

Lecture 2: Theory on the greatest Common Divisor and the Linear Combinations

Theorem 1.3.2 Given integers a and b , not both of which are zero, there exist integers x and y such that $\gcd(a, b) = ax + by$.

Proof. Consider the set S of all positive linear combinations of a and b :

$$S = \{au + bv \mid au + bv > 0; u, v \text{ integers}\}.$$

Notice first that S is not empty. For example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ lies in S , where we choose $u = 1$ or $u = -1$ according as a is positive or negative. By the Well-Ordering Principle, S must contain a smallest element d . Thus, from the definition of S , there exist integers x and y for which $d = ax + by$. So it can claim that $d = \gcd(a, b)$.

Using the Division Algorithm, one can obtain the integers q and r such that $a = qd + r$, where $0 \leq r < d$. Then r can be written in the form

$$\begin{aligned} r &= a - qd = a - q(ax + by) \\ &= a(1 - qx) + b(-qy). \end{aligned}$$

If r were positive, then this representation would imply that r is a member of S , contradicting the fact that d is the least integer in S (recall that $r < d$). Therefore, $r=0$, and so $a = qd$, or equivalently $d|a$. By similar reasoning, $d|b$, so d is a common divisor of a and b .

Now if c is an arbitrary positive common divisor of the integers a and b , then part (g) of Theorem (1.3.1) allows us to conclude that $c|(ax + by)$; that is, $c|d$. By part (f) of the same theorem, $c = |c| \leq |d| = d$, so that d is greater than every positive common divisor of a and b . One can see that $d = \gcd(a, b)$. ■

Based on the proof of Theorem (1.3.2), the greatest common divisor of a and b may be described as the smallest positive integer of the form $ax + by$. Consider the case in which $a = 6$ and $b = 15$. Here, the set S becomes

$$\begin{aligned} S &= \{6(-2) + 15 \cdot 1, 6(-1) + 15 \cdot 1, 6 \cdot 1 + 15 \cdot 0, \dots\} \\ &= \{3, 9, 6, \dots\} \end{aligned}$$

So, it observes that the 3 is the smallest integer in S , whence $3 = \gcd(6, 15)$.

The nature of the members of S appearing in this illustration suggests another result, which we give in the next corollary.

Corollary. If a and b are given integers, not both zero, then the set

$$T = \{ax + by \mid x, y \text{ are integers}\} \text{ is}$$

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

Proof. Because $d|a$ and $d|b$, it can know that $d = (ax + by)$ for all integers x, y . Thus, every member of T is a multiple of d .

Conversely, d may be written as $d = ax_0 + by_0$ for suitable integers x_0 and y_0 , so that 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, by definition, lies in T . ■

It may happen that 1 and -1 are the only common divisors of a given pair of integers a and b , whence $\gcd(a, b) = 1$. For example:

$$\gcd(2, 5) = \gcd(-9, 16) = \gcd(-27, -35) = 1$$

This situation occurs often enough to prompt a definition.

Definition 1.3.3 Two integers a and b , not both of which are zero, are said to be *relatively prime* whenever $\gcd(a, b) = 1$.

- The following theorem characterizes relatively prime integers in terms of linear combinations.

Theorem 1.3.3 Let a and b be integers, not both zero. Then a and b are relatively prime if and only if there exist integers x and y such that $1 = ax + by$.

Proof. If a and b are relatively prime, so that $\gcd(a, b) = 1$, then Theorem

(1.3.2) guarantees the existence of integers x and y satisfying $1 = ax + by$. As for the converse, suppose that $1 = ax + by$ for some choice of x and y , and that $d = \gcd(a, b)$. Because $d \mid a$ and $d \mid b$, Theorem (1.3.1-g) yields $d \mid (ax + by)$, or $d \mid 1$. Since d is a positive integer, this last divisibility condition forces d to equal 1 (part (b) of Theorem (1.3.1) plays a role here), and the desired conclusion follows.

This result leads to an observation that is useful in certain situations, namely,

Corollary 1. If $\gcd(a, b) = d$, then $\gcd(a/d, b/d) = 1$.

Proof. It should observe that a/d and b/d , because d is a divisor both of a and of b . Now, knowing that $\gcd(a, b) = d$, it is possible to find integers x and y such that $d = ax + by$. Upon dividing each side of this equation by d , we obtain the expression

$$1 = (a/d)x + (b/d)y.$$

Because a/d and b/d are integers, the conclusion is that a/d and b/d are relatively prime. ■

For an illustration of the last corollary, let us observe that $\gcd(-12, 30) = 6$ and $\gcd(-12/6, 30/6) = \gcd(-2, 5) = 1$ as it should be.

It is not true, without adding an extra condition, that $a \mid c$ and $b \mid c$ together give $ab \mid c$. For instance, $6 \mid 24$ and $8 \mid 24$, but $6 \cdot 8$ not divide 24. If 6 and 8 were relatively prime, of course, this situation would not arise. This brings us to Corollary 2.

Corollary 2. If $a \mid c$ and $b \mid c$, with $\gcd(a, b) = 1$, then $ab \mid c$.

Proof. Since $a \mid c$ and $b \mid c$, integers r and s can be found such that $c = ar = bs$.

Now the relation $\gcd(a, b) = 1$ allows us to write $1 = ax + by$ for some choice of integers x and y . Multiplying the last equation by c , it appears that

$$c = c \cdot 1 = c(ax + by) = acx + bcy$$

If the appropriate substitutions are now made on the right-hand side, then

$$c = a(bs)x + b(ar)y = ab(sx + ry)$$

or, as a divisibility statement, $ab \mid c$. ■

Our next result is a fundamental importance result.

Theorem 1.3.4. (Euclid's lemma). If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.

Proof. Let us start from relation $1 = ax + by$, where x and y are integers. Multiplication of this equation by c produces

$$c = 1 \cdot c = (ax + by)c = acx + bcy.$$

Because $a \mid ac$ and $a \mid bc$, it follows that $a \mid (acx + bcy)$, which can be recast as $a \mid c$. ■

If a and b are not relatively prime, then the conclusion of Euclid's lemma may fail to hold.

Here is a specific example: $12 \mid 9 \cdot 8$, but 12 not divide 9 and 12 not divide 8.

The subsequent theorem often serves as a definition of $\gcd(a, b)$. The advantage of using it as a definition is that order relationship is not involved. Thus, it may be used in algebraic systems having no order relation.

Theorem 1.3.5. Let a, b be integers, not both zero. For a positive integer

d , $d = \gcd(a, b)$ if and only if

- (i) $d \mid a$ and $d \mid b$.
- (ii) Whenever $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. Suppose that $d = \gcd(a, b)$. Certainly, $d \mid a$ and $d \mid b$, so that (a) holds. In light of Theorem (), d is expressible as $d \mid (ax + by)$ for some integers x, y . Thus, if $c \mid a$ and $c \mid b$, then $c \mid (ax + by)$, or rather $c \mid d$. In short, condition (b) holds.

Conversely, let d be any positive integer satisfying the stated conditions. Given any common divisor c of a and b , we have $c \mid d$ from hypothesis (b). The implication is that $d \geq c$, and consequently d is the

greatest common divisor of a and b . ■

Dr. Ruma Kareem K. Ajeena