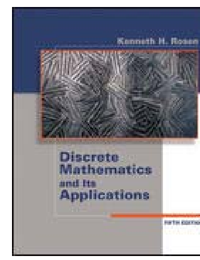
Chapter 2 (Part 1): The Fundamentals: Algorithms, the Integers & Matrices

- The Integers and Division (Section 2.4)



- Introduction
  - Review basics concepts of number theory
  - Divisibility, greatest common divisors, modular arithmetic
  - Computer arithmetic using binary expansions
  - Application to computer arithmetic, cryptology, secret messages

- Division

  – Definition 1:

If a and b are integers with $a \neq 0$, we say that a divides b if there is an integer c such that $b = ac$. When a divides b we say that a is a factor of b and that b is multiple of a. The notation $a \mid b$ denotes that a divides b. We write a b when a does not divide b

– Example :

$4 \mid 12$ 4 18

3 7, since $7 \mid 3$ is not an integer.

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

Solution: They are of the form {dk}, where k is a positive integer.

$$0 < dk \leq n \Leftrightarrow 0 < k \leq n/p$$

$\Leftrightarrow$ There are $\lfloor n/p \rfloor$ positive integers not exceeding n that are divisible by d.

– Theorem 1:

Let a, b and c be integers. Then

1. If $a|b$ and $a|c$, then $a \mid (b + c)$;
2. If $a|b$, then $a|bc$ $\forall c \in Z$;
3. If $a|b$ and $b|c$, then $a|c$

Proof: Suppose $a|b$ and $a|c \Rightarrow \exists\, s \in Z, \exists\, t \in Z$ such that: $b = as$ and $c = at$. Therefore:

$b + c = as + at = a(s + t)$; which means that $a \mid (b + c)$. This establishes part 1 of the theorem. Parts 2 and 3 are left to you! Q.E.D.

Corollary 1: if a, b and c are integers such that $a|b$ and $a|c$, then $a \mid mb + nc$ whenever m and n are integers.

Proof: Part 2 of theorem 1 shows that: $a \mid mb$ and $a \mid nc$ whenever m and n are integers. Using part 1 of the theorem $\Rightarrow a \mid mb + nc$. Q.E.D.

- Primes

  – Definition 2:

  > A positive integer p greater than 1 is called prime if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called composite.

  – Example: 7 is prime, 9 is composite.

  – Theorem 2:

  > The Fundamental Theorem of Arithmetic (FTA)
  > Every positive integer greater than 1 can be written in a unique way as a prime or as the product of two or more primes where the prime factors are written in a nondecreasing size

Example: $100 = 2.2.5.5 = 2^2.5^2$

$641 = 641$

$999 = 3.3.3.37 = 3^3.37$

$1024 = 2.2.2.2.2.2.2.2.2.2 = 2^{10}$

Large numbers are used for secret messages in cryptology.

– Theorem 3:

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

Proof: if n is composite, n has a factor such that: $1 < a < n$ and $\exists b \in Z$ such that: $n = ab$, where both a and b are positive integers greater than 1. Therefore $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$, since otherwise $ab > \sqrt{n} \,.\, \sqrt{n} = n \Rightarrow$ n has positive divisor $\leq \sqrt{n}$. This divisor is either prime or using the FTA, has a prime divisor. In either case, n has a prime divisor $\leq \sqrt{n}$.
Q.E.D.

Example: Prove that the integer 101 is prime.

Solution: Using the contrapositive form of theorem 3, states that :

"n has not a prime number divisor $\leq \sqrt{n} \Rightarrow$ n prime"

The only primes not exceeding $\sqrt{101}$ are {2, 3, 5, 7}, since these numbers do not divide 101 $\Rightarrow$ 101 is prime!

Q.E.D.

– Theorem 4:

$\boxed{\text{There are infinitely many primes.}}$

Proof: Let's assume there are only finitely many primes $p_1, p_2, \ldots, p_n$. Let $Q = p_1 p_2 \ldots p_n + 1$. Using FTA, Q is prime or Q can be written as the product of two or more primes. However, none of the primes p_j divides Q, (since $p_j | Q \Rightarrow p_j \mid (Q - p_1 p_2 \ldots p_n) = 1$ $\Rightarrow$ impossible since p_j prime) if none of the primes p_j divides $Q \Rightarrow Q$ is prime. $Q \neq P_j$ contradiction, because we assumed that we have listed all the primes. Q.E.D.

<u>Remark:</u> the largest prime known has been an integer of the form $2^p - 1$, where p is also prime (Mersenne primes.)

Example: $2^2 - 1 = 3$, $2^3 - 1 = 7$, $2^5 - 1 = 31$ are Mersenne primes, whereas $2^{11} - 1 = 2047$ is not a Mersenne prime since $2047 = 23 \, . \, 89$

<u>Remark:</u> the largest number known so far (year 2001) is

$2^{13,466,917} - 1$ (over four million digits!!!)

Visit GIMPS (Great Internet Mersenne Search)

– Theorem 5:

The Prime Number Theorem

The ratio of the number of primes not exceeding x and (x/lnx) approaches 1 as x grows without bound.

(Conjectured by Legendre & Gauss)

- The Division Algorithm

– Theorem 6:

The Division Algorithm

Let a be an integer and d a positive integer. Then $\exists!(q, r) \in Z^2; 0 \leq r < d: a = dq + r$.

– Definition 3:

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

q = a **div** d, r = a **mod** d.

– Example: 101 = 11.9 + 2

Quotient = 101 **div** 11

Remainder = 2 = 101 **mod** 11

- Greatest Common Divisors & Least Common Multiples
  – Definition 4

Let a and b be integers, not both zero. The largest integer d such that d|a and d|b is called the greatest common divisor of a and b. It is denoted gcd (a, b).

Example: gcd (24, 36)

Div (24) = {1,2,3,4,6,8,12,24}

Div (36) = {1,2,3,4,6,8,9,12,18,36}

Com(24,36) = = {1,2,3,4,6,12}

gcd(24,36) = 12

– Definition 5:

The integers a and b are relatively prime (rp) if gcd(a, b) =1.

Example: 17 and 22 are rp since gcd(17,22) = 1.

– Definition 7:

The least common multiple (lcm) of the positive integers a and b is the smallest positive integer that is divisible by both a and b.

$$lcm(a,b) = p_1^{max(a_1,b_1)} p_2^{max(a_2,b_2)} \ldots p_n^{max(a_n,b_n)}$$

where max(x,y) denotes the maximum of x and y.

Example : What is the least common multiple of:

$2^3 3^5 7^2$ and $2^4 3^3$?

Solution: $lcm(2^3 3^5 7^2, 2^4 3^3) = 2^{max(3,4)} . 3^{max(5,3)} . 7^{max(2,0)}$

$= 2^4 3^5 7^2$

– Theorem 7:

Let a and b be positive integers. Then ab = gcd(a,b).lcm(a.b).

- Modular Arithmetic
  - Definition 8:

Let $(a, b) \in Z^2$, $m \in Z^+$ then a is a congruent to b modulo m if m divides a –b.
Notation: $a \equiv b \pmod{m}$.

  - Theorem 8

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if a **mod** m = b **mod** m.

– Example: $17 \equiv 5 \pmod 6$

$24 \equiv 14 \pmod 6$?

Since: $6|(17 - 5) = 12 \Rightarrow 17 \equiv 5 \pmod 6$

6 does not divide 10

$\Rightarrow$ 24 is not congruent to 14 (mod 6)

– Theorem 9:

> Let m be a positive integer. The integers a and b are congruent modulo m if and only if
>
> $$\exists k \in Z;\ a = b + km$$

- Applications of Congruences

1. Hashing Functions
2. Pseudorandom Numbers
3. Cryptology (Caesar Cepher)

1. Hashing Functions

Assignment of memory location to a student record

$$h(k) = k \textbf{ mod } m$$

Example: h (064212848) = 064212848 mod 111 = 14 when m = 111

2. Pseudorandom Numbers

- Needed for computer simulation
- Linear congruential method :
  $x_{n+1} = (ax_n + c) \textbf{ mod } m$
- Put them between 0 and 1 as: $y_n = x_n/m$

3. Cryptology (Caesar Cepher)

a) Encryption:

- Making messages secrets by shifting each letter three letters forward in the alphabet

$$B \rightarrow E \qquad X \rightarrow A$$

- Mathematical expression:

$$f(p) = (p + 3) \textbf{ mod } 26 \qquad 0 \le p \le 25$$

– Example: What is the secret message produced from the message "Meet you in the park"

Solution:

1. Replace letters with numbers:
   meet = 12 4 4 19
   you = 24 14 20
   in = 8 1 3
   the = 19 7 4
   park = 15 0 17 10
2. Replace each of these numbers p by $f(p) = (p + 3)$ **mod** 26
   meet = 15 7 7 22
   you = 1 17 23
   in = 11 16
   the = 22 10 7
   park = 18 3 20 13
3. Translate back into letters: "PHHW BRX LQ WKH SDUN"

b) Decryption (Deciphering)

$f(p) = (p + k)$ **mod** 26 (shift cepher)
$\Rightarrow f^{-1}(p) = (p - k)$ **mod** 26

Caesar's method and shift cipher are very vulnerable and thus have low level of security (reason frequency of occurrence of letters in the message)
$\Rightarrow$ Replace letters with blocks of letters.