

claim

claim:

any integer  $n$  can be factored  
into a product of primes.  
possibly trivial, i.e.  $n$  is itself prime

Proof: by induction on  $N$ .  
(Flavor 2)

Base case: Show true when  
 $N=1$

how 'bout	$N=2$	yes - is prime
	$N=3$	yes - is prime
	$N=4$	yes - $2 \cdot 2$ product of primes
	$N=5$	yup
	$N=6$	yup $2 \cdot 3$ ✓

So the hypothesis ~~is~~ is true  $\forall n$  with  
 $n \leq 6$ .

So now assume true  
ie  $n$  can be written as  
a product of primes

$\forall n \leq N-1$

and look at  $N$ .

if  $N$  is prime, we're done.

otherwise  $N = ab$  for integers

$$1 < a, b$$

by induction hypothesis (hence  $a, b \leq N-1$ )

$a$  and  $b$  are both products of primes

Thus  $N$  is a product of primes ✓

side note: two "flavors" of induction

Both start with a Base  
case

Flavor 1

assume true  
for  $N-1$

→ Show true for  $N$

Flavor 2

assume true

for all  $n \leq N-1$

and show true  
for  $n = N$

Claim:

if  $n = p_1 \cdot \dots \cdot p_r$  is a factorization of  $n$  into primes, then any other factorization is just a reordering.

Proof:

$$\text{suppose } n = g_1 g_2 \dots g_s$$

for primes  $g_i$

Then

$$p_1 p_2 \dots p_r = g_1 \dots g_s$$

so since  $p_1 \mid \text{left hand side}$

$$\text{Then } p_1 \mid g_1 \dots g_s$$

$$\therefore p_1 \mid g_i \text{ for some } i$$

but the  $g_i$ 's are prime,  $\therefore p_1 = g_i$  for  
some  $i$

so reorder the  $g_i$ 's to make it the first  
one.

Thus

$$p_1 p_2 p_3 \cdots p_r = p_1 q_2 q_3 \cdots q_s$$

So  $p_2 \cdots p_r = q_2 \cdots q_s$

$$p_2 \mid q_2 \cdots q_s,$$

so  $p_2 \mid q_i$  for some  $i$   
assume the first

Thus

$$P_2 P_3 \cdots P_r = P_2 Q_3 \cdots Q_s$$

$$P_3 \cdots P_r = Q_3 \cdots Q_s$$

etc.

$$\text{Thus } P_1 \cdots P_r = Q_1 \cdots Q_s$$

( $r$ -must= $s$ )  
wrt to reordering.

This means that any

$$N = \prod_i p_i^{\alpha_i}$$

Right now -

Suppose  $M = \prod_i p_i^{\beta_i}$ ,  $N = \prod_i p_i^{\alpha_i}$

What is  $\gcd(M, N)$

$\text{lcm}(M, N)$