

Prove: If  $m$  is even and  $n$  is odd then  $m^2 + 3n$  is odd

Starting point: Suppose  $m$  is even and  $n$  is odd.

Show:  $m^2 + 3n$  is odd.

---

Suppose  $m$  is even and  $n$  is odd  
 So  $m=2s$  and  $n=2r+1$   
 where  $s, r \in \mathbb{Z}$  by def. of even/odd

Now  $m^2 + 3n = (2s)^2 + 3(2r+1)$   
 by subst.  
 $= 4s^2 + 6r + 3$   
 $= (4s^2 + 6r + 2) + 1$   
 $= 2(2s^2 + 3r + 1) + 1$

Let  $k = 2s^2 + 3r + 1$   
 So  $k \in \mathbb{Z}$  because it is a sum of products of integers.  
 $= 2k + 1$  by subst.

We have shown that

$m^2 + 3n = 2k + 1, k \in \mathbb{Z}$   
 Therefore  $m^2 + 3n$  is odd by def. of odd.

QED

Sep 24-10:40 AM

### 3.3 Divisibility

If  $n$  and  $d$  are integers then  $n$  is divisible by  $d$ ,  
 iff  $n = d \cdot k$  for some integer  $k$ .

$n$  is a multiple of  $d$   
 $d$  is a factor of  $n$   
 $d$  is a divisor of  $n$   
 $d$  divides  $n$

---

$d | n$

if  $n, d \in \mathbb{Z}$  and  $d \neq 0$   
 $d | n \iff \exists k \in \mathbb{Z}$  st.  $n = d \cdot k$

Sep 27-10:10 AM

For all integers  $a, b, c$   
 if  $a | b$  and  $b | c$ , then  $a | c$

Start:  
 Let  $a, b, c \in \mathbb{Z}$  and  $a | b$  and  $b | c$

Show:  $a | c$

Since  $a | b, b = am, m \in \mathbb{Z}$   
 and since  $b | c, c = bn, n \in \mathbb{Z}$

$c = b \cdot n$   
 $= (am)n$  by subst.  
 $= a(mn)$  assoc.

Let  $k = mn$ . Now  $k \in \mathbb{Z}$  since it is the product of integers

So  $c = a \cdot k$  for some integer  $k$ .  
 $\therefore a | c$

Sep 27-10:15 AM

Any integer  $n > 1$  is divisible by a prime number.

---

Suppose  $n \in \mathbb{Z}$  and  $n > 1$

case 1:  $n$  is prime  $\checkmark$   
 case 2:  $n$  is not prime  
 $n = r_0 s_0, r_0, s_0 \in \mathbb{Z}$   
 and  $1 < r_0 < n$   
 $1 < s_0 < n$

By def of divisibility  $r_0 | n$

case 1:  $r_0$  is prime  $\checkmark$  done  
 case 2:  $r_0$  is not prime  
 $r_0 = r_1 s_1, r_1, s_1 \in \mathbb{Z}$   
 and  $1 < r_1 < r_0$   
 $1 < s_1 < r_0$

⋮  
 ?

Sep 27-10:24 AM

### Unique Factorization Theorem for Integers (Fundamental Theorem of Arithmetic).

Given any integer  $n > 1$ , there exists a positive integer  $k$  and distinct prime numbers  $p_1, p_2, \dots, p_k$  and pos. integers  $e_1, e_2, \dots, e_k$  st.

$n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \cdot \dots \cdot p_k^{e_k}$

and any other expression of  $n$  as a product of prime numbers is identical to this except for the  $e_i$  in which they are written.

Sep 27-10:36 AM

Prove or give a counter example:  
 $\forall a, b \in \mathbb{Z}$  if  $a | b$  and  $b | a$  then  $a = b$

Suppose  $a, b \in \mathbb{Z}$  st.  $a | b$  and  $b | a$

$a | b \implies b = k \cdot a, k \in \mathbb{Z}$   
 $b | a \implies a = l \cdot b, l \in \mathbb{Z}$

---

so  $b = k \cdot a$   
 $= k \cdot (lb)$   
 $= (k \cdot l) b$   
 so  $k \cdot l = 1$

$k = l = 1 \implies b = ka = a$   
 $k = l = -1 \implies b = ka = -1 \cdot (-a) = a$   
 $b = -a$   
 counter example  
 $b = 3$   
 $a = -3$

Sep 27-10:42 AM