Chapter 4

Divisibility

4.1 The division algorithm

For the next few lectures we will exercise our ability to prove mathematical statements, using the fertile ground of number theory. In the process we will learn new proof techniques and tricks of trade. The number-theoretic concepts and results we will cover will be useful throughout your computer science studies, and, indeed, throughout your involvement with mathematics.

The following result is commonly known as the *division algorithm*, even though it is not an algorithm at all.

Theorem 4.1.1. *If a and b are integers and $b \neq 0$, then there is a unique pair of integers q and r, such that $a = qb + r$ and $0 \leq r < |b|$.*

Proof. We need to prove two things: that there is some such pair q, r (existence) and that this pair is unique (uniqueness).

Let's begin with existence. First we show that there is a pair $q, r \in \mathbb{Z}$ that satisfies $a = qb + r$ for some $r \geq 0$. This is easy after some playing around: Take $q = -|ab|/b$ and $r = a + |ab|$. Since $|b| \geq 1$, it holds that $r \geq 0$. Now we need to show that such $q, r \in \mathbb{Z}$ exist with r in addition being smaller than $|b|$. For this, consider the set S of all $r \in \mathbb{N}$ that satisfy $a = qb + r$ for some $q \in \mathbb{Z}$. We've just shown that S is nonempty, so it must have a smallest element, call it r_0. We have $a = q_0 b + r_0$. If $r_0 < |b|$ we're done. Otherwise, we have $a = (q_0 b + |b|) + (r_0 - |b|)$, which means that $r_0 - |b|$ is a smaller element of S than r_0, leading to a contradiction. This completes the existence proof.

To prove uniqueness, suppose that $a = qb + r = sb + t$, with $0 \leq r, t < |b|$. Thus $(q - s)b + (r - t) = 0$. Since $0 \leq r, t < |b|$, we have $|r - t| < |b|$, hence $|(q - s)b| < |b|$ and $|q - s| < 1$. Since q and s are integers, this implies $q = s$. From this we have $r = t$ and the uniqueness proof is complete. □

Proof tip: When we need to prove that some mathematical object exists and is unique, it is useful to approach in two stages. First prove that at least one such object exists. This can be done either by directly constructing an object and demonstrating that it fulfills the requirements, or by assuming that no such object exists and reaching a contradiction. Then show that any two such objects must be the same.

The Well-Ordering Principle. In proving the division algorithm, we considered a certain set $S \subseteq \mathbb{N}$ and argued that since it is nonempty, it must have a smallest element. Why is this true? As with induction, we accept this proposition as an axiom. In general, the "well-ordering principle" states that *any nonempty set of natural numbers must have a smallest element.* As you will prove in the homework, the well-ordering principle is equivalent to the principles of induction and strong induction.

4.2 Remainders

A more algorithmic view of Theorem 4.1.1 is as follows: If we divide the equation

$$a = qb + r$$

by b we get

$$\frac{a}{b} = q + \frac{r}{b}.$$

Since $0 \leq r < |b|$, we get that if $b > 0$, then $0 \leq \frac{r}{b} < 1$ and thus $q = \left\lfloor \frac{a}{b} \right\rfloor$, the greatest integer less than or equal to $\frac{a}{b}$. If $b < 0$, then $0 \geq \frac{r}{b} > -1$ and thus $q = \left\lceil \frac{a}{b} \right\rceil$, the least integer greater or equal to $\frac{a}{b}$. This can be used to calculate q, from which we can derive r.

In Theorem 4.1.1, we call q the *quotient* and r the *remainder*. We use the notation $r = a \text{ rem } b$ to denote that r is the remainder when a is divided by b. There is no need for a special notation for quotient, since we can just use $\left\lfloor \frac{a}{b} \right\rfloor$ and $\left\lceil \frac{a}{b} \right\rceil$, depending on the sign of b.

Definition: If a and b are such that $a \text{ rem } b = 0$ we say that a is a *multiple* of b, or that b *divides* a (or is a *divisor* of a). Note that this holds when there exists some integer q, such that $a = qb$. In particular, every integer divides 0, and every integer is a multiple of 1. When b divides a we write $b|a$, and when b does not divide a we write $b \not| a$.

Definition: An integer u is called a *linear combination* of a set of integers $a_1, a_2, \ldots, a_n$ if and only if there exist integer coefficients $c_1, c_2, \ldots, c_n$ that satisfy

$$u = \sum_{i=1}^{n} c_i a_i.$$

Theorem 4.2.1. *Properties of divisibility:*

(a) If $b|a$ and $c|b$ then $c|a$.

(b) If $b|a$ and $a \neq 0$ then $|b| \leq |a|$.

(c) If b divides each of $a_1, a_2, \ldots, a_n$, then b divides all linear combinations of $a_1, a_2, \ldots, a_n$.

(d) $a|b$ and $b|a$ if and only if $a = \pm b$.

Proof. We prove the properties in turn:

(a) Since $b|a$, there exists an integer q, such that $a = qb$. Similarly, there exists an integer r, such that $b = rc$. Thus $a = qb = qrc$. Since qr is an integer, it holds that $c|a$.

(b) Since $b|a$, there exists an integer q, such that $a = qb$. This implies $|a| = |q| \cdot |b|$. Assume for the sake of contradiction that $a \neq 0$ but $|b| > |a|$. Then $|q| \cdot |b| < |b|$. Since $|b| > |a| > 0$, we can divide by $|b|$ to get $|q| < 1$, implying $q = 0$. Thus $a = qb = 0$, which is a contradiction.

(c) Consider a linear combination $u = \sum_{i=1}^n c_i a_i$. Since $b|a_i$, there exists an integer q_i, such that $a_i = q_i b$, for all $1 \leq i \leq n$. Thus

$$u = \sum_{i=1}^n c_i a_i = \sum_{i=1}^n c_i q_i b = b \cdot \sum_{i=1}^n c_i q_i.$$

Since $\sum_{i=1}^n c_i q_i$ is an integer, we have $b|u$.

(d) For the "if" statement, note that if $a = \pm b$ then $b = qa$ and $a = qb$, for $q = \pm 1$, so $a|b$ and $b|a$. To prove the "only if" statement, assume that $a|b$ and $b|a$. This implies the existence of integers q and r, such that $b = qa$ and $a = rb$. Thus $b = qrb$. If $b = 0$ then $a = 0$ and the claim that $a = \pm b$ holds. Otherwise we can divide by b to get $qr = 1$. Note that in this case $q, r \neq 0$. Part (b) of the theorem implies that $|q| \leq 1$ and $|r| \leq 1$. Thus $q, r = \pm 1$ and the claim that $a = \pm b$ follows.

□

Proof tip: Often we need to prove that a proposition A holds if and only if some other proposition B holds. Such an "if and only if" (sometimes abbreviated as "iff") statement is really composed of two implications, each of which needs to be proved. It is often useful to decouple these and prove them separately. First prove that "If A then B," and then prove that "If B then A." Another strategy is to prove that "If A then B" and "If not A then not B."

4.3 Greatest common divisors

If $d|a$ and $d|b$ then d is a *common divisor* of a and b. For example, 1 is a common divisor of any pair a, b. If a and b are not both 0 then, by Theorem 4.2.1(b), any common divisor of a and b is not greater than $\max(|a|, |b|)$. Thus the set of common divisors of a and b has a largest element, called the *greatest common divisor* of a and b, or $\gcd(a, b)$. This is the integer d that satisfies the following two criteria:

- $d|a$ and $d|b$.

- If $c|a$ and $c|b$ then $c \leq d$.

Note that when $a = b = 0$, there is no greatest common divisor, since any integer divides 0. When a and b are not both 0, we often want to compute $\gcd(a, b)$ efficiently. Note that the set of divisors of a and $-a$ is the same, and similarly for b and $-b$. Furthermore, if $a = 0$ then $\gcd(a, b) = b$, and if $a = b$ then $\gcd(a, b) = a = b$. Thus it suffices to concentrate on the case $a > b > 0$, without loss of generality.

Since $1 \leq \gcd(a, b) \leq b$, we can just test all integers between 1 and b and choose the largest one that divides both a and b. However, there is a much more efficient way to find greatest common divisors, called Euclid's algorithm. This algorithm, one of the earliest in recorded history, is based on the following lemma.

Lemma 4.3.1. *If* $a = qb + r$ *then* $\gcd(a, b) = \gcd(b, r)$.

Proof. By Theorem 4.2.1(c), all common divisors of b and r also divide a, since a is a linear combination of b and r. Thus a common divisor of b and r is also a common divisor of a and b. Similarly, since $r = a - qb$, a common divisor of a and b also divides r, so it is a common divisor of b and r. Thus a, b and b, r have the same set of common divisors, and in particular the same greatest common divisor. □

With this lemma in our toolbelt, Euclid's algorithm is easy to describe. To find $\gcd(a, b)$, use the division algorithm (Theorem 4.1.1) to represent $a = qb + r$, where $0 \leq r < b$. (Remember that we are assuming that $a > b > 0$.) If $r = 0$ then $b|a$ and $\gcd(a, b) = b$. Otherwise $\gcd(a, b) = \gcd(b, r)$ and $b > r > 0$. We can thus repeat the above procedure recursively with the pair b, r. Every recursive call strictly reduces both numbers in the pair, so after at most b steps the algorithm will terminate with a valid greatest common divisor of a and b. You will formally prove the correctness of the algorithm in the homework.

4.4 Greatest common divisors and linear combinations

We have seen that a common divisor of a and b divides any linear combination of a and b. Now we will prove a surprising property known as *Bezout's identity* that shows that the greatest common divisor of a and b is itself a linear combination of a and b.

Theorem 4.4.1. *For two integers a and b that are not both* 0, $\gcd(a, b)$ *is a linear combination of a and b.*

Proof. As above, we can concentrate on the case $a > b > 0$. The proof proceeds by strong induction on the value of a. In the base case, $a = 2$, $b = 1$, and $\gcd(a, b) = 1 = 0 \cdot a + 1 \cdot b$. Assume that the theorem holds for all pairs a, b with $0 < b < a \leq k$. Consider a pair a', b' with $0 < b' < a' = k + 1$. If $b'|a'$ then $\gcd(a', b') = b'$ and the theorem trivially holds. Otherwise use the division algorithm to express $a' = qb' + r$, where $0 < r < b'$. By the induction hypothesis, there exist coefficients u and v, such that $\gcd(b', r) = ub' + vr$. Lemma 4.3.1 shows that $\gcd(a', b') = \gcd(b', r)$, therefore $\gcd(a', b') = ub' + vr = ub' + v(a' - qb') = va' + (u - vq)b'$. This shows that $\gcd(a', b')$ is a linear combination of a' and b' and completes the proof by induction. □

Bezout's identity implies that the set of linear combinations of a and b is the same as the set of multiples of their greatest common divisor (!):

Corollary 4.4.2. *An integer z is a linear combination of a and b if and only if it is a multiple of $\gcd(a, b)$. In particular, $\gcd(a, b)$ is the least positive linear combination of a and b.*

Proof. By Theorem 4.2.1(c), since $\gcd(a, b)$ divides both a and b, it divides any linear combination z of a and b, and thus z is a multiple of $\gcd(a, b)$. On the other hand, we know by Bezout's identity that there are coefficients u and v, such that $\gcd(a, b) = ua + vb$, so if $z = c \cdot \gcd(a, b)$, then $z = c(ua + vb) = (cu)a + (cu)v$. □