Math 321

Base-b representations of numbers

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

① add
② mult.
③ convert: $n = (1,7)_{10} = (\ ?\ )_3$

use: $n = a_k b^k + \cdots + a_2 b^2 + a_1 b + a_0$

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

$n \bmod b = r$

$n = (1,7)_{10}$ — expansion → mod 3 → div 3

mod 3	div 3
2	5
5 mod 3	5 div 3
2	1
1 mod 3	1 div 3
1	

$n = (1,2,2)_3$

check $(1,2,2)_3 = 1 \cdot 9 + 2 \cdot 3 + 2 \cdot 1 = 17$

$9\ \ 3\ \ 1$

---

basic numbers $(1,1)_{10} = (1,3)_8$

$1\ \ 1$

8's $\ \ 1$'s

$$(3,7,2)_8 \times (4,3)_8$$

$$+(1,7,5,0,0)_8$$

$$(2,4,0,5,6)_8$$

$21 = (2,5)_8$

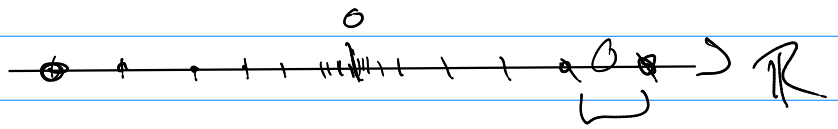
$11 = (1,3)_8$

$29 = (3,5)_8$

$15 = (1,7)_8$

---

app $b^n \bmod m$



$(21)(17) \bmod 5 = (1 \cdot 2) \bmod 5 = 2$

$b^n \bmod m$

tech #1 (slow) $(b \cdot b \cdot b \cdot b \cdot b \cdot \cdots b) \bmod m$ — n times

$b^2 \bmod m$

$4^7 \bmod 7 = (4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \cdot 4) \bmod 7 = \boxed{4}$

tech #2 $n = (a_k 2^k + \cdots + a_2 2^2 + a_1 2 + a_0) = (a_k, \ldots, a_2, a_1, a_0)_2$

$a_i = 0$ or 1

$b^n = b^{a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_2 2^2 + a_1 2 + a_0}$

$a^{b+c} = a^b a^c \quad a^{bc} = (a^b)^c$

$= (b^{2^k})^{a_k} (b^{2^{k-1}})^{a_{k-1}} \cdots (b^{2^2})^{a_2} (b^2)^{a_1} (b)^{a_0} \bmod m$

$B^1 \quad B^2$

$(1,0,1,1,0,1)_2 = 45$ (32 16 8 4 2 1)

$17^{45} \pmod 5$

$(17^1)(17^4)(17^8)(17^{32}) \pmod 5 = \boxed{2}$

4.3 Primes 1, (2), (3), 4, (5), 6, 7, 8, 9, 10, 11, 12, ...

Prime: p is prime if its only factors are $1 \cdot p$

not prime: composite: n has a factor, c, such that $2 \le c \le n-1$

Fund. th^m of Arithmetic 1, (2), (3), (2^2), (5), (2·3), (7), (2^3), (3^2), ...

n is prime or a unique prod of primes in non-dec. order.