Lecture 3: The Greatest common divisor

Definition An integer b is said to be divisible by an integer $a \neq 0$ (i.e. $a|b$) if $\exists$ some integer c such that $b = ac$.

$a \nmid b$ means b is not divisible by a.

We also say: a is a divisor of b, a is a factor b, b is a multiple of a.

* **Note** If a is a divisor of b then b is also divible by $-a$. Therefore divisors of an integer always occur in pairs. We will only study the positive divisors.

Theorem 3.1 For $a, b, c \in \mathbb{Z}$ the following holds:

(a) $a|0$, $1|a$, $a|a$

(b) $a|1$ if and only if $a = \pm 1$

(c) $a|b$, $c|d \Rightarrow ac|bd$

(d) $a|b$, $b|c \Rightarrow a|c$

(e) $a|b$ and $b|a$ if and only if $a = \pm b$

(f) If $a|b$ and $b \neq 0$ then $|a| \leq |b|$

(g) If $a|b$ and $a|c$ then $a|(bx+cy)$ for arbitrary integers x and y.

Proof (a) and (b) obvious.

(c) $\because a|b$ and $c|d$ then $\exists$ $x, y \in \mathbb{Z}$ such that

$b = ax$ and $d = cy$

$\Rightarrow b \cdot d = ac \cdot xy$

$\Rightarrow ac | bd$

(d) $\because a|b$ and $b|c$ then $\exists\ x, y \in \mathbb{Z}$ such that

$b = xa$ and $c = yb$

$\Rightarrow c = yxa$

$\Rightarrow a|c$

(e) $\because a|b$ and $b|a$ then $\exists\ x, y \in \mathbb{Z}$ such that $(a, b \neq 0)$

$b = xa$ and $a = yb$

$\Rightarrow a = xya$

$\Rightarrow xy = 1$

$\Rightarrow x = y = \pm 1$

Hence $b = \pm a$

(f) $\because a|b$ and $b \neq 0$ $\exists\ x \in \mathbb{Z}$ such that

$b = xa$

$\Rightarrow |b| = |xa| = |x||a|$

$\Rightarrow |b| \geq |a|$

(g) $\because a|b$ and $a|c$ $\exists\ r, s \in \mathbb{Z}$ such that

$b = ra$ and $c = sa$

For any $x, y \in \mathbb{Z}$

$bx + cy = rax + say = a(rx + sy)$

$\Rightarrow a|(bx + cy)$

Definition Let a and b be given integers with atleast one of them different from zero. The greatest common divisor of a and b denoted by $\gcd(a,b)$ is the positive integer 'd' satisfying the following:

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

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

Thm 3.2 Let $a, b \in \mathbb{Z}$ not both of which are zero, $\exists\ x, y \in \mathbb{Z}$ such that

$$\gcd(a,b) = ax + by$$

Proof Consider the set:

$$S = \{ au + bv \mid au + bv > 0;\ u, v \in \mathbb{Z} \}$$

Choose u such that: if $a \neq 0$ then

$$u = \begin{cases} 1 & \text{if } a > 0 \\ -1 & \text{if } a < 0 \end{cases} \Rightarrow au = \begin{cases} a & \text{if } a > 0 \\ -a & \text{if } a < 0 \end{cases}$$

Then $au = |a| > 0$. Hence $|a| \in S$ which implies that $S \neq \emptyset$

By well-ordering principle S contains a least element (say) d.

Thus from the definition of S. $\exists\ x, y \in \mathbb{Z}$ such that

$$d = ax + by$$

Claim $d = \gcd(a,b)$

Applying Division algorithm on a and d gives us unique integers q and r such that:

$$a = qd + r \qquad 0 \leq r < d$$

$$\Rightarrow r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$$

If $r>0$ then $r \in S$ [by defn of S] which is a contradiction [as $r<d$]

$\therefore$ r cannot be negative, therefore the only possibility is that $r=0$

which given: $a=qd$ i.e. $d \mid a$.

Similarly we can show that $d \mid b$.

Hence d is a common divisor of a and b.

Now suppose c is an arbitrary positive common divisor of a and b

Then $c \mid ax+by$ ~~for some $x, y \in \mathbb{Z}$~~ [Thm 3.1(g)]

i.e. $c \mid d$

Also $c = |c| \leq |d| = d$ [Thm 3.1(f)]

Hence d is the greatest common divisor of a and b.

Corollary 3.3 If $a, b \in \mathbb{Z}$, not both zero then the set

$$T = \{ax+by \mid x, y \in \mathbb{Z}\}$$

is precisely the set of all multiples of $d = \gcd(a,b)$

Proof. Since $d \mid a$ and $d \mid b$, therefore $d \mid ax+by \quad \forall \ x, y \in \mathbb{Z}$

Hence every member of T is a multiple of d.

Conversely let $d = ax_0 + by_0 \qquad x_0, y_0 \in \mathbb{Z}$

Hence any multiple nd of d is of the form.

$$nd = n(ax_0+by_0) = a(nx_0)+b(ny_0)$$

Hence nd is a linear combination of a and b, and hence lies in T.