Divisibility

Prof. NSN Sastry

IIT Dharwad

2. DIVISIBILITY

2.1 Def. Let m, n $\in \mathbb{Z}$. We say that m <u>divides</u> n if n = mr for some r $\in \mathbb{Z}$.

We write $m \mid n$. If m does not divide n, we write m†n,

Ex: $2 \mid 6$ because $6 = 2 \times 3$

$10 \mid 0$ because $0 = 10 \times 0$†

0†n for any $n \neq 0$

The definition immedietly yields

Theorem 2.1: Let m, n, r $\in \mathbb{Z}$.

(i) $n \mid n$; (ii) $m \mid n$ and $n \mid r \Rightarrow m \mid r$

(iii) $n \mid m$, $n \mid r \Rightarrow n \mid am + br$ *for all* a, b $\in \mathbb{Z}$

(iv) $n \mid m \Rightarrow rn \mid rm$ *for each* r $\in \mathbb{Z}$

(v) $rn \mid rm$, $r \neq 0 \Rightarrow n \mid m$

(vi) $1 \mid 0$, more generally $n \mid 0$

(vii) $0 \mid n \Rightarrow n = 0$

(viii) $m \mid n$, $n \neq 0 \Rightarrow |m| \leq |n|$

(ix) $m \mid n$ and $n \mid m \Rightarrow |m| = |n|$

(x) $m \mid n$ and $m \neq 0 \Rightarrow (n/m) \mid n$

Proof: Exercise $\square$

Definition : If $m \mid n$, then m is called a **divisor** of n. Note that if $m \neq 0$, then n/m also is a divisor of n.

2.2. gcd (a,b), a, b $\in \mathbb{Z}$

The greatest common divisor (gcd, for short) **of** a, b, $\in \mathbb{Z}$ is a number $d \in \mathbb{N}$ such that:

($\propto$) $d \mid a$ and $d \mid b$;

(β) if $c \in \mathbb{Z}$ is such that $c|a$ and $c|b$, then $c \mid d$.

Notation : gcd of a and b is written as (a, b) or gcd (a , b).

By Theorem 2.1 (ix), there is at most one such non-negative integer d.

The next theorem shows that there is one.

So, the gcd of any two integers is unique.

THEOREM 2.2. Let $a, b \in \mathbb{Z}$. Then, there exists $d \in \mathbb{Z}$ which is a common divisor of both a and b. Further,

$$d = a\,x + b\,y$$

for some $x, y \in \mathbb{Z}$ and each common divisior of a and b divides d.

<u>Note</u> : If $d \in \mathbb{Z}$ satisfies the above properties, so does –d. So, the non negative number among {d,-d} then is the gcd of a and b.

Proof of Theorem 2.2.

(i) First, we consider the case when $a \geq 0$ and $b \geq 0$. Let $c = a + b$.

If $c=0$, then $a = 0$ and $b = 0$, and we can take $d = 0$ and $x = 0 = y$.

Assume that the theorem is proved for 1, 2,…., c-1. Renaming a and b, if need be, we can assume that $a \geq b$.

If $b=0$, take $d=a$, $x=1$ and $y=0$.

If $b \geq 1$, apply the theorem to the pair (a-b) and b to get integers d_1, x_1, y_1 such that

$d_1 = (a-b)\,x_1 + b\,y_1$ and $d_1|(a-b)$ and $d_1|b$.

Now, $d_1 = a\,x_1 + b\,(y_1 - x_1)$ and $d_1|(a-b)+b = a$ and $d_1|b$.

So, the first two parts of the theorem hold with $d = d_1$, $x = x_1$ and $y = y_1 - x_1$.

The third part is clear.

(ii) Now consider the case when $a<0$ or $b<0$ or both a and b are negative.
By (i), there exists $d, x, y \in \mathbb{Z}$ such that

$$d = |a|x + |b|y .$$

Since $|a|=|-a|$ and $|b|=|-b|$, we can write $d = a(-x) + b\,(-y)$

(if $a<0$ and $b<0$, for example) .

So, Theorem 2.2 holds . □

(2.3) . Some Properties of greatest common divisor

Proposition: 2.3 : Let a, b, c $\in \mathbb{Z}$. Then:

(i) $(a, b) = (b, a)$

(ii) $(a, (b, c)) = ((a, b), c)$

(iii) $(ac, bc) = |c|\,(a, b)$

(iv) $(a, 1) = 1$

Proof . Exercise. $\square$

Proposition: 2.4 (Euclid's Lemma): Let a,b,c $\in \mathbb{Z}$.

If $a|bc$ and $(a, b) = 1$, then $a|c$.

Proof. Since $(a, b) = 1$, by Theorem 2.2, $1= ax + by$ for some $x, y \in \mathbb{Z}$. So,

$$c = acx + bcy$$

Since $a|ac$ and $a|bc$, it follows that $a|c$. $\square$

EXCERCISE : Show that

(i) (a, b) = 1, (a, c)= 1 => (a, bc)=1

(ii) (a, b) = 1 => (a + b, a – b) = 1 or 2

(iii) (a, b) = 1 => (a + b, a^2- ab + b^2) = 1 or 3.

--------------------------x------------------------------