# Math 321

**Q's**

$(4,0,5)_6$

$+ \underline{(2,5,4)_6}$

$(1,1,0,3)_6$

$(9)_{10} = (1,3)_6$

$(6)_{10} = (1,0)_6$

$(7)_{10} = (1,1)_6$

$(4,0,5)_6$

$\times \underline{(2,3)_6}$

$(2,0,2,3)_6$

$+ \underline{(1,2,4,0)_6}$

$(1,4,2,0,3)_6$

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

$\times \underline{(2,4)_{10}}$

$(4,9,2)_{10}$

$+ \underline{(2,4,6,0)_{10}}$

$(2,9,5,2)_{10}$

---

Algorithms for ① div, mod

② $b^n \bmod m$

---

div_mod $(a,b)$ returns $q = \text{div}(a,b)$, $r = \text{mod}(a,b)$

$q = 0$

$r = |a|$

while $r \geq d$

$q = q + 1$

$r = r - d$

end while

$a = q \cdot b + r$

if $a<0$ and $r>0$

$q = -(q+1)$

and if $r = -(r-d)$ $\{= d-r\}$

---

② $b^n \bmod m = (b \cdot b \cdot b \cdots b) \bmod m$ ($n$-times)

Ver #1 →

```
ans = 1
loop K = 1 to n
    ans = (ans * b) mod m
end
```

Version #2

$b^n \bmod m$ ← base 2 expansion

where $a_i = 0$ or $1$

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

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

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

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

ex $(3)^n \bmod 4$

$(3^{a_k} \cdots (3^{a_3})(3^{a_2})(3^{a_1})(3^{a_0}) \bmod 4$

$3 \bmod 4 = 3$

$3^2 \bmod 4 = 1$

$3^4 \bmod 4 = (3^2)^2 \bmod 4 = 1^2 \bmod 4 = 1$

algorithm $b^n \bmod m$

part ① $n = a_k 2^k + \cdots + a_2 2^2 + a_1 2 + a_0$

$n = (a_k, \ldots, a_2, a_1, a_0)_2$

part ② $ans = 1$

$inside = b \bmod m$

for $a_0, a_1, a_2, \ldots, a_k$

if $a_i = 1$

$ans = (ans * inside) \bmod m$

end if

$inside = (inside^2) \bmod m$

end for

---

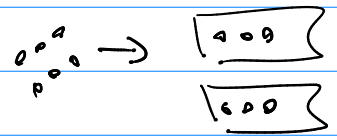
why? $b^{(n \text{ million})}$

version #1 loop is $\sim 1{,}000{,}000$

version #2 loop is $\sim 20$

Primes

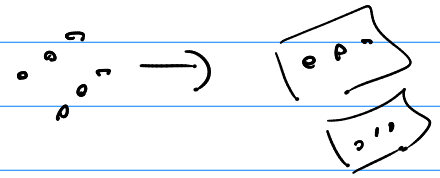
Divisible → 2|6



Note: $1 \mid n$, $n \mid n$ for all $n \geq 1$ (trivial truth)

Ignore that

what about number that have more than this?



2|6 and 3|6

→ numbers that only have $1 \mid n$, $n \mid n$

call prime

→ numbers that have other divisors (2|12)

call composite