Izmir Institute of Technology

CENG 115
Discrete Structures

Slides are based on the Text
***Discrete Mathematics & Its Applications* (6th Edition)**
by Kenneth H. Rosen

Slides were prepared by Dr. Michael P. Frank
for COT 3100 course in University of Florida

Module #10:
Basic Number Theory

Rosen 6th ed., Sections 3.4-3.6

§ 3.4: The Integers and Division

- Of course you already know what the integers are, and what division is…
- **But:** There are some specific notations, terminology, and theorems associated with these concepts which you may not know.
- These form the basics of *number theory*.
  - Vital in many important algorithms today (hash functions, cryptography, digital signatures).

Divides, Factor, Multiple

- Let $a,b \in \mathbf{Z}$ with $a \neq 0$.
- $a|b \equiv$ "*a divides b*" $:\equiv$ "$\exists c \in \mathbf{Z}$: $b=ac$"
  "There exists an integer c such that c times a equals b."
  - Example: $3|-12 \Leftrightarrow$ **True**, but $3|7 \Leftrightarrow$ **False**.
- If a divides b, then we say a is a *factor* or a *divisor* of b, and b is a *multiple* of a.
- "b is even" means $2|b$. Is 0 even? Is -4?

Facts about the Divides Relation

- $\forall a,b,c \in \mathbf{Z}$:
  1. $a|0$
  2. $(a|b \wedge a|c) \rightarrow a \mid (b + c)$
  3. $a|b \rightarrow a|bc$
  4. $(a|b \wedge b|c) \rightarrow a|c$
- **Proof** of (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. ■

The Division "Algorithm"

- Actually it is a *theorem*, not an algorithm. The name is used here for historical reasons.
- Let a an integer and d a positive integer, There are unique integers q and r such that $a = dq + r$ with $0 \le r < d$.
- a is *dividend, d is divisor*, q is *quotient* and r is *remainder.*
- $\forall a,d \in \mathbf{Z}, d>0: \exists! q,r \in \mathbf{Z}: 0 \le r < |d|, a = dq + r.$

The **mod** and **div** operators

- **mod** is the "division remainder" operator:

  $r = a \textbf{ mod } d$

- **div** operator give the *quotient*:

  $q = a \textbf{ div } d$

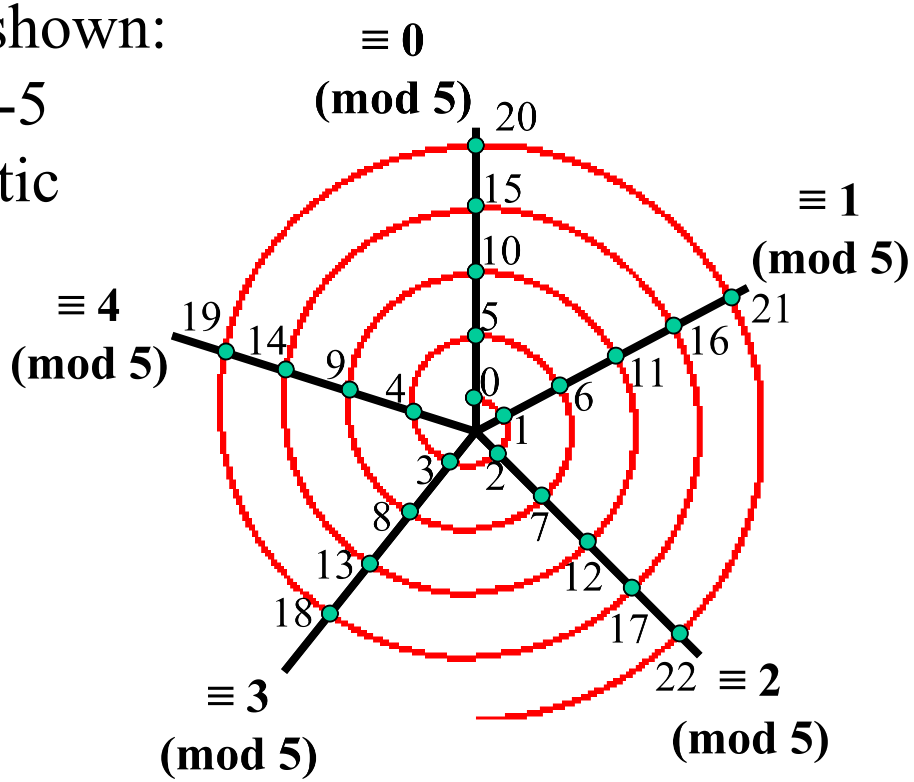
  Also, $q = \lfloor a/d \rfloor$

Modular Arithmetic

- Let $\mathbf{Z}^+=\{n\in\mathbf{Z} \mid n>0\}$, the positive integers.
- Let $a,b\in\mathbf{Z}$, $m\in\mathbf{Z}^+$.
- Then *a is congruent to b modulo m*, written "$a\equiv b \pmod{m}$", iff $m \mid (a-b)$.
- Also equivalent to: $(a-b) \bmod m = 0$.

Spiral Visualization of **mod**

Example shown:
modulo-5
arithmetic



Useful Congruence Theorems

- Let $a,b \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then:
  $a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbf{Z}\ a = b + km.$
- Let $a,b,c,d \in \mathbf{Z}$, $m \in \mathbf{Z}^+$. Then if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then:
  - $a+c \equiv b+d \pmod{m}$, and
  - $ac \equiv bd \pmod{m}$

Simple Encryption

Variations of the following have been used to encrypt messages for thousands of years.

1. Convert a message to capitals.
2. Think of each letter as a number between 1 and 26.
3. Apply an invertible modular function to each number.
4. Convert back to letters (0 becomes 26).

Letter ←→ Number Conversion Table

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Caesar's Cipher

- One of the earliest use of cryptology was by Julius Caesar.
- He made messages secret by shifting each letter three letters forward in the alphabet:

$f(a) = (a+3)\ \mathbf{mod}\ 26$

E.g.

MEET ME

12 4 4 19 12 4

15 7 7 22 15 7

PHHW PH

A Harder Encryption Example

Let the encryption function be

$$f(a) = (3a + 9) \textbf{ mod } 26$$

Encrypt “Stop Thief”

1. STOP THIEF
2. 19,20,15,16   20,8, 9, 5, 6
3. 14,17, 2, 5   17,7,10,24,1
4. NQBE QGJXA

Decryption example

In decryption, you apply the inverse function.

E.g.: Find the inverse of

$$f(a) = (3a + 9) \textbf{ mod } 26$$

Unfortunately, inverse is not

$$f^{-1}(a) = 3^{-1}(a - 9)$$

We' ll see later that

- gcd(3,26)=1, there is an inverse of 3 modulo 26.
- The inverse of 3 modulo 26 is the number 9.

Thus: $f^{-1}(a) = 9(a - 9) \textbf{ mod } 26 = (9a - 3) \textbf{ mod } 26$

§ 3.5: Prime Numbers

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

$$p>1 \land \neg\exists a,b\in\mathbf{N}\ (a>1 \land b>1 \land ab=p)$$

- The only positive factors of a prime 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.

Prime Factorization

Every positive integer greater than 1 can be written uniquely as a prime or a product of a non-decreasing series of two or more primes.

- $2 = 2$ (a prime number)
- $4 = 2 \cdot 2$ (product of series with two elements 2,2)
- $2000 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5$; $2001 = 3 \cdot 23 \cdot 29$;
  $2002 = 2 \cdot 7 \cdot 11 \cdot 13$; $2003 = 2003$

A Theorem on Composite Numbers

- If n is a composite number, then n has a prime divisor less than or equal to $\sqrt{n}$.
- Can you prove this?

  Hint: Proof by contradiction.

- Use the theorem to show that 101 is prime.

Greatest Common Divisor

- 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: $d|a \wedge d|b$) $\Leftrightarrow$
  $d|a \wedge d|b \wedge \forall e \in \mathbf{Z}, (e|a \wedge e|b) \rightarrow d \geq e$

- Example: gcd(24,36)=?
  Positive common divisors: 1,2,3,4,6,12…
  Greatest is 12.

GCD shortcut

- If the prime factorizations are written as

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

then the GCD is given by:

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

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

Relatively Prime

- Integers *a* and *b* are called *relatively prime* iff their gcd = 1.
  - E.g. Neither 21 and 10 are prime, but they are *relatively prime*. $21=3\cdot 7$ and $10=2\cdot 5$, so they have no common factors > 1, so their gcd = 1.

Least Common Multiple

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

$$m = \text{lcm}(a,b) = \min(m\!: a|m \wedge b|m) \Leftrightarrow$$
$$a|m \wedge b|m \wedge \forall n \in \mathbf{Z}\!: (a|n \wedge b|n) \rightarrow (m \leq n)$$

- If the prime factorizations are written as

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

then the LCM is given by

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

§ 3.6: Integers & Algorithms

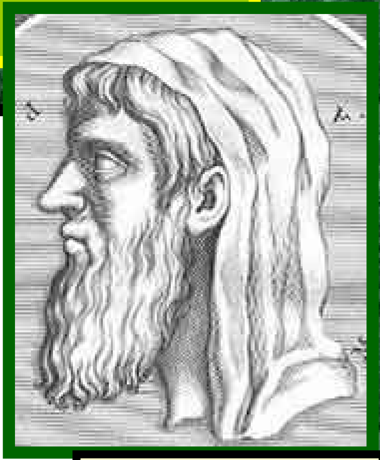
- Topics:
  - Euclidean algorithm for finding GCD
  - Modular exponentiation
  - Base-*b* representations of integers.
    - Especially: binary, hexadecimal, octal

Euclid's Algorithm for GCD

- Euclid discovered:

  For all integers a, b,
  $\gcd(a, b) = \gcd((a \bmod b), b)$.

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



Euclid of Alexandria 325-265 B.C.

Euclid's Algorithm Example

- $\gcd(372,164) = \gcd(372 \bmod 164, 164)$.
  - $372 \bmod 164 = 372-164\lfloor 372/164\rfloor = 372-164\cdot 2 = 372-328 = 44$.
- $\gcd(164,44) = \gcd(164 \bmod 44, 44)$.
  - $164 \bmod 44 = 164-44\lfloor 164/44\rfloor = 164-44\cdot 3 = 164-132 = 32$.
- $\gcd(44,32) = \gcd(44 \bmod 32, 32) = \gcd(12, 32) = \gcd(32 \bmod 12, 12) = \gcd(8,12) = \gcd(12 \bmod 8, 8) = \gcd(4,8) = \gcd(8 \bmod 4, 4) = \gcd(0,4) = 4$.

Euclid's Algorithm Pseudocode

procedure $gcd(a, b$: positive integers)

while $b \neq 0$

$r := a$ **mod** b; $a := b$; $b := r$

end

{gcd is a}

Sorting inputs (a,b) not needed, order will be reversed each iteration.

Fast! Number of while loop iterations turns out to be $O(\log(\max(a,b)))$.

Modular Exponentiation

$7^{194} \bmod 11 = ?$

$7^{194} \bmod 11 = (7^{128} \bmod 11) \cdot (7^{64} \bmod 11) \cdot (7^{2} \bmod 11)$

Modular Exponentiation

$7^{194} \bmod 11 = ?$ $\qquad 194 = (11000010)_2 \rightarrow 7^{194} = 7^{128} \cdot 7^{64} \cdot 7^{2}$

$7^{1} \pmod{11} \equiv 7 \pmod{11} \equiv 7$

$7^{2} \pmod{11} \equiv 5$ $\qquad$ 5 is stored into x.

$7^{4} \pmod{11} \equiv 5^{2} \pmod{11} \equiv 3$

$7^{8} \pmod{11} \equiv 3^{2} \pmod{11} \equiv 9$

$7^{16} \pmod{11} \equiv 9^{2} \pmod{11} \equiv 4$

$7^{32} \pmod{11} \equiv 4^{2} \pmod{11} \equiv 5$

$7^{64} \pmod{11} \equiv 5^{2} \pmod{11} \equiv 3$ $\qquad$ x is updated as $3 \cdot 5 = 15$.

$7^{128} \pmod{11} \equiv 3^{2} \pmod{11} \equiv 9$ $\qquad$ x is updated as $9 \cdot 15 = 135$.

The result is returned as $135 \pmod{11} = 3$.

Modular Exponentiation

procedure modular exponentiation (b:integer,
$n=(a_{k-1}\ a_{k-2} \ldots a_1\ a_0)_2$, m: positive integers)

x:=1

$power$:=b **mod** m

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

begin

if a_i=1 **then** x:=(x*$power$) **mod** m

$power$:=($power$*$power$) **mod** m

end

{x equals b^n **mod** m}

Base-b number systems

- Ordinarily we write *base*-10 representations of numbers (using digits 0-9).
- 10 isn't special; any base b>1 will work.
- For any positive integers n,b there is a unique sequence $\underbrace{a_k\, a_{k\text{-}1} \ldots\, a_1 a_0}$ of *digits* $a_i<b$ such that

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

The "*base b expansion of n*"

Particular Bases of Interest

- Base b=10 (decimal):
  10 digits: 0,1,2,3,4,5,6,7,8,9.
- Base b=2 (binary):
  2 digits: 0,1. ("Bits"="binary digits.")
- Base b=8 (octal):
  8 digits: 0,1,2,3,4,5,6,7.
- Base b=16 (hexadecimal):
  16 digits: 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

Used only because we have 10 fingers

Used internally in all modern computers

Octal digits correspond to groups of 3 bits

Hex digits give groups of 4 bits

Converting to decimal expansion

- What is the decimal expansion of hexadecimal expansion $(2AE0B)_{16}$?

$2\cdot 16^4+10\cdot 16^3+14\cdot 16^2+0\cdot 16+11\cdot 1=(175627)_{10}$