LECTURE 8

Divisibility

DEFINITION 8.1. *Let a and b be integers with $b \neq 0$. We say that a* ***divides*** *b if $b = ac$ for some integer c. In symbols, we write*

$$a \,|\, b$$

for "a divides b" and

$$a \nmid b$$

for "a does not divide b".

Remarks:

1. If $a \in \mathbb{Z}$, then $a \,|\, 0$ is always true, since $0 = a \cdot 0$.

2. If $b \in \mathbb{Z}$, then $1 \ \mid b$ is always true, since $b = 1 \cdot b$.

3. If $a \mid b$, then $(-a) \mid b$ and $a \mid (-b)$ and $(-a) \mid (-b)$.

4. If a and b are integers and $a \mid b$, then either $|a| \leq |b|$ or $b = 0$.

DEFINITION 8.2. *Let a and b be integers not both zero. A* ***common divisor*** *of a and b is any integer c that divides both a and b. The* ***greatest common divisor*** *(or* ***gcd****) of a and b is the largest integer that divides both a and b.*

The text denotes the greatest common divisor of a and b by (a, b). We shall, however, try to use a little more explicit notation, by denoting the gcd of a and b by

$$GCD(a, b) \quad .$$

Note that remarks 2 and 3 above imply that the GCD of two integers is always a integer greater than or equal to 1;

$$GCD(a, b) \geq 1 \quad , \quad \forall\, a, b \in \mathbb{Z} \quad .$$

Example. To find the gcd of 12 and 42, we first list all the divisors of 12 and 42:

$$\begin{aligned} \{z \in \mathbb{Z} \mid z|12\} &= \{\pm1, \pm2, \pm3, \pm4, \pm6\} \\ \{z \in \mathbb{Z} \mid z|42\} &= \{\pm1, \pm2, \pm3, \pm6, \pm7, \pm14, \pm21\} \end{aligned}$$

The gcd of 12 and 42 is evidently 6.

Listing all the divisors of two large integers in order to find their gcd can be quite time consuming. In what follows below we shall present an alternative method of finding the gcd of two integers.

First, we observe from the last example that the gcd of 12 and 42 can also be expressed as certain linear combinations of 12 and 42:

$$\begin{aligned} 6 &= (-3)(12) + (1)(42) \\ &= (10)(12) + (-3)(42) \\ &= (17)(12) + (5)(42) \end{aligned}$$

One can readily find other integers u and v such that

$$6 = 12u + 42v \quad .$$

The following theorem shows that the phenomenon occurs anytime a number d is the gcd of two integers a and b.

THEOREM 8.3. *Let a and b be integers, not both zero, and let $d = GCD(a,b)$. Then there exists (not necessarily unique) integers u and v such that*

$$d = au + bv \quad .$$

Proof.

Let

$$S = \{z \in \mathbb{Z} \mid z = am + bn \quad ; \quad a,b \in \mathbb{Z} \quad \text{and} z > 0\} \quad .$$

The set S is subset of $\mathbb{N}$ (since each element $z \in S$ is prescribed to be non-negative) and non-empty since

$$a^2 + b^2 = (a)(a) + (b)(b) \in S$$

and is non-negative and greater than zero (since by hypothesis a and b are not both zero). By the Well-Ordering Axiom, S then has a smallest element t, which is a positive integer. By the definition of S we know that

$$t = au + bv$$

for some $u, v \in \mathbb{Z}$. We claim that t is the gcd of a and b.

To prove this, we first show that t divides b. By the Division Algorithm, there exists numbers q and r, with $0 \leq r < t$ such that

$$b = qt + r \quad .$$

Consequently,

$$\begin{aligned} r &= b - qt \\ &= b - q(au + bv) \\ &= -a(qu) + b(1 - qv) \quad . \\ &= au' + bv' \end{aligned}$$

Hence, now if r is not zero, then r would lie in S. But t is the smallest element of S and by the Division Algorithm cited above $r < t$. Therefore, $r = 0$. Hence,

$$b = qt$$

and so t divides b. One similarly shows that t divides a. Hence, t is a common divisor of a and b.

Now suppose that c is any other common divisor of a and b. The $a = cx$ and $b = cy$ for some integers x and y. Hence

$$\begin{aligned} t &= au + bv \\ &= (cx)u + (cy)v \\ &= c(xu + yv) \quad , \end{aligned}$$

which shows that c divides t. This implies that $|c| \leq |t| = t$. Hence $c \leq t$. Hence t is the gcd of a and b. ∎

Corollary 8.4. *Let a and b be integers, not both zero, and let d be a positive integer. Then $d = GCD(a,b)$ if and only if d satisfies*

(i) $d \,|\, a$ *and* $d \,|\, b$.
(ii) *if* $c \,|\, a$ *and* $c \,|\, b$, *then* $c \,|\, d$.

Proof.

Suppose $d = GDC(a,b)$. Then $d \geq 1$ and d satisfies (i) by definition. By the previous theorem, d can be expressed as

$$d = ua + vb$$

so if c is any other common factor of a and b, then there exist $s,t \in \mathbb{Z}$ such that $a = sc$ and $b = tc$; and so

$$\begin{aligned} d &= u(sc) + v(tc) \\ &= c(us + vt) \quad . \end{aligned}$$

In other words, c divides d.

Conversely, suppose d is a positive integer satisfying (i) and (ii); i.e., d divides a and b and every integer c dividing a and b also divides d. In particular, the gcd of a and b, call it D, must divide d. But if D divides d we must have

$$|D| \leq |d|$$

or

$$D \leq d \tag{8.1}$$

since both D and d must be positive. On the other hand, $D \equiv GCD(a,b)$ so all other common divisors of a and b must be less than or equal to D. In particular,

$$d \leq D \quad . \tag{8.2}$$

Comparing (8.1) and (8.2) we conclude

$$d = D = GCD(a,b) \quad .$$

▮

Theorem 8.5. *If $a \mid (bc)$ and $GCD(a,b) = 1$, then $a \mid c$.*

Proof.

Since $GCD(a,b) = 1$, Theorem 1.3 shows

$$au + bv = 1$$

for some integers u and v. Multiplying this equation by c yields

$$cau + cbv = c \quad . \tag{8.3}$$

Since a divides bc, we must have

$$bc = at$$

for xome $t \in \mathbb{Z}$. Inserting this expression for bc into (8.3) yields

$$cau + atv = c$$

or

$$a(au + tv) = c$$

and so a divides c. ▮

LEMMA 8.6. *If $a, b, q, r \in \mathbb{Z}$ and $a = bq + r$, then*

$$GCD(a,b) = GCD(b,r) \quad .$$

Proof.

Suppose c is a common divisor of a and b. Then $a = cs$ and $b = ct$ for some $s, t \in \mathbb{Z}$. Consequently,

$$\begin{aligned} r &= a - bq \\ &= cs - (ct)q \\ &= c(s - tq) \quad . \end{aligned}$$

Hence c divides r and so c is a common divisor of b and r. On the other hand, suppose e is a common divisor of b and r. Then $b = ex$, $r = ey$, and

$$\begin{aligned} a &= bq + r \\ &= (ex)q + ey \\ &= e(xq + y) \quad . \end{aligned}$$

So e divides a, and thus e is a common divisor of a and b. Therefore, the set S of all common divisors of a and b is the same as the set T of all common divisors of b and r. Hence,

$$GCD(a,b) = \mathrm{Max}(S) = \mathrm{Max}(T) = GCD(b,r) \quad .$$

∎