

# Mash 321

Q15

$3^{2003} \pmod{99}$

inside = power

$x = \text{ans.}$

2003

$a_0$  (1)

3 → 1

1001

$a_1$  (7)

9 → 3

500

$a_2$  0

81 → 27

250

$a_3$  0

27 → 27

125

$a_4$  (1)

36 → 27

62

$a_5$  0

9 → 81

31

$a_6$  (1)

81 → 81

15

$a_7$  (1)

27 → 27

7

$a_8$  (1)

36 → 36

3

$a_9$  (1)

9 → 9

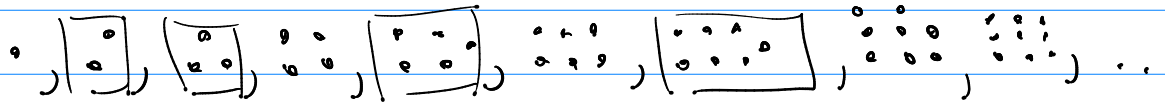
1

$a_{10}$  (1)

81 → 81

27

Primes:



Primes:

$p \geq 2$ , and  $p$  has only 1 and  $p$  as factors.

Composite

(not prime)  $c \geq 2$  is composite

$\exists a, 2 \leq a \leq c-1$   
exists such that  $a|c$

Fund. th<sup>m</sup> of Arith for all integers  $n \geq 2$ ,  
 $n$  can be written as a unig. prod. of primes  
in non-dec. order.

Note:  $3 = (3)$  & 'product' of 1 prime

$$12 = (2^2 \cdot 3)$$

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, ...

$(2), (3), (2^2), (5), (2 \cdot 3), (7), (2^3), (3^2), (2 \cdot 5), (11), (2^2 \cdot 3), \dots$

---

Finding Primes. (prime factorization)

th<sup>m</sup> if  $n$  is composite then there is a prime,  $p$ ,  
such that  $p | n$  &  $p \leq \sqrt{n}$

ex  $12 \rightarrow$  b/c of th<sup>m</sup> check 2, 3

$$12 = 2 \cdot \boxed{6} = 2^2 \cdot 3$$

ex  $\boxed{101} \rightarrow 2 \nmid 101, 3 \nmid 101, 5 \nmid 101, 7 \nmid 101$   
Prime.

# Sieve of Eratosthenes

Prime Sieve ..

1, 2, 3, ~~4~~, 5, ~~6~~, 7, ~~8~~, ~~9~~, ~~10~~  
11, ~~12~~, 13, ~~14~~, ~~15~~, ~~16~~, 17, ~~18~~, 19, ~~20~~  
~~21~~, ~~22~~, 23, ~~24~~, ~~25~~, ...

How many primes?

Guess: primes are finite

Primes =  $\{ p_1, p_2, p_3, \dots, p_n \}$

Consider:  $Q = (p_1 \cdot p_2 \cdot \dots \cdot p_n) + 1$

Note: all numbers have a prime factor.

(ex  $3|3$  <sub>? prime</sub>,  $2|12$  <sub>? composite?</sub>)

→ so some prime,  $p_i$ , divides  $Q$

→  $p_i | Q$  and obviously  $p_i | p_1 \cdot p_2 \cdot \dots \cdot p_n$

(know:  $a|b \wedge a|c \rightarrow a|mb+nc$ )

→  $p_i | (Q) - (p_1 \cdot p_2 \cdot \dots \cdot p_n) \rightarrow p_i | 1 \equiv 1$

Th<sup>n</sup> Primes of infinite.

PF see above

How dense?

Def  $\pi(n) = \#$  of primes at or below  $n$

ex  $\pi(10) = 4$ ,  $\pi(11) = 5$ ,  $\pi(12) = 5$

$$\pi(25) = 9$$

Th<sup>n</sup>  $\pi(x) \sim \left\lfloor \frac{x}{\ln x} \right\rfloor$

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln(x)} = 1$$

ex  $\pi(10^6) \sim \frac{10^6}{\ln(10^6)} = \frac{10^6}{6 \ln(10)}$

% Prims:  $\frac{\pi(x)}{x} \sim \frac{x / \ln x}{x} = \frac{1}{\ln x}$

oops

gcd(a,b) vs lcm(a,b)

largest int (g) such that g|a and g|b

Smallest int (l) such that a|l and b|l

finding gcd, lcm

Prime factors

a = p1^a1 p2^a2 ... pk^ak

b = p1^b1 p2^b2 ... pk^bk

ex

a = 2^0 3^2 5^1 7^3

b = 2^1 3^0 5^2 7^0

min(a1,b1) min(a2,b2) min(ak,bk)

gcd(a,b) = p1 p2 ... pk

ex gcd(a,b) = 2^0 3^0 5^1 7^0 = 5

lcm(a,b) = p1^max(a1,b1) p2^max(a2,b2) ... pk^max(ak,bk)

ex lcm(a,b) = 2^1 3^2 5^2 7^3

Thm

gcd \* lcm = a \* b