Math 103 algebra

correct url for course website:

math.ucsd.edu/~hwen26/103.html

Integers:

important axiom:

Well Ordering Principle (WOP)

Any nonempty subset S of the integers has a smallest member

Divisibility

t, s integers

t is a divisor of s, (notation: $t \mid s$)

if we can find an integer u s.t.

$$s = tu$$

notation: if t is not a divisor of s: $t \nmid s$

Division Algorithm

a, b integers, $b > 0$

$\Rightarrow$ There exist unique numbers q and r such that

$$a = bq + r$$

where $0 \leq r < b$

Proof @ Existence

use WOP

Consider set $S = \{ a - bk, \; k \text{ integer s.t. } a - bk \geq 0 \}$

case 1: $0 \in S \Rightarrow \exists$ integer, say q, s.t.

$a - bq = 0 \Rightarrow a = bq + 0$

can take $r = 0$ and given q ✓

case 2 $0 \notin S$

can use WOP

$\Rightarrow \exists q$ s.t. $a - qb$ is smallest element in S

enough to show: $a - qb < b$

(because then $a = qb + \underbrace{(a-qb)}_{\text{positive, can take as } r}$

$= qb + r$)

proof by contradiction:

assume $a - qb \geq b \quad | -b$

$\Rightarrow a - qb - b \geq 0$

$\Rightarrow \underbrace{0 \leq a - (q+1)b < a - qb}_{\text{implies } a-(q+1)b \text{ in } S.}$ ↯ to $a-qb$ smallest elem. in S

$\Rightarrow$ $r = a - qb$ does the job

(b) uniqueness.

assume $a = bq + r$

and $a = bq' + r'$

where q, q', r, r' integers

with $0 \le r, r' < b$

$\Rightarrow$ $bq + r = bq' + r' \quad | -r - bq'$

assume $r' \ge r$

$b(q-q') = bq - bq' = r' - r \ge 0$

observe: $0 \le r' - r \le r' < b$

$\Rightarrow 0 \le b(q-q') = r' - r < b$

($b(q-q')$: multiple of b; $r' - r < b$)

$\Rightarrow b(q-q') = 0 = r' - r.$

$\Rightarrow r' = r$ and $q' = q$.

Example:

$a = -27$

$b = 6$

$\Rightarrow -27 = (-5)6 + 3$

$= -30 + 3$

$q = -5$ $r = 3$

Def. a, b integers

$\gcd(a,b)$ = greatest common divisor of a and b

Ex. $\gcd(12, 18) = 6$

Theorem ($\gcd(a,b)$ as a linear comb. of a and b)

a, b integers $\Rightarrow$ $\exists$ integers s and t s.t.

$$\gcd(a,b) = as + bt$$

(e.g $6 = (-1)\cdot 12 + 1 \cdot 18$)

Proof. Let $S = \{am + bn, \text{ m,n integers such that } am + bn > 0\}$

can use WOP

Let $d = as + bt$ be the smallest element in S

claim: $d \mid a$

division algorithm: $a = qd + r$ with $0 \le r < d$

$$0 \le r = a - qd$$
$$= a - q(as + bt)$$
$$= a(1 - qs) - btq$$
$$= a(1 - qs) + b(-tq) < d$$

$\Rightarrow r = 0$ (otherwise $r \in S$ contradicting our choice of d)

$\Rightarrow$ $d \mid a$

Same way one shows: $d \mid b$

$\Rightarrow$ d is a common divisor of a and b.

Let d' be another common divisor of a and b

$\Rightarrow$ $a = d'h$
$b = d'k$ for some integers h and k.

$d = as + bt$
$= d'hs + d'kt$
$= d'(hs + kt)$ $\rightarrow$ $d' \mid d$

$\Rightarrow$ d greatest common divisor ✓