Math 321

Q's 7) $ac \mid bc \rightarrow a \mid b$

Show $(ac \cdot k_1 = bc \rightarrow a \cdot k_2 = b)$

assume $ac \cdot k_1 = bc$

$$ac k_1 = bc$$
$$ak = b$$
$$a \mid b$$

(4.2) Numbers (of any base)

ops: $+, \times, \text{div\_mod}, b^n \bmod n$

$$n = (a_k, \ldots, a_2, a_1, a_0)_b = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$$
$$0 \le a_k < b$$

base conversion:

$$(1,2,3)_5 = 1 \cdot 5^2 + 2 \cdot 5 + 3 = (3,2)_{10}$$

otherway (ex) $(1,2,3)_{10}$ into base $(2)_4$

$$n = (a_k b^k + \cdots + a_2 b^2 + a_1 b) + a_0$$

$$n = \underbrace{(a_k b^{k-1} + \cdots + a_2 b + a_1)}_{\text{quotient}} b + a_0$$

n: dividend; b: divisor; a_0: remainder

apply division algorithm recursively

$(1,2,3)_{10} = (1,3,2,3)_4$

$123 = (30)4 + (3)$
$30 = (7)4 + (2)$
$7 = (1)4 + (3)$
$1 = (0)4 + (1)$

Check: $(1,3,2,3)_4 = 1 \cdot 64 + 3 \cdot 16 + 2 \cdot 4 + 3$

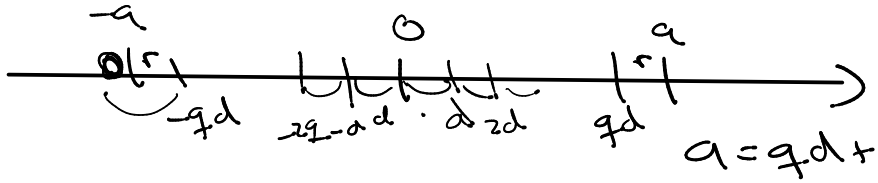
Add | Multiply

$$\begin{array}{r} {}^{1}(1,2,3)_{10} \\ +\ (9,4)_{10} \\ \hline (2,1,7)_{10} \end{array} \qquad \begin{array}{r} {}^{1\ 1}(1,2,3)_4 \\ +\ (1,3)_4 \\ \hline (2,0,2)_4 \end{array} \qquad (3)_4 + (3)_4 = (1,2)_4$$

$$\begin{array}{r} (1,2,3)_4 \\ \times\ (1,3)_4 \\ \hline (1,1,0,1)_4 \\ (1,2,3,0)_4 \\ \hline (2,3,3,1)_4 \end{array} \qquad \begin{array}{r} (1,2,3)_{10} \\ \times\ (2,4)_{10} \\ \hline (4,9,2)_{10} \\ (2,4,6,0)_{10} \\ \hline \end{array}$$

---

(3) Div_Mod



p. 253

function $[q, r] = \text{div\_mod}(a, d)$

$q = 0$

$r = |a|$

while $r \geq d$

$q = q + 1$

$r = r - d$

end

if $a < 0$ and $r \neq 0$

$q = -(q+1)$

$r = d - r$

else if $a < 0$ and $r = 0$

$q = -q$

end

end

$b^n \bmod m$

$5678^{9101} \bmod 12371$

1234

① $b^n = \underbrace{b \cdot b \cdot b \cdot b \cdots b}_{n \text{ times}}$ ② $(a \cdot b) \bmod m$

$(a \bmod m)(b \bmod m) \bmod m$

Slow way: ans = 1 $b^n \bmod m$

for K=1 to n

ans = ans · b mod m

end

Ex $14^{1025} \bmod 17$ — loop 1025 times

Fast Way $b^n \bmod m$ $n = (a_k, \ldots, a_2, a_1, a_0)_2$

$n = a_k \cdot 2^k + \cdots + a_2 \cdot 4 + a_1 \cdot 2 + a_0$

$b^n \bmod m = b^{(a_k 2^k + \cdots + a_2 4 + a_1 2 + a_0)} \bmod m$

$(b^{2^k})^{a_k} \cdots (b^4)^{a_2} (b^2)^{a_1} (b)^{a_0} \bmod m \quad a_i = \{0,1\}$

$1025 = (1,0,0,0,0,0,0,0,0,0,1)_2$

1 — loop 1025

loop of 11

Ex $3^{2003} \bmod 99$

$2003 = (1,1,1,1,1,0,1,0,0,1,1)_2$

$2003 = (1001)_2 + 1$

$1001 = (500) \cdot 2 + 1$

$500 = (250) \cdot 2 + 0$

$250 = (125) \cdot 2 + 0$

$125 = (62) \cdot 2 + 1$

$62 = (31) \cdot 2 + 0$

bits	3^{bits}	mod 99
1	3	3
1	3^2	9
0	3^4	81
0	3^8	$81^2 \bmod 99 =$
1	3^{16}	
0	;	
1		

Numbers → useful operators...

Need Primes

Def: $n \geq 2$ is prime if its only factors are $1, n$

otherwise it is composite
