Discrete Math

Arnav Patri

September 15, 2022

Contents

Chapter 4

Number Theory and Cryptography

4.2 Integer Representations and Algorithms

Definition of a Number A number is dependent on a given base and its place value and digits.

4.2.2 Representations of Integers

A base b has $b-1$ digits. The first digit from the right is multiplied by b^0, the second by b^1, and so on. The number itself is the sum of each digit multiplied by b raised to the power of its respective place value.
0 is a member of every base (except sometimes base 1).

Let b be an integer greater than 1. If b is an integer greater than 1 and n is positive, then n can be expressed uniquely in the form

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

A number in base b is denoted by $(n)_b$.

A number is a linear combination of its digits and their place values.

Constructing Base b Expansions Given an integer n to be represented in base b,

$$
\begin{aligned}
&q := n \\
&k := 0 \\
&\text{while } q \neq 0 \\
&\qquad a := a \bmod b \\
&\qquad q := q \operatorname{div} b \\
&\qquad k := k + 1 \\
&\text{return } (a_{k-1}, \ldots, a_1, a_0)\{(a_{k-1} \ldots a_1 a_0)_b \text{ is the base } b \text{ expansion of } n\}
\end{aligned}
$$

A number in its own base is always represented as 10.
Addition and multiplication in base b follows the same conventions as that of base 10.

To add two numbers a and b in base 2, their rightmost bits a_0 and b_0 can be added such that

$$a_0 + b_0 = 2c_0 + s_0$$

where s_0 is s_0 is the rightmost bit of the binary expansion of the sum and c_0 is the **carry**, being either 0 or 1. This process can be repeated.

$$c_0 = \frac{a_0 + b_0 - s_0}{2}$$

4.3 Primes and Greatest Common Divisors

4.3.2 Primes

A **prime number** is a whole number whose only factors are 1 and itself. By definition, it does not appear on the multiplication table. A nonprime positive integer is called **composite**

The Fundamental Theorem of Arithmetic Every integer greater greater than 1 can be written uniquely as the the product of one or more primes.

Two numbers are relatively prime or coprime if their greatest common factor (GCF) is 1.
If n is divisible by a and b, then it is also divisible by $a \times b$.

4.1 Divisibility and Modular Arithmetic

4.1.2 Division

If a and b are nonzero integers such that $\frac{b}{a}$ is an integer, it is said that *a factor/divisor* of b and that b is a multiple of a. This is denoted as $a \mid b$. If a is not a factor of b, it is denoted as $a \nmid b$.

Let a, b, and c be nonzero integers.

1. If $a \mid b$ and $b \mid c$, then $a \mid (b + c)$.
2. If $a \mid b$, then $a \mid bc$ for any integer c.
3. If $a \mid b$ and $b \mid c$, then $a \mid c$.

4.1.3 The Division Algorithm

The Division Algorithm Let a and b be integers, the latter of which is positive. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

In this equality, d is called the *divisor*, a the *dividend*, q the *quotient*, and r the *remainder*. The notation used is

$$q = a \operatorname{div} d \qquad r = a \bmod d$$

4.1.4 Modular Arithmetic

If a and b are integers and m is a positive integer, then a is *congruent* to b *modulo* m if $m \mid (a - b)$. The notation $a \equiv b \pmod{m}$ to denote this **congruence** in **modulo** m, m being the **modulus**. An incongruency is denoted $a \not\equiv b \pmod{m}$

$a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

Let m be a positive integer. a is congruent modulo m to b if there exists an integer k such that $a = b + km$.

Let m be a positive integer. If $a \equiv b$ and $c \equiv d$ modulo m, $a + c \equiv b + d$ and $ac = bd$ modulo m as well.

Divisibility Rules

7. If the difference between a 2 times a number's last digit and the rest of the number is divisible by 7 or 0, the number is as well. If the difference between a number's last digit multiplied by 5 and the rest of the numbers is divisible by 17 or 0, the number is divisible by 17.

19. If the sum of 2 times the last digit of a number and the rest of the digits is divisible by 19, the number is divisible by 19.

23. If the sum of 7 times the last digit of a number and the rest of the number is divisible by 23, then so is the number.

31. If the difference between 3 times the last digit of a number and the rest of the number is divisible by 31, then so is the number.

Chapter 6

Counting

6.1 The Basics of Counting

6.1.2 Basic Counting Principle

The Product Rule If a procedure can be decomposed into a sequence of two tasks, one with n_1 possible ways of being completed and another with n_2 ways, there are $n_1 n_2$ total ways to carry out the procedure.

The Sum Rule If a task can be completed either in one of n_1 ways or in one of $n_1 2$ ways, where there is no overlap between the sets of n_1 and n_2 ways, then there are $n_1 + n_2$ ways to complete the task.

6.1.3 The Subtraction Rule (Inclusion-Exclusion for Two Sets)

The Subtraction Rule If a task can be completed in either n_1 or n_2 ways, then the number of ways to do the task is $n_1 + n_2$ minus the number of ways that are shared between both.

The subtraction rule is also known as the **principle of exclusion principle**. For two sets A_1 and A_2,

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

This uses an exclusive or rather than an inclusive or.

6.1.4 The Division Rule

The Division Rule If a task can be done using a procedure that can be carried out n ways and exactly d of n ways correspond to every way, there are n/d ways to complete the task.

6.1.5 Tree Diagrams

Counting problems are often solvable using **tree diagrams**, which consist of a root, a number of branches leaving the root, possible further branches extending from them, and so on.

6.3 Permutations and Combinations

6.3.2 Permutations

A **permutation** of a set of distinct objects is an ordered arrangement of these objects. An ordered arrangement of a set of r distinct elements of a set is called an ***r*-permutation**.

If n is a positive integer and r is an integer within $[1, n]$, then there are

$$P(n,r) = {}_nC_r = n(n-1)(n-2)\cdots(n-r+1) = \prod_{i=0}^{r-1}[n-i]$$

r-permutations of a set with n distinct elements.

If n and r are integers with $0 \le r \le n$, then

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

6.3.3 Combinations

A **combination** is an unordered selection of objects. An unordered selection of r elements from a set is an ***r*-combination**

The number of r-combinations of a set of n elements, where n is a nonnegative integer and $0 \le r \le n$, is

$$C(n,r) = {}_nC_r = \frac{n!}{r!(n-r)!} = \binom{n}{r}$$

If n and r are nonnegative integers with $r \le n$,

$$C(n,r) = C(n, n-r)$$

6.4 Binomial Coefficients and Identities

6.4.2 The Binomial Theorem

The binomial theorem allows the coefficients of the terms of exponential powers of binomials to be found. A **binomial** expression is simply the sum of two terms.

The Binomial Theorem If x and y are variables and n is a nonnegative integer, then

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

If n is a nonnegative integer, then

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n \qquad \sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0 \qquad \sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$$

6.4.3 Pascal's Identity and Triangle

Pascal's Identity If n and k are positive integers such that $k \leq n$, then

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

6.4.4 Other Identities Involving Binomial Coefficients

Vandermonde's Identity If m, n, and r are nonnegative integers with $r \leq m, n$, then

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

If n is a nonnegative integer, then

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

If n and r are nonnegative integers such that $r \leq n$, then

$$\binom{n+1}{r+1} = \sum_{i=r}^{n} \binom{i}{r}$$

6.5 Generalized Permutations and Combinations

6.5.2 Permutations with Repetition

The number of r-permutations of a set of n elements with repetitions allowed is n^r.

6.5.3 Combinations with Repetition

The number of r-combinations of a set of n elements with repetitions allowed is $C(n+r-1, r) = C(n+r-1, n-1)$.

6.5.4 Permutations with Indistinguishable Objects

The number of distinct permutations of n objects, where n_1 are indistinguishable objects of type 1, n_2 are indistinguishable objects of type 2, …, and n_k are indistinguishable objects of type k is

$$\frac{n!}{n_1!n_2!\cdots n_k!} = \frac{n!}{\prod_{i=1}^{k} n_i!}$$

6.5.5 Distributing Objects into Boxes

The number of ways to distribution n distinguishable objects into k distinguishable boxes such that n_i objects are placed into box i is

$$\frac{n!}{n_1!n_2!\dots n_k!} = \frac{n!}{\prod_{i=1}^{k} n_i!}$$

The number of ways of placing n indistinguishable objects into k distinguishable boxes is equal to that of n-combinations of a set of k elements with repetition allowed, being $C(n+r-1, r$.
The number of ways to place n distinguishable objects into k indistinguishable boxes is equal to

$$\sum_{j=1}^{k} S(n,j) = \sum_{j=1}^{k} \left\{ {n \atop j} \right\} = \sum_{j=1}^{k} \frac{1}{j!} \sum_{i=0}^{j-1} (-1)^j \binom{j}{i} (j-i)^n$$

where $S(n,j)$ and $\left\{ {n \atop k} \right\}$ denote **Stirling numbers of the second kind**:

$$S(n,j) = \frac{1}{j!} \sum_{i=1}^{j-1} (-1)^i \binom{j}{i} (j-i)^n$$

Distributing n indistinguishable objects into k indistinguishable boxes is the same as writing n as the sum of at most k positive integers in nonincreasing order. If $a_1 + a_2 + \cdots + a_i = n$ where $a_1, a_2, \dots, a_i$ are descending positive integers, it is said that this list is a **partition** of the positive integer n into i positive integers. If $p_k(n)$ is the number of partitions of n into at most k positive integers, then there are $p_k(n)$ ways to sort n indistinguishable objects into k indistinguishable boxes. No simple closed formula for this number exists.

Chapter 5

Induction and Recursion

5.1 Mathematical Induction

5.1.2 Mathematical Induction

Mathematical induction[1] can be used to prove statements asserting that a propositional function $P(n)$ is true for all positive integers n.

Principle of Mathematical Induction In order to prove that $P(n)$ is true for all positive integers n, two steps must be completed:

1. The **basis step** must verify that $P(1)$ is true.
2. The **inductive step** must show that $P(k) \Rightarrow P(k+1)$ is true for all positive integers k.

To complete the inductive step, it is assumed that $P(k)$ is true for an arbitrary positive integer k and that this assumption guarantees that $P(k+1)$ is true as well. This assumption is called the **inductive hypothesis**.
The inductive step shows that $\forall k(P(k) \Rightarrow P(k+1))$ is true where the domain is $\mathbb{Z}^+$.
Expresses as a rule of inference, this proof technique can be written as

$$(P(1) \wedge \forall k(P(k) \Rightarrow P(k+1))) \Rightarrow \forall n P(n)$$

with the domain $\mathbb{Z}^+$.

[1] In logic, **deductive reasoning** uses inference to draw conclusions from premises while **inductive reasoning** draws conclusions that are supported by not ensured by the evidence. Mathematical proofs, including those that employ induction, are deductive.

5.1.5 Guidelines for Proofs by Mathematical Induction

Template for Proofs by Mathematical Induction

1. Express the statement to be proven in the form of "for all $n \geq b$, $P(n)$" for a fixed integer b.
2. Denote the basis step, showing that $P(b)$ is true.
3. Identify the inductive hypothesis in the form "Assume that $P(k)$ is true for an arbitrary fixed integer $k \geq b$".
4. State what must be proven under the assumption in order to prove the validity of the inductive hypothesis.
5. Prove the statement $P(k+1)$ under the assumption.
6. Identify the conclusion of the inductive step.
7. State the conclusion that "by mathematical induction, $P(n)$ is true for all integers n with $n \geq b$".

5.3 Recursive Definitions and Structural Induction

5.3.2 Recursively Defined Functions

A function with the set of nonnegative integers as its domain can be defined by a **basis step**, setting the value of the function at 0, and a **recursive step**, providing a rule for finding its value at an integer from its values at smaller integers. This describes a **recursive/inductive definition**. Recursively defined functions are **well-defined**, meaning that for every positive integer, the corresponding function value is unambiguously determined.

5.3.3 Recursively Defined Sets and Structures

Recursive definitions may include an **exclusion rule**, excluding all elements other than those specified by the basis step of those generated by the rule.

The set Σ^* of strings over the alphabet Σ is defined recursively as

1. $\lambda \in \Sigma^*$, where λ is an empty string.
2. If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$.

Concatenation, denoted by $\cdot$ is an operation by which two strings can be combined. It is defined as follows:

1. If $w \in \Sigma^*$, then $w \cdot \lambda = w$.
2. If $w_1, w_2 \in \Sigma^*$ and $x \in \Sigma$, then $w_1 \cdot w_2x = (w_1 \cdot w_2)x$

A *rooted tree* consists of a set of vertices containing a distinguished vertex known as the *root* and edges connecting the vertices. The set of all rooted trees can be defined as

1. A single vertex r is a rooted tree.
2. Suppose $T_1, T_2, \ldots, T_n$ are disjoint rooted trees with respective roots $r_1, r_2, \ldots, r_n$. The graph formed by adding a vertex from the root r, which is not part of any of the trees, to each of the roots is also a rooted tree.