Discrete Math

Arnav Patri

September 8, 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,

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

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 $a \times b$.

4.3.3 Trial Division

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

6.3 Permutations and Combinations

6.4 Binomial Coefficients

6.5 Generalized Permutations and Combinations