University of Hawaii

ICS141: Discrete Mathematics for Computer Science I

Dept. Information & Computer Sci., University of Hawaii

Jan Stelovsky

based on slides by Dr. Baek and Dr. Still

Originals by Dr. M. P. Frank and Dr. J.L. Gross

Provided by McGraw-Hill

Quiz

University of Hawaii

- What is the big-theta of a polynomial?
- What is the worst-case algorithmic complexity of:
  - linear search
  - binary search
  - bubble sort
  - insertion sort
- Use pseudocode to define the "division algorithm"

Lecture 17

Chapter 3. The Fundamentals

3.4 The Integers and Division

3.5 Primes and Greatest Common Divisors

The Division "Algorithm"

- It's really just a *theorem*, not an algorithm…
  - Only called an "algorithm" for historical reasons.

- **Theorem:** For any integer ***dividend*** a and ***divisor*** $d \in \mathbf{Z}^+$, there are <u>unique</u> integers ***quotient*** q and ***remainder*** $r \in \mathbf{N}$ such that $a = dq + r$ and $0 \leq r < d$. Formally, the theorem is:

$$\boxed{\forall a \in \mathbf{Z}, d \in \mathbf{Z}^+ : \exists! q, r \in \mathbf{Z} : 0 \leq r < d,\ a = dq + r}$$

- We can find q and r by: $q = \lfloor a/d \rfloor$, $r = a - dq$

The mod Operator

- An integer "division remainder" operator.
- Let $a,d \in \mathbf{Z}$ 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.
  Also, a **div** d denotes the quotient q.
- We can compute (a **mod** d) by:

$$a - d \cdot \lfloor a/d \rfloor = a - dq.$$

- In C/C++/Java languages, "%" = mod.

The mod Operator: Examples

University of Hawaii

- $101 = 11 \cdot 9 + 2$ (dividend: 101, divisor: 11)
  - 101 **div** 11 = 9 101 **mod** 11 = 2
- $-11 = 3 \cdot (-4) + 1$ or $\cancel{-11 = 3 \cdot (-3) - 2}$?
  (dividend: –11, divisor: 3)
  - –11 **div** 3 = –4 –11 **mod** 3 = 1
    (quotient: –4, remainder: 1)
- Note that the remainder must not be negative.

Modular Congruence

University of Hawaii

- Let $a,b\in\mathbf{Z}$, $m\in\mathbf{Z}^+$, where $\mathbf{Z}^+ = \{n\in\mathbf{Z} \mid n > 0\} = \mathbf{N} - \{0\}$ (the positive integers).
- Then ***a is congruent to b modulo m***, written "$a \equiv b$ (**mod** m)", iff $m|(a - b)$.
  - Note: this is a different use of "≡" than the meaning "equivalent" or "is defined as" used before.
- It's also equivalent to: $(a - b)$ **mod** $m = 0$.
- E.g. $17 \equiv 5$ (**mod** 6), $24 \not\equiv 14$ (**mod** 6)

Useful Congruence Theorems

University of Hawaii

- **Theorem:** Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:

  $a \equiv b \ (\mathbf{mod}\ m) \Leftrightarrow a \ \mathbf{mod}\ m = b \ \mathbf{mod}\ m$.

- **Theorem:** Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:

  $a \equiv b \ (\mathbf{mod}\ m) \Leftrightarrow \exists k \in \mathbf{Z}\colon a = b + km$.

- **Theorem:** Let $a,b,c,d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \ (\mathbf{mod}\ m)$ and $c \equiv d \ (\mathbf{mod}\ m)$, then:
  - $a + c \equiv b + d \ (\mathbf{mod}\ m)$, and
  - $ac \equiv bd \ (\mathbf{mod}\ m)$

Congruence Theorem Example

- $7 \equiv 2$ (**mod** 5) and $11 \equiv 1$ (**mod** 5).
  - $7 + 11 = 18$ and $2 + 1 = 3$

    Therefore, $7 + 11 \equiv 2 + 1$ (**mod** 5)
  - $7 \times 11 = 77$ and $2 \times 1 = 2$

    Therefore, $7 \times 11 \equiv 2 \times 1$ (**mod** 5)

Applications of Congruence

- Hashing Functions (hashes)
- Pseudorandom Numbers
- Cryptology
- Universal Product Codes
- International Standard Book Numbers

Hashing Functions

University of Hawaii

- We want to quickly store and retrieve records in memory locations.
- A hashing function takes a data item to be stored or retrieved and computes the first choice for a location for the item.
- $h(k) = k \textbf{ mod } m$
  - A hashing function h assigns memory location $h(k)$ to the record that has k as its key.
  - $h(064212848) = 064212848 \textbf{ mod } 111 = 14$
  - $h(037149212) = 037149212 \textbf{ mod } 111 = 65$
  - $h(107405723) = 107405723 \textbf{ mod } 111 = 14 \Rightarrow$ collision!
  - Find the first unoccupied memory location after the occupied memory.
    - In this case, assign memory location 15.
- If collision occurs infrequently, and if when one does occur it is resolved quickly, then hashing provides a very fast method of storing and retrieving data.

Cryptology (I)

University of Hawaii

- The study of secret messages
- **Encryption** is the process of making a message secret. **Decryption** is the process of determining the original message from the encrypted message.
- Some simple early codes include *Caesar's cipher*:
  - Assign an integer from 0 to 25 to each letter based on its position in the alphabet.
  - Caesar's encryption method: $f(p) = (p + 3) \textbf{ mod } 26$
  - Caesar's decryption method: $f^{-1}(p) = (p - 3) \textbf{ mod } 26$
  - MEET YOU IN THE PARK $\Rightarrow$
    PHHW BRX LQ WKH SDUN

Cryptology (II)

University of Hawaii

- Caesar's encryption method does not provide a high level of security
- A slightly better approach: $f(p) = (ap + b)$ **mod** 26
  - **Example 10:**

    What letter replaces the letter *K* when the function $f(p) = (7p + 3)$ **mod** 26 is used for encryption?

  - 10 represents *K*
  - $f(10) = (7\times10 + 3)$ **mod** $26 = 73$ **mod** $26 = 21$
  - 21 represents *V*
  - Therefore, *K* is replaced by *V* in the encrypted message

Prime Numbers

- An integer $p > 1$ is ***prime*** iff the only positive factors of p are 1 and p itself.
- Some primes: 2, 3, 5, 7, 11, 13,...
- 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

University of Hawaii

Its "Prime Factorization"

- Every positive integer greater than 1 has a *unique* representation as a prime or as the product of a non-decreasing series of two or more primes.
  - Some examples:
    - $2 = 2$ (a prime 2)
    - $4 = 2 \cdot 2 = 2^2$(product of series 2, 2)
    - $2000 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^4 \cdot 5^3$

      $2001 = 3 \cdot 23 \cdot 29$

      $2002 = 2 \cdot 7 \cdot 11 \cdot 13$

      $2003 = 2003$ (no clear pattern!)

Prime Numbers: Theorems

- **Theorem 2**: If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$
  - **Proof**: If n is composite then we have $n = ab$ for $1 < a < n$ and a positive integer b greater than 1. Show that $a \le \sqrt{n}$ or $b \le \sqrt{n}$. (Use proof by contradiction)

    If $a > \sqrt{n}$ and $b > \sqrt{n}$, then $ab > n$ (Contradiction!)

    Therefore, $a \le \sqrt{n}$ or $b \le \sqrt{n}$, i.e. n has a positive divisor not exceeding $\sqrt{n}$ (a or b).

    By the *Fundamental Theorem of Arithmetic*, this divisor is either a prime, or has a prime divisor less than itself. In either case, n has a prime divisor less than or equal to $\sqrt{n}$

Prime Numbers: Theorems

- Contrapositive of Theorem 2:

  An integer is prime if it is not divisible by any prime less than or equal to its square root $\sqrt{n}$

- Example: Show that 101 is prime
  - Primes not exceeding $\sqrt{101}$: 2, 3, 5, 7
  - 101 is not divisible by any of 2, 3, 5, or 7
  - Therefore, 101 is a prime

Prime Factorization

- **Example 4**: Fine the prime factorization of 7007 ($\sqrt{7007} \approx 83.7$)
  - Perform division of 7007 by successive primes

    $7007 / 7 = 1001 \qquad (7007 = 7 \cdot 1001)$
  - Perform division of 1001 by successive primes beginning with 7

    $1001 / 7 = 143 \qquad (7007 = 7 \cdot 7 \cdot 143)$
  - Perform division of 143 by successive primes beginning with 7

    $143 / 11 = 13 \qquad (7007 = 7 \cdot 7 \cdot 11 \cdot 13$

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

Greatest Common Divisor

University of Hawaii

- The ***greatest common divisor*** gcd(a,b) of integers a, b (not both 0) is the largest integer d that is a divisor both of a and of b.

$$d = \gcd(a,b) = \max(d\colon d|a \wedge d|b)$$
$$\Leftrightarrow d|a \wedge d|b \wedge \forall e\in \mathbf{Z}, (e|a \wedge e|b) \rightarrow (d \geq e)$$

- **Example:** gcd(24,36) = ?
  - Positive divisors of 24: 1, 2, 3, 4, 6, 8, 12, 24
  - Positive divisors of 36: 1, 2, 3, 4, 6, 9, 12, 18, 36
  - Positive common divisors: 1, 2, 3, 4, 6, 12. The largest one of these is 12.

Relative Primality

- Integers a and b are called ***relatively prime*** or ***coprime*** iff their gcd = 1.
- **Example:** Neither 21 nor 10 is prime, but they are *relatively prime*. (divisors of 21: 1, 3, 7, 21; divisors of 10: 1, 2, 5, 10; so they have no common factors > 1, so their gcd = 1.
- A *set* of integers $\{a_1, a_2, a_3,\ldots\}$ is ***pairwise relatively prime*** if all pairs (a_i, a_j), for $i \neq j$, are relatively prime.

GCD Shortcut

University of Hawaii

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

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

- Example of using the shortcut:
  - $a = 84 = \underline{2 \cdot 2} \cdot \underline{3} \cdot 7 \qquad = 2^2 \cdot 3^1 \cdot 7^1$
  - $b = 96 = \underline{2 \cdot 2} \cdot 2 \cdot 2 \cdot 2 \cdot \underline{3} \quad = 2^5 \cdot 3^1 \cdot 7^0$
  - $\gcd(84,96) \qquad = 2^2 \cdot 3^1 \cdot 7^0 = 2 \cdot 2 \cdot 3 = 12.$

Least Common Multiple

- lcm(a,b) of positive integers a, b, is the smallest positive integer that is a multiple both of a and of b. *E.g.* lcm(6,10) = 30

$$m = \text{lcm}(a,b) = \min(m\colon a|m \wedge b|m)$$

$$\Leftrightarrow a|m \wedge b|m \wedge \forall n\in\mathbf{Z}\colon (a|n \wedge b|n) \rightarrow (m \leq n)$$

- **Example:** lcm(24,36) = ?
  - Positive multiples of 24: 24, 48, $\underline{72}$, 96, 120, $\underline{144}$,…
  - Positive multiples of 36: 36, $\underline{72}$, 108, $\underline{144}$,…
  - Positive common multiples: 72, 144,…

    The smallest one of these is 72.

LCM Shortcut

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

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

- Example of using the shortcut:
  - $a = 84 = 2 \cdot 2 \cdot 3 \cdot 7 = 2^2 \cdot 3^1 \cdot 7^1$
  - $b = 96 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 = 2^5 \cdot 3^1 \cdot 7^0$
  - $\operatorname{lcm}(84,96) = 2^5 \cdot 3^1 \cdot 7^1 = 32 \cdot 3 \cdot 7 = 672$

LCM: Another Example

University of Hawaii

- Example 15:

  What is the least common multiple of $2^3 \cdot 3^5 \cdot 7^2$ and $2^4 \cdot 3^3$?

- Solution:

  $\mathrm{lcm}(2^3 \cdot 3^5 \cdot 7^2,\ 2^4 \cdot 3^3)$

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

  $= 2^4 \cdot 3^5 \cdot 7^2$

GCD and LCM

- **Theorem**: Let a and b be positive integers. Then

$$ab = \gcd(a,b) \times \mathrm{lcm}(a,b)$$

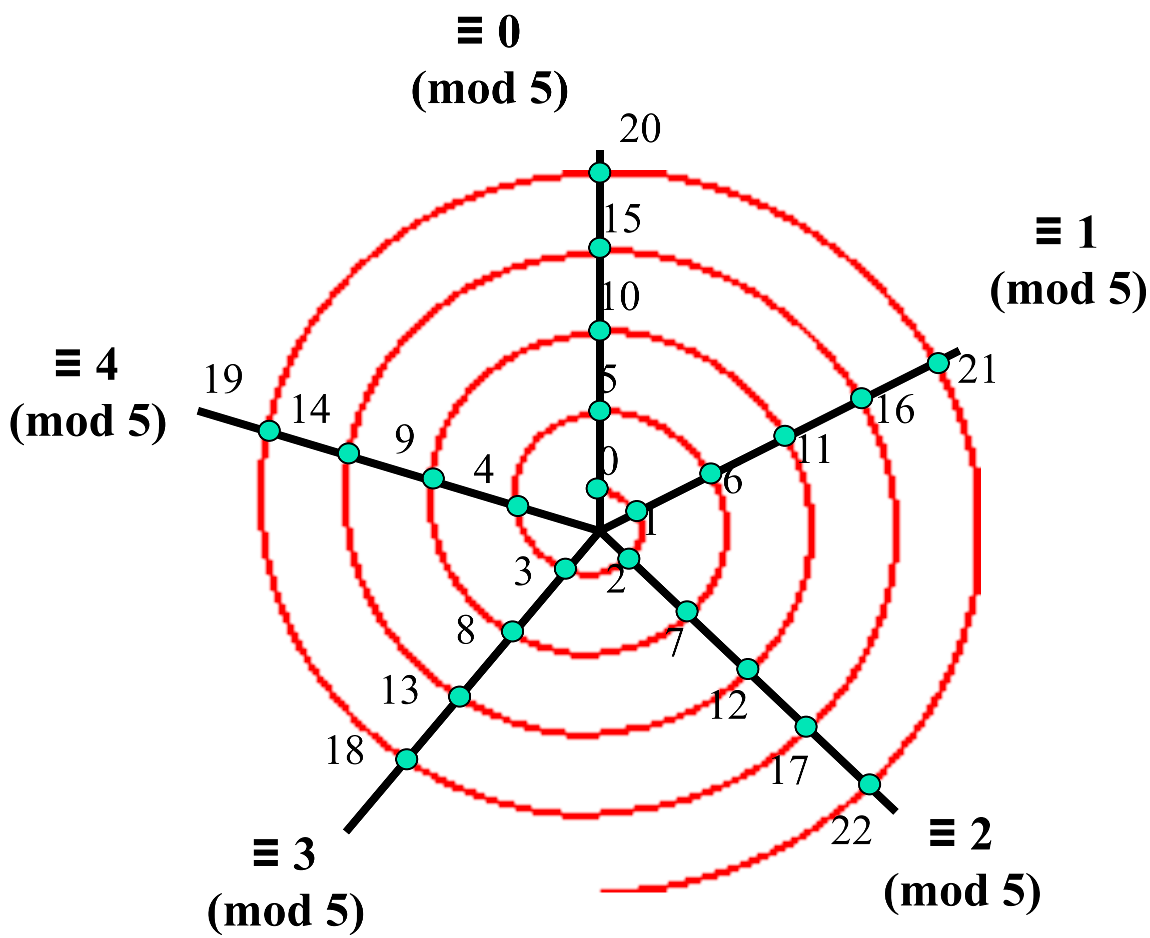
- Example
  - $a = 84 = 2\cdot2\cdot3\cdot7 \qquad = 2^2\cdot3^1\cdot7^1$
  - $b = 96 = 2\cdot2\cdot2\cdot2\cdot2\cdot3 = 2^5\cdot3^1\cdot7^0$
  - $ab = (2^2\cdot3^1\cdot7^1)\cdot(2^5\cdot3^1\cdot7^0) = 2^2\cdot3^1\cdot7^0\cdot2^5\cdot3^1\cdot7^1$

$$= \underline{2^{\min(2,5)}\cdot3^{\min(1,1)}\cdot7^{\min(1,0)}}\cdot\underline{2^{\max(2,5)}\cdot3^{\max(1,1)}\cdot7^{\max(1,0)}}$$

$$= \gcd(a,b) \times \mathrm{lcm}(a,b)$$

Spiral Visualization of mod

- Example shown: modulo-5 arithmetic



Pseudorandom Numbers

- Numbers that are generated deterministically, but that appear random for all practical purposes.
  - We need to repeat the same sequence when testing!
- Used in many applications, such as:
  - Hash functions
  - Simulations, games, graphics
  - Cryptographic algorithms
- One simple common pseudo-random number generating procedure:
  - The *linear congruential method*
    - Uses the **mod** operator

Linear Congruential Method

University of Hawaii

- Requires four natural numbers:
  - The *modulus m,* the *multiplier a*, the *increment c*, and the *seed* x_0.
    - where $2 \leq a < m$, $0 \leq c < m$, $0 \leq x_0 < m$.
- Generates the pseudo-random sequence $\{x_n\}$ with $0 \leq x_n < m$, via the following:

$$x_{n+1} = (ax_n + c) \textbf{ mod } m$$

- Tends to work best when a, c, m are prime, or at least relatively prime.
- If $c = 0$, the method is called a *pure multiplicative generator*.

Example

University of Hawaii

- Let modulus $m = 1{,}000 = 2^3 \cdot 5^3$.
  - To generate outputs in the range 0-999.
- Pick increment $c = 467$ (prime), multiplier $a = 293$ (also prime), seed $x_0 = 426$.
- Then we get the pseudo-random sequence:

$x_1 = (ax_0 + c)$ **mod** $m = 285$

$x_2 = (ax_1 + c)$ **mod** $m = 972$

$x_3 = (ax_2 + c)$ **mod** $m = 263$ and so on…

Prime Numbers: Theorems

University of Hawaii

- **Theorem 3**: There are infinitely many primes. (Euclide)

- Assume: there are only finite many primes $p_1, p_2, \ldots, p_n$
- Let $Q = p_1 p_2 \cdots p_n + 1$
- Then, Q is prime or it can be written as the product of two or more primes (by Fundamental Theorem of Arithmetic)
- None of the primes p_i divides Q
  (if $p_i | Q$ then $p_i | (Q - p_1 p_2 \cdots p_n)$, i.e. $p_i | 1$)
- Hence there is a prime not in the list $p_1, p_2, \ldots, p_n$, which is either Q itself or a prime factor of Q (CONTRADICTION!!)

Mersenne Primes

- **Definition**: A ***Mersenne prime*** is a prime number of the form $2^p - 1$, where p is prime.

prime p	$2^p - 1$	Mersenne?
2	$2^2 - 1 = 3$	yes
3	$2^3 - 1 = 7$	yes
5	$2^5 - 1 = 31$	yes
7	$2^7 - 1 = 127$	yes
11	$2^{11} - 1 = 2047 = 23 \cdot 89$	no
11,213	$2^{11,213} - 1$	yes
19,937	$2^{19,937} - 1$	yes
3,021,377	$2^{3,021,377} - 1$	Yes (late 1998)
43,112,609	$2^{43,112,609} - 1$	Yes (MID 2008)

largest Mersenne prime known (with almost 13 million digits)