Discrete Mathematics

CS204: Spring, 2008

Jong C. Park
Computer Science Division, KAIST

Today's Topics

The Euclidean Algorithm

The RSA Public-Key Cryptosystem

Introduction to Number Theory

The Euclidean Algorithm

- Note
  - If $r = a \bmod b$, then $\gcd(a,b) = \gcd(b,r)$.
- Example
  - Compute gcd(105,30).
    - Since 105 mod 30 = 15, gcd(105,30) = gcd(30,15).
    - Since 30 mod 15 = 0, gcd(30,15) = gcd(15,0).
    - By inspection, gcd(15,0) = 15.
    - Therefore, gcd(105,30) = gcd(30,15)
      = gcd(15,0)
      = 15.

The Euclidean Algorithm

- Theorem
  - If a is a nonnegative integer, b is a positive integer, and $r = a \bmod b$, then $\gcd(a,b) = \gcd(b,r)$.
  - Proof.
    - By the quotient-remainder theorem, there exist q and r satisfying $a = bq + r$, $0 \le r < b$. We show that the set of common divisors of a and b is equal to the set of common divisors of b and r, thus proving the theorem.
    - Let c be a common divisor of a and b. Thus, $c \mid bq$.
    - Since $c \mid a$ and $c \mid bq$, $c \mid a - bq$ $(= r)$.
    - Thus c is a common divisor of b and r.
    - Conversely, if c is a common divisor of b and r, then $c \mid bq$ and $c \mid bq + r$ $(= a)$ and c is a common divisor of a and b.
    - Thus the set of common divisors of a and b is equal to the set of common divisors of b and r. Therefore, $\gcd(a,b) = \gcd(b,r)$.

The Euclidean Algorithm

Algorithm 5.3.3: Euclidean Algorithm

Input: a and b (nonnegative integers, not both zero)

Output: Greatest common divisor of a and b

```
gcd(a, b) {
    // make a largest
    if (a < b)
        swap(a, b)
    while (b ¬= 0) {
        r = a mod b
        a = b
        b = r
    }
    return a
}
```

The Euclidean Algorithm

- Example
  - Find gcd(504, 396).

The Euclidean Algorithm

- Theorem
  - Suppose that the pair a, b, $a > b$, requires $n \geq 1$ modulus operations when input to the Euclidean algorithm. Then $a \geq f_{n+2}$ and $b \geq f_{n+1}$, where $\{f_n\}$ denotes the Fibonacci sequence.
  - Proof.
    - The proof is by induction on n.

The Euclidean Algorithm

- Theorem
  - If integers in the range 0 to m, $m \geq 8$, not both zero, are input to the Euclidean algorithm, then at most $\log_{3/2} 2m/3$ modulus operations are required.
- Note
  - This means that the algorithm is quite efficient.

The Euclidean Algorithm

- Note
  - We use the following special result to compute inverses modulo an integer.
  - Such inverses are used in the RSA cryptosystem.
- Theorem
  - If *a* and *b* are nonnegative integers, not both zero, there exist integers *s* and *t* such that $\gcd(a,b) = sa + tb$.
  - Proof.
    - page 211.

The Euclidean Algorithm

- Example
  - Compute *s* and *t* from gcd(273, 110).
    - We begin with $a = 273$ and $b = 110$.
      - $r = 273 \bmod 110 = 53$.
    - We then compute $a = 110$ and $b = 53$.
      - $r = 110 \bmod 53 = 4$.
    - We then compute $a = 53$ and $b = 4$.
      - $r = 53 \bmod 4 = 1$.
    - We then compute $a = 4$ and $b = 1$.
      - $r = 4 \bmod 1 = 0$.
    - To find *s* and *t*, we work back from $r \neq 0$.
      - $1 = 53 - 4\cdot13 = 53 - (110 - 53\cdot2)\cdot13 = 27\cdot53 - 13\cdot110$.
      - $1 = 27\cdot53 - 13\cdot110 = 27\cdot(273 - 110\cdot2) - 13\cdot110 = 27\cdot273 - 67\cdot110$.
    - Taking $s = 27$ and $t = -67$, we obtain $\gcd(273,110) = 1 = s\cdot273 + t\cdot110$.

$53 = 273 - 110\cdot2$

$4 = 110 - 53\cdot2$

$1 = 53 - 4\cdot13$

Computing an Inverse Modulo an Integer

- Note
  - Suppose that we have two integers $n > 0$ and $\phi > 1$ such that $\gcd(n,\phi) = 1$.
  - We show how to efficiently compute an integer s, $0 < s < \phi$ such that $ns \bmod \phi = 1$.
  - We call s the inverse of n mod ϕ. Efficiently computing this inverse is required by the RSA cryptosystem.
  - Since $\gcd(n,\phi) = 1$, we use the Euclidean algorithm to find numbers s' and t' such that $s'n + t'\phi = 1$.
  - Then $ns' = -t'\phi + 1$, and, since $\phi > 1$, 1 is the remainder. Thus,

    $$ns' \bmod \phi = 1.$$

    Note that s' is almost the desired value; the problem is that s' may not satisfy $0 < s' < \phi$.

Computing an Inverse Modulo an Integer

- Note (continued)
  - However, we can convert s' to the proper value by setting

    $$s = s' \bmod \phi.$$

    Now $0 \leq s < \phi$.
    - In fact $s \neq 0$ since, if $s = 0$, then $\phi \mid s'$, which contradicts the fact that $ns' \bmod \phi = 1$.
  - Since $s = s' \bmod \phi$, there exists q such that

    $$s' = q\phi + s.$$
  - Combining the previous equations,

    $$\begin{aligned} ns &= ns' - \phi nq \\ &= -t'\phi + 1 - \phi nq \\ &= \phi(-t' - nq) + 1. \end{aligned}$$
  - Therefore $ns \bmod \phi = 1$.

Computing an Inverse Modulo an Integer

- Example
  - Let $n = 110$ and $\phi = 273$.
  - We know that $\gcd(n,\phi) = 1$ and $s'n + t'\phi = 1$, where $s' = -67$ and $t' = 27$.
  - Thus, $110(-67) \bmod 273 = ns' \bmod \phi = 1$.
  - Here $s = s' \bmod \phi = -67 \bmod 273 = 206$.
  - Therefore, the inverse of 110 modulo 273 is 206.

Computing an Inverse Modulo an Integer

- Show that the number s in the equation

$$ns \bmod \phi = 1$$

is unique.
  - Proof.
    - Suppose that $ns \bmod \phi = 1 = ns' \bmod \phi$, $0 < s < \phi$, $0 < s' < \phi$.
    - We must show that $s' = s$.
    - Now $s' = (s' \bmod \phi)(ns \bmod \phi)$

$$= s'ns \bmod \phi$$

$$= (s'n \bmod \phi)(s \bmod \phi)$$

$$= s.$$

The RSA Public-Key Cryptosystem

- Note
  - Cryptology is the study of systems, called cryptosystems, for secure communications.
  - In a cryptosystem, the sender transforms the message before transmitting it, hoping that only authorized recipients can reconstruct the original message.
  - The sender is said to encrypt the message, and the recipient is said to decrypt the message.

The RSA Public-Key Cryptosystem

- Example
  - If a key is defined as

    character:
    ABCDEFGHIJKLMNOPQRSTUVWXYZ

    replaced by:

    EIJFUAXVHWP GSRKOBTQYDMLZNC

    the message SEND MONEY would be encrypted as QARUESKRAN.
  - The encrypted message SKRANEKRELIN would be decrypted as MONEY ON WAY.

The RSA Public-Key Cryptosystem

- The RSA Public-Key Cryptosystem
  - Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman
  - Each participant makes public an encryption key and hides a decryption key.
  - To send a message, all one needs to do is look up the recipient's encryption key in a publicly distributed table.
  - The recipient then decrypts the message using the hidden decryption key.
  - Messages are represented as numbers.

The RSA Public-Key Cryptosystem

- Each prospective recipient chooses two primes p and q and computes $z = pq$.
  - p and q are typically chosen so that each has 100 or more digits.
- Next, the prospective recipient computes $\phi = (p - 1)(q - 1)$ and chooses an integer n such that $\gcd(n,\phi) = 1$.
  - In practice, n is often chosen to be a prime.
- The pair (z, n) is then made public.
- Finally, the prospective recipient computes the unique number s, $0 < s < \phi$, satisfying $ns \bmod \phi = 1$.
- The number s is kept secret and used to decrypt messages.

The RSA Public-Key Cryptosystem

- Example
  - Suppose that we choose $p = 23$, $q = 31$, and $n = 29$.
  - Then $z = pq = 713$ and $\phi = (p - 1)(q - 1) = 660$.
  - Now $s = 569$ since $ns \bmod \phi = 29 \cdot 569 \bmod 660 = 16501 \bmod 660 = 1$.
  - The pair $(z, n) = (713, 29)$ is made publicly available.
  - To transmit $a = 572$ to the holder of public key $(713, 29)$, the sender computes $c = a^n \bmod z = 572^{29} \bmod 713 = 113$ and sends 113.
  - The receiver computes $c^s \bmod z = 113^{569} \bmod 713 = 572$ in order to decrypt the message.

The RSA Public-Key Cryptosystem

- Example (continued)
  - The main result that makes encryption and decryption work is that

$$a^u \bmod z = a \quad \text{for all } 0 \leq a < z \text{ and}$$
$$u \bmod \phi = 1.$$

  - Since $ns \bmod \phi = 1$,

$$\begin{aligned} c^s \bmod z &= (a^n \bmod z)^s \bmod z \\ &= (a^n)^s \bmod z \\ &= a^{ns} \bmod \mathrm{z} \\ &= a. \end{aligned}$$

Today's Topics

Basic Principles

Permutations and Combinations

Algorithms for Generating Permutations

Generalized Permutations and Combinations

Binomial Coefficients and Combinatorial Identities

The Pigeonhole Principle

Counting Methods and the Pigeonhole Principle

Basic Principles

- Examples
  - Kay's Quick Lunch
    - Appetizers: Nachos, Salad
    - Main courses: Hamburger, Cheeseburger, Fish Filet
    - Beverages: Tea, Milk, Cola, Root Beer
  - How many different lunches consist of one main course and one beverage?
    - $3 \cdot 4 = 12$
  - How many different lunches consist of one main course and one *optional* beverage?
    - $3 \cdot 5 = 15$

Basic Principles

- Multiplication Principle
  - If an activity can be constructed in t successive steps and step 1 can be done in n_1 ways, step 2 can then be done in n_2 ways, ..., and step t can then be done in n_t ways, then the number of different possible activities is $n_1 \cdot n_2 \cdots n_t$.

Basic Principles

- Examples
  - Melissa Virus
    - The virus sends the e-mail to the first 50 addresses from the user's address book.
    - How many copies of the message are sent after four iterations?
      - $1 + 50 + 50 \cdot 50 + 50 \cdot 50 \cdot 50 + 50 \cdot 50 \cdot 50 \cdot 50 = 6{,}377{,}551$
  - ABCDE

    (a) How many strings of length 4 can be formed using the letters ABCDE if repetitions are not allowed?

    (b) How many strings of (a) begin with the letter B?

    (c) How many strings of (a) do not begin with the letter B?

Basic Principles

- Examples
  - Use the Multiplication Principle to show that a set $\{x_1, ..., x_n\}$ containing n elements has 2^n subsets.
  - Let X be an n-element set. How many ordered pairs (A, B) satisfy $A \subseteq B \subseteq X$?
    - We see that each element in X is in exactly one of A, $B - A$, or $X - B$.
    - 3^n

Basic Principles

- Addition Principle
  - Suppose that $X_1, ..., X_t$ are sets and that the ith set X_i has n_i elements.
  - If $\{X_1, ..., X_t\}$ is a pairwise disjoint family (i.e., if $i \neq j$, $X_i \cap X_j = \varnothing$), the number of possible elements that can be selected from X_1 or X_2 or ... or X_t is $n_1 + n_2 + ... + n_t$.
  - (Equivalently, the union $X_1 \cup ... \cup X_t$ contains $n_1 + n_2 + ... + n_t$ elements.)

Basic Principles

- Examples
  - In how many ways can we select two books from different subjects among five distinct computer science books, three distinct mathematics books, and two distinct art books?
    - $15 + 10 + 6 = 31$

Permutations and Combinations

- Definition
  - A permutation of n distinct elements $x_1, ..., x_n$ is an ordering of the n elements $x_1, ..., x_n$.
- Example
  - List all the permutations of three elements A, B, C.
    - There are six permutations:
      - ABC, ACB, BAC, BCA, CAB, and CBA.

Permutations and Combinations

- Theorem
  - There are $n!$ permutations of n elements.
  - Proof.
    - We use the Multiplication Principle.
    - A permutation of n elements can be constructed in n successive steps:
      - Select the first element; select the second element; ...; select the last element.
      - The first element can be selected in n ways. Once the first element has been selected, the second element can be selected in $n - 1$ ways.
      - Once the second element has been selected, the third element can be selected in $n - 2$ ways, and so on.
      - By the Multiplication Principle, there are $n(n - 1)(n - 2) \cdots 2 \cdot 1 = n!$ permutations of n elements.

Permutations and Combinations

- Examples
  - How many permutations of 10 elements are there?
    - $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 3{,}628{,}800$
  - How many permutations of the letters *ABCDEF* contain the substring *DEF*?
    - $4! = 24$
  - How many permutations of the letters *ABCDEF* contain the letters *DEF* together in any order?
    - $4! \cdot 3! = 24 \cdot 6 = 144$
  - In how many ways can six persons be seated around a circular table? If a seating is obtained from another seating by having everyone move *n* seats clockwise, the seatings are considered identical.
    - $5! = 120$

Permutations and Combinations

- Definition
  - An *r*-permutation of *n* (distinct) elements $x_1, \ldots, x_n$ is an ordering of an *r*-element subset of $\{x_1, \ldots, x_n\}$. The number of *r*-permutations of a set of *n* distinct elements is denoted $P(n,r)$.
- Example
  - Examples of 2-permutations of *a*, *b*, *c*
    - *ab*, *ba*, *ca*.

Permutations and Combinations

- Theorem
  - The number of r-permutations of a set of n distinct objects is $P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$, $r \leq n$.
  - Proof.
    - Exercise
- Examples
  - The number of 2-permutations of $X = \{a, b, c\}$
    - $P(3,2) = 3 \cdot 2 = 6$.
  - In how many ways can we select a chairperson, vice-chairperson, secretary, and treasurer from a group of 10 persons?
    - $P(10,4) = 10 \cdot 9 \cdot 8 \cdot 7 = 5040$

Permutations and Combinations

- Note
  - We may write $P(n,r)$ in terms of factorials:
    - $P(n,r) = n(n-1)\cdots(n-r+1)$
      $= n(n-1)\cdots(n-r+1)(n-r)\cdots 2\cdot 1/(n-r)\cdots 2\cdot 1$
      $= n!/(n-r)!$
- Examples
  - $P(10,4)$
    - $10!/(10-4)! = 10!/6!$
  - In how many ways can seven distinct Martians and five distinct Jovians wait in line if no two Jovians stand together?
    - $7!\cdot P(8,5) = 5040\cdot 6720 = 33{,}868{,}800$

Summary

- Introduction to Number Theory
  - The Euclidean Algorithm
  - The RSA Public-Key Cryptosystem
- Counting Methods and the Pigeonhole Principle
  - Basic Principles
  - Permutations