

# Discrete Mathematical Structures

## CS 3233 Lecture 24

Prof. William Winsborough

November 2 and 7, 2005

# Business

- This makeup lecture replaces the lecture scheduled for October 24 which Prof. Winsborough had to cancel due to illness

# The Division Algorithm

- The algorithm that isn't an algorithm:
- Theorem: Let  $a$  and  $d$  be integers with  $d > 1$ 
  - There are unique integers  $q$  and  $r$  with  $0 \leq r < d$ , such that  $a = dq + r$
  - $d$  is the *divisor*,  $a$  is the *dividend*,  $q$  is the *quotient*, and  $r$  is the *remainder*
  - $q = a \operatorname{div} d$
  - $r = a \operatorname{mod} d$

- Examples

$$11 \operatorname{div} 3 = 3$$

$$-11 \operatorname{div} 3 = 4$$

$$11 \operatorname{mod} 3 = 2$$

$$-11 \operatorname{mod} 3 = 1$$

# Modular Arithmetic

- Def: Let  $a$ ,  $b$ , and  $m$  be integers and let  $m$  be positive.  $a$  is *congruent to  $b$  modulo  $m$*  if  $m$  divides  $a - b$ 
  - Notation:  $a \equiv b \pmod{m}$

# Modular Arithmetic

- Theorem: Let  $a$ ,  $b$ , and  $m$  be integers and let  $m$  be positive.

$a \equiv b \pmod{m}$  if and only if

$a \bmod m = b \bmod m$

$\Leftarrow$ ) By definition of mod, there exists  $q_a$  and  $q_b$  such that  $a = mq_a + r_a$  and  $b = mq_b + r_b$  in which  $r_a = a \bmod m = b \bmod m = r_b$ .

Thus  $a - b = (mq_a + r_a) - (mq_b + r_b)$

$= m(q_a - q_b) + 0$ , showing that  $m$  divides  $a - b$

$\Rightarrow$ ) Assignment 9, exercise 22, section 2.4

# Congruence Classes

- Theorem: Let  $m$  be a positive integer. The integers  $a$  and  $b$  are congruent modulo  $m$  if and only if there is an integer  $k$  such that  $a = b + km$
- Definition: The *congruence class* of  $a$  modulo  $m$  is the set of all integers congruent to  $a$  modulo  $m$ 
  - The theorem gives us a way of constructing this set

# Properties of Modular Arithmetic

- Let  $m$  be a positive integer.  
If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then  
 $a + c \equiv b + d \pmod{m}$  and  
 $ac \equiv bd \pmod{m}$

# One Application of Congruence

- Rudimentary Cryptology: The Caesar cipher
  - Letters correspond to integers from 0 to 25
    - $A \approx 0, \dots, Z \approx 25$
  - Encrypt:  $f(p) = (p+3) \bmod 26$
  - Decrypt:  $f^{-1}(p) = (p - 3) \bmod 26$

# Euler's Observation

- Sum of  $i$  between 1 and  $n$