Math 321

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

my notation $a \underset{m}{\equiv} b$

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

thm → (2) $a \bmod m = b \bmod m$

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

---

thm given $a \underset{m}{\equiv} b$, $c \underset{m}{\equiv} d$

ex $2 \underset{5}{\equiv} 7 \underset{5}{\equiv} -3 \qquad 4 \underset{5}{\equiv} 14 \underset{5}{\equiv} -6$

(1) $a + c \underset{m}{\equiv} b + d$

(2) $ac \underset{m}{\equiv} bd$

ex $3x \underset{2}{\equiv} 4$

$\rightarrow 0 \cdot x \underset{2}{\equiv} 4$

$x \underset{2}{\equiv} 4 \underset{2}{\equiv} 0 \qquad$ so $x \underset{2}{\equiv} 0$

$\ldots \underset{2}{\equiv} 1 \underset{2}{\equiv} 3 \underset{2}{\equiv} 5 \underset{2}{\equiv} 7 \underset{2}{\equiv} \ldots$

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

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

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

$(101)^{102} \bmod 3 = 2^{102} \bmod 3 = \underbrace{(2 \cdot 2) \cdot 2 \cdots 2}_{102} \bmod 3$ ($4 \equiv_3 1$)

$= 2^{102} \bmod 3 = 4^{51} \bmod 3 = (1)^{51} \bmod 3 = 1$

---

numbers: ·, ··, ···, ····, ····· ... (unary)

4.2 Representing Numbers

① unary

② grouping

Roman: VI = ····· (V) IV = ···· (X)

IIIIV

Egyptian: | (1), ∩ (10), 𓍢 (100), 𓆼 (1000), 𓂭 (10,000), 𓆐 (100,000), 𓁨 (1,000,000)

(3) positional grouping (base b expansion)

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

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

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

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

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

9^3 9^2 9

convert

base 10 → base b?

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

$$n = (a_k b^{k-1} + \cdots + a_2 b + a_1) \cdot b + a_0$$

$$n = (\quad) \cdot b + \square$$

div mod

$n \bmod b = a_0$

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

loop

$i = 0$

loop on this till $n = 0$:

$q_i = n \bmod b$

$n = n \operatorname{div} b$

$i = i + 1$

$(1,2,3,4)_{10} =$ ~~$(0,0,0,0,0,0,0,0,0,0,0)_2$~~

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

6 17

3 0 5 → 1 5 4 → 7 7 → 3 8 → 1 9 → 9, 4

Operations ① $(\quad)_b + (\quad)_b$

② $(\quad)_b * (\quad)_b$

$(1,2,3)_4$ $\quad$ $(1,2,3)_4$

$+ (2,0,3)_4$ $\quad$ $\times (3)_4$

$(3,3,2)_4$ $\quad$ $(1,1,0,1)_4$

Next class

Convert to base 10 and check