§2. The Euclidean Algorithm

Divisibility is a most useful concept in mathematics. We will explore this idea and present a famous algorithm for finding the greatest common divisor (GCD) of two numbers.

Our intuitive understanding of divisibility is probably this: an integer b is said to divide another integer a if and only if a is a multiple of b. Another common way to think about it is that dividing a by b leaves no remainder. This definition suffices for most purposes, but sometimes it is useful to have a more formal notion of the concept: b divides a if there is some integer m for which $a = mb$. This is useful in using divisibility information within an algebraic context.

Now that we have established the notion of divisibility, we can turn to the concepts of divisors (which are also called the 'factors' of a number) and the greatest common divisor. The *divisors* of an integer a are all the integers that divide a. For example, the divisors of 24 are $1, 2, 3, 4, 6, 8, 12, 24$. Note that a divisor must be less than or equal to the number it is a divisor of.

Given two integers, we can ask which divisors they have in common. For example, 2 is a common divisor of any pair of even numbers, and 3 is a common divisor of 9 and 24. The *greatest common divisor* (GCD) of two numbers is the largest of the two numbers' common divisors; in other words, it is the largest number that divides both of them. This value is of such important that it has its own notation; it is commonly denoted by $\gcd(a, b)$, where a and b are nonzero integers. If $\gcd(a, b) = 1$, then a and b are *coprime* or *relatively prime*.

How do we find the GCD of two numbers? Of course, we could just list the divisors of each and find the greatest number that is in both lists. However this is slow and not convenient for large numbers. Fortunately, there is an elegant algorithm of Euclid's that finds the GCD of two numbers in a much more efficient way.

Suppose we have two positive integers a and b that we want to find the GCD of. The core of the Euclidean algorithm is *Euclidean division*, which means expressing a in the form

$$a = qb + c,$$

where q and c are nonnegative integers and $c < b$. We call q the *quotient* and c the *remainder*. Writing this equation is really the same as dividing a by b with remainder; for example, if $a = 104$ and $b = 24$ we would write

$$104 = 4 \times 24 + 8.$$

Now let d be any common divisor of a and b; we know there must be at least one because 1 divides every positive integer. Note that d divides c too, because $c = a - qb$. To make this conclusion we rely on a simple theorem that you can prove for yourself: if two numbers m and n are both divisible by a third number k, then so is their sum $m + n$ and their difference $m - n$. In our specific case, we assume that d divides both a and qb, and so it must divide their difference $c = a - qb$.

By definition d divides b, and we have just shown that d also divides c; it follows from this that d is also a common factor of b and c. We have assumed nothing about d as a common divisor of a and b, so we are justified in saying that the set of common divisors of a and b is the same as the set of common divisors of b and c. Hence the GCD of a and b is equal to the GCD of b and c.

This may not seem like progress, but it is. We have essentially reduced the original problem to a smaller one: finding the GCD of b and c. It is "smaller" because $c < b$, whereas before $b < a$.

So now we just play the game again; we want to find the GCD of b and c and so we write

$$b = q'c + c'$$

where q' and c' are nonnegative integers and $c' < c$. Again we deduce that the GCD of b and c must be the same as that of c and c'.

Obviously we can't just keep going on like this forever, or else we wouldn't be solving the original problem of finding $\gcd(a, b)$. Where does it stop?

Note that the sequence of remainders we obtain by successive use of Euclidean division is a strictly decreasing sequence. The second time we did the division we had $c' < c$, and if we had continued we would have $c'' < c'$, $c''' < c''$, and so on. A decreasing sequence of nonnegative integers must reach 0 at some point. That is, one of the terms in the sequence $c, c', c'', \ldots$ must be 0. Let the term directly preceding it be t and the term preceding t be s. Recall that each term in the sequence comes from the Euclidean division of the preceding terms: c is the remainder when a is divided by b, the next term c' is the remainder when b is divided by c, and so on.

How did we get this 0 in our list of remainders? We must have used the division algorithm on s and t, the two previous terms. Therefore the relationship between s and t is

$$s = tu + 0$$

for some positive integer u. From this we infer that s is actually a multiple of t. But if s is a multiple of t, then the GCD of s and t must be t.

So we have found the GCD of t and s, but we haven't solved our original problem, which was to find the GCD of a and b. Actually, we have! Recall that we showed the GCD of a and b is the

same as that of b and c. In the same way, the GCD of b and c is the same as that of c and c'. Continuing in this fashion. we find that the GCD of a and b is the same as that of s and t; hence $\gcd(a, b) = t$, the last nonzero remainder in our list of remainders supplied by repeated application of Euclidean division.

That, in a nutshell, is the Euclidean algorithm for finding the GCD of two numbers. To summarise, here is the algorithm in two simple steps. Assume we want to find $\gcd(a, b)$.

1) If a is a multiple of b, then $\gcd(a, b) = b$.
2) Otherwise, let c be the remainder when a is divided by b. Then $\gcd(a, b) = \gcd(b, c)$.

Up until now, we have been using only algebraic symbols, which may have made the process of the algorithm confusing. Let's now do a concrete example and find $\gcd(177, 48)$. We begin by writing

$$177 = 3 \times 48 + 33.$$

Now the problem is reduced to finding $\gcd(48, 33)$, for which we continue with

$$48 = 1 \times 33 + 15.$$

The remainder is not 0 yet so the algorithm continues.

$$33 = 2 \times 15 + 3.$$

It is clear that the next remainder will be 0. One more application of the division algorithm yields

$$15 = 5 \times 3 + 0.$$

We have reached a 0 remainder, so $\gcd(177, 48) = 3$, the last nonzero remainder. Note we could also have deduced that since $\gcd(15, 3) = 3$, then $\gcd(177, 48) = \gcd(15, 3) = 3$.

This was a small example, so you might have been able to do it the naiv́e way (listing the factors of both numbers) or even in your head. Now try finding

$$\gcd(1160718174, 316258250).$$

(Despite the size of the numbers, you can get the answer using only a scientific calculator. Your immediate objection might be that the calculator has no button to give the remainder upon division; how might you get the remainders manually?)

A simple linear equation

In this section, let $g = \gcd(a, b)$.

Surprisingly, Euclid's algorithm answers the question of when the equation

$$ax - by = c \tag{1}$$

has natural number solutions in x and y. It is clear that $ax - by$ is always a multiple of g, because both ax and by are multiples of g. Thus (1) has natural number solutions only when c is a multiple of g.

Now that we know when (1) has solutions, the next question is whether there is always a solution with $c = g$; that is, whether a linear combination of a and b can ever equal their GCD. The answer is yes; the equation $ax - by = g$ always has solutions in natural numbers x and y. To see why, we need Euclid's algorithm.

If c is the sum or difference of multiples of a and b (this is the same as saying there are integer solutions to $ax - by = c$), we say that c is *linearly dependent* on a and b. We now aim to prove the following results:

1) If c is linearly dependent on a and b, so is kc for any natural number k.
2) If both c and d are linearly dependent on a and b, so are $c + d$ and $c - d$.
3) Both a and b are linearly dependent on themselves.

The first is easy; if $c = ax - by$ then $kc = akx - bky$, so kc is also linearly dependent on a and b, with solution (kx, ky). The second is only slightly more difficult. Let

$$c = ax_1 - by_1$$

and

$$d = ax_2 - by_2.$$

Then

$$c + d = (ax_1 - by_1) + (ax_2 - by_2),$$

which implies

$$c + d = a(x_1 + x_2) - b(y_1 + y_2).$$

showing that $c + d$ is also linearly dependent on a and b. Similarly,

$$c - d = (ax_1 - by_1) - (ax_2 - by_2),$$

and so

$$c - d = a(x_1 - x_2) - b(y_1 - y_2).$$

We verify the third statement simply by seeing that $a = a(b + 1) - b(a)$ and $b = b(a + 1) - a(b)$.

Note that we cannot write $a = a \cdot 1 + b \cdot 0$, because x and y are natural numbers.

We are now ready to use Euclid's algorithm to show that the equation $ax - by = g$ is soluble in the natural numbers. Recall that the first line of the algorithm is to write $a = qb + c$, which implies $c = a - qb$. Since a and qb are both linearly dependent on a and b (from the first and third rules), so is their difference, which is c (from the second rule).

Now we know that both b and c are linearly dependent on a and b. We can again arrange the next line, $b = q'c + c'$, for the remainder: $c' = b - q'c$. Applying the same reasoning as before, we deduce that c' is also linearly dependent on a and b.

In other words, a and b being linearly dependent on themselves implies that each remainder of the Euclidean algorithm is also linearly dependent on them. In particular $\gcd(a, b)$ is linearly dependent on a and b because it is the last nonzero remainder in the algorithm.

Thus we have accomplished what we set out to show: linear equations of the form $ax - by = \gcd(a, b)$ are always soluble in the natural numbers. Note this also means that the equation $ax - by = c$ always has natural number solutions when a and b are coprime, as every natural number is a multiple of 1.

The preceding logic, although beautiful, only provides us insight as to why Equation (1) is always soluble. It doesn't actually give us a way to solve the equation in practice. Fortunately, the process isn't difficult; we illustrate with a concrete example.

Suppose we want to solve the equation $177x - 48y = 3$ (previously we found that $\gcd(177, 48) = 3$). We begin by writing the lines of the Euclidean algorithm. To make things easier, replace 177 by a and 48 by 3; the reason will become apparent soon.

$$\begin{aligned} a &= 3b + 33 \\ b &= 1 \times 33 + 15 \\ 33 &= 2 \times 15 + 3 \end{aligned}$$

Rearranging the first line for the remainder, we get $33 = a - 3b$. Substitute this into the next equation, and solve for its remainder again:

$$\begin{aligned} b &= (a - 3b) + 15 \\ 15 &= b - (a - 3b) \\ &= 4b - a \end{aligned}$$

If we keep repeating this process we'll eventually end up with 3, the last remainder, expressed as a combination of a and b. For the third line we substitute in both $33 = a - 3b$ and $15 = 4b - a$.

$$\begin{aligned} a - 3b &= 2(4b - a) + 3 \\ a - 3b &= 8b - 2a + 3 \\ 3 &= 3a - 11b \end{aligned}$$

Finally, read off the coefficients of a and b to find that the solution is $x = 3$ and $y = 11$.

Problems

1) Describe a general procedure for solving the equation $ax - by = n$ in the natural numbers where n is a multiple of $\gcd(a, b)$.
2) Solve the equation

$$1769x - 551y = \gcd(1769, 551)$$

for natural numbers x and y.
3) Try using Euclid's algorithm to solve the equation $7200x - 3132y = \gcd(7200, 3132)$ for positive integers x and y. What seems to be wrong at the end? How can this be fixed?
4) Show that if $a^x \equiv 1 \pmod{n}$ and $b^y \equiv 1 \pmod{n}$, then

$$a^{\gcd(x,y)} \equiv 1 \pmod{n}.$$

5) Let a and b be coprime positive integers. Show that for any integer k, there exists another positive integer N such that N is divisible by a and $N + k$ is divisible by b.
6) Prove that if a prime p divides a product ab, then p divides at least one of a and b. (Do this without relying on the Fundamental Theorem of Arithmetic.)