Discrete Mathematics:
Lecture 10. Number Theory

Chapter 4.1
Divisibility and Modular Arithmetic

division

- a divides b if there is an integer c such that $b = ac$,

  when a, b, c : integer, $a \neq 0$
- a is a factor or divisor of b
- b is a multiple of a
- $a \mid b$: a divides b, $\exists c\ (ac = b)$
- $a \nmid b$: a does not divide b

$3 \nmid 7$

$3 \mid 12$

division

Let, a, b, and c $\in$ Z, where a $\neq$ 0

(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

by direct proof

(i) if a | b => b = as, a | c => c = at, (s, t $\in$ Z)

then b + c = as + at = a (s + t)

(ii) if a | b => b = as,

then bc = asc => a |bc for all integers c

(iii) if a | b and b | c => b = as, c= bk,

then c = ask => a | c

division

- $a \in Z, d \in Z^+$

  there are unique integers q and r with $0 \le r < d$, such that $a = dq + r$

- d: divisor, a: dividend, q: quotient, r: remainder

  q = a div d, r = a mod d

what are the quotient and remainder when 101 is divided by 11?

$101 = 11 \cdot 9 + 2$

what are the quotient and remainder when -11 is divided by 3?

$-11 = 3\ (-4) + 1$

modular arithmetic

- if $a, b \in Z$ and $m \in Z^+$,

  a is congruent to b modulo m if m divides a-b
- $a \equiv b \pmod{m}$ is a congruence

  m is its modulus

determine whether 17 is congruent to 5 modulo 6?

$(17-5) / 6 = 2$

determine whether 24 is congruent to 14 modulo 6?

$(24 - 14)$ is not divided by 6

modular arithmetic

$a, b \in Z, m \in Z^+$

$a \equiv b \pmod{m}$ iff $(a \bmod m) = (b \bmod m)$

$(a - b) = mk$ where $a = mk_1 + c$, $b = mk_2 + c$

$m \in Z^+$, $a, b \in Z$

a and b are congruent modulo m

$\leftrightarrow$ there is an integer k such that $a = b + km$

if $a \equiv b \pmod{m}$, $m \mid (a - b)$

this means that there is an integer k such that $a - b = km$

modular arithmetic

$m \in Z^+$

If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$,

$a + c \equiv b + d \pmod{m}$ and $ac \equiv bd \pmod{m}$

$b - a = sm, \; d - c = tm$

$b + d = a + sm + c + tm = (a + c) + m(s + t)$

$b \cdot d = (a + sm) \cdot (c + tm) = ac + atm + csm + stm^2$

$= ac + m(at + cs + stm)$

modular arithmetic

$m \in Z+$, $a, b \in Z$

$(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$

$ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$

If $a = mk + t$, $a \bmod m = t$ $\Rightarrow (a - (a \bmod m)) = mk$

$\Rightarrow a \equiv (a \bmod m) \pmod{m}$

$b \equiv (b \bmod m) \pmod{m}$

from the theorem

"If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, $a + c \equiv b + d \pmod{m}$"

$a + b \equiv ((a \bmod m) + (b \bmod m)) \pmod{m}$

arithmetic modulo m

$a +_m b = (a + b) \bmod m$

$a \cdot_m b = (a \cdot b) \bmod m$

find $7 +_{11} 9$ and $7 \cdot_{11} 9$?

$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$

$7 \cdot_{11} 9 = (7 \cdot 9) \bmod 11 = 63 \bmod 11 = 8$

Chapter 4.2

Integer Representations and Algorithms

representations of integers

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

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

where k is a nonnegative integer, $a_0, a_1, \ldots a_k$ are nonnegative integers less than b and $a_k \neq 0$

$965 = 9 \cdot 10^2 + 6 \cdot 10 + 5$

$(245)_8 = 2 \cdot 8^2 + 4 \cdot 8 + 5 = 128 + 32 + 5 = 165$

$(101011111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351$

$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16^1 + 11 \cdot 16^0 = 175627$

base conversion

base b expansion of an integer n

$n = bq_0 + a_0, \quad 0 \leq a_0 < b$

$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b$

:

$(a_n a_{n-1} \ldots a_0)_b$

find octal expansion of $(12345)_{10}$?

$12345 = 8 \cdot 1543 + 1$

$1543 = 8 \cdot 192 + 7$

$192 = 8 \cdot 24 + 0$

$24 = 8 \cdot 3 + 0$

$3 = 8 \cdot 0 + 3$

$$12345 = 8 \cdot (8 \cdot (8 \cdot (8 \cdot (8 \cdot 0+3) + 0) + 0) + 7) + 1$$
$$= 3 \cdot 8^4 + 0 \cdot 8^3 + 0 \cdot 8^2 + 7 \cdot 8^1 + 1 \cdot 8^0 = (30071)_8$$

base conversion

find the octal and hexadecimal expansion of $(11111010111100)_2$?

$(11\ 111\ 010\ 111\ 100)_2 = (37274)_8$

$(11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$

find the binary expansion of $(765)_8$?

$(765)_8 = (111\ 110\ 101)_2$

base conversion

Hexadecimal, octal, and binary representation of the integers

decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

algorithms for integer operations: addition

$a = (a_{n-1}\ a_{n-2} \ldots a_1 a_0)_2$

$b = (b_{n-1}\ b_{n-2} \ldots b_1 b_0)_2$

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

$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1$

$a + b = (s_n s_{n-1} s_{n-2} \ldots s_1 s_0)_2$

$a = (1110)_2 \qquad b = (1011)_2$

$a0 + b0 = 0 + 1 = 0 \cdot 2 + 1$

$a1 + b1 + c0 = 1 + 1 + 0 = 1 \cdot 2 + 0$

$a2 + b2 + c1 = 1 + 0 + 1 = 1 \cdot 2 + 0$

$a3 + b3 + c2 = 1 + 1 + 1 = 1 \cdot 2 + 1$

$a + b = (1\ 1001)_2$

```
  1110
 +1011
 ---------
 11001
```

algorithms for integer operations: addition

procedure add(a, b: positive integers)
{the binary expansions of $a=(a_{n-1}a_{n-2}\ldots a_1a_0)_2$ and $b=(b_{n-1}b_{n-2}\ldots b_1b_0)_2$}

```
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 }
```

algorithms for integer operations: multiplication

$a = (a_{n-1}\ a_{n-2} \ldots a_1 a_0)_2$

$b = (b_{n-1}\ b_{n-2} \ldots b_1 b_0)_2$

$ab = a(b_0 2^0 + b_1 2^1 + \ldots + b_{n-1} 2^{n-1})$

$\quad = a(b_0 2^0) + a(b_1 2^1) + \ldots + a(b_{n-1} 2^{n-1})$

$a = (110)_2 \quad b = (101)_2$

$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2$

$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2$

$ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2$

$a \cdot b = (1\ 1110)_2$

```
   110
  x101
   -------
   110
  000
 110
-----------
 11110
```

algorithms for integer operations: multiplication

procedure multiply (a, b: positive integer)
{the binary expansion of a and b are $a=(a_{n-1}a_{n-2}\dots a_1a_0)_2$ and $b=(b_{n-1}b_{n-2}\dots b_1b_0)_2$}

for j := 0 to n-1
    if b_j = 1 then c_j := a shifted j places
    else c_j := 0
{$c_0, c_1, \dots c_{n-1}$ are the partial products}

p := 0
for j := 0 to n-1
    p := p + c_j

return p   {p is the value of ab}

algorithms for integer operations: div and mod

procedure division (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}
```

Chapter 4.3
Primes and Great Common Divisors

primes

- prime number is an integer that is greater than 1 and has only two positive integer factors of 1 and itself
- composite number is an integer that is greater than 1 and is not prime
- every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes

find the prime factorization of 7007

$7007 / 7 = 1001$
$1001 / 7 = 143$
$143 / 11 = 13$

$7007 = 7^2 \cdot 11 \cdot 13$

primes

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

$n = ab$, $1 < a < n$, $b > 1$
we want to show $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$
if $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > \sqrt{n}\sqrt{n} = n$, which is contradiction
thus, $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.
this divisor is either prime or has a prime divisor less than itself

show that 101 is prime

if 101 is composite integer, 101 should have a prime divisor that is < $\sqrt{101}$: 2, 3, 5, 7
because 101 is not divisible by 2, 3, 5, or 7, 101 is not composite integer

greatest common divisors

- the greatest common divisor of a and b, gcd(a, b), is the largest integer d such that $d \mid a$ and $d \mid b$, $a, b \in Z$, $a \neq 0$, $b \neq 0$
- the way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers.

  $a = p_1^{a1} p_2^{a2} \cdot \cdot \cdot p_n^{an}$, $b = p_1^{b1} p_2^{b2} \cdot \cdot \cdot p_n^{bn}$

  $\gcd(a, b) = p_1^{\min(a1, b1)} p_2^{\min(a2, b2)} \ldots p_n^{\min(an, bn)}$
- integer a and b are relatively prime if gcd(a, b) = 1

find gcd(120, 500)?

$120 = 2^3 \cdot 3 \cdot 5$
$500 = 2^2 \cdot 5^3$

$\gcd(120, 500) = 2^{\min(3,2)} 3^{\min(1,0)} 5^{\min(1,3)} = 2^2 3^0 5^1 = 20$

least common multiple

- the least common multiple of the positive integers a and b is the smallest positive integer that is divisible by both a and b, lcm(a, b)
- $a = p_1^{a1} p_2^{a2} \cdot \cdot \cdot\ p_n^{an}$, $\quad b = p_1^{b1} p_2^{b2} \cdot \cdot \cdot\ p_n^{bn}$

  $lcm(a, b) = p_1^{max(a1,\, b1)} p_2^{max(a2,\, b2)} \ldots p_n^{max(an,\, bn)}$

find least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

$lcm(2^3 3^5 7^2 \text{ and } 2^4 3^3) = 2^{max(3,4)} 3^{max(5,3)} 7^{max(2,0)} = 2^4 3^5 7^2$