1.2 Divisibility

Definition. Let a and b be integers with $b \neq 0$. We say that b *divides* a, written $b \mid a$, if $a = bc$ for some integer c. If b divides a, we can also say that b is a *divisor* of a, or that b is a *factor* of a. If b does not divide a, we write $b \nmid a$.

Example. We have $3 \mid 24$, $\quad -5 \mid 10$, $\quad 7 \nmid 13$.
Example. $1 \mid a$ for any integer a, because $a = 1 \cdot a$.
Example. $b \mid 0$ for any $b \neq 0$, because $0 = b \cdot 0$.

Note that $b \mid a$ if and only if the remainder is 0 when a is divided by b. Indeed, both of these statements are different ways of saying that $a = bq$ for some integer q.

Now we prove some basic properties of divisibility:

Theorem. *If $a \mid b$ and $b \mid c$, then $a \mid c$.*

Proof. The given information says that $b = am$ and $c = bn$ for some $m, n \in \mathbb{Z}$. Therefore $c = amn$, so $a \mid c$. □

Theorem. *For any integer a, the numbers a and $-a$ have the same divisors.*

Proof. In order to prove this, we must prove that every divisor of a is a divisor of $-a$, and vice versa.

Let b be any divisor of a. Then $a = bc$ for some integer c, so $-a = b(-c)$. Therefore b is a divisor of $-a$ as well.

It follows that any divisor of $-a$ is also a divisor of $-(-a) = a$, so we are done. □

Theorem. *Let a and b be integers with $b \neq 0$. Then $b \mid a$ if and only if $-b \mid a$.*

Proof. If $b \mid a$, then $a = bc$ for some $c \in \mathbb{Z}$. Therefore $a = (-b)(-c)$ with $-c \in \mathbb{Z}$, so $-b \mid a$.

Thus, if $-b$ divides a, then $b = -(-b)$ divides a as well. □

Theorem. *If a is a nonzero integer and b is a divisor of a, then $|b| \leq |a|$.*

Proof. By definition, $a = bc$ for some integer c. Thus

$$|a| = |b||c| \geq |b|.$$ □

Corollary. *A nonzero integer has only finitely many divisors.*

Proof. If a is a nonzero integer, then any divisor b of a satisfies $|b| \leq |a|$; there are only finitely many such integers b. □

Corollary. *If a is a nonzero integer, then the greatest divisor of a is $|a|$.*

Proof. We know that $a = |a| \cdot (\pm 1)$, so $|a|$ is a divisor of a. The previous theorem shows that a does not have any divisors greater than $|a|$, so $|a|$ is the greatest divisor of a. □

Example. The divisors of 18 are $\pm 1, \pm 2, \pm 3, \pm 6, \pm 18$. You can prove this by brute force, since we know that we need only find the positive divisors, and that the positive divisors must be among $1, 2, \ldots, 18$. Later, we'll see more efficient ways to find all the divisors.

Example. The divisors of 30 are $\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30$.

Definition. If c is a divisor of both a and b, we say that c is a *common divisor* of a and b.

Example. Comparing the previous two examples, we see that the common divisors of 18 and 30 are

$$\pm 1, \pm 2, \pm 3, \pm 6$$

Definition. Let a and b be integers, not both zero. The *greatest common divisor* (gcd) of a and b is, well, the greatest common divisor. Formally, d is the gcd of a and b if:

- $d \mid a$ and $d \mid b$, and
- if $c \mid a$ and $c \mid b$, then $c \leq d$.

The gcd of a and b is usually denoted (a, b).

We know that a and b have a common divisor, namely 1. Since a and b have finitely many divisors, it follows that they must have a greatest common divisor. The fact that 1 is always a common divisor of a and b also shows that $(a, b) \geq 1$.

Example. By the previous example, $(18, 30) = 6$. Later, we'll see more efficient ways to find the gcd of two numbers that don't require us to find all the common divisors.

Since every nonzero integer is a divisor of 0, the common divisors of a and 0 are simply the divisors of a. Hence $(a, 0)$ is the greatest divisor of a. That is, $(a, 0) = |a|$.

Definition. If $(a, b) = 1$, we say that a and b are relatively prime.

The statement that $(a, b) = d$ is sometimes difficult to work with directly in proofs, since we can't manipulate this equation algebraically. Therefore we want to be able to express the statement that d is the gcd of a and b as an algebraic equation. Before doing that, we first give a definition:

Definition. We say that c is a *linear combination* of a and b if $c = au + bv$ for $u, v \in \mathbb{Z}$.

Example. Note that $6 = (18, 30)$ is a linear combination of 18 and 30 because $6 = 2 \cdot 18 + (-1) \cdot 30$. This is not a coincidence, as we will see later. On the other hand, 15 is not a linear combination of 18 and 30; any linear combination of 18 and 30 must be even, but 15 is odd.

Theorem. *Suppose $d \mid a$ and $d \mid b$. If c is any linear combination of a and b, then $d \mid c$.*

Proof. We have $a = dm$ and $b = dn$ for some $m, n \in \mathbb{Z}$ and $c = au + bv$ for some $u, v \in \mathbb{Z}$. Therefore

$$c = au + bv = dmu + dnv = d(mu + nv),$$

so $d \mid c$. □

Lemma. ***(Bézout's identity)*** *Let a and b be integers, not both 0. Then there exist integers u and v such that $(a, b) = au + bv$.*

In other words, (a, b) is always a linear combination of a and b. In fact, we will prove an even stronger statement:

Lemma. *Let a and b be integers, not both 0. Then (a, b) is the smallest positive linear combination of a and b.*

Proof. Let S denote the set of all positive linear combinations of a and b. Then S is nonempty, because it contains $a^2 + b^2$. Therefore it has a smallest positive element; call this element t, so that $t = au + bv$ for some $u, v \in \mathbb{Z}$. We must prove that $t = (a, b)$.

We first prove that $t \mid a$. By the division algorithm,

$$a = tq + r \qquad \text{for some } q, r \in \mathbb{Z} \text{ with } 0 \leq r < t.$$

Therefore r is a linear combination of a and b, since

$$r = a - tq = a - (au + bv)q = a(1 - uq) + b(-vq).$$

But t is the smallest such positive linear combination, and $r < t$, so r cannot be positive. Therefore $r = 0$, which proves that $t \mid a$. The same argument shows that $t \mid b$. Thus t is a common divisor of a and b; we need only check that it is the greatest common divisor.

Let c be any common divisor of a and b. By the previous theorem, $c \mid t$. Thus $c \leq |c| \leq |t| = t$, as we wanted to show. □

The integers u and v in the statement of Bézout's identity are called Bézout coefficients. However, they are not uniquely defined. For example,

$$6 = 2 \cdot 18 + (-1) \cdot 30 = 7 \cdot 18 + (-4) \cdot 30 = (-8) \cdot 18 + 5 \cdot 30$$

so $u = 2, v = -1$ or $u = 7, v = -4$ or $u = -8, v = 5$ are all valid choices of Bézout coefficients for 18 and 30.

As an example of the power of Bézout's identity, we use it to prove the following theorem. Note that the theorem would be difficult to prove without Bézout, since we wouldn't have any good way to use the information that $(a, b) = 1$.

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

Proof. The given information tells us that $bc = ak$ for some $k \in \mathbb{Z}$. Bézout's identity says that $1 = au + bv$ for some $u, v \in \mathbb{Z}$. Thus

$$c = c(au + bv) = auc + bcv = auc + akv = a(uc + kv),$$

so $a \mid c$. □

We end with another characterization of the gcd.

Theorem. *Let a and b be integers, not both zero. Let d be a positive integer. Then d is the gcd of a and b if and only if it satisfies:*

(i) $d \mid a$ and $d \mid b$, and

(ii) if $c \mid a$ and $c \mid b$, then $c \mid d$.

Proof. First suppose $d = (a, b)$. The d satisfies (i) by definition. It satisfies (ii) by Bézout, because any linear combination of a and b satisfies (ii).

Now suppose d satisfies (i) and (ii). Then (ii) says that $(a, b) \mid d$, so $d = |d| \geq (a, b)$. Since (a, b) is the greatest common divisor and d is a common divisor, this shows that $d = (a, b)$. □