Discrete Mathematics (2009 Spring)
Basic Number Theory (§3.4~§3.7, 4 hours)

Chih-Wei Yi

Dept. of Computer Science
National Chiao Tung University

April 4, 2009

§3.4 The Integers and Division

Division, Factors, Multiples

Definition

Let $a, b \in \mathbb{Z}$ with $a \neq 0$.
$a|b :\equiv$ "a divides b" $:\equiv$ "$\exists c \in \mathbb{Z} : b = ac$".
"There is an integer c such that c times a equals b."

- We say a is a factor or a divisor of b, and b is a multiple of a.

Example

$3 \mid -12 \iff$ **T**; but $3 \mid 7 \iff$ **F**.

Example

"b is even" $:\equiv 2|b$. Is 0 even? Is -4?

Facts: the Divides Relation

Theorem

$\forall a, b, c \in \mathbb{Z}$:

1. $a|0$ *for any* $a \neq 0$.
2. $(a|b \wedge a|c) \rightarrow a|(b+c)$.
3. $a|b \rightarrow a|bc$.
4. $(a|b \wedge b|c) \rightarrow a|c$

Proof.

(2) $a|b$ *means there is an* s *such that* $b = as$, *and* $a|c$ *means that there is a* t *such that* $c = at$, *so* $b + c = as + at = a(s+t)$, *so* $a|(b+c)$ *also.* $\square$

The Division "Algorithm"

Theorem

For any integer dividend a and divisor $d \neq 0$, there is a unique integer quotient q and remainder $r \in \mathbb{N}$ such that (denoted by $\ni$) $a = dq + r$ and $0 \leq r < |d|$.

- $\forall a, d \in \mathbb{Z} \wedge d \neq 0 \, (\exists! q, r \in \mathbb{Z} \ni 0 \leq r < |d| \wedge a = dq + r)$.

- We can find q and r by: $q = \lfloor a/d \rfloor, r = a - qd$.
- Really just a theorem, not an algorithm ...
  - The name is used here for historical reasons.

The Mod Operator

Definition (An integer "division remainder" operator)

Let $a, d \in \mathbb{Z}$ with $d > 1$. Then $a \bmod d$ denotes the remainder r from the division "algorithm" with dividend a and divisor d; i.e. the remainder when a is divided by d.

- We can compute $(a \bmod d)$ by: $a - d \cdot \lfloor a/d \rfloor$.
- In C programming language, "%" $= \mathrm{mod}$.

Modular Congruence

Definition

Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then a is congruent to b modulo m, written "$a \equiv b \pmod{m}$", if and only if $m | a - b$.

- Also equivalent to $(a - b) \bmod m = 0$.
- Note: this is a different use of ":$\equiv$" than the meaning "is defined as" I've used before.
- Visualization of mod.

Useful Congruence Theorems

- Let $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then,
  $a \equiv b \pmod{m} \iff \exists k \in \mathbb{Z} : a = b + km.$
- Let $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$. Then, if $a \equiv b \bmod m$ and $c \equiv d \bmod m$, we have
  - $a + c \equiv b + d \bmod m$, and
  - $ac \equiv bd \bmod m$

Problem

Prove!!!

§3.5 Primes and Greatest Common Divisors

Prime Numbers

Definition (Prime)

An integer $p > 1$ is prime iff it is not the product of any two integers greater than 1,

- $p > 1 \wedge \neg \exists a, b \in \mathbb{N} : a > 1, b > 1, ab = p$.

The only positive factors of a prime p are 1 and p itself.

- Some primes: $2, 3, 5, 7, 11, 13, \cdots$

Definition (Composite)

Non-prime integers greater than 1 are called composite, because they can be composed by multiplying two integers greater than 1.

The Fundamental Theorem of Arithmetic

Theorem

Every positive integer has a unique representation as the product of a non-decreasing series (its "Prime Factorization") of zero or more primes. E.g.,

- $1 =$ *(product of empty series)* $= 1$;
- $2 = 2$ *(product of series with one element 2)*;
- $4 = 2 \cdot 2$ *(product of series* $2, 2$*)*;
- $2000 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5$;
- $2001 = 3 \cdot 23 \cdot 29$;
- $2002 = 2 \cdot 7 \cdot 11 \cdot 13$;
- $2003 = 2003$.

Theorem

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

Theorem

There are infinitely many primes.

Problem

Are all numbers in the form $2^n - 1$ for $n \in Z^+$ primes?

- $2^2 - 1 = 3$, $2^3 - 1 = 7$, *and* $2^5 - 1 = 31$ *are primes.*
- $2^4 - 1 = 15$ *and* $2^{11} - 1 = 2047 = 23 \cdot 89$ *are composites.*

Greatest Common Divisor

Definition

The greatest common divisor $\gcd(a, b)$ of integers a, b (not both 0) is the largest (most positive) integer d that is a divisor both of a and of b.

- $d = \gcd(a, b) = \max_{d|a \wedge d|b} d$.
- $d|a \wedge d|b \wedge (\forall e \in \mathbb{Z} : (e|a \wedge e|b) \rightarrow d \geq e)$.

Example

$\gcd(24, 36) = ?$

Solution

Positive common divisors: $1, 2, 3, 4, 6, 12$. *The greatest one is* 12.

GCD Shortcut

- If the prime factorizations are written as $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{bn}$, then the GCD is given by

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}.$$

Example

$a = 84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^1 \cdot 7^1;$
$b = 96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3^1 \cdot 7^0;$
$\gcd(84, 96) = 2^2 \cdot 3^1 \cdot 7^0 = 2 \cdot 2 \cdot 3 = 12.$

Relative Primality

Definition (Coprime)

Integers a and b are called relatively prime or coprime iff their GCD is 1. E.g.,

- 21 and 10 are coprime. $21 = 3 \cdot 7$ and $10 = 2 \cdot 5$, so they have no common factors > 1, so their GCD is 1.

Definition (Relatively prime)

A set of integers $\{a_1, a_2, \cdots\}$ is (pairwise) relatively prime if all pairs a_i, a_j for $i \neq j$ are relatively prime. E.g.,

- $\{7, 8, 15\}$ is relatively prime, but $\{7, 8, 12\}$ is not relatively prime.

Least Common Multiple

Definition (Least Common Multiple (LCM))

$\mathrm{lcm}(a, b)$ of positive integers a and b is the smallest positive integer that is a multiple both of a and of b.

- $m = \mathrm{lcm}(a, b) = \min_{a|m \wedge b|m} m$.
- $a|m \wedge b|m \wedge (\forall n \in \mathbb{Z} : (a|n \wedge b|n) \rightarrow (m \leq n))$.

Example

$\mathrm{lcm}\,(6, 10) = 30$

- If the prime factorizations are written as $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{bn}$,then the LCM is given by

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

§3.6 Integers & Algorithms

Topics

- Euclidean algorithm for finding GCD's.
- Base-b representations of integers.
  - Especially: binary, hexadecimal, octal.
  - Also: Two's complement representation of negative numbers.
- Algorithms for computer arithmetic.
  - Binary addition, multiplication, division.

Euclid's Algorithm for GCD

- Finding GCDs by comparing prime factorizations can be difficult if the prime factors are unknown.
- Euclid discovered that for all integers a and b,

$$\gcd(a, b) = \gcd((a \bmod b), b).$$

- Sort a, b so that $a > b$, and then (given $b > 1$) $(a \bmod b) < a$, so problem is simplified.

Example (Euclid's Algorithm Example)

Find $\gcd(372, 164)$.

Solution

$\gcd(372, 164) = \gcd(372 \mod 164, 164)$;

- $372 \bmod 164 = 372 - 164\lfloor 372/164 \rfloor = 372 - 164 \cdot 2 = 372 - 328 = 44$.

$\gcd(164, 44) = \gcd(164 \bmod 44, 44)$;

- $164 \bmod 44 = 164 - 44\lfloor 164/44 \rfloor = 164 - 44 \cdot 3 = 164 - 132 = 32$.

$\gcd(44, 32) = \gcd(44 \bmod 32, 32) = \gcd(12, 32)$;
$\gcd(32, 12) = \gcd(32 \bmod 12, 12) = \gcd(8, 12)$;
$\gcd(12, 8) = \gcd(12 \bmod 8, 8) = \gcd(4, 8)$;
$\gcd(8, 4) = \gcd(8 \bmod 4, 4) = \gcd(0, 4) = 4$.

Euclid's Algorithm Pseudocode

procedure gcd(a, b: positive integers)
  while $b \neq 0$
    $r = a \bmod b$; $a = b$; $b = r$;
  return a;

- Sorted inputs are not necessary.
- The number of while loop iterations is $O(\log \max(a, b))$.

Base-b Number Systems

Definition (The "base b expansion of n")

For any positive integers n and b, there is a unique sequence $a_k a_{k-1} \cdots a_1 a_0$ of digits $a_i < b$ such that

$$n = \sum_{i=0}^{k} a_i b^i.$$

- Ordinarily we write base-10 representations of numbers (using digits $0 - 9$).
- 10 isn't special; any base $b > 1$ will work.

Particular Bases of Interest

- Base $b = 10$ (decimal): used only because we have 10 fingers
  10 digits: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.
- Base $b = 2$ (binary): used internally in all modern computers
  2 digits: $0, 1$. ("Bits" = "binary digits.")
- Base $b = 8$ (octal): octal digits correspond to groups of 3 bits
  8 digits: $0, 1, 2, 3, 4, 5, 6, 7$.
- Base $b = 16$ (hexadecimal): hex digits give groups of 4bits
  16 digits: $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$

Converting to Base b

- Informal algorithm to convert any integer n to any base $b > 1$:
  1. To find the value of the rightmost (lowest-order) digit, simply compute $n \bmod b$.
  2. Now replace n with the quotient $\lfloor n/b \rfloor$.
  3. Repeat above two steps to find subsequent digits, until n is gone (i.e., $n = 0$).

Problem

Write down the pseudocode.

Addition of Binary Numbers

procedure add($a_{n-1} \cdots a_0, b_{n-1} \cdots b_0$: binary representations of non-negative integers a and b)

$carry = 0$
for $bitIndex = 0$ **to** $n-1$ {go through bits}
begin
$bitSum = a_{bitIndex} + b_{bitIndex} + carry$ {2-bit sum}
$s_{bitIndex} = bitSum \bmod 2$ {low bit of sum}
$carry = \lfloor bitSum/2 \rfloor$ {high bit of sum}
end
$s_n = carry$
return $s_n \cdots s_0$ {binary representation of integer s}

Multiplication of Binary Numbers

procedure multiply($a_{n-1} \cdots a_0, b_{n-1} \cdots b_0$: binary representations of $a, b \in \mathbb{N}$)

    product = 0
    for $i = 0$ **to** $n - 1$
        if $b_i = 1$ **then** $\mathit{product} = \mathrm{add}(a_{n-1} \ldots a_0 0^i, \mathit{product})$
    return *product*

- $a_{n-1} \ldots a_0 0^i$: i extra 0-bits appended after $a_{n-1} \ldots a_0$.

Modular Exponentiation

procedure mod_exp($b \in \mathbb{Z}$, $n = (a_{k-1}a_{k-2}\ldots a_0)_2$, $m \in \mathbb{Z}^+$)

$x = 1$

$power = b \bmod m$

for $i = 0$ **to** $k - 1$

begin

if $a_i = 1$ **then** $x = (x \cdot power) \bmod m$

$power = (power \cdot power) \bmod m$

end

return x

§3.7 Applications of Number Theory

Extended Euclidean Algorithm

- If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

Example

Express $\gcd(252, 198) = 18$ as a linear comination of 252 and 198.

Solution

Step 1: Euclidean algorithm

$$\begin{aligned} \gcd(252, 198) &= \gcd(54, 198) && 252 = 1 \times 198 + 54 \\ &= \gcd(54, 36) && 198 = 3 \times 54 + 36 \\ &= \gcd(36, 18) && 54 = 1 \times 36 + 18 \\ &= \gcd(18, 0) \end{aligned}$$

Solution ((Cont.))

Step 2: Backward substitution

$$\begin{aligned} 18 &= 54 - 36 \\ &= 54 - (198 - 3 \times 54) \\ &= 4 \times 54 - 198 \\ &= 4 \times (252 - 198) - 198 \\ &= 4 \times 252 - 5 \times 198. \end{aligned}$$

Some Lemmas

Lemma

If a, b, and c are positive integers such that $\gcd(a, b) = 1$ and $a|bc$, then $a|c$.

Proof.

Since $\gcd(a, b) = 1, \exists s, t$: $sa + tb = 1$.
Multiply by c, *then* $sac + tbc = c$.
$\because a|sac$ *and* $a|tbc \therefore a|sac + tbc$ $\square$

Lemma

If p is a prime and $p|a_1a_2 \ldots a_n$ where each a_i is an integer, then for some i, $p|a_i$.

Cancellation Rule

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 $a \equiv b \pmod{m}$.

Proof.

Since $ac \equiv bc \pmod{m}$, $ac - bc = c(a - b) \equiv 0 \pmod{m}$.
In other words, $m | c(a - b)$.
$\because \gcd(c, m) = 1 \therefore m | a - b$.
$a \equiv b \pmod{m}$. $\square$

Existence of Inverse

Definition

a, b, and $m > 1$ are integers. If $ab \equiv 1 \bmod m$, b is called an inverse of a modulo m.

Theorem

If a and m are relatively prime integers and $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.

Proof.

Since a and m are relatively prime, i.e. $\gcd(a, m) = 1$, there exist integers s and t such that $1 = sa + tm$. Then,

1. $sa \equiv 1 \bmod m$.
2. *s is unique.*

□

Example

Find the inverse of 5 modulo 7.

Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)

Let $m_1, m_2, \cdots, m_n$ be pairwise relatively prime positive integers, and $m = m_1 m_2 \cdots m_n$. The system

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution modulo m.

Solutions

- Let $M_k = m/m_k$ for $k = 1, 2, \cdots, n$.
- Since $\gcd(m_k, M_k) = 1$, we can find y_k such that $M_k y_k \equiv 1 \bmod m_k$ for $k = 1, 2, \cdots, n$.
- Let $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n \bmod m$.
- Note that $M_j \equiv 0 \bmod m_k$ whenever $j \neq k$.
- We have $x \equiv a_k M_k y_k \equiv a_k \bmod m_k$.

Example

Find the solution of the system

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

Solution

$m = 3 \cdot 5 \cdot 7$
$M_1 = m/3 = 35,\ y_1 \equiv (M_1)^{-1} \equiv 2 \pmod{3}$
$M_2 = m/5 = 21, y_2 \equiv (M_2)^{-1} \equiv 1 \pmod{5}$
$M_3 = m/7 = 15,\ y_3 \equiv (M_3)^{-1} \equiv 1 \pmod{7}$
$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233 \equiv 23 \pmod{105}$.

Variations of CRT

Example

Find the solution of the system

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 2 \pmod 7 \end{aligned}$$

Fermat's Little Theorem

Theorem

If p is prime and a is an integer not divisible by p, then

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Furthermore, for every integer a we have

$$a^p \equiv a (\mathrm{mod}\, p).$$

RSA Systems

- Choose two large prime p and q.
  - $n = pq$: modulus
  - e: encryption key which is coprime to $(p-1)(q-1)$
  - d: decryption key such that $de \equiv 1 \bmod (p-1)(q-1)$
- M: message
- RSA encryption:
  - $C \equiv M^e \bmod n$: ciphertext (the encrypted message)
- RSA decryption:
  - $M \equiv C^d \bmod n$

Example

Here is an example of RSA.

- Let $p = 43$, $q = 59$, and $n = pq = 2537$.
- Choose $e = 13$ and $d = 937$.
  - $\gcd(13, (p-1)(q-1)) = \gcd(13, 42 \times 58) = 1$.
  - $d = e^{-1} \bmod (p-1)(q-1)$
- Assume $M = 1819$
- Encryption: $C \equiv M^e \bmod n$
  - $C = 1819^{13} \bmod 2537 = 2081$.
- Decryption: $M \equiv C^d \bmod n$
- $M = 2081^{937} \bmod 2537 = 1819$.

Why Does It Work?

- Correctness
  - $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} (\bmod n)$.
  - By Fermat's Little Theorem, we have
    - $C^d \equiv M \cdot (M^{p-1})^{k(q-1)} \equiv M \cdot 1 \equiv M (\bmod p)$.
    - $C^d \equiv M \cdot (M^{q-1})^{k(p-1)} \equiv M \cdot 1 \equiv M (\bmod q)$.
  - By Chinese Remainder Theorem, we have
    - $C^d \equiv M (\bmod n)$.
- The factor decomposition is a hard problem

Public Key System

- Make n and e public. (e is call public key and d is call private key.)
- A wants to send a secret message to B
  - A uses B's public key to encrypt the message and then sends the ciphertext to B.
  - After B receives the ciphertext, he can use his own private key to decrypt the ciphertext.
- A wants to send a message to B and prove his identity
  - A first generates a hash value from the message and encrypts the hash value by his own private key and then sends the plaintext message and the encrypted hash value to B.
  - After B receives the message, he decrypts the hash value by A's public key. Besides, he also generates a hash value from the plaintext message. If both match, it proves the message comes from A.