

# Proofs from the Board, II

CIS 400/628

Spring 2005

## Fundamental Theorem of Arithmetic

**Claim 1:**  $K = \emptyset$

Assume the contrary, i.e.,  $K \neq \emptyset$ .

Then the Well-Ordering Axiom says that  $\exists c$  such that  $c$  is the least member of  $K$ .

$c$  cannot be prime, else it's automatically a product of primes (namely, itself). Therefore,  $c = c_1 \cdot c_2, 1 < c_1 < c, 1 < c_2 < c$ .

Neither  $c_1$  or  $c_2$  can be in  $K$ , because they are both less than  $c$  and  $c$  is the smallest member of  $K$ .

But therefore, by the definition of  $K$ ,  $c_1$  and  $c_2$  can both be expressed as the products of positive primes. Which means  $c$  can be expressed as the product of positive primes.

There is a contradiction, so our assumption that  $K \neq \emptyset$  is false.

**Claim 2: Uniqueness**

Let  $c = p_1 \cdot p_2 \cdots p_r = q_1 \cdot q_2 \cdots q_t$  where all  $p_i$  and  $q_j$  are prime.

Cancel out any  $p_i$  that equals a  $q_j$ . This leaves  $p_q \cdot p_2 \cdots p_s = q_1 \cdot q_2 \cdots q_m$  for  $1 \leq s \leq r$  and  $1 \leq m \leq t$ .

Obviously,  $p_1 | p_q \cdot p_2 \cdots p_s$  and  $p_1 | q_1 \cdot q_2 \cdots q_m$ .

Then by Theorem 1.6,  $p_1 | q_v$  for some  $1 \leq v \leq m$ .

But all  $q_i$  were prime, so  $p_1 = q_v$ .

We can cancel out these two, and then continue similarly. We are left with  $1 = 1$ , i.e., we have canceled out all primes, thus showing the two representations are the same.

## Theorem 1.8

a.  $x \cong x \pmod{n}$ .

$x - x = 0$ . 0 is divisible by any non-zero integer, so  $n|0$ , and  $x \cong x \pmod{n}$ .

b.  $x \cong y \pmod{n} \iff y \cong x \pmod{n}$

Suppose  $x \cong y \pmod{n}$ ; then  $n|(x - y) \Rightarrow x - y = kn$ . Therefore,  $y - x = -kn$ , so  $n|y - x$ , and  $y \cong x \pmod{n}$

Now suppose  $y \cong x \pmod{n}$ ; then  $n|(y - x) \Rightarrow y - x = kn$ . Therefore,  $x - y = -kn$ , so  $n|x - y$ , and  $x \cong y \pmod{n}$

c.  $x \cong y \pmod{n} \& y \cong z \pmod{n} \Rightarrow x \cong z \pmod{n}$

$n|x - y \Rightarrow x - y = rn$  and  $n|y - z \Rightarrow y - z = sn$ . Therefore,  $y = sn + z = x - rn$ .  
 $\Rightarrow sn + rn = x - z$   
 $\Rightarrow (s + r)n = x - z$   
 $\Rightarrow n|x - z$   
 $\Rightarrow x \cong z \pmod{n}$ .

d.  $x \cong y \pmod{n} \& w \cong z \pmod{n} \Rightarrow$   
 $x + w \cong y + z \pmod{n} \& x \cdot w \cong y \cdot z \pmod{n}$

We know that  $n|x - y$  and  $n|w - z$ , or, equivalently  $nr = x - y$  and  $ns = w - z$ .

$\Rightarrow nr + ns = x - y + w - z$   
 $\Rightarrow n(r + s) = (x + w) - (y + z)$   
 $\Rightarrow n|(x + w) - (y + z)$   
 $\Rightarrow (x + w) \cong (y + z) \pmod{n}$ .

Again,  $nr = x - y$  and  $ns = w - z$ .

$\Rightarrow wrn = wx - wy$  and  $ysn = yw - yz = wy - yz$ .  
 $\Rightarrow wrn + ysn = wx - wy + wy - yz$ .  
 $\Rightarrow n(wr + ys) = wx - yz$ .  
 $\Rightarrow n|wx - yz$ .  
 $\Rightarrow wx \cong yz \pmod{n}$ .