in A$ and $x \in (B \cup C)$
- $A \oplus B = (A \cup B) - (A \cap B) = (A - B) \cup (B - A)$

2 Logic

Way of formally organizing knowledge studies inference rules i.e. which arguments are valid and which are fallacies.

2.1 Propositional Calculus

A proposition is a statement (sentence) which is either true or false.

Some examples:

- $2 + 2 = 4 \rightarrow$ true
- $2 + 3 = 7 \rightarrow$ false

- "If it is sunny tomorrow, I will go to the beach." → valid proposition
- "What is going on?" → not a proposition
- "Stop at the red light" → not a proposition
- We are given 4 cards. Each card has a letter (A-Z) on one side, a number (0-9) on the other side. "If a card has a vowel on one side then it has an even number on the other" Two ways to refute this proposition: Either turn over a vowel card and find an odd number. Or turn over an odd number and find a vowel.

2.2 Notation

- Letters will be used to denote statements: p, q, r
- $p \wedge q$: "and", "conjunction", "p and q" (are both true)
- $p \vee q$: "or", "disjunction", "either p or q" (is true)
- $\neg p$: "not", "p is false"

2.3 Truth Tables

Making tables in LaTeX is so tedious. Check out Wesley's notes.

2.4 Rules of Logic

1. Double negation: $\neg(\neg p) \leftrightarrow p$
2. Indempotent rules: $p \wedge p \leftrightarrow p \qquad p \vee p \leftrightarrow p$
3. Absorption rules: $p \wedge (p \vee q) \leftrightarrow p \qquad p \vee (p \wedge q) \leftrightarrow p$
4. Commutative rules: $p \wedge q \leftrightarrow q \wedge p \qquad p \vee q \leftrightarrow q \vee p$
5. Associative rules: $p \wedge (q \wedge r) \leftrightarrow (q \wedge p) \wedge r \qquad p \vee (q \vee r) \leftrightarrow (p \vee q) \vee r$
6. Distributive rules: $p \wedge (q \vee r) \leftrightarrow (p \wedge q) \vee (p \wedge r) \qquad p \vee (q \wedge r) \leftrightarrow (p \vee q) \wedge (p \vee r)$
7. De Morgan's rule: $\neg((\neg p) \vee (\neg q)) \leftrightarrow p \wedge q \qquad \neg((\neg p) \wedge (\neg q)) \leftrightarrow p \vee q$
   $p \vee (\neg((\neg p) \wedge (\neg q))) \leftrightarrow p \vee (p \vee q) \leftrightarrow (p \vee p) \vee q \leftrightarrow p \vee q$

2.4.1 Conditional Statements

1. $p \rightarrow q$
   - Theorem: if (an assumption holds), then (the conclusion holds).
   - Implication: "if p then q"
     p = "a, b, & c are two sides and the hypthenuse of a triangle"
     q = "$a^2 + b^2 = c^2$"
   - $p \rightarrow q$ "If p then q" p implies q, p is sufficient for q
     $(p \rightarrow q) \leftrightarrow (q \vee (\neg p))$
   - Examples:

  - "If the Riemann hypothesis is true then 2 + 2 = 4" TRUE
    p = "the Riemann hypothesis"
    q = "2+2=4"
    True proposition is implied by any proposition.
  - "If pigs can fly then pigs can get sun burned" TRUE
    False statement implies any statement
  - "If 2+2 =4 then pigs can fly" FALSE
    The implication is false only if the assumption holds and the conclusion does not.

- $p \to q \leftrightarrow (\neg p) \to (\neg q)$
- $(p \to q) \wedge (q \to p) \leftrightarrow (p \leftrightarrow q)$

Puzzle There are three boxes A, B, C. Exactly one contains gold in it.

- Box A: Gold is not in this box
- Box B: Gold is no in this box
- Box C: Gold is in box A

Exactly one of these propositions is true. Where is the gold? Let us formalize the propositions.

- p: "Gold is in box A"
- q: "Gold is in box B"
- r: "Gold is in box C"
- Box A: $q \vee r$
- Box B: $p \vee r$
- Box C: p
- $p \to (p \vee r)$
- $\neg(p \vee r) \to q$

2.5 Tautologies & Contradictions

Definition

- A **tautology** is a statement that is always true (the rightmost column of the corresponding truth table has T in every row) e.g. $p \vee (\neg p)$
- A **contradiction** is a statement that is always false e.g. $p \wedge (\neg p)$

Notation

- 1 denotes a tautology
- 0 denotes a contradiction
- $1 \vee p \leftrightarrow 1$
- $0 \vee p \leftrightarrow p$
- $1 \wedge p \leftrightarrow p$

- $0 \wedge p \leftrightarrow 0$
- $p \wedge (p \vee q)$

p	1	$p \vee q$	$p \wedge (p \vee q)$
T	T	T	T
T	F	T	T
F	T	T	F
F	F	F	F

$\rightarrow$ Not a tautology and not a contradiction
$p \wedge (p \vee q) \leftrightarrow p$ (one of the rules)

- $p \vee (p \wedge q) \vee (p \rightarrow q) \leftrightarrow (p \vee (p \wedge q)) \vee (p \rightarrow q)$
$(p \rightarrow q) \leftrightarrow (\neg p) \vee q \leftrightarrow p \vee (p \rightarrow q)$
$\leftrightarrow p \vee ((\neg p) \vee q)(absorption)$
$\leftrightarrow (p \vee (\neg p)) \vee q$
$\leftrightarrow 1 \vee q \leftrightarrow 1$

2.6 Proofs

- $(p \rightarrow q) \wedge (q \rightarrow r) \rightarrow (p \rightarrow r)$ (always true)
- Implication is transitive: $p \rightarrow q \rightarrow r$
- A **proof** of a conclusion q given premise p is a sequence of implications (valid) $p \rightarrow p_2 \rightarrow p_3 \rightarrow .. \rightarrow p_k \rightarrow q$
- To prove $(p \leftrightarrow q)$
$(p \leftrightarrow q) \leftrightarrow (p \rightarrow q) \wedge (q \rightarrow p)$
- Theorem: Let p(x) be a polynomial then p(0) = 0 if and only if p(x) = x q(x) for some polynomial q(x)
- Proof: "p(0) = 0" and "p(x) = x q(x) for some polynomial q(x)"
  1. $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$
  $p(0) = 0 \rightarrow a_0 = 0 \rightarrow$
  $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x \rightarrow$
  $p(x) = x(a_n x^{n-1} + a_{n-1}x^{n-2} + ... + a_1$
  $p(x) = xq(x)$
  $q(x) = a)nx^{n-1} + a_{n-1}x^{n-2} + ... + a_2$
  True so proven.
  2. $p(x) = xq(x) \rightarrow p(0) = 0 \cdot q(0) \rightarrow q(0) = 0$
- Proof by contradiction: $(p \rightarrow q) \leftrightarrow ((\neg q) \rightarrow (\neg p))$
- Pigeonhole principle: We place an objects into m bins. If $n > m$ then some bin contains at least 2 objects.
- Proof: p = "$n > m$" and q = "Some bin contains at least 2 objects"
$\neg q$ = "every bin contains at most 1 object"
$\neg p$ = "$n \leq m$" $\neg q \rightarrow \neg p$ is trivial
- Theorem: There are infinitely many prime numbers
Direct proof of this theorem is unlikely, there is no known simple formula producing prime numbers
- Proof: Assume $\neg p$. There are infinitely many prime numbers $p_1, p_2, p_3..p_k$
Consider $p = p_1 p_2 ... p_k + 1$ Every integer greater than 1 is divisible by a prime. (Prime number is the

integer divisible by only 1 and itself). Suppose $p = p_i m$ for some $1 \leq i \leq k$ and an integer m, then $p_i(p_1 p_2 ... p_{i-1} p_{i+1} ... p_k) + 1 = p_i m \; p_i(m - p_1 p_2 .. p_k) = 1$ (except p_1) "1 is divisible by p_i, a contradiction"

3 Circuit Complexity

3.1 Boolean Logic

- **Objects**: statements p, 1
- **Operators**: $\vee, \wedge, \neg$, etc

3.2 Logic Gates

Will insert logic gate diagrams later when I figure how to insert images.

p	q	r	$p \oplus q$	$(p \oplus q) \oplus r$
1	1	1	0	1
1	1	0	0	0
1	0	1	1	0
1	0	0	1	1
0	1	1	0	0
0	1	0	1	1
0	0	1	1	1
0	0	0	0	0

Majority Circuit (for 3 inputs) p, q, r $\rightarrow \begin{cases} 1 \text{ (or T) if at least 2 of p, q \& r are 1's} \\ 0 \text{ (or F) otherwise} \end{cases}$

Size A logical circuit has size equal to the number of gates in it and depth equal to the length (or number of gates) of the longest path from an input to the final output.

Given a boolean formula, what is the minimum size (or depth) of a circuit necessary to compute it? (depth is frequently assumed to be constant).

Given a circuit C with inputs $p_1, p_2, ..., p_n$

Can we test if C is always a contradiction? The answer is trivially yes, if we test all possible inputs. It would take 2^n.

3.3 Algorithms

- Every logic formula can be represented as a combinational circuit
- Can we represent a given formula by a "simple" circuit
- Given a circuit (with inputs $p_1, p_2, ..., p_n$ can we test quickly if C is a contradiction? (we can test in $2^n steps$
- **Algorithm**: A step-by-step procedure for solving a problem, precise enough to be carried out on a computer

4 Polytime algorithms and the P $\neq$ NP conjecture

4.1 Definition

Given algorithm A its running time $t_A(n)$ = maximum number of steps the algorithm can require on inputs of size n

A is a **polynomial time** algorithm if $t_A(n)$ is polynomially bounded ($t_A(n) = O(n^2)$) $\leftrightarrow$ fast, efficient

P is class of problem which allow polynomial time algorithms.

Examples

1. Evaluating the median of a set of numbers
   - Problem: $x_1, x_2, .., x_n \leftarrow$ Input
   - Question: decide whether the median of the list is ≤ 1000
   - Algorithm:
     - Sort the list going once through the list ($\leq n$ steps) we can find smallest x_i
     - Repeat to find the second smallest number and so on
     - Requires $O(n^2)$ time to sort
     - Check if $x_{\frac{n}{2}}$ is at most 1000 (roughly n^2 steps polytime).
2. Multiplication
   - Input: $2n$ digit numbers
   - Output: $a \times b$
     roughly n^2 steps
3. Problem Factoring
   - Input: a composite number C
   - Output: Find natural numbers $a, b > 1$ such that $c = a \times b$
   - Brute-Force search: Try all prime numbers up to c. Time: $10^{n/2} \rightarrow$ exponential time algorithm
   - RSA ran contests until 2007 offering prizes for factoring (roughly 20 computer years for factoring 200 digit numbers)

4.2 P problems

A **polytime algorithm** is an algorithm whose running time is in order p(n) for some polynomial p.

A **decision problem** is a problem with a yes/no answer.
Example:

- Input: a combinatorial circuit C (with n inputs)
- Output: Is C **not** a contradiction? In other words, will C output T.

Given a decision problem D, D is in class P if there exists a polytime algorithm which solves D. It is considered to be "fast" or "efficient".

4.3 NP problems (non-deterministic polynomial time)

A decision problem is in the class NP if a "yes" answer always has a certificate which can be verified in polynomial time. In other words, if there is an easy way to check that the answer is yes **when** the answer is yes.

4.3.1 The magician

Suppose that King Arthur poses a yes/no problem to his magician Merlin. To answer such a question seems to require a tremendous amount of toil. On the other hand, if the answer to the problem is yes, there is a piece of evidence or **certificate** to quickly verify the yes-ness.

Examples

- In the circuit example above, if there exists a set of values for inputs so that the circuit outputs 1 (or T) then given this collection of inputs, we can easily verify that the circuit is not contradictory.
- Traveling salesman problem:
  - Input: Collection of n cities where the ith city is located at (x_i, y_i) and the distances between them
  - Output: A tour such that each city is visited exactly once and the total length ≤ 1000 miles
  - Checking each possible tour amounts to (a) fixing some city from which to start then (b) choosing a second city (999 choices) and a third city (998 choices and so on. Thus the number of tours is 999!. This requires a tremendous amount of computation that is way beyond polynomial time.
  - If however, you somehow come up with a tour (use magic), you can easily test if it matches the requirements by computing the sum of distances between two adjacent cities i.e. $\sqrt{(x_{1000} - x_1)^2 + (y_{1000} - y_1)^2} + \sum \sqrt{(x_i - x_{i+1})^2 + (y_i - y_{i+1})^2} \leq 1000$
  - It doesn't matter if Merlin didn't heck all 999! possible tours, only that he found one that worked and that we could prove quickly that it did work
- Factoring
  - Input: n digit number
  - Output: Is this number composite and if it is, factor it.
  - If the magician comes up with a set of factors, it is easy to check if the factors are prime and easy to check if their product is the n-digit number.

4.3.2 Definition

A decision problem D is in class NP if there is a polytime algorithm M (called the checking algorithm) and a polynomial p which given an input and some "extra information" called certificate can verify that x is indeed in L.

It is easy to see that $P \subseteq NP$ i.e. every P-class decision problem is in class NP since if A is a polytime algorithm which solves the decision problem D, then it will also suit as the checking algorithm in the definition of NP. We do not even need a certificate to prove it.

4.4 $P \neq NP$

There exist problems which cannot be solved efficiently but for which a positive answer can be verified efficiently. There exists problems for which brute-force search is essentially the best possible strategy. If there are problems where you need a magician, then it is NP.

If there exists a problem in NP but not in P (if the conjecture is true) then testing if a circuit is a contradiction, travelling salesman problem, and a very large class of similar problems are all not in P

If P = NP then airline scheduling, protein folding, packing boxes, finding short proof for theorems all can be done efficiently but certain cryptography becomes impossible.

The universal opinion is that $P \neq NP$

4.4.1 Scott Aoronson's reasons for $P \neq NP$

Empirical: Problems in NP remain heuristically hard, however problems which are now known to be in P (linear programming, primality testing) but efficient heuristics existed long before.

(N.B. I don't know what this is supposed to mean. Here's a Scott Aoranson quote though:

If P = NP, then the world would be a profoundly different place than we usually assume it to be. There would be no special value in "creative leaps," no fundamental gap between solving a problem and recognizing the solution once it's found. Everyone who could appreciate a symphony would be Mozart; everyone who could follow a step-by-step argument would be Gauss...)

5 Proof Techniques: Predicate calculus

Reminder A proof is a sequence of implications deriving a conclusion q from a premise p: $p \to q$

- Direct Proof: $p \to p_1 \to p_2 \to p_3. \to ... \to p_k \to q$
- Proof by contradiction: $p \to q \leftrightarrow (\neg q \to \neg p)$
- Case Analysis: $(p \wedge q \to r) \leftrightarrow (p \to r) \wedge (q \to r)$ See below
- Counter Examples: See below

Case Analysis

- **Proposition**: For positive integer n: $3 \nmid n \to 3 \mid n^2 + 2$
  ($a \mid b \to$ "a divides b" there exists an integer c, b = ac)
  Proof: Divide n by 3 with remainder such as $n = 3q + r \qquad q \in \mathbb{N}, 0 < r < 3$
  - $r = 1 \to n = 3q + 1$
    $n^2 + 2 = 9q^2 + 1 + 6q + 2 = 3 \cdot (3q^2 + 2q + 1)$
    therefore divisible by 3
  - $r = 2 \to n = 3q + 2$
    $n^2 + 2 = 9q^2 + 4 + 12q + 2 = 3 \cdot (3q^2 + 6q + 2)$
    therefore divisible by 3

Counter Example

- Proposition: $n^2 + n + 1$ is prime for every positive integer n ≤ 10
- $4^2 + 4 + 1 = 21 = 7 \cdot 3$
- This is a counter example: the statement is false
- Mathematical Notation
  - $p \to q \wedge r \to p \to q$ if $\neg(p \to q) \to \neg(p \to q \wedge r)$
  - q is a counter example to the implication "$n^2 + n + 1$ is prime for all integers n "
  - "$n^2 + n + 1$ is prime" $\leftarrow$ P(n) predicate proposition depending on a variable $\forall n \in \mathbb{Z}(P(n))$
    Note: $\forall$ means "for all" e.g. "For all n in the set of integers the predicate "$n^2 + n + 1$"is prime" is true
  - "There exists an integer n so that $n^2 + n + 1$ is not prime" is noted $\exists n \in \mathbb{Z}(Q(n))$ where Q(n) "$n^2 + n + 1$ is not prime" i.e. $Q(n) = \neg P(n)$

Goldback's conjecture Every even integer bigger than 2 is expressible as a sum of 2 primes.

- $\forall n \in$ "even integers", $n > 2 \to (\exists a, b \in \{primes\}(n = a + b)))$
- In predicate calculus, "71 is prime" is equivalent to the notation:
  $\forall a, b \in \mathbb{N}(a \cdot b = 71) \to ((a = 1) \wedge (b = 71))$

Limits Various ways to say the same thing:

- "As x approaches a, f(x) becomes closer and closer to L"
- "f(x) has a limit L as x $\to$ a"
- "$lim_{x \to a} f(x) = L$"
- "For every $\epsilon > 0$, there exists $\delta > 0$ so that if $|x - a| < \delta$ then $|f(x) - L| < \epsilon$"
- "$\forall \epsilon > 0 \quad (\exists \delta > 0 \quad (|x - a| < \delta \to |f(x) - L| < \epsilon))$
- "$lim_{x \to \infty} f(x) = L$" $\leftrightarrow \quad \forall \epsilon > 0 \quad (\exists X : \quad (\forall x > X \quad (|f(x) - L| < \epsilon)))$

Negation

- $\neg(\forall n \in A : P(n)) \leftrightarrow \exists n \in A \quad (\neg P(n))$
- $\forall n \in A : P(n) \leftrightarrow \neg(\exists n \in A \quad (\neg P(n)))$
- This is very useful in proofs, since proving $(\forall n \quad (p(n))$ might be hard if we consider all values of n, whereas checking that there can't be a value of n such that p(n) does not hold could be easier.

"$\sin x$ does not have a limit as $x \to \infty$"

$$\begin{aligned}
\neg(\exists L : lim_{x \to \infty} \sin x = L) &\leftrightarrow \forall L : (\neg(lim(\sin x) = L) \\
&\leftrightarrow \forall L \quad (\neg(\forall \epsilon > 0 \quad (\exists X \quad (\forall x > X \quad (|\sin x - L| < \epsilon))))) \\
&\leftrightarrow \forall L \quad (\exists \epsilon > 0 \quad (\neg(\exists X \quad (\forall x > X \quad (|\sin x - L| < \epsilon))))) \\
&\leftrightarrow \forall L \quad (\exists \epsilon > 0 \quad (\forall X \quad (\exists x > X \quad (|\sin x - L| \geq \epsilon))))
\end{aligned}$$

5.1 Divisibility Problem

We want to prove the following theorem:

- Any collection of n+1 numbers chosen from the set {1,2,...,2n} contains two numbers so that one is divisible by the other.
- $\forall n \in \mathbb{N} \quad (\forall S \subseteq \{1, 2, ..., 2n\} \quad ((|S| = n + 1) \rightarrow \exists a, b \in S \quad ((a|b) \wedge (a \neq b))))$

Reminder: the pigeonhole principle If $n + 1$ objects are placed into n boxes then some box contains ≥ 2 objects. To apply the principle we want to partition $\{1, 2, ..., 2n\}$ into n subjects.

Partition We say that a collection $A_1, A_2, ...A_k$ of subsets of a set B is a **partition** of B if

1. $\forall i, j : 1 \leq i < j \leq k \qquad A_i \cap A_j = \emptyset$ (no element of B belongs to two different parts)
2. $A_1 \cup A_2 \cup ... \cup A_k = B$

Example: {1,2,3,4,5,6,7,8} can be partitioned into {1,2,4,6,8} , {3, 5} , {7}

Proof By the pigeonhole principle it suffices to find a partition $A_1, A_2, ...A_n$ of {1,2,...,2n} so that $(\forall i \quad (\exists a, b \in A_i \quad (a|b \vee b|a)))$

Here is a construction: $A_i = \{(2i - 1), 2(2i - 1), 4(2i - 1), ..., 2^m(2i - 1)\}$ up to maximum m: $2^m(2i - 1) \leq 2n$

1. A_i satisfies the desired property for all i
2. $A_1, A_2, .., A_n$ is a partition of {1,2,...,2n}
   Ever positive integer can be uniquely written in a form $2^m(2i - 1)$ for some $i \geq 1, m \geq 0$

Note: Is it true for some n: "Every collection of n numbers chosen from {1,2,...,2n} contains 2 numbers one dividing the other"?

Counter-example: $n = 2 \quad \{1, 2, 3, 4\} \rightarrow \{3, 4\}$

5.2 Strangers and Clubs

For a collection of people any two of them either have met or haven't . A club is a group of people who have pairwise met each other. A group of strangers is a group of people who pairwise have not met each other

Theorem: In any collection of 6 people there is either a club of 3 people or a group of 3 strangers.

Proof Let x be one of the people in the collection. The following cases apply

1. x has at least 3 acquaintances
   (a) Some two of acquaintances of x, say y & z know each other. Then {x, y, z} form a club.
   (b) No two acquaintances of x know each other. Then they form a group of strangers.
2. x has at most 2 acquaintances. There are at least 3 people that x does not know. Now the argument is in case 1 with acquaintances replaced by strangers.

6 Social Choice Function

6.1 Definition

3 candidates A, B & C:

- 49% of electorate $A > B > C$
- 48 % of electorate $B > A > C$
- 3% of electorate $C > B > A$

Given a collection of voters $v_1, v_2, ..., v_n$ and several candidates A, B, C, D, ...

Each voter ranks the candidates according to his preferences:

$A >^{v_2} B >^{v_2} C >^{v_2} D$ where $>^{v_i}$ is the ordering produced by the i^{th} voter

Permutation (A, D, B, C) of the set of candidates {A, B, C, D }

Social choice function takes as an input voter's ordering and produces a consensus ordering $f(>^{v_1}, >^{v_2}, , ..., >^{v_n}) = \ >$

What conditions should a good SCF satisfy?

1. **Unanimity**: If every voter prefers α to β then the consensus ordering must rank α above β $(\forall v \quad (\alpha >^v \beta)) \rightarrow (\alpha > \beta)$
2. **Independence on irrelevant alternatives (IAA)** The final relative ordering of α and β (higher, lower or indifferent) should depend only on relative orderings of α and β by every individual (If a candidate withdraws from election this doesn't affect the order of others).

Which social choice functions satisfy these properties?

What happens with majority? $\alpha > \beta$ if more than half of the voters prefer α to β:

- $v_1 : A >^{v_1} B >^{v_1} C$
- $v_2 : C >^{v_2} A >^{v_2} B$
- $v_3 : B >^{v_3} C >^{v_3} A$

How does this work? There is a conflict here...

Dictatorship: For some fixed voter d we have $(\alpha > \beta)$ if and only if $(\alpha >^d \beta)$ i.e. society prefers α to β whenever d strictly prefers α to β

6.2 Arrow's impossibility Theorem (1951)

Theorem: Any constitution that respects independence of irrelevant alternatives and unanimity is a dictatorship.

Proof Unanimity $\wedge$ IIA $\rightarrow$ dictatorship

Let $>$ satisfy these two properties β is called a polarizing candidate if every voter ranks him.her at the very top or the very bottom of the list.

Claim A polarizing candidate ranks first or last in the consensus ordering $>$

Proof Suppose not $\alpha > \beta > \gamma$ where β is a polarizing candidate

$$\left|\begin{array}{c|c|c|c} \beta & \beta & \alpha & \gamma \\ \alpha & \gamma & \gamma & \alpha \\ \gamma & \alpha & \beta & \beta \end{array}\right|$$

Switch α and γ in voter's preferences so that every voter prefers γ to α. We should still have $\alpha > \beta > \gamma$ because relative positions of α and β and relative positions of β and γ are unchanged. By unanimity we should now have $\gamma > \alpha$ (contradiction QED)

Choose a candidate β

$$\left|\begin{array}{c|c|c|c} \beta & \beta & \alpha & \gamma \\ \alpha & \gamma & \gamma & \alpha \\ \beta & \beta & ... & \beta \\ v_1 & v_2 & ... & v_n \end{array}\right| \rightarrow \left|\begin{array}{c|c|c|c} \beta & - & - & - \\ \alpha & \gamma & \gamma & \alpha \\ - & \beta & ... & \beta \\ v_1 & v_2 & ... & v_n \end{array}\right|$$

So there exists a voter v^* so that $\left|\begin{array}{c|c|c|c} \beta & - & - & - \\ \alpha & \gamma & \gamma & \alpha \\ - & \beta & ... & \beta \\ v_1 & v_2 & ... & v_n \end{array}\right|$

Goddammit. Disregard this last section (the whole theorem). I will fix it later.

7 Proofs

7.1 The well-ordering principle

- **The well-ordering principle**
  Every non empty subset of non-negative integers has a smallest element.
- **The induction principle**
  "P(n) is true for all natural numbers b"

7.1.1 Proofs using the well-ordering principle

Claim There exists subsets of non-negative rational numbers with no smallest element.

$\{x \in \mathbb{Q} | x > 1\}$ ($\mathbb{Q}$ is the set of rational numbers}

Suppose $x_0 < x_1$, $x_0 \in \mathbb{Q}$ is a smallest element of this set $x_0 = \frac{m}{n} \quad m > n$

(missed)

Proving the irrationality of $\sqrt{2}$

- **Theorem** $\sqrt{2}$ is irrational.
- **Proof** Suppose $\sqrt{2}$ is rational (Proof by contradiction)
  $c = \{m \in \mathbb{N} | \exists n \in \mathbb{N}(\sqrt{2} = m/n)\}$
  Our assumption is equivalent to the statement $C \neq \emptyset$
  By the well-ordering principle there exists m_0 the smallest element of C
  $\sqrt{2} = \frac{m_0}{n_0} \rightarrow 2 = \frac{m_0^2}{n_0^2} \rightarrow 2n_0^2 = m_0^2 \rightarrow m_0 = 2m' \rightarrow 2n_0^2 = 4m'^2 \rightarrow n_0^2 = 2m'^2 \rightarrow n_0 = 2n' \rightarrow (2n')^2 = 2m'^2 \rightarrow 2n'^2 = m'^2 \rightarrow \sqrt{2}n' = m' \rightarrow \sqrt{2} = \frac{m'}{n'} \rightarrow m \in C$ but $m' < m_0$

- There is a contradiction as m_0 was chosen to be the smallest element of C.

7.1.2 Method

Structure of the proofs using well-ordering principle:
"P(n) is true for all positive integeres n" (In our theorem P(m) := "$\neg(\exists n \in \mathbb{N} \quad \sqrt{2} = \frac{m}{n}$)"

1. $C = \{n \in \mathbb{N} |$ P(n) is False $\}$
2. Assume for a contradiction that $C \neq \emptyset$
3. By the well-ordering principle we can choose n_0 the smallest element of C
4. Obtain the contradiction to this choice (for example show that $n_0 \notin C$)

Theorem Every positive integer bigger than 1 can be expressed as a product of prime numbers (being prime counts).

Statement P(n) = "If n ¿ 1, then n can be expressed as product of prime numbers

C = $\{n \in \mathbb{N} : n > 1$ n can be expressed as such a product$\}$

Choose n_0 to be a smallest element of C (We are using proof by contradiction)

- Case 1: n_0 is prime
  This can't happen. n_0 by itself would be a valid product
- Case 2: n_0 is not prime
  $n_0 = ab \qquad 1 < a, b < n_0 \qquad a, b \in \mathbb{N}$
  Therefore as $a, b \notin C$, so $a = p_1p_2p_3...p_k \quad p_i$ is prime and $b = q_1q_2...q_i \quad q_j$ is prime
  $n = p_1p_2p_3...p_k.q_1q_2q_3...q_k$ So n is a product of primes
  $n \notin C \rightarrow$ contradiction

What is the sum of the first n odd (+) integers? 1 + 3+ 5 +... + (2n-1)

$$1 = 11 + 3 \qquad = 41 + 3 + 5 = 91 + 3 + 5 + 7 \qquad = 16$$

It looks like the answer is n^2 (but this is not enough to prove it)

Theorem: $1 + 3 + 5 + 7 + ... + (2n - 1) = n^2$

Proof: Suppose for a contradiction that n_0 is the smallest positive integer for which this formula is false

$1 + 3 + 5 + ... + 2n - 1 \neq n_0$

The formula is true for $n_0 - 1 \qquad (n_0 \neq 1)$

$1 + 3 + 5 + ... + 2(n_0 - 1) - 1 = (n_0 - 1)^2$

So $1 + 3 + 5 + ... + (2n - 1) = (n_0 - 1)^2 + 2n_0 - 1 = n_0^2 \rightarrow$ contradiction!

7.2 Induction

Method "P(n) is true for all n $\in \mathbb{N}$ if

1. Base of induction: "P(1) is true"
2. Induction steps: "P(n-1) implies P(n) for all $n \geq 2$
   (Equivalently "P(n) implies P(n+1) for all $n \geq 1$"

7.2.1 A few examples

Sum of n first Integers

- **Theorem**: $1 + 2 + ... + n = \frac{n(n+1)}{2}$
- **Proof**: By induction on n
- **Base case n =1**: $1 = \frac{1}{1+1}/2 = 1$
- **Induction step:** $P(n) \rightarrow P(n+1) for n \geq 1$
  $1+2+...+n = \frac{n(n+1)}{2}$ $P(n+1) : 1+2+...+n+(n+1) = \frac{n(n+1)}{2} + (n+1) = (n+1)\cdot(\frac{n}{2}+1) = \frac{(n+1)\cdot(n+2)}{2}\square$

$2^n \geq n^2$

- **Theorem**: $2^n \geq n^2 \forall n \geq 4$
- Base case: $n = 4, 2^4 = 16 = 4^2$
- Induction step: $(2^n \geq n^2) \rightarrow (2^{n+1} \geq (n+1)^2)$

$$\begin{aligned} 2^{n+1} &= 2^n \cdot 2 \\ &\geq 2n^2 = n^2 + n^2 \\ &\geq n^2 + 4n \qquad (n \geq 4) \\ &\geq n^2 + 2n + 1 = (n+1)^2 \qquad (2n \geq 1) \end{aligned}$$

A flawed induction proof

- Theorem: All horses are the same colour
- Base Case: One horse is the same colour as its self
- Induction step: Any n horse are the same colour. Any n + 1 horses are the same colour.

Flaw: P(n) does not imply P(n+1)

8 Number Theory

Definition Studies properties of integers: divisibility, primes. an integer a divides an integer b if $(\exists x \in \mathbb{Z} : \quad (xa = b)$

Division with remainder: for any two integers $a > 0$ and b there exists integers q and d so that $b = qa + r \rightarrow$ r is the remainder with $0 \leq r \leq a$

We write $a|b$, if and only if $r = 0$

A positive integer $p > 1$ is prime if the only positive integers dividing p are 1 and p

An integer $n > 1$ is composite if it is not prime

Expression of a positive integer as product of primes is called prime factorization.

The fundamental theorem of arithmetic Every integer greater than 1 admits unique prime factorization

Proof using contradiction: Suppose some n admits at least two distinct prime factorizations. Choose the minimum such n.

$n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_k = q_1 \cdot q_2 \cdot ... \cdot q_l$

We may assume that p_1 is the smallest prime among all the primes p_i and q_j

Suppose $p_1 = q_1$ then $\frac{n}{p_i} = p_2 \cdot ... \cdot p_k = q_2 \cdot ... \cdot q_l$

It is a smaller number admitting two different factorizations

$p_1 < q_1$ so $q1 = xp_1 + r \qquad 0 \leq r \leq p_1$

$n = (xp_1 + r)q_2...q_i$ also we may assume $q_2, q_3, ...q_l \neq p_1$

$p_1|n$

$n = xp_1 \cdot q_2 \cdot ... \cdot q_l + r \cdot q_2 \cdot .... \cdot q_l$

n is divisible by p_1

$n > m > 1 \qquad m = r \cdot q_2...q_l$ is divisible by p_1

$m < n$ as $x > 0$ because $q_1 > p_1 > r$

We will sow that m also has two different prime factorizations

$m = p_1 m = p_1 r_1 r_2 ... r_s \rightarrow$ there exists a prime factorization of m which includes

A contradiction to the choice of..

(missed)

8.1 Primes

Fundamental theorem of arithmetic Every integer greater than 1 can be uniquely expressed as a product of primes

$a = p_1^{r1} p_2^{r_2} ... p_k^{r_k} \;\; b = p_1^{s_1} p_2^{s_2} ... p_k^{s_k}$

$1200 = 2^4 \cdot 3 \cdot 5^2$

$[ab = p_1^{r_1+s_1} p_2^{r_2+s_2} ... p_k^{r_k+s_k}]$

$a|b$ if and only if $r_i \leq s_i$ for all $1 \leq i \leq k$

- **Theorem** $\sqrt{2}$ is irrational

- **Proof**: Suppose $\sqrt{2}$ is not
  then $\sqrt{2} = \frac{m}{n} = 2 = \frac{m^2}{n^2}$
  $(m = 2^r p_1^{r_1} \dots p_k^{r_k})$
  $(n = 2^s p_1^{s_1} \dots p_k^{s_k})$
  $(2n^2 = m^2)$
  $(2n^2 = 2^{2s+1} p_1^{2s_1} \dots p_k^{2s_k})$
  $(m^2 = 2^{2r} p_1^{2r_1} \dots p_k^{2r_k})$
  Contradiction as $(2s + 1 \neq 2r)$
- **Theorem:** $\sqrt{n}$ is rational for any integer n if and only if $n = k^2$ for some k

Proof: Exercise. Modify the proof for $\sqrt{2}$

- **Theorem**: If a prime $p|ab$ then either $p|a$ or $p|b$
- **Proof**: if p is not present in the prime factorization of either a or b, then it is not present in the prime factorization of $a \cdot b$ and so $p \nmid ab$
- Is this true when p is not prime? Suppose we have $p_1 \cdot p_2$ instead of p_1 then $p_1|a$ or $p_1|b$ $p_2|1$ or $p_2|b$

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$

1. There are infinitely many prime numbers.
2. Prime numbers are not everywhere dense in natural numbers. There are large gaps

- **Theorem** For any positive integer k there exists two consecutive prime numbers with difference $\geq k$
- **Proof** It suffices to exhibit a sequence of $\geq k$ consecutive composite numbers
  $n! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \dots \cdot (n-1) \cdot n$
  Let $n = k + 1$
  $n! + 2, n! + 3, n! + 4, n! + 5, \dots, n! + n \to k$ consecutive integers all composite
  $n! + m$ is composite for all $2 \leq m \leq n$ $m|n! + m \leftarrow m|n!$ $2 \leq m \leq n! + m$
- **Twin prime conjecture** There exist infinitely many pairs $p, p+2$ so that they are both primes. (This question has been asked more than 2000 years ago.)
- **The prime number theorem:** For a number n let $\pi(n)$ denote the number of primes $\leq n$. Then
  $\pi(n) \cong \frac{n}{\ln n}$ $lim_{n\to\infty} \frac{\pi(n)}{n/\ln n} = 1$
  Average gaps between primes are $\cong \ln n$
- **Conjecture** For every positive integer n there exists a prime p $n^2 \leq p \leq (n+1)^2$

1. It is possible to efficiently test whether a number is prime or composite.
2. It is believed not to be possible to efficiently produce prime factorisations.

8.2 Greatest common divisors and linear combinations

Die Hard 3 Problem A jug containing precisely 4 gallons of water deactivates the bomb. He has a 3 gallon, a 5 gallon jug and 5 minutes. Given an a-gallon jug and a b-gallon jug, what ammounts can we get?

$a \leq b$ let (x,y) record current amounts of water in jugs of size a and b respectively

Here is an example of our approach

1. (a,0) - fill in the first jug
2. (0,a) - pour first jug into the second
3. (a,a) - fill in the first one again
4. (2a-b, b) - pour first into second
5. (2a-b, 0) - empty the second jug
6. (0, 2a-b)
7. (a, 2a-b)
8. (0, 3a-b) $\rightarrow$ John Mclane survives $3 \cdot 3 - 5 = 4$!

8.3 Linear Combinations

- A linear combination of a and b is an integer expressible as $sa + tb$ where both s and t are integers.
- **Claim 1** The amounts of water in jugs are always linear combinations of a and b.
  (By induction on the number of operations performed)

- **Question:** Which numbers can we express as linear combinations of a and b?

Theorem The amount of water in jugs is always a linear combination of a and b.

Let $L = \{m : m = sa + tb$ for some $s, t \in \mathbb{Z}$

1. $0, a, b \in L$ $0 = o \cdot a + 0 \cdot b$ $a = 1 \cdot a + 0 \cdot b$
2. $j_1, j_2 \in L$ then $j_1 + j_2 \in L, -j \in L$

Proof By induction on # steps performed

- Base case (0 steps): $(0, 0)$ $0 \in L$
- Induction step: Assume that after n steps we have amounts j_1, j_2 and $j_1, j_2 \in L$. we want to show that after the next step the amounts are still a linear combination.
  $(j_1, j_2) \rightarrow (0, j_2)$ or $(j_1, 0)$ or (a, j_2) or (j_1, b) or $(0, j_1 + j_2)$ or $(j_1 + j_2, 0)$ or $(j_1 + j_2 - b, b)$ or $(a, j_1 + j_2 - a)$
  $j_1 + j_2 - b \in L$ and $j_1 + j_2 - a$
- Theorem If $a \leq b$, $c \leq b$. Then if c is a linear combination of a and b, it is possible to measure exactly c liters.
- Proof: $c = sa + tb$ for some $s, t \in \mathbb{Z}$
  - Case 1: $c = b$
  - Case 2: $c < b$ We may assume that $s > 0, t \leq 0$
    $c = (s + kb)a + (t - ka)b = sa + tb + kba - kab$
    Choose k large so that $s + kb > 0$
    $c = sa - tb \rightarrow$ fill in the jug with capacity a s times repeatedly and pour it into a jug with capacity b as soon as the jug with capacity b becomes full pour it out
    $sa = t'b + c'$
    $sa = tb + c$

$0 \leq c, c' < b$
$c' = sa - t'b \rightarrow$ amount we poured out
$s \rightarrow$ total amount we took
In the end we have amounts $(0, c')$
Example:
$b = 5, a = 3, c = 4$
$4 = 3 \times 3 - 5$
$(0,0) \rightarrow (3,0) \rightarrow (0,3) \rightarrow (3,3) \rightarrow (1,5) \rightarrow (1,0) \rightarrow (0,1) \rightarrow (3,1) \rightarrow (0,4)$
There are many more ways to achieve the same result.

What about $b = 6, a = 3, c = 4$ Do there exist integers s and t such as 3s + 6t = 4? d is a common divisor of a and b if d — a and d—b

Definition If d is a **common divisor** of a & b then every linear combination of a & b is divisible by d.

The largest common divisor of a and b is denoted by gcd(a, b) and is called the **greatest common divisor**.

Theorem $gcd(a, b)$ is the smallest positive linear combination of a and b.

Proof $d = gcd(a, b)$, let m be the smallest positive linear combination of an and b
$m = sa + tb$. We want to show that d = m.

1. $d \leq m$
   $d|m$ Because d is a common divisor of a and b and m is a linear combination
   $d \leq m$ as they are both positive
2. $m \leq d$
   It is enough to show that m is a common divisor of a and b.
   We'll show $m|a$ (showing $m|b$ is exactly the same).
   Proof:
   - Suppose not $m \nmid a$ dividing with remainder
     $a = qm + r \qquad 0 < r < m$ ($r \neq 0$ because $m \nmid a$)
   - $r = a - qsa - qtb = a(1 - qs) + (-qt)b$
   - r is a linear combination of a & b, contradicting the choice of m.

Corollary An integer c is a linear combination of a and b if and only if gcd(a,b) — c
Proof:

- If $c = sa + tb$ then $gcd(a, b)|sa$ and $gcd(a, b)|tb$ so $gcd(a, b)|c$
- On the other hand, we know $gcd(a, b) = s'a + t'b$ for some $s', t' \in \mathbb{Z}$
- If $c = dgcd(a, b) then c = d(s'a + t'b) = (ds')a + (dt')b$

Midterm information

- **Material**:
  1. Logic and Proofs
  2. Number theory (up to modular arithmetic at the end of the week)

8.4 Greatest common divisors

Let a and b be positive integers. $c = gcd(a, b)$ is the largest integer c such as $c|a$ & $c|b$.

- **Theorem**:gcd(a, b) is the smallest positive linear combination of a & b.
- **Corollary**: c is a linear combination of a & b if and only if $gcd(a, b)|c$
- **Theorem**:
  1. $gcd(a, b)$ is divisible by every common divisor of a & b
  2. $gcd(ka, kb) = k \cdot gcd(a, b)$ for any positive integer k
  3. $gcd(a, b) = 1, \quad gcd(a, c) = 1 \rightarrow gcd(a, bc) = 1$
     If a and b do not have a common divisor and a and c do not have a common divisor then a and bc do not have anything in common either.
  4. $gcd(a, b) = 1, a|bc \rightarrow a|c$
  5. $a = qb + r \rightarrow gcd(a, b) = gcd(b, r)$

Proof of 3 $s_1a + t_1b = 1 \qquad s_2a + t_2c = 1$

It suffices to show that 1 is a linear combination of a and bc.

$1 = (s_1 \cdot a + t_1 \cdot b)(s_2 \cdot a + t_2 \cdot c) = a(s_1 \cdot s_2 \cdot a + s_1 \cdot t_2 \cdot c + s_2 \cdot t_1 \cdot b) + bc(t_1 \cdot t_2 \qquad)$ (can also be derived from prime decomposition)

Proof of 5 $d_1 = gcd(a, b) \qquad d_2 = gcd(b, r)$

- $d_1 \leq d_2$ It is enough to show that $d_1|b$ and $d_1|r$
  $d_1|b$ is trivial since d_1 is gcd(a, b)
  $r = a - qb$ a is divisble by d_1 and b is divisible by d_1 therefore d_1 divides r
- $d_2 \leq d_1$ It is enough to show that $d_2|a$ and $d_2|b$
  $d_2|b$ is trivial
  $a = r + qb$ since d_2 is a divisor of r and b then d_2 is a linear combination of r and b and $d_2|a$

9 Euclid's algorithm

9.1 Computing gcd with prime factorization

- $a = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{r_k}$
- $b = p_1^{s_1} \cdot p_2^{s_2} ... p_k^{s_k} = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{s_k}$
- $gcd(a, b) = p_1^{min(r_1, s_1)} \cdot p_2^{min(r_2, s_2)} ... p_k^{min(r_k, s_k)}$

- **Example**: $1200 = 2^4 \cdot 3 \cdot 5^2$
- $280 = 2^3 \cdot 5 \cdot 7$ $a = p_1^{r_1} \cdot p_2^{r_2} ... p_k^{s_k} =$
- $gcd(1200, 280) = 2^3 \cdot 5 = 40$

9.2 Computing gcd with Euclid's algorithm

$a = qb + r$ $\quad gcd(a, b) = gcd(b, r)$
$gcd(962, 230) = \quad 962 = 4 \cdot 230 + 42$
$gcd(230, 42) = \quad 230 = 5 \cdot 42 + 20$
$gcd(42, 20) = \quad 42 = 20 \cdot +2$
$gcd(20, 2) =$
2

9.3 Statement of Euclid's algorithm

GCD(a, b)
Input: integers a & b (in binary)
Steps:

1. $a \geq b$
2. Divide with remainder $a = qb + r, 0 \leq r < b$
3. $If r = 0 \rightarrow$ **output** : b
4. Otherwise, run GCD(b,r)

9.4 Analysis of Euclid's algorithm

1. It is valid by part 5 of the preceding theorem ($a = qb + r \rightarrow gcd(a, b) = gcd(b, r)$)
2. It terminates in at most a + b $\rightarrow$ in each recursive step we replace a by r.
   So the sum of the inputs decreases.
3. Is it efficient (polytime)?
   We want to show that it terminates in $O((loga + logb)^k)$
   - **Claim**: $a = qb + r \quad 0 \leq r \leq b, a \geq b$ then $ab \geq 2br$
   - **Proof**: We need to show that $a \geq 2r$
     $q \geq 1 \rightarrow a \geq b + r \rightarrow a \geq r + r = 2r$
   - The claim implies that the product of the inputs is reduced by at least a factor of 2 in each step.
     So there are at most $\log(ab)$ steps in recursion
     $\log(ab) = \log a + \log b \rightarrow$ **linear algorithm**

9.5 Expressing gcd(a,b) as a linear combination of a & b

$gcd(962, 230) = \quad 962 = 4 \cdot 230 + 42$
$gcd(230, 42) = \quad 230 = 5 \cdot 42 + 20$

$gcd(42, 20) =$ $42 = 20 \cdot +2$
$gcd(20, 2) =$
2

$$\begin{aligned} 2 &= 42 - 2 \cdot 20 \\ &= 42 - 2 \cdot (230 - 5 \cdot 42) \\ &= 11 \cdot 42 - 2 \cdot 230 \\ &= 11 \cdot (962 - 4 \cdot 230) - 2 \cdot 230 \\ &= 11 \cdot 962 - 46 \cdot 230 \end{aligned}$$

Wesley's notes. Will format later.

== Euclid's Algorithm ==

The algorithm takes at most <> iterations to terminate.

Each individual step can also be performed quickly. (Division with remainder)

Arithmetic operations: additions, multiplication, division with remainder take time polynomial in input

Input is usually in binary.

=== Adding ===

<>

<>

<>

Adding a & b takes <>

=== Multiplication ===

Multiplication is similar. At most <>

=== Division ===

Division with remainder can also be done efficiently

Each individual step can also be performed quickly. (Division with remainder)

Aritmetic operations addition, multiplication, division with remainder take time polynomial in input si

9.6 Homework problem

:

Show that deciding whether $ax^2 + by = c$ has an integer solution for given $a, b \leq c$ in NP.

Size of the input; $log_2 a + log_2 b + log_2 c$

Certificate $x\&y$ exist such that $ax^2 + by = c$.

Essence of the problem : If there exists x & y which solve the solution, then there exist some x_0, y_0 so that $ax_0^2 + b \cdot y_0 = c$ and x_0 and y_0 are not too large

With x_0 and y_0 of polynomial size of some power of fixed size k

$x_0 and y_0 = O((a + b + c)^k)$

General diophantine equation : It is not always the case that a certificate is of reasonable size. Famous example:

$P(x_1, x_2, ..., x_k) = 0$ where P is polynomial with integer coefficients.

E.g. $x_1 x_2 x_3 - 5x_1 + 1000 = 0$

Not in NP in general, there is no systemic algorithm to figure out if it has a solution or not.

Back to Euclid Euclid's algorithm takes at most $log_2 a + log_2 b$ steps (but maybe it always terminates in 5 or $\log(\log a)$

In worst case scenario is takes $\Omega(log_2 a + log_2 b)$ steps

Example: Fibonacci numbers: $F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3$

1, 1, 2, 3, 5, 8, 13, 21 $\rightarrow F_n = F_{n-1} + F_{n-2}$

Running Euclid's algorithm to compute $gcd(F_n, F_n + 1)$

$F_n = F_{n-1} + F_{n-2}$

$F_{n-1} = F_{n-2} + F_{n-3}$

$F_n = 1 + \sqrt{5}/2^{n+1}/\sqrt{5}$

10 Modular arithmetic

10.1 Notation

We say that a is **congruent** to b **modulo** m if $m|a - b$. We note it $a \equiv b(mod m)$

$rem(a, m)$: the remainder of a after division by m

$a = km + rem(a, m)$

$0 \leq rem(a, m) < m$

Fact: $a \equiv b(mod m)$ if and only if $rem(a, m) = rem(b, m)$ **Proof**: $a = k_1 m + rem(a, m)$

$b = k_2 m + rem(b, m)$

$0 \leq rem(a, m), rem(b, m) < m$

If $rem(a, m) = rem(b, m)$ then $a - b = (k_1 - k_2)m$. Therefore $a = b(mod m)$

$a - b = (k_1 - k_2)m + (rem(a, m) - rem(b, m)$

Therefore $rem(a, m) = rem(b, m) = 0$.

In many senses you can operate with congruences as with equations.

Theorem: (Properties of congruences)

1. **Reflexitivity** $a \equiv a(\mod m)$
2. **Symmetry** $a \equiv b(\mod m)$ if and only if $b \equiv a(\mod m)$
3. **Transitivity** if $a \equiv b(\mod m) \quad \& \quad b \equiv c(\mod m)$ then $a \equiv c(\mod m)$

Suppose $a \equiv b(\mod m), c \equiv d(\mod m)$:

Then:

1. $a + b \equiv b + d(\mod m)$
2. $ac \equiv bd(\mod m)$

Proof:

- 1, 2, 3: is based on the preceding fact
- 3. If $rem(a, m) = rem(b, m)$ and $rem(b, m) = rem(c, m)$, then $rem(a, m) = rem(c, m)$.
- 4. $m|a - b$, $m|c - d$ therefore $m|(a - b) + (c - d) = (a + c) - (b + d)$

Reminder: Congruences $a \equiv b(modm)$ if $m|a - b$

1. $a \equiv b(modm)$ if and only if a and b have the same remainde after division by m
2. $a \equiv b(modm) \quad c \equiv d(modm)$ then
   $a + c \equiv b + d(modm)$
   $a \cdot c \equiv b \cdot d(modm)$
   Proof: $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$
   Since $(a - b)$ and $(c - d)$ are divisible by m then $(ac - bd)$ is divisible by m

10.2 Multiplicative inverses

What about division for congruences? Turing's code:
Select p: a large prime number.
Let a message be represented by a number $0 \leq m \leq p$.
Choose a key k which also is going to be $0 \leq k \leq p$, transmit the remainder of mk after division by p.

$0 \leq m^* \leq p$
$m^* = m(modp)$

Two questions:

1. Can our counterpart decode m from p, m^*, k?
2. How vulnerable is this code? (How easy is it to figure out k?)

We say that $\bar{k}$ is a multiplicative inverse for k modulo p

$\bar{k} \cdot k = a(modp)$

If we have a multiplicative inverse, then we can decode m.

$$m^* \equiv mk(modp)$$
$$m^*\bar{k} \equiv m(k \cdot \bar{k}) \equiv m(modp)$$

So m is just the remainder of $m^*\bar{k}$ after division by p

Theorem If p is a prime, k is non divisible by p, then there exists a multiplicative inverse for k (mod p).

Proof: We want to find $\bar{k}$ such that:
$k\bar{k} - 1 = tp$
$k\bar{k} - tp = 1 \rightarrow$ linear combination of k and p equal to 1

We can find such $\bar{k}$ and t if and only if $gcd(k, p) = 1$.

Why is the greatest common divisor of k and p?

$gcd(k, p)|p$ so $gcd(k, p) = 1$ or $gcd(k, p) = p$ Second is impossible as $p \nmid k$

Example:

Find a multiplicative inverse for 10 modulo 17.

We need to express 1 as a linear combination of 10 and 17.

We use Euclid's algorithm:

$17 = 10 + 7$ (remainder of the division of 17 by 10)
$10 = 7 + 3$
$7 = 2 * 3 + 1$

We track-back to get:

$1 = 7 - 2 \cdot 3$
$1 = 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 2 \cdot 10$
$1 = 3 \cdot (17 - 10) - 2 \cdot 10 = 3 \cdot 17 - 5 \cdot 10$

-5 is a multiplicative inverse for 10
$-5 \equiv -5 + 17(mod17) \equiv 12(mod17)$

Decoding Turing's code :

$p = 17, k = 10, m = 3$
We send m^* remainder $3 \cdot 10 = 30$ after division by $17 \rightarrow 13$
Counterparty receives **13**.

$13 \cdot 12 = 156 = 17 \cdot 9 + 13$

Corollary If p is a prime,

$p + k$ $xk \equiv yk(modp)$ then $x \equiv (modp)$

Proof $(xk)\bar{k} \equiv (yk)\bar{k}(modp)$ where $\bar{k}$ is multiplicative

$x(k\bar{k}) \equiv y(k\bar{k})(modp)$

$x \equiv y(modp)$ Q.E.D.

If $p \neq 2$, $2x \equiv 2y(modp)$ then $x \equiv y$

Note: Cancellation does not work on modulo composite numbers.

- $2 \neq 0(mod4)$
- $2 \times 2 \equiv 0(mod4)$

10.3 Fermat's Little Theorem

Let p be a prime $p \nmid k$

then $k^{p-1} \equiv 1(modp)$. (e.g. 2^{1000} has remainder 1 after division by 101)

Proof: $1, 2, ..., p-1$ for every number i in this collection. Let r_i be the remainder of k_i after the division by p

$(r \equiv k_i(modp) \quad 0 \leq r_i < p$

We get a collection of members, $r_1, r_2, r_3, ..., r_{p-1}$.

- $1 \leq r_i \leq p-1$ because $p \nmid k_i$ for $i = 1, 2, ..., p-1$
- $r_i \neq r_j$ for $i \neq j$ $\quad$ $k_i \neq k_j$ for $i \neq j$ $\quad$ $i \leq i, j < p-1$
  So $r_1, r_2, ..., r_{p-1} = 1, 2, ..., p-1$ (perhaps in different order)
  $r_1, r_2, ..r_{p-1} = 1 \cdot 2 \cdot ... \cdot (p-1) = (p-1)!$ On the other hand, $r_i \equiv k_i(modp)$
  $(p-1)! = r_1, r_2, ..r_{p-1} \equiv (1 \cdot k)(2 \cdot k)(3 \cdot k)....(p-1)k = k^{p-1} \cdot (p-a)!$
  $(p-1)! = k^{p-1} \cdot (p-1)!(modp)$
  We can cancel (p-1)! as long as $p \nmid (p-1)!$
  The product of numbers all smaller than p. So none of them is divisible by p, therefore the product is not.
  Cancelling $(p-1)!$ gives the theorem.

Corollary: $k \cdot k^{p-2}$ is a multiplicative inverse for k modulo p if $p \nmid k$.

Fermat's test if $2m \nmid t^{m-1} - 1$ then m is composite or $m = 2$.

10.4 Side-Note: The proof on the midterm exam

$$gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right)$$

Incorrect proof:

You cannot just say $gcd(\frac{a}{gcd(a,b)}, b) = 1$, as it can be greater than 1.

If $a = 16$ and $b = 24$, then $gcd(\frac{16}{8}, 24) = 2$.

Proof 1:

For every positive integer k, $gcd(ka, kb) = k \cdot gcd(a, b)$

$gcd(a,b)gcd(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}) = gcd(\frac{gcd(a,b)\cdot a}{gcd(a,b)}, \frac{gcd(a,b)\cdot b}{gcd(a,b)}) = gcd(a,b)$

$\rightarrow gcd(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}) = 1$

Proof 2: By contradiction

Suppose $d = gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) > 1$

$d|gcd\left(\frac{a}{gcd(a,b)}\right) \qquad d|gcd\left(\frac{b}{gcd(a,b)}\right)$

$d \cdot gcd(a,b)|a \qquad d \cdot gcd(a,b)|b$

$d \cdot gcd(a,b)$ is a common divisor of $a\&b \rightarrow$ Contradiction ■

Proof 3

$a = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot ... \cdot {p_k}^{r_k}$

$b = {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot ... \cdot {p_k}^{s_k}$

$gcd(a,b) = {p_1}^{min(r_1,s_1)} \cdot {p_2}^{min(r_2,s_2)} \cdot ... \cdot {p_k}^{min(r_k,s_k)}$

$\frac{a}{gcd(a,b)} = {p_1}^{r_1-min(r_1,s_1)} \cdot {p_2}^{r_2-min(r_2,s_2)} \cdot ... \cdot {p_k}^{r_k-min(r_k,s_k)}$

$\frac{b}{gcd(a,b)} = {p_1}^{s_1-min(r_1,s_1)} \cdot {p_2}^{s_2-min(r_2,s_2)} \cdot ... \cdot {p_k}^{s_k-min(r_k,s_k)}$

$gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = p_1^{min(r_1-min(r_1,s_1),s_1-min(r_1,s_1))} \cdot ... \cdot p_k^{min(r_k-min(r_k,s_k),s_k-min(r_k,s_k))}$

$\forall(1 \le i \le k) \begin{cases} r_i \le s_i \rightarrow min(r_i - min(r_i,s_i), s_i - min(r_i,s_i)) = min(r_i - r_i, s_i - r_i) = min(0, s_i - r_i) = 0 \\ s_i \le r_i \rightarrow min(r_i - min(r_i,s_i), s_i - min(r_i,s_i)) = min(r_i - s_i, s_i - s_i) = min(r_i - s_i, 0) = 0 \end{cases}$

$gcd\left(\frac{a}{gcd(a,b)}, \frac{b}{gcd(a,b)}\right) = p_1^0 \cdot p_2^0 ... \cdot p_k^0 = 1$

10.5 Applications of Fermat's Little Theorem

Theorem: If p is prime, $p \nmid a$ then $a^{p-1} \not\equiv 1(mod p)$

Corollary: a^{p-2} is a multiplicative inverse for $a(mod p)$
(Our previous method computed multiplicative inverse for a by expressing 1 as a linear combination of $p\&a$.)

Example 1: Multiplicative inverse for 5 (modulo 17)

How can we compute $5^{15}(mod 17)$ quickly?

1. Let's first compute $5^5(mod 17)$:
   $5^2 = 25 \equiv 8(mod 17)$
   $5^4 = (5^2)^2 \equiv 8^2 = 64 = 3 \cdot 17 + 13 \equiv 13(mod 17)$
   $5^4 \cdot 5 = 13 \cdot 5 = 65 \equiv 14(mod 17) \qquad 5^5 = 5^4 \cdot 5 \equiv 135 = 65 \equiv 14(mod 17)$

2. Compute $(5^5)^3 = 14^3 (mod 17)$
   $14^3 \equiv (-3)^3 = -27 \equiv 10 \equiv 17 - 10 = 7 (mod 17)$

Conclusion: $7 \cdot 5 \equiv 1 (mod 17)$

Example 2: Compute $3^{100} (mod 7)$

$$3^6 \equiv 1 (mod 7)$$
$$(3^6)^k \equiv 1^k = 1 (mod 7)$$
$$100 = 6k + r = 6 \cdot 16 + 4$$
$$3^{6k+r} \equiv 1 \cdot 3^r = 3^r (mod 7)$$
$$3^100 \equiv 3^4 (mod 7) = 81 (mod 7) = 4 (mod 7)$$

Example 3: Compute $3^{100} (mod 21)$

$$3^{100} \equiv r (mod 21 = 7 \cdot 3) \rightarrow 0 \leq r < 21$$
$$21 | 3^100 - r \rightarrow 3 | r$$
$$r = 3s \rightarrow 0 \leq s \leq 6$$
$$3^{100} \equiv 3^4 \equiv 81 = 77 + 4 \equiv 4 (mod 7)$$
$$3^{100} \equiv r (mod 7)$$
$$r \equiv 4 (mod 7)$$
$$r = 3s \equiv 4 (mod 7)$$

$\rightarrow$ Solve $3s \equiv 4 (mod 7)$
Find multiplicative inverse for $3 (mod 7)$

$$3^5 \equiv (3^2)^3 \cdot 3 \equiv 9^2 \cdot 3 \equiv 2^2 \cdot 3 \equiv 42 \equiv 5 (mod 7)$$
$$s = 5 \cdot 3s \equiv 4 \cdot 5 = 20 \equiv 6 (mod 7)$$
$$s = 6$$

Answer: $3^{100} \equiv 3 \cdot 6 \equiv 18 (mod 21)$

In our computations, we implicitly relied on number,the fact that if we know the remainder of a number (3^100) modulo 3 and modulo 7, then we can compute the remainder modulo $3 \cdot 7 = 21$.

10.6 Testing primality

10.6.1 Fermat's test

Corollary: If $2^{n-1} \not\equiv 1 (mod n)$ then n is not prime or $n = 2$.

Algorithm: Fermat's test

---

1. Compute $2^{n-1}(mod n)$
2. If the remainder of $2^{n-1}(mod n)$ is not 1 (and $n \neq 2$), output "n is composite".

Issues with this algorithm:

1. We want to efficiently compute the remainder of $2^{n-1}(mod n)$
2. We don't have guarantees that this algorithm detects all composite numbers.
   In fact, $2^{560} \equiv 1(mod 561)$ and 561 is composite.

Questions:

1. Is this algorithm efficient (polytime)?
2. Does it recognize all composite numbers?

Answers

1. We can compute $2^{n-1}(mod n)$ (the remainder of 2^{n-1} after division by n) in time polynomial in $log_2 n$

   Procedure:

   (a) Write down binary representation of $n-1$
   $n-1:\quad n-1 = 2^{k_1} + 2^{k_2} + ...2^{k_r} \qquad k_1 > k_2 > ... > k_r$
   $2^{n-1} = 2^{2^{k_1}} \cdot 2^{2^{k_2}} \cdot ... \cdot 2^{2^{k_r}} \qquad k_1 \leq log_2 n, \quad r \leq log_2 n$

   (b) Computing 2^{2^k} quickly: $\rightarrow$ Using at most $O((\log_2 n)^3)$ elementary operations
   $2^{2 \cdot 2 \cdot 2 \cdot ... \cdot 2} = ((((2^2)^2)^2)^2)$
   Thus we can square a number efficiently (in time $\leq (log_2 n)^2$) and we need to repeat this procedure $k \in log_2 n$ time).
   (We work with congruence classes modulo n and so never perform arithmetic with numbers larger than n).
   This procedure takes time $\leq O(log_2 n^4)$.

   Example: Use Fermat's test for $n = 35$.

   Compute $2^{34}(mod\ 35)$

   $34 = 32 + 2$

   $2^{34}(mod\ 35) = 2^{32} \cdot 2^2 (mod\ 35) = 2^{2^5} \cdot 2^2 (mod\ 35)$

   $1:\quad 2^2 = \mathbf{4}(mod\ 35)$

   $2:\quad 4^2 = \mathbf{16}(mod\ 35)$

   $3:\quad 16^2 = 256 = 7 \cdot 35 + \mathbf{11}(mod\ 35)$

   $4:\quad 11^2 = 121 = 3 \cdot 35 + \mathbf{16}(mod\ 35)$

   $5:\quad 16^2 = 256 = \mathbf{11}(mod\ 35)$

   $2^{34} = 2^{32} \cdot 2^2 \equiv 11 \cdot 4 = 44 \equiv 9(mod\ 35)$

2. Fermat's test does not detect all composite numbers (example: $n = 561$)
   $2^{560} \equiv 1(mod\ 3 \cdot 11 \cdot 17 = 561) for all a : gcd(a, 561) = 1$
   $3 \cdot 11 \cdot 17 | 2^{560} - 1 \rightarrow 3 | 2^{560} - 1 \qquad 11 | 2^{560} - 1 \qquad 17 | 2^{560} - 1$
   $2^{560} \equiv 1(mod\ 3)$
   $2^{10} = 1(mod\ 11)$
   $2^{560} = 2^{10 \cdot 56} = (2^{10})^{56} \equiv 1^{56} = 1(mod\ 11) 2^{16} \equiv 1(mod 17)$

$2^{560} \equiv 2^{16 \cdot 35} \equiv 1^{35} = 1(mod\ 17)$
$\rightarrow a^{560} \equiv 1(mod\ 3 \cdot 11 \cdot 17 = 561)$
A number n with the property that n is composite but $a^{n-1} \equiv 1(mod\ n)$ for all a such that $gcd(a, n) = 1$ is called a **Carmichael number**. There are infinitely many of such numbers.

10.6.2 Miller-Rabin's test

Definition Miller-Rabin's test is an improvement of Fermat's test

if $n-1$ is even test if $n \mid a^{\frac{n-1}{2}} - 1$ or $n \mid a^{\frac{n-1}{2}} + 1$

if $\dfrac{n-1}{2}$ is even instead of working with $a^{\frac{n-1}{2}} - 1$ repeat the procedure again.

If none of the terms in the factorization is divisible by n $\rightarrow$ n is composite.

Example:

$$\begin{aligned} 561 | a^{560} - 1 &= (a^{280})^2 - 1 = (a^{280} - 1)(a^{280} + 1) \\ &= ((a^{140})^2 - 1)(a^{280} + 1) = (a^{140} - 1)(a^{140} + 1)(a^{280} + 1) \\ &= (a^{70} - 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1) \\ &= (a^{35} - 1)(a^{35} + 1)(a^{70} + 1)(a^{140} + 1)(a^{280} + 1) \end{aligned}$$

For $a = 2$, none of the factors is divisible by 561.

At least $\frac{3}{4}$ of all numbers $2 \leq a \leq n$ work for Miller-Rabin's test.

Performing the test once has probability $\dfrac{3}{4}$ of success, but performing the test twice has probability of failure $1 - (\frac{1}{4})^2$. More generally, performing the test k times has probability of failure $(\frac{1}{4})^k$

Probabilistic algorithms$\leftarrow$ typically easy to implement.

If Generalized Riemann's Hypothesis is true, then testing all numbers a between 1 and $c(\log n)^2$ always works.