

# Math 321

Properties:  $f$   $a \equiv b \pmod{m}$

my notation  $a \equiv_m b$

(1) (Def)  $m \mid (a-b)$

Th<sup>m</sup>  $\Rightarrow$  (2)  $a \pmod{m} = b \pmod{m}$

$\Rightarrow$  (3)  $a = b + km \quad k \in \mathbb{Z}$

Th<sup>m</sup> given  $a \equiv_m b, c \equiv_m d$

ex  $2 \equiv_5 7 \equiv_5 -3$

$4 \equiv_5 14 \equiv_5 -6$

(1)  $a + c \equiv_m b + d$

(2)  $ac \equiv_m bd$

ex  $(3) x \equiv_2 4$

$\Rightarrow (1) x \equiv_2 4$

$x \equiv_2 4 \stackrel{?}{=} 0$

$\dots \equiv_2 1 \equiv_2 3 \equiv_2 5 \equiv_2 7 \equiv_2 \dots$

so  $x \equiv_2 0$

Corollary ①  $(a+b) \pmod m = ((a \pmod m) + (b \pmod m)) \pmod m$

②  $(ab) \pmod m = ((a \pmod m)(b \pmod m)) \pmod m$



Ex  $(99)^{102} \pmod 3 = \underbrace{99 \cdot 99 \dots 99}_{102} \pmod 3 = 0$  b/c  $99 \pmod 3 = 0$


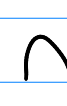





$(101)^{102} \pmod 3 = 2^{102} \pmod 3 = \underbrace{(2 \cdot 2 \cdot 2 \dots 2)_{102}}_{4 \equiv 1} \pmod 3$   
 $= 2^{102} \pmod 3 = 4^{51} \pmod 3 = (1)^{51} \pmod 3 = 1$

Numbers:  $\cdot, \cdot\cdot, \cdot\cdot\cdot, \cdot\cdot\cdot\cdot, \cdot\cdot\cdot\cdot\cdot, \cdot\cdot\cdot\cdot\cdot\cdot, \dots$  (Unary)

4.2 Representing Numbers

- ① unary
- ② grouping

Roman: VI =  IV = 

Egyptian:  ,  ,  ,  ,  ,  , 

1            10            100            1000            10,000            100,000            1,000,000

(3) positional grouping (base b expansion)

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_1 b + a_0$$

$$b \geq 2, 0 \leq a_i < b, a_k \neq 0$$

$$n = (a_k, a_{k-1}, \dots, a_1, a_0)_b$$

ex)  $1,204 = (1, 2, 0, 4)_{10}$

$\uparrow \quad \uparrow \quad \uparrow \quad \uparrow$   
 1000's 100's 10's 1's

(ex)  $(1, 0, 1, 1)_2 = 1 \cdot 8 + 0 \cdot 4 + 1 \cdot 2 + 1 = (11)__{10}$

(ex)  $(3, 7, 2, 1)_9 = 3 \cdot 9^3 + 7 \cdot 9^2 + 2 \cdot 9 + 1 = ( )_{10}$

$\underbrace{\quad}_9^3 \quad \underbrace{\quad}_9^2 \quad \underbrace{\quad}_9^1$

convert

base 10  $\rightarrow$  base b?

$$n = a_k b^k + \dots + a_1 b + a_0$$

$$n = \underbrace{(a_k b^{k-1} + \dots + a_2 b + a_1)}_{\text{div}} \cdot b + \underbrace{a_0}_{\text{mod}}$$

$$n \bmod b = a_0$$

$$n \operatorname{div} b = (a_k b^{k-1} \dots a_1)$$

loop

loop  
on this  
till  $n=0$

$i = 0$   
 $a_i = n \bmod b$   
 $n = n \operatorname{div} b$   
 $i = i + 1$

$$(1, 2, 3, 4)_{10} = (1, 2, 3, 4)_2$$

↓

$$617 = (1, 0, 0, 1, 1, 0, 1, 0, 0, 1, 0)_2$$

↓

$$308 \rightarrow 154 \rightarrow 77 \rightarrow 38 \rightarrow 19 \rightarrow 9, 4$$

Operations ①  $( )_b + ( )_b$

②  $( )_b * ( )_b$

$$\begin{array}{r} 1 \\ (1, 2, 3)_4 \end{array}$$

$$\begin{array}{r} 2 \quad 2 \\ (-1, 2, 3)_4 \end{array}$$

$$+ (2, 0, 3)_4$$

$$\times (3)_4$$

$$\hline (3, 3, 2)_4$$

$$\hline (1, 1, 0, 1)_4$$

Next

class

convert  
to base 10

and check

✓