Lecture 2

Theorem: Let a, b be integers with $b > 0$. Then there exist unique integers q and r such that

$$a = bq + r \quad \text{and} \quad 0 \leq r < b.$$

Proof:

Suppose we have fixed integers a and b with $b > 0$. Let S be the set

$$S := \{ a - bx \mid x \in \mathbb{Z} \text{ and } a - bx \geq 0 \} \subseteq \mathbb{N}$$

Step 1: $\boxed{\text{Show that } S \text{ is not empty by finding a number } x \text{ s.t. (such that) } a - bx \geq 0.}$

Observe that the number $-|a|$ is s.t. $a - b(-|a|) \geq 0$:

$b \geq 1$ because by hypothesis $b \in \mathbb{Z}$ and $b > 0$

$\Rightarrow \; |a|\, b \geq |a|$ because $|a| \geq 0$

$\Rightarrow \; |a|\, b \geq -a$ because $|a| \geq -a$

$\Rightarrow \; a + b|a| \geq 0$

Thus, $a + b|a| \in S$, i.e. $S \neq \emptyset$.

STEP 2: $\boxed{\text{Find } q \text{ and } r \text{ such that } a = bq + r \text{ and } r \geq 0.}$

By step 2 and the Well-Ordering Axiom, S contains a smallest element, call it r.

$$r \in S \implies r = a - bq \text{ for some } q \in \mathbb{Z} \ \& \ a - bq \geq 0$$

$$\implies r = a - bq \ \& \ r \geq 0$$

$$\implies a = bq + r \text{ with } r \geq 0$$

STEP 3: $\boxed{\text{Show that } r < b.}$

By contradiction.

because $b > 0$

Suppose that $r \geqslant b$. Then $r - b \geqslant 0$ and $r > r - b$.

Observe that $0 \leq r - b = (a - bq) - b = a - b(q+1)$.

because $r = a + bq$ from step 2

Then $r - b$ must be an element of S.

Thus we have that

$$\underbrace{r - b < r \quad \text{and} \quad r - b \in S}_{\text{contradiction !!!}}$$

because r was the smallest, not $r - b$.

Then $r < b$.

STEP 4: Show that q and r are the only numbers s.t. $a = qb + r$ with $0 \leq r < b$.

Suppose there are integers q_1 and r_1 s.t.

① $a = qb + r$ and $a = q_1 b + r_1$

② $0 \leq r < b$ and $0 \leq r_1 < b$

From ①, $qb + r = q_1 b + r_1$ then $b(q - q_1) = r_1 - r$ $(*)$

From ②, $-b < -r \leq 0$ then $-b < r_1 - r < b$ $(\dagger)$
$0 \leq r_1 < b$

By (*) and (†) we have

$$-b < b(q - q_1) < b$$

$$-1 < q_1 - q_1 < 1$$

Since $q - q_1 \in \mathbb{Z}$, then $q - q_1$ must be equal to zero. This is $q - q_1 = 0$, i.e. $q = q_1$.

Using (*) again, $r - r_1 = b(q - q_1) = 0$, i.e. $r = r_1$.

$\blacksquare$

Divisibility (when the remainder is zero)

Def: Let $a, b \in \mathbb{Z}$ with $b \neq 0$. We say that b divides a (or that a is a multiple of b) if $a = bc$ for some $c \in \mathbb{Z}$.

Notation: $b \mid a$ — b divides a; $b \nmid a$ — b does not divide a

Ex:

- $(-3) \mid 9$ because $9 = (-3) \times (-3)$
- $5 \nmid 14$ because $14 = 2 \times 7 = (-2) \times (-7)$
- $b \mid 0$ $\forall b \in \mathbb{Z}$ because $0 = b \times 0$ for all $b \in \mathbb{Z}$.
- $1 \mid a$ $\forall a \in \mathbb{Z}$ because $a = 1 \times a$ for all $a \in \mathbb{Z}$.

Proposition 1: $b \mid a$ if and only if $b \mid (-a)$.
(iff or $\Longleftrightarrow$)

Proof:

($\Rightarrow$) $b \mid a \Rightarrow \exists c \in \mathbb{Z}$ s.t. $a = bc$

$\Rightarrow -a = -bc = b(-c)$

$\Rightarrow b \mid (-a)$

($\Leftarrow$) Similar to the other direction.

Conclusion: a and $-a$ have the same divisors.

Proposition 2: If $a \neq 0$ and $b \mid a$, then $b \leq |a|$

Proof: Exercise.

Def: Let $a, b \in \mathbb{Z} \setminus \{0\}$. The greatest common divisor (gcd) of a and b is an integer d such that:

(1) $d \mid a$ and $d \mid b$.

(2) If $c \mid a$ and $c \mid b$, then $c \leq d$.

d is the largest integer dividing both a and b.

Notation: $\gcd(a,b) = d$ or $(a,b) = 1$

Def: If $\gcd(a,b) = 1$, then a and b are said to be relatively prime.

Ex: Find the gcd of 12 and -30.

$D_{12} := \{-12, -6, -4, -2, -1, 1, 2, 4, 6, 12\}$

$D_{-30} := \{-30, -15, -10, -6, -5, -3, -2, -1, 1, 2, 3, 5, 6, 10, 15, 30\}$

$\gcd(12, -30) = 6$

Observe: $\underline{\gcd}(12, 30) = \underline{\gcd}(-12, -30) = \underline{\gcd}(-12, 30) = \underline{\gcd}(12, -30) = 6$

- 5 and 14 are relatively prime.

- $\gcd(a, 0) = a$ because $D_a \cap D_0 = \{\pm a, \pm 1\}$.

Proposition 3: The $\gcd(a,b)$ is unique. Why does the $\gcd(a,b)$ exist?

Proof: Suppose d and d' are two gcd's of a and b.

Since d is a gcd, then $d|a$ and $d|b$. condition (1) in def

But d' is also a gcd, then $d \leq d'$. condition (2) in def

Similarly, since d' is a gcd, then $d'|a$ and $d'|b$. condition (1) in def

But d is also a gcd, then $d' \leq d$. condition (2) in def

Thus, $d = d'$.

The Bézout's Identity

Theorem: Let $a, b \in \mathbb{Z} \setminus \{0\}$. Then there exist (not necessarily unique) integers u and v such that $\gcd(a,b) = au + bv$.

Moreover, $\gcd(a,b)$ is the smallest positive integer of the form $au + bv$.

If a number d is equal to $au + bv$ for some u and v in $\mathbb{Z}$, it does not mean that $d = \gcd(a,b)$.

Example: $2 = 1(1) + 1(1)$ but $\gcd(1,1) = 1$ not 2.