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
Definition

Let \( a, b \in \mathbb{Z} \) with \( a \neq 0 \).

\[ a \mid b \equiv \text{“} a \text{ divides } b \text{” \equiv “} \exists c \in \mathbb{Z} : b = ac \text{”}. \]

“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

\[ 3 \mid -12 \iff \text{T}; \text{ but } 3 \mid 7 \iff \text{F}. \]

Example

“\( b \) is even” \( \equiv 2 \mid b \). Is 0 even? Is \(-4\)?
Facts: the Divides Relation

Theorem

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

1. \( a \mid 0 \) for any \( a \neq 0 \).
2. \( (a \mid b \land a \mid c) \rightarrow a \mid (b + c) \).
3. \( a \mid b \rightarrow a \mid bc \).
4. \( (a \mid b \land b \mid c) \rightarrow a \mid c \)

Proof.

(2) \( a \mid b \) means there is an \( s \) such that \( b = as \), and \( a \mid c \) means that there is a \( t \) such that \( c = at \), so \( b + c = as + at = a(s + t) \), so \( a \mid (b + c) \) also.
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 $\exists$) $a = dq + r$ and $0 \leq r < |d|$.

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

- 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 $a \mod d$ 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 $(a \mod d)$ by: $a - d \cdot \lfloor a/d \rfloor$.
- In C programming language, “%” = 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 $m \mid a - b$.

- Also equivalent to $(a - b) \mod m = 0$.
- 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 $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we have
  - $a + c \equiv b + d \pmod{m}$, and
  - $ac \equiv bd \pmod{m}$

**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,

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

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

- Some primes: 2, 3, 5, 7, 11, 13, ... 

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.,

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

If $n$ is a composite 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 $n \in \mathbb{Z}^+$ 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 $b$.

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

**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 $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, 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.
Definition (Least Common Multiple (LCM))

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

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

Example

\( \text{lcm}(6, 10) = 30 \)

- If the prime factorizations are written as \( a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \) and \( b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n} \), then the LCM is given by
  \[
  \text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}.
  \]
§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 \(b\),
  \[
  \gcd(a, b) = \gcd((a \mod b), b).
  \]
- Sort \(a, b\) so that \(a > b\), and then (given \(b > 1\)) \((a \mod b) < a\), so problem is simplified.
Example (Euclid’s Algorithm Example)

Find gcd (372, 164).

Solution

\[ \text{gcd} (372, 164) = \text{gcd} (372 \mod 164, 164); \]

- \[ 372 \mod 164 = 372 - 164 \lfloor \frac{372}{164} \rfloor = 372 - 164 \cdot 2 = 372 - 328 = 44. \]

\[ \text{gcd} (164, 44) = \text{gcd} (164 \mod 44, 44); \]

- \[ 164 \mod 44 = 164 - 44 \lfloor \frac{164}{44} \rfloor = 164 - 44 \cdot 3 = 164 - 132 = 32. \]

\[ \text{gcd} (44, 32) = \text{gcd} (44 \mod 32, 32) = \text{gcd} (12, 32); \]
\[ \text{gcd} (32, 12) = \text{gcd} (32 \mod 12, 12) = \text{gcd} (8, 12); \]
\[ \text{gcd} (12, 8) = \text{gcd} (12 \mod 8, 8) = \text{gcd} (4, 8); \]
\[ \text{gcd} (8, 4) = \text{gcd} (8 \mod 4, 4) = \text{gcd} (0, 4) = 4. \]
Euclid’s Algorithm Pseudocode

```pseudocode
procedure gcd(a, b: positive integers)
    while b ≠ 0
        r = a mod b; a = b; b = r;
    return a;
```

- Sorted inputs are not necessary.
- The number of while loop iterations is $O(\log \max(a, b))$.
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 4 bits.
  - 16 digits: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.
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 $n \mod b$.
2. Now replace $n$ with the quotient $\left\lfloor n/b \right\rfloor$.
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 $b$)

1. $carry = 0$
2. for $bitIndex = 0$ to $n - 1$ {go through bits}
3. \begin{align*}
    bitSum &= a_{bitIndex} + b_{bitIndex} + carry \quad \{2$-bit sum\} \\
    s_{bitIndex} &= bitSum \mod 2 \quad \{low \ bit \ of \ sum\} \\
    carry &= \lfloor bitSum/2 \rfloor \quad \{high \ bit \ of \ sum\}
\end{align*}
4. end
5. $s_n = carry$
6. 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 product = add($a_{n-1} \cdots a_00^i$, product)
    return product

- $a_{n-1} \cdots a_00^i$: $i$ extra 0-bits appended after $a_{n-1} \cdots a_0$. 
Modular Exponentiation

\[
\text{procedure } \text{mod\_exp}(b \in \mathbb{Z}, n = (a_{k-1} a_{k-2} \ldots a_0)_2, m \in \mathbb{Z}^+) \\
\begin{aligned} 
& x = 1 \\
& \text{power} = b \mod m \\
& \text{for } i = 0 \text{ to } k - 1 \\
& \quad \text{begin} \\
& \qquad \text{if } a_i = 1 \text{ then } x = (x \cdot \text{power}) \mod m \\
& \qquad \text{power} = (\text{power} \cdot \text{power}) \mod m \\
& \quad \text{end} \\
& \text{return } x
\end{aligned}
\]
§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 combination of 252 and 198.

**Solution**

*Step 1: Euclidean algorithm*

\[
\begin{align*}
gcd(252, 198) & = gcd(54, 198) & 252 = 1 \times 198 + 54 \\
& = gcd(54, 36) & 198 = 3 \times 54 + 36 \\
& = gcd(36, 18) & 54 = 1 \times 36 + 18 \\
& = gcd(18, 0)
\end{align*}
\]
Solution (Cont.)

Step 2: Backward substitution

\[
18 = 54 - 36 \\
= 54 - (198 - 3 \times 54) \\
= 4 \times 54 - 198 \\
= 4 \times (252 - 198) - 198 \\
= 4 \times 252 - 5 \times 198.
\]
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 $sac + tbc = c$.
\[\therefore a | sac \text{ and } a | tbc \therefore a | sac + tbc\]

Lemma

If $p$ is a prime and $p | a_1 a_2 \ldots a_n$ 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, $m | c(a - b)$.

$\therefore \gcd(c, m) = 1 \therefore m | a - b$.

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

\square$
**Existence of Inverse**

**Definition**

$a, b, \text{ and } m > 1$ are integers. If $ab \equiv 1 \mod m$, $b$ 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. $sa \equiv 1 \mod m$.
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

\[
\begin{align*}
x & \equiv a_1 \pmod{m_1} \\
x & \equiv a_2 \pmod{m_2} \\
& \quad \vdots \\
x & \equiv a_n \pmod{m_n}
\end{align*}
\]

has a unique solution modulo $m$. 
Solutions

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

Find the solution of the system

\[
\begin{align*}
x & \equiv 2 \pmod{3} \\
x & \equiv 3 \pmod{5} \\
x & \equiv 2 \pmod{7}
\end{align*}
\]

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

\[ x \equiv 2 \pmod{3} \]
\[ x \equiv 3 \pmod{5} \]
\[ x \equiv 2 \pmod{7} \]
Fermat’s Little Theorem

Theorem

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

$$a^{p-1} \equiv 1 \pmod{p}.$$  

Furthermore, for every integer $a$ we have

$$a^p \equiv a \pmod{p}.$$
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 $de \equiv 1 \mod (p - 1)(q - 1)$
- $M$: message
- RSA encryption:
  - $C \equiv M^e \mod n$: ciphertext (the encrypted message)
- RSA decryption:
  - $M \equiv C^d \mod n$
Example

Here is an example of RSA.

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

- Correctness
  - $C^d \equiv (M^e)^d = M^{de} = M^{1+k(p-1)(q-1)} \pmod{n}$.
  - By Fermat’s Little Theorem, we have
    - $C^d \equiv M \cdot (M^{p-1})^k(q-1) \equiv M \cdot 1 \equiv M \pmod{p}$.
    - $C^d \equiv M \cdot (M^{q-1})^k(p-1) \equiv M \cdot 1 \equiv M \pmod{q}$.
  - By Chinese Remainder Theorem, we have
    - $C^d \equiv M \pmod{n}$.

- 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.