

(65)

Every Composite number has a prime divisor.

(Alternatively: You can Prove the Next Theorem: (every integer is either prime or Product of primes) - which automatically proves the above theorem. But you will get penalty in marks!!!)

Proof by contradiction:

$$21 = 7 \times 3$$

Suppose, there exists a number which is composite but doesn't have any prime divisor. Let  $n$ ,



Informal: Divisors usually appear in pairs ... Suppose: divisors of  $n = \{1, \dots, a, \dots, b, \dots, n\}$  where  $n = a \cdot b$   
 Now, either  $a$  or  $b$  are Prime (proved) OR if not ( $a$  and  $b$  composite), they will gradually break down to  
 smaller numbers ( $a = p \cdot q$ ,  $b = r \cdot s$  where  $p, q, r, s$  smaller) until we hit any prime, or go down upto  
 very small primes like 2, 3 ... Example:  $120 = 10 \cdot 12 = 2 \cdot 5 \cdot 3 \cdot 4$  <sup>(66)</sup>  $= 2 \cdot 5 \cdot 3 \cdot 2 \cdot 2$ ;  $256 = 16 \cdot 16 = 2 \cdot 8 \cdot 2 \cdot 8$   
 $= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$

be such smallest number (this is a prime factorization which is an example of the next theorem)

Because,  $n$  is a composite number,  
 it has a divisor  $m$  greater than  
 1.

Now,  $m$  is also a composite  
 number and is not prime according  
 to induction. But,  $m$  is smaller  
 than  $n$  which contradicts that  $n$   
 is such smallest number. So,  
 no number can be found of  
 such type (Proved).

Any positive integer  $> 1$  is either  
 prime or product of primes;

Alternatively (but with marks penalty) You can just State the Fundamental Theorem of Arithmetic and  
 prove  $\Rightarrow$  Every integer has a unique prime factorization !!!

$$n = p_1 \cdot p_2 \cdot \dots \cdot p_n = \prod_{k=1}^n p_k = 2 \times 2 \times 3$$

Basis: lowest integer greater than 1 is  
 2. 2 is prime

Let Let, this statement is true for



all numbers between <sup>(67)</sup>  $2 \leq n \leq k$ .

we show for  $k+1$  that this statement is true for  $n = k+1$ .

if  $n = k+1$  is itself prime, then we are done.

So  $n$  has a divisor 'a' such that  $1 < a < n$ . Since divisors always appear in pairs, Let:  $n = k+1 = a * b$ , for some integers  $a, b$

if  $n$  is not prime, then  $n$  is a composite number. Let  $k+1 = a * b$ .

for some integers  $a, b$ . But

$2 \leq a < k+1$  and  $2 \leq b < k+1$ .

By induction,  $a, b$  are either prime or product of primes.

So,  $k+1 = a * b$  is also a product of primes. (Proved)