Discrete Mathematics: Lecture 12

- Last time:
  - Chap 3.3: Complexity of algorithms
  - Chap 4.1: Divisibility and modular arithmetic
- Today:
  - Chap 4.2: Integer representations and algorithms
  - Chap 4.3: Primes and greatest common divisors
- Assignment 4 due in two weeks
- Next time:
  - Chap 4.4: Solving congruences
  - Chap 4.6: Cryptography (a simple introduction)

Review of last time

- Worst-case complexity, average-case complexity
- Tractable problems, P, NP, NP-complete problems
- Divisibility and modular arithmetic

Primes(质数)

- Definition: 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.
- THE FUNDAMENTAL THEOREM OF ARITHMETIC: Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in nondecreasing order.
- Example: $100 = 2^5 5^2$, $999 = 3^3 \cdot 37$
- Theorem: If n is a composite integer, then n has a prime divisor $\leq \sqrt{n}$.
- Example: show that 101 is prime.

Finding the prime factorization (质因数分解) of integers

procedure prime factorization(n :integers)
$p := 2$
while $p \leq \sqrt{n}$ and $p \nmid n$
    $p :=$ next prime
if $p \leq \sqrt{n}$ prime factorization(n/p)

Example: 7007

The infinitude of primes

- Theorem: There are infinitely many primes
- Express this theorem in logic
- Proof

Mersenne Primes

- There is an ongoing quest for finding larger and larger prime numbers
- The largest known prime has usually been a Mersenne prime, a prime of the form $2^p - 1$, where p is a prime
- The reason is that there is an extremely efficient test to determine if $2^p - 1$ is prime
- Examples: 3,7,31, but $2047 = 23 \cdot 89$ is not
- The Great Internet Mersenne Prime Search (GIMPS)

Conjectures and open problems about primes

- A false conjecture: Let $f(n) = n^2 - n + 41$. Then $f(n)$ is prime for all positive integers.
- Goldbach's conjecture: Every even integer n, $n > 2$, is the sum of two primes.
- There are infinitely many primes of the form $n^2 + 1$.
- There are infinitely many twin primes, that is, primes that differ by 2.

Greatest common divisors (最大公约数)

- Definition: Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the greatest common divisor of a and b, denoted by $gcd(a, b)$.
- Definition: The integers a and b are relatively prime if their gcd is 1.
- Definition: The integers $a_1, a_2, \ldots, a_n$ are pairwise relatively prime if $gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.
- One way to find the gcd of two integers is to use the prime factorizations of them.
  - Let $a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$, and $b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$.
    Then $gcd(a, b) = p_1^{min(a_1, b_1)} p_2^{min(a_2, b_2)} \ldots p_n^{min(a_n, b_n)}$

Least common multiples (最小公倍数)

- Definition: Let a and b be positive integers. The least common multiply of a and b, denoted by $lcm(a, b)$, is the smallest positive integer that is divisible by both a and b.
- $lcm(a, b) = p_1^{max(a_1, b_1)} p_2^{max(a_2, b_2)} \dots p_n^{max(a_n, b_n)}$
- Theorem: Let a and b be positive integers. Then $ab = gcd(a, b) \cdot lcm(a, b)$.

Computing div and mod

procedure division(a: integer, d: positive integer)
$q := 0$
$r := |a|$
while $r \geq d$
    $r := r - d$
    $q := q + 1$
if $a < 0$ and $r > 0$ then
    $r := d - r$
    $q := -(q + 1)$

Assuming $a > d$, the algorithm uses $O(q)$ subtractions

The Euclidean algorithm (欧几里德算法)

Lemma: Let $a = bq + r$, where a, b, q, and r are integers. Then $gcd(a, b) = gcd(b, r)$.

procedure gcd(a, b: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ mod y
    $x := y$
    $y := r$

Complexity: $O(\log b)$ divisions, assuming $a > b$

Example: $gcd(414, 662)$

Some useful results

- Theorem: If a and b are positive integers, then there exist integers s and t such that $gcd(a, b) = sa + tb$.
- Example: $gcd(252, 198) = 18$
- Lemma 1: If a, b, and c are positive integers such that $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$.
- Lemma 2: If p is a prime and $p \mid a_1 a_2 \dots a_n$, where each a_i is an integer, then $p \mid a_i$ for some i.
- The uniqueness of prime factorization of integers
- Theorem: Let m be a positive integer and let a, b, and c be integers. If $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

Representations of integers

- Decimal (base 10), binary, octal (base 8), hexadecimal (base 16) representations
- Theorem: 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 $a_k \neq 0$.
- Base b expansion of n, denoted by $(a_k \ldots a_1 a_0)_b$
- *e.g.*, $(7016)_8$, $(2AE0B)_{16}$, octal representation of 12345
  $1543, 192, 24, 3, (30071)_8$

ALGORITHM 1 Constructing Base b Expansions.

procedure *base b expansion*(n, b: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ **mod** b
    $q := q$ **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 $n\}$

Conversion between binary, octal, and hexadecimal expansions

- Octal and hexadecimal expansions of $(11111010111100)_2$
- Binary expansions of $(765)_8$ and $(A8D)_16$

Addition of integers

ALGORITHM 2 Addition of Integers.

procedure *add*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\dots a_1a_0)_2$
and $(b_{n-1}b_{n-2}\dots b_1b_0)_2$, respectively}
$c := 0$
for $j := 0$ **to** $n - 1$
  $d := \lfloor (a_j + b_j + c)/2 \rfloor$
  $s_j := a_j + b_j + c - 2d$
  $c := d$
$s_n := c$
return $(s_0, s_1, \dots, s_n)$ {the binary expansion of the sum is $(s_ns_{n-1}\dots s_0)_2$}

- *e.g.*, add 1110 and 1011
- Complexity: $O(n)$ bit additions

Multiplication of integers

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

ALGORITHM 3 Multiplication of Integers.

procedure *multiply*(a, b: positive integers)
{the binary expansions of a and b are $(a_{n-1}a_{n-2}\ldots a_1a_0)_2$
  and $(b_{n-1}b_{n-2}\ldots b_1b_0)_2$, respectively}
for $j := 0$ **to** $n-1$
  if $b_j = 1$ **then** $c_j := a$ shifted j places
  else $c_j := 0$
{$c_0, c_1, \ldots, c_{n-1}$ are the partial products}
$p := 0$
for $j := 0$ **to** $n-1$
  $p := p + c_j$
return p {p is the value of ab}

- *e.g.*, multiply 110 and 101
- Complexity: $O(n^2)$ shifts and $O(n^2)$ bit additions

Modular exponentiation

In cryptography, it is important to find b^n mod m efficiently, where b, n, and m are large integers

procedure modular exponentiation(b: integer,
$\quad n = (a_{k-1} \dots a_1 a_0)_2$, m: positive integer)
$x := 1$
$power := b$ mod m
for $i := 0$ to $k - 1$
$\quad$ if $a_i = 1$ then $x := (x \cdot power)$ mod m
$\quad power := (power \cdot power)$ mod m

Example: compute 3^{20} mod 645

Modular exponentiation

In cryptography, it is important to find b^n mod m efficiently, where b, n, and m are large integers

procedure modular exponentiation(b: integer,
    $n = (a_{k-1} \dots a_1 a_0)_2$, m: positive integer)
$x := 1$
$power := b$ mod m
for $i := 0$ to $k - 1$
    if $a_i = 1$ then $x := (x \cdot power)$ mod m
    $power := (power \cdot power)$ mod m

Example: compute 3^{20} mod 645
81^2 mod 645 $= 111$, $81 \cdot 111$ mod 645 $= 606$,

Complexity: $O(\log n)$ operations on $\log m$-bit integers