Math 321

Q's $3^{2003} \bmod 99$

			inside = power	x = ans.
			3	1
2003	a_0	1	9	3
1001	a_1	1	81	27
500	a_2	0	27	27
250	a_3	0	36	27
125	a_4	1	9	81
62	a_5	0	81	81
31	a_6	1	27	27
15	a_7	1	36	36
7	a_8	1	9	9
3	a_9	1	81	81
1	a_{10}	1		27

Primes: 1, 2, 3, 5, 7, 11, 13, ...

Primes: $p \geq 2$, and p has only 1 and p are factors.

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

if a, $2 \leq a \leq c-1$

exists such that $a \mid c$

Fund. thm of Arith for all integers $n \geq 2$, n can be written as a unique 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, ...

$(1), (3), (2^2), (5), (2 \cdot 3), (7), (2^3), (3^2), (2 \cdot 5), (11), (2^2 \cdot 3), \ldots$

Finding Primes. (prime factorization)

thm If n is composite then there is a prime, p, such that $p \mid n \wedge p \leq \sqrt{n}$

ex 12 → b/c of thm check 2, 3

$12 = 2 \cdot 6 = 2^2 \cdot 3$

ex 101 → $2 \nmid 101$, $3 \nmid 101$, $5 \nmid 101$, $7 \nmid 101$

∴ 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

$\text{Primes} = \{ p_1, p_2, p_3, \ldots, p_N \}$

Consider: $Q = (p_1 \cdot p_2 \cdot \ldots \cdot p_N) + 1$

Note: all numbers have a prime factor.

(ex $3 \mid 3$, prime ; $2 \mid 12$, composite?)

→ So some prime, p_i, divides Q

→ $p_i \mid Q$ and obviously $p_i \mid p_1 \cdot p_2 \cdot \ldots \cdot p_N$

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

→ $p_i \mid (Q) - (p_1 \cdot p_2 \cdot \ldots \cdot p_N) \rightarrow p_i \mid 1 \equiv \text{F}$

Thm primes ∞ infinite.

pf see above

How dense?

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

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

$\pi(25) = 9$

Thm $\pi(x) \sim \frac{x}{\ln x}$

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

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

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

ops

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

largest int (g) such that $g|a \wedge g|b$

smallest int (l) such that $a|l \wedge b|l$

finding gcd, lcm

prime factors!

① $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$

$b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$

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

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

② $\gcd(a,b) = p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \cdots p_k^{\min(a_k,b_k)}$

ex $\gcd(a,b) = 2^0 3^0 5^1 7^0 = \boxed{5}$

③ $\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_k^{\max(a_k,b_k)}$

ex $\text{lcm}(a,b) = \boxed{2^1 3^2 5^2 7^3}$

Thm $\boxed{\gcd \cdot \text{lcm} = a \cdot b}$