

# Proofs from the Board

CIS 400/628

Spring 2005

## Theorem 1.1

(a) if  $d|a$  and  $a|b$ , then  $d|b$ .

By the definition of  $|$ ,  $\exists m, n \ni a = dm$  and  $b = na$   
 $\Rightarrow b = ndm = d(nm)$   
 $\Rightarrow d|b$ .  $\square$

(b)  $d|a \Leftrightarrow d|-a$ .

First,  $\Rightarrow$ . Assume  $d|a$ . By defn.,  $\exists n \ni -a = dn$   
 $\Rightarrow a = -dn$   
 $\Rightarrow a = d(-n)$   
 $\Rightarrow d|a$ .

Now for  $\Leftarrow$ . Assume  $d|-a$ . By defn.,  $\exists m \ni -a = dm$   
 $\Rightarrow -a = -dm$   
 $\Rightarrow -a = d(-m)$   
 $\Rightarrow d|-a$ .  $\square$

(f) if  $a \neq 0$  and  $d|a$ , then  $|d| \leq |a|$

By defn.,  $a = bd$   
 $\Rightarrow |a| = |bd| = |b| \cdot |d|$   
 $\Rightarrow a \neq 0$ , so  $b \neq 0$   
 $\therefore |b| \geq 1$ .  
 $\therefore |a| = |b| \cdot |d| \geq 1 \cdot |d| = |d|$   $\square$

(j) if  $d|a$  and  $d|b$ , then  $d|(ax + by)$  for arbitrary  $x, y \in \mathbb{Z}$ .

By defn.,  $a = md$  and  $b = nd$  for some  $m, n \in \mathbb{Z}$ .  
 $\Rightarrow ax + by = mdx + ndy = d(mx + ny)$   $\square$

## Division Algorithm

Suppose  $a, b \in \mathbb{Z}$  and  $b > 0$ . Then  $\exists$  *unique*  $q$  and  $r$  such that  $a = q \cdot b + r$  and  $0 \leq r < b$ .

Define  $S = \{a - xb \mid x \in \mathbb{Z} \text{ and } a - xb \geq 0\}$

Show that  $S$  is not empty: choose  $x = -|a|$ .

We know  $a, b \in \mathbb{Z}$  from the theorem statement, so  $x (= -|a|) \in \mathbb{Z}$ .

$$a - xb = a - (-|a| \cdot b) = a + (|a| \cdot b)$$

$$a + (|a| \cdot b) \geq a + |a| \tag{b > 0}$$

$$a + |a| \geq 0 \tag{\text{if } a \leq 0, a + |a| = 0; \text{if } a > 0, a + |a| = 2a}$$

So  $a - xb \geq 0$ , and so it is in  $S$  (i.e.,  $S$  is not empty).

Notice by defn. that  $S \subseteq \mathbb{N}$  (i.e., all elements of  $S$  are greater than or equal to 0). Therefore, if  $0 \in S$ , then 0 is the smallest element. If 0 is not in  $S$ , then the Well-Ordering Axiom assures us that there is some least member of  $S$ . Call this smallest element (whether 0 or not)  $r$ .

Then, by the defn. of  $S$ ,  $\exists q$  such that  $a - qb = r$  and  $a = qb + r$

This is the proper form, but we must still show three things:

1.  $r \geq 0$
2.  $r < b$
3.  $q, r$  are a unique solution.

(1)  $r \in S$ , and as all elements of  $S$  are in  $\mathbb{N}$ ,  $r \geq 0$ .

(2) (proof by contradiction) Assume  $r \geq b$ . Then  $r - b \geq 0$  and  $r - b = (a - qb) - b = a - (q+1)b$ , so  $r - b \in S$  (see the definition of  $S$ , and substitute  $q+1$  for  $x$ ). This contradicts  $r$  being the least element of  $S$ ,  $\therefore r < b$ .

(3) Suppose there is another representation such that  $a = q_1b + r_1$ , then

$$\begin{aligned} bq - bq_q &= r_1 - r \\ b(q - q_1) &= r_1 - r \\ \therefore |b(q - q_1)| &= |r_1 - r| \\ \therefore b|q - q_1| &= |r_1 - r| \end{aligned}$$

From steps (1) and (2), we know that  $0 \leq r < b$  and  $b|q - q_1| < b$ . However, for integers, the only way this inequality can hold is if  $|q - q_1| = 0$ , or equivalently,  $q = q_1$ . But if  $q = q_1$ , then  $r = r_1$  as well.  $\square$

### Theorem 1.3

For  $a, b \in \mathbb{Z}^+$ , if  $\gcd(a, b)$  exists, it is unique.

(Proof by contradiction): Assume there are two integers,  $m$  and  $n$ , that are each a  $\gcd(a, b)$ . Then by definition,

$$m|a, m|b, n|a, n|b.$$

The defn. of gcd says  $c|a \& c|b \Rightarrow c|d$ .  $m$  is a  $\gcd(a, b)$ , so  $n|a, n|b \Rightarrow n|m$ . Symmetrically,  $n$  is a  $\gcd(a, b)$ , so  $m|a, m|b \Rightarrow m|n$ . So both  $m|n$  and  $n|m$ .

From Theorem 1.1 (i), if  $a|b$  and  $b|a$ , then  $a = \pm b$ , so  $m = \pm n$ . But the definition of gcd says it must be positive, so  $m = +n$ .  $\square$

### Theorem 1.4

#### Proof of Claim 1: $d|a$ and $d|b$

Recall that  $d$  is the least element of  $S$ .

From the division algorithm:  $\exists q, r$  such that  $a = qd + r$  and  $0 \leq r < d$ . We can rewrite  $a = qd + r$  as  $r = a - qd = a - q(ax_1 + by_1) = a - qax_1 - qby_1 = a(1 - qx_1) + b(-qy_1)$ . This is the proper form to be in  $S$ , if  $r > 0$ . But  $r < d$ , so if  $r \in S$ , then this contradicts  $d$  being the least member of  $S$ .  $\therefore r = 0$ , and thus  $a = qd$ , so  $d|a$ .

We can do the same demonstration for  $b$ , so  $d|b$ .

#### Proof of Claim 2: $c|a$ & $c|b \Rightarrow c|d$

Assume  $c|a$  &  $c|b$ ; then  $\exists m, n \in \mathbb{Z}$  such that  $a = cm$  and  $b = cn$ . So  $d = ax_1 + by_1 = cmx_1 + cny_1 = c(mx_1 + ny_1)$ , so  $c|d$ .

## Towards a GCD Algorithm

### Why #1

Why does the induction hypothesis make  $d = \gcd(b, r)$ ? By the induction hypothesis,  $d = \gcd(b, r)$  because  $r < b$ , so  $r$  is found in  $A(1), A(2), \dots, A(b-1)$  the induction hypothesis assumes that  $\forall a, f(a, r) = \gcd(a, r)$ , so  $f(b, r) = \gcd(b, r)$ .

### Why #2

Given  $a = qb + r$ , why does  $d|\gcd(a, b)$ ? By the defn. of gcd,  $d|b$ .  $\therefore \exists m, r$  such that  $b = md$  &  $r = nd$ . So  $a = qmd + nd = d(qm + n)$ . Thus,  $d|a$ . By the second part of the gcd defn.,  $d|a$  and  $d|b \Rightarrow d|\gcd(a, b)$ .

### Why #3

Why does  $\gcd(a, b) \mid d$ ?  $\gcd(a, b)$  is the smallest positive integer express as a linear combination of  $a$  and  $b$ . By the corollary to Theorem 1.4, any linear combination of  $a$  and  $b$  is a multiple of  $\gcd(a, b)$ .  $d$  was expressed as a linear combination of  $a$  and  $b$ , so  $\gcd(a, b) \mid d$ .

### Why #4

Why is  $d = \gcd(a, b)$ ? By Theorem 1.1 (i), if  $a \mid b$  and  $b \mid a$  then  $a = \pm b$ . But both  $d$  and  $\gcd(a, b)$  are positive, so  $d = \gcd(a, b)$ .

## Theorem 1.5

$\forall a, b \in \mathbb{Z}, a, b \neq 0, p$  is a positive prime:  $p \mid ab \Rightarrow (p \mid a \text{ or } p \mid b)$ .

Proof by contradiction: assume  $p \nmid a$ . Then  $\gcd(a, p) = 1$  ( $p$  is prime, so its only factors are  $\pm 1$  and  $\pm p$ ; if  $p \nmid a$ , then the only possible positive common divisor is 1).

$1 = ax + py$  (by theorem 1.4), so multiply both sides by  $b$ , yielding  $b = bax + bpy = (ab)x + p(by)$ . Theorem 1.1 (j) states that if  $d \mid a$  and  $d \mid b$ , then  $d \mid (ax + by)$  for arbitrary  $x, y \in \mathbb{Z}$ . As stated in the theorem,  $p \mid ab$ , and obviously  $p \mid p$ , so  $p$  divides the linear combination  $(ab)x + p(by)$ , which is the same as saying  $p \mid b$ . We can use the same reasoning to show that if we start assuming  $p \nmid b$ , then  $p \mid a$ .

## Theorem 1.6

Proof by induction:

Let  $S(n)$  be the statement "if  $p \mid a_1 a_2 \cdots a_n$ , then  $p \mid a_i$  for at least one  $i, 1 \leq i \leq n$ ."

Base case:  $S(1)$ . if  $p \mid a_1$ , then  $p \mid a_1$ . A tautology, and obviously true.

Induction hypothesis: Assume  $S(k)$  is true. Show  $S(k + 1)$  is true as well. We are given  $p \mid a_1 a_2 \cdots a_k a_{k+1}$ . Note that  $a_1 a_2 \cdots a_k a_{k+1} = (a_1 a_2 \cdots a_k)(a_{k+1})$ . From theorem 1.5, if  $p \mid xy$ , then either  $p \mid x$  or  $p \mid y$ . So, either  $p \mid a_{k+1}$  or  $p \mid a_1 a_2 \cdots a_k$ . The former case obviously satisfies the requirement, and by the induction hypothesis, the latter case does as well.