Math 321

Q's 4.1 #3 $a \mid b \to a \mid bc$, $c \in \mathbb{Z}$

means $a \cdot k_1 = b$, $k_1 \in \mathbb{Z}$ $\longrightarrow$ $a \cdot k_2 = bc$, $k_2 \in \mathbb{Z}$ goal

pf direct assume $a \mid b$. by def is $a \cdot k_1 = b$, $k_1 \in \mathbb{Z}$

$\to a \cdot k_1 \cdot c = b \cdot c \to a \mid bc$ ∎

integer by closure prop. of mult. of ints

Understand: "9 is a mult. of 5"

in algebra: $5 \cdot c = 9$, $c \in \mathbb{Z}$

in Number theory: $5 \mid 9$

4.2 #27 $3^{2003} \bmod 99$

2003 products

$243 \bmod 99 = 45$

slow tech: $(3 \cdot 3 \cdot 3 \cdot 3 \cdot 3) \cdot 3 \cdot \ldots \cdot 3 \bmod 99$

9 27 81 243 = 45

fast: $2003 = (\,?\,)_2$

	div	mod
2003	1001	1
1001	500	1
500	250	0
250	125	0
125	62	1

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

62	31	0
31	15	1
15	7	1
7	3	1
3	1	1
1	0	1

3^{2003} mod 99

$3^{(11111010011)_2}$ mod 99

$(\ )^1(\ )^1(\ )^1(\ )^1(\ )^1(3^{32})^0(3^{16})^1(3^8)^0(3^4)^0(3^2)^1(3)^1$ mod 99

81^2 mod 99   81   9   3

	base	ans
1	3	
1	9	
0	81	
0	$81^2 \equiv_{99} 27$	
1	$27^2 \equiv_{99}$	
0		
1		

$\boxed{\text{Fund. th}^m}$ for all $n \geq 2$. n is prime or a uniq prod. of primes written in non-dec. order

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

$\boxed{\text{Fund. th}^m}$ → $(2), (3), (2^2), (5), (2\cdot 3), (7), (2^3), \ldots$

Finding prime factors

$\boxed{\text{Th}^m}$ If n is composite, then n has a prime factor, p, such that $2 \leq p \leq \sqrt{n}$

(ex) Factor 100 → check: 2, 3, 5, 7

$100 = (2^2 5^2)$

100
2   50
2   25
5^2

ex factor 101   check: 2, 3, 5, 7

$2 \nmid 101 \quad 3 \nmid 101 \quad 5 \nmid 101 \quad 7 \nmid 101$

$\Rightarrow$ 101 is prime

Prime Sieves   1, $\boxed{2}$, $\boxed{3}$, ~~4~~, $\boxed{5}$, ~~6~~, $\boxed{7}$, ~~8~~, ~~9~~, ~~10~~

$\boxed{11}$, ~~12~~, $\boxed{13}$, ~~14~~, ~~15~~, ~~16~~, $\boxed{17}$, ~~18~~, $\boxed{19}$, ~~20~~

~~21~~, ~~22~~, $\boxed{23}$, ~~24~~, ~~25~~, ~~26~~, ~~27~~, ~~28~~, 29, ~~30~~,

31, ..

Th^n infinitely many primes.

pf (by contradiction)

assume finite primes: $p_1, p_2, p_3, \ldots, p_n$ n is finite.

Consider: $P = \boxed{p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_n + 1}$

by fund. th^m some prime (call it p_*) must divide P,

so $p_* \mid P$ and $p_* \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_n)$

so $p_* \mid \boxed{P - (p_1 \cdot p_2 \cdots p_n)} \to p_* \mid 1 \equiv F$

(Density)

Def: $\pi(n) =$ (counts number of primes $\leq n$)

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

Th^n $\displaystyle\lim_{n \to \infty} \frac{\pi(n)}{n/\ln(n)} = 1$ so for large n $\pi(n) \sim \frac{n}{\ln(n)}$

% of primes $\dfrac{\pi(n)}{n} \sim \dfrac{n/\ln(n)}{n} = \dfrac{1}{\ln(n)}$