MATH 25 CLASS 4 NOTES, SEP 28 2011

Contents

Quick links to definitions/theorems

- The main theorem on solving a linear equation in integers

1. Bezout's Identity

It turns out that the Euclidean algorithm can help us solve other problems related to gcds. First, we'll see that the Euclidean algorithm provides a method for us to solve the equation

$$ax + by = \gcd(a, b),$$

in integers x, y. For instance, the Euclidean algorithm will give us a way to find an integer solution to the equation $994x+399y = 7$. (Notice that without the Euclidean algorithm, it's not even obvious whether this has an integer solution.)

How do we do this? Suppose we calculate $\gcd(a, b)$ by applying the Euclidean algorithm to a, b. Then this gives a sequence of Euclidean divisions of the form

$$a = q_1 b + r_1, b = q_2 r_1 + r_2, r_1 = q_3 r_2 + r_3, \ldots, r_{n-2} = q_n r_{n-1} + r_n,$$

for some positive integer n, where $r_n = 0$. Why does this algorithm eventually terminate? Notice that $a > b > r_1 > r_2 > \ldots$ is a strictly decreasing sequence of non-negative integers, so we eventually have to reach a point where one of the $r_n = 0$, and at that point the Euclidean algorithm terminates.

Let's look at the last two equations. We have

$$r_{n-2} = q_n r_{n-1} + 0, r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}.$$

Since $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \ldots = \gcd(r_{n-2}, r_{n-1}) = r_{n-1}$, we want to rewrite r_{n-1} in the form $ax + by$, for some to-be-determined integers x, y. If we just take the second to last equation in our list and rewrite try to get an expression $r_{n-1} = \ldots$, we obtain

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}.$$

Another way of writing this is

$$\gcd(a, b) = x_{n-2} r_{n-3} + y_{n-2} r_{n-2},$$

where x_{n-2}, y_{n-2} are integers; more specifically, $x_{n-2} = 1, y_{n-2} = -q_{n-1}$.

Well, this isn't exactly what we want, since we have written $\gcd(a, b)$ not as an integral combination of a, b, but rather of r_{n-3}, r_{n-2}. But the third to last equation in our list is $r_{n-4} = q_{n-2}r_{n-3} + r_{n-2}$. How does this help? We can rearrange this equation to $r_{n-2} = r_{n-4} - q_{n-2}r_{n-3}$. And then we can plug this expression for r_{n-2} back into the second to last equation to get

$$\begin{aligned}\gcd(a,b) &= x_{n-2}r_{n-3} + y_{n-2}(r_{n-4} - q_{n-2}r_{n-3}) \\ &= y_{n-2}r_{n-4} + (x_{n-2} - y_{n-2}q_{n-2})r_{n-3} \\ &= x_{n-3}r_{n-4} + y_{n-3}r_{n-3},\end{aligned}$$

where x_{n-3}, y_{n-3} are some integers (which we can compute in terms of the preceding pair x_{n-2}, y_{n-2} and q_{n-2}). This looks more messy (in a way, it is), but it expresses $\gcd(a,b)$ as a multiple of r_{n-3} plus a multiple of r_{n-4}. This looks like progress! As a matter of fact, we can continually replace r_{n-k} by using the equation $r_{n-k} = r_{n-k-2} - q_{n-k}r_{n-k-1}$ to convert an expression involving r_{n-k-1}, r_{n-k} to one involving r_{n-k-2}, r_{n-k-1}. If we continue doing this, we eventually will be able to write $\gcd(a,b)$ as a multiple of a plus a multiple of b.

If this sounds kind of confusing, a few examples should make this algorithm more clear.

Examples.

- Going back to our example where $a = 994, b = 399$, several applications of Euclidean division gave the equations

$$994 = 399 \cdot 2 + 196, 399 = 196 \cdot 2 + 7, 196 = 7 \cdot 24.$$

  We found that $\gcd(994, 399) = 7$. We want to find integers x, y such that $7 = 994x + 399y$. The first step is to look at the second to last equation, and rearrange it so that $7 = \gcd(a,b)$ is on one side by itself:

$$7 = 399 - 196 \cdot (2).$$

  The next step is to take the previous equation, and rewrite it so that its remainder is on one side by itself:

$$196 = 994 - 399 \cdot (2).$$

  We then substitute this expression for 196 into the previous equation:

$$7 = 399 - (994 - 399 \cdot (2)) \cdot (2).$$

  This looks a bit messy, but we expand and gather terms so that the right hand side looks like a multiple of 399 plus a multiple of 994:

$$7 = 994 \cdot (-2) + 399 \cdot (5).$$

  So the integer pair $x = -2, y = 5$ solves the equation $7 = 994x + 399y$ in integers.
- Let's do a slightly more complicated example. Let $a = 273, b = 94$. The Euclidean algorithm yields the following:

$$\begin{aligned}273 &= 94\cdot(2)+85,\\ 94 &= 85\cdot(1)+9,\\ 85 &= 9\cdot(9)+4,\\ 9 &= 4\cdot(2)+1,\\ 4 &= 1\cdot(4).\end{aligned}$$

The last nonzero remainder was 1, so this tells us $\gcd(273,94)=1$. Let's find a pair of integers x,y which solves $273x+94y=1$:

$$1 = 9 - 4\cdot(2).$$

Replacing 4 with $4 = 85 - 9\cdot(9)$ gives

$$1 = 9-(85-9\cdot(9))\cdot(2) = 85\cdot(-2)+9\cdot(19).$$

Replacing 9 with $9 = 94-85$ gives

$$1 = 85\cdot(-2)+(94-85)\cdot(19) = 94\cdot(19)+85\cdot(-21).$$

Finally, replacing 85 with $85 = 273-94\cdot(2)$ gives

$$1 = 94\cdot(19)+(273-94\cdot(2))\cdot(-21) = 273\cdot(-21)+94\cdot(61).$$

So we find that $x=-21, y=61$ solves $273x+94y=1$. Notice that this is probably a much more efficient way of solving $273x+94y=1$ in integers than, say, guess and check.

The fact that we can solve $ax+by=\gcd(a,b)$ in integers x,y is sometimes called *Bezout's identity*. This is useful not only for actually solving equations, but for theoretical knowledge as well:

Theorem 1 (Theorem 1.8 of Chapter 1)**.** *Let a,b be non-zero integers, and c some integer. Then the equation $ax+by=c$ has a pair of integer solutions x,y if and only if* $\gcd(a,b)|c$.

Proof. If we want to prove an "if and only if" statement, there are really two things to prove: the if direction and the only if direction. Let's start by proving that if $ax+by=c$ has a pair of integer solutions x,y, then $\gcd(a,b)|c$. We'll let $d=\gcd(a,b)$. Then $d|a,b$, by definition of gcd, so $d|(ax+by)$. But then $d|c$, as desired.

Now let's prove the "only if" direction: that if $\gcd(a,b)|c$, then $ax+by=c$ has a pair of integer solutions. We've already seen that $ax+by=d$ has a pair of integer solutions x_0,y_0, say. So we have $ax_0+by_0=d$. Since $d|c$, we have $c=qd$ for some integer q. But then we can multiply our equation by q to get $q(ax_0+by_0)=d$, or $a(qx_0)+b(qy_0)=dq=c$. Then the pair $x=qx_0, y=qy_0$ give integer solutions to $ax+by=c$, as desired. □