4. Divisibility and the Greatest Common Divisor

Definition. Let $a, b \in \mathbb{Z}$. We say that a *divides* b and write $a \mid b$ if $b = ak$ for some $k \in \mathbb{Z}$.

The following lemma collects some basic properties of divisibility:

Lemma 4.1. *Let $a, b, c \in \mathbb{Z}$. The following hold:*

(δ_1) *$a \mid 0$ and $1 \mid a$ for all $a \in \mathbb{Z}$*

(δ_2) *If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$*

(δ_3) *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$*

(δ_4) *If $a \mid b$, then $a \mid bk$ for every $k \in \mathbb{Z}$.*

Proof. (δ_1) follows directly from definition since $0 = a \cdot 0$ and $a = 1 \cdot a$ for any $a \in \mathbb{Z}$.

(δ_2) Since $a \mid b$, we have $b = ak$ for some $k \in \mathbb{Z}$, and since $b \neq 0$, we must have $k \neq 0$. But then $|k| \geq 1$, and therefore $|b| = |ak| = |a||k| \geq |a|$, as desired.

(δ_3) Since $a \mid b$ and $a \mid c$, we have $b = ak$ and $c = al$ for some $k, l \in \mathbb{Z}$. Adding these equalities, we get $b + c = ak + al = a(k + l)$. Since $k + l \in \mathbb{Z}$, by definition we have $a \mid (b + c)$.

(δ_4) is proved similarly to (δ_3). □

Definition. Let a, b be integers, at least one of which is nonzero. The *greatest common divisor* of a and b, denoted by $gcd(a, b)$, is the largest integer d which divides both a and b.

Before proceeding, we make some basic remarks about this definition.

(i) We have to exclude the pair $(a, b) = (0, 0)$ since in this case any integer divides both a and b, so there is no largest integer with this property.

(ii) On the other hand, if $a \neq 0$ or $b \neq 0$ and if some d divides both a and b, then by property (δ_2) we have $|d| \leq |a|$ (if $a \neq 0$) or $|d| \leq |b|$ (if $b \neq 0$). This ensures that there are only finitely many integers dividing both a and b, so in particular there exists the largest integer with this property. Thus, $gcd(a, b)$ is indeed defined.

(iii) We always have $gcd(a, b) \geq 1$ (so $gcd(a, b)$ is always positive). Indeed, 1 divides a and b by (δ_1), so the largest integer dividing both a and b must be at least 1.

We now formulate our main theorem about the greatest common divisor:

Theorem 4.2 (GCD Theorem). *Let $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$. The following hold:*

(a) *There exist $u, v \in \mathbb{Z}$ such that $gcd(a, b) = au + bv$. Moreover, $gcd(a, b)$ is the smallest positive integer representable in the form $am + bn$ with $m, n \in \mathbb{Z}$.*

(b) *If c is any integer such that $c \mid a$ and $c \mid b$, then $c \mid gcd(a, b)$.*

Before proving this theorem, we give an illustration of part (a). Let $a = 20$ and $b = 12$, in which case $gcd(a, b) = 4$. We can write $4 = 20\cdot(-1)+12\cdot 3$ (so we can take $u = -1$, $v = 2$ in GCD Theorem(a)); this representation is not unique as we can also write $4 = 20\cdot 2+12\cdot(-3)$. For the 'moreover' part, take any integer k of the form $k = 20m + 12n$. Then 4 divides k since 4 divides both 20 and 12, so if k is also positive, we must have $k \geq 4 = gcd(a, b)$.

Proof of GCD Theorem. We begin by explaining the general logic in the argument below. The proof will be completed in three steps:

Step 1: Define d to be the smallest positive integer of the form $am + bn$ with $m, n \in \mathbb{Z}$.

Step 2: Show that if $c \mid a$ and $c \mid b$ for some $c \in \mathbb{Z}$, then $c \mid d$.

Step 3: Show that d defined as in step 1 satisfies the definition of the greatest common divisor of a and b (that is, $d = gcd(a, b)$).

Note that Steps 1 and 2 alone do not prove any parts of GCD Theorem since at the end of Step 2 we do not know anything about the relationship between d and $gcd(a, b)$. However, once Step 3 is completed, we can replace d by $gcd(a, b)$ in the statements of Steps 1 and 2 and thereby deduce both parts of GCD Theorem. We now proceed with the actual proof.

Step 1: As suggested above, we let

$$S = \{x \in \mathbb{Z}_{>0} : x = am + bn \text{ for some } m, n \in \mathbb{Z}\}$$

and define d to be the minimal element of S. [1] Thus in particular, $d = au+bv$ for some $u, v \in \mathbb{Z}$.

Step 2: If $c \mid a$ and $c \mid b$, then c divides $d = au + bv$ by the combination of divisibility properties (δ_3) and (δ_4).

Step 3: Finally we check that $d = gcd(a, b)$. This, in turn, is completed in two substeps. First we prove that $d \mid a$ and $d \mid b$. We will show that $d \mid a$ (verification of the condition $d \mid b$ is analogous). We shall argue by contradiction.

[1] Note that S indeed has minimal element by the well-ordering principle since S is a subset of $\mathbb{Z}_{>0}$ (by definition) and S is non-empty (to ensure that $S \neq \emptyset$ note that integers $a, -a, b, -b$ are all of the form $am + bn$ and at least one of those integers is positive since a and b are not both zero).

So suppose that $d \nmid a$. As proved in Lecture 3, we can always divide a by d with remainder: $a = dq + r$ with $q, r \in \mathbb{Z}$ and $0 \le r < d$. But if $r = 0$, then by definition $d \mid a$ (contrary to our assumption), so we must have $r > 0$. Note that we can write

$$r = a - dq = a - (au + bv)q = a(1 - uq) + b(-v).$$

Thus, r is a positive integer of the form $am + bn$ with $m = 1 - uq \in \mathbb{Z}$ and $n = -v \in \mathbb{Z}$, so by definition, r is an element of S. This is impossible since $r < d$ and d was defined to be the minimal element of S.

Thus, we proved that $d \mid a$ and $d \mid b$ (so d is a common divisor of a and b), and it remains to show that there is no common divisor of a and b which is larger than d. This follows easily from the result of Step 2. Indeed, suppose that $c \mid a$ and $c \mid b$ for some $c \in \mathbb{Z}$. Then $c \mid d$ by Step 2, so by divisibility property (δ_2) we must have $c \le |c| \le |d| = d$. Therefore, d is indeed the greatest common divisor of a and b. □

We note that our definition of the greatest common divisor is different from the one in the book. The definition that we gave has two advantages: it is probably more intuitive, and it clearly implies that $gcd(a, b)$ exists and is unique. The “price” that we had to pay is the more convoluted structure of the proof of GCD theorem than the one in the book. Anyway, once GCD theorem is proved, it is clear that the two definitions are equivalent, so either definition can be used in all subsequent applications.

We finished the lecture with the discussion of the Euclidean algorithm for computing $gcd(a, b)$ as well as integers u and v satisfying $gcd(a, b) = au + bv$.