CLASS 3, GIVEN ON 9/27/2010, FOR MATH 25, FALL 2010

1. Greatest common divisor

Suppose a, b are two integers. If another integer d satisfies $d|a, d|b$, we call d a *common divisor* of a, b. Notice that as long as at least one of a, b is nonzero, then there will be a largest positive common divisor. We call this number the *greatest common divisor* of a, b. We will write this number as $\gcd(a, b)$, or if we are really lazy, just (a, b). (Yes, this last notation is very ambiguous, since (a, b) is more familiar as the ordered pair (a, b), but the context should usually make what we mean clear. To make things worse, (a, b) sometimes might even mean the open interval $a < x < b$. These three totally unrelated uses of the same notation is not the best, but it usually should be clear what we mean!)

Examples.

- Suppose $a = 8, b = 12$. The (positive) divisors of a are $1, 2, 4, 8$, while the divisors of b are $1, 2, 3, 4, 6, 12$. Looking at this list, the greatest common divisor of $8, 12$ is evidently 4.
- Suppose $a = 72, b = 74$. The most naive way of computing the gcd is to enumerate all the divisors of 72 and 74, and then compare the list. But suppose we don't want to do that – after all, it looks like it'll take a lot of work to find all the divisors of 72 and 74! How might we save the amount of calculations we have to make? Suppose $d|a, b$, so that d is any common divisor of a, b. Then $d|(b - a)$. But in this case, $b - a = 2$, so $d|2$. Therefore, the only possible common divisors are $1, 2$. We easily can see that $2|72, 74$, so this means that $\gcd(72, 74) = 2$. The moral of this example is that there are more efficient ways of calculating gcds than simply jumping right in and enumerating divisors, which in general will take a very long time.
- Suppose $b|a$, and $b \neq 0$. What is $\gcd(a, b)$?
- We can also extend the definition of gcd to more than two integers. The greatest common divisor of a set of integers $a_1, \ldots, a_k$ is the largest positive integer d such that $d|a_1, \ldots, a_k$. For example, if $a = 4, b = 6, c = 8$, then $\gcd(4, 6, 8) = 2$. We can show this by either enumerating all the divisors of a, b, c, or by applying the following fact (exercise 1.9 of the text): If $a_1, \ldots, a_k$ are integers, then $\gcd(a_1, \ldots, a_k) = \gcd(\gcd(a_1, a_2), a_3, \ldots, a_k)$. In practice, what this means is that we can calculate the gcd of k integers by taking the gcd of $k - 1$ pairs of integers. For example, $\gcd(4, 6, 8) = \gcd(\gcd(4, 6), 8) = \gcd(2, 8) = 2$.
- Notice that $1|a$ for all integers a. So a greatest common divisor is always at least 1. In the case that $\gcd(a, b) = 1$, we say that a, b are *relatively prime* or *coprime*. A list of integers $a_1, \ldots, a_k$ is called *coprime* if $\gcd(a_1, \ldots, a_k) = 1$, and is called mutually coprime if $\gcd(a_i, a_j) = 1$ for all distinct pairs a_i, a_j.
- For instance, since $\gcd(8, 9) = 1$, $8, 9$ are coprime. To see that a list of integers being coprime is distinct from being mutually coprime, consider the list $8, 12, 7$. This list is coprime, since $\gcd(8, 12, 7) = 1$, but is not mutually coprime, because $\gcd(8, 12) = 4$. A list like $6, 11, 17$ is both coprime and mutually coprime.

2. The Euclidean algorithm for calculating gcds

What's the relationship between Euclidean division and gcds? It turns out that Euclidean division is the key tool for a very efficient way of calculating the gcd of two integers. We call this method the Euclidean algorithm, and it is based on the following simple lemma:

Lemma 1. *Let a, b be integers with $b > 0$. Let $a = bq + r$ be the result of Euclidean division, so that $0 \leq r < b$. Then $\gcd(a, b) = \gcd(b, r)$.*

Proof. Suppose $d|a, b$, so $\gcd(a, b)$ is the largest possible d that satisfies these properties. Since $r = a - qb$, we must also have $d|r$. Therefore, $d|a, b \implies d|b, r$. This means that $\gcd(a, b) \leq \gcd(b, r)$. Conversely, if $d|b, r$, then $a = bq + r$ implies that $d|a$. So $d|b, r$ implies that $d|a, b$, so $\gcd(b, r) \leq \gcd(a, b)$. The only way both of these inequalities is true is if $\gcd(a, b) = \gcd(b, r)$. □

Example. For instance, suppose $a = 124, b = 24$. Instead of listing all the divisors of 124 and 24, we use Euclidean division to find $124 = 5 * 24 + 4$, so $q = 5, r = 4$. Therefore $\gcd(124, 24) = \gcd(24, 4) = 4$.

This lemma is really useful, because it allows us to replace the computation of $\gcd(a, b)$ by the computation of $\gcd(b, r)$ for the cost of one Euclidean division. The advantage to this replacement is that we can always select $a > b$ (we'll just assume $a > 0$; if $a < 0$, replace a with $|a|$), so that b, r are smaller numbers than a, b. If we are lucky, r will be really small and we will be able to compute b, r via inspection or brute force.

But even if we aren't lucky, so that b, r are still somewhat large, we can just repeat this process! That is, we can divide b by r with remainder, to get something like $b = q_2 r + r_2$, where $0 \leq r_2 < r$, and then $\gcd(b, r) = \gcd(r, r_2)$. So we can continually replace the calculation of a gcd of a pair of integers with the calculation of the gcd of a pair of smaller integers at the cost of one Euclidean division. This process, where we repeatedly calculate Euclidean divisions to help us calculate a gcd, is called the *Euclidean algorithm*. Let's look at an example.

Example. Compute the gcd of $a = 994$ and $b = 399$ using the Euclidean algorithm.

We begin by doing a Euclidean division on 994 by 399:

$$994 = 399 \cdot 2 + 196.$$

So $q = 2, r = 196$. Since we'll be repeating Euclidean division, let's write $q = q_1 = 2, r_1 = 196$. So we have

$$994 = a = q_1 b + r_1 = 2 \cdot 399 + 196.$$

Remember, right now we know that $\gcd(994, 399) = \gcd(399, 196)$. However, it's not immediately obvious what $\gcd(399, 196)$ is, so let's do a Euclidean division with that pair of numbers:

$$399 = 196 \cdot 2 + 7.$$

We can rewrite this as

$$399 = b = q_2 r_1 + r_2,$$

where $q_2 = 2, r_2 = 7$. So this tells us that $\gcd(399, 196) = \gcd(196, 7)$. It might not be immediately obvious what $\gcd(196, 7)$ is, but a Euclidean division tells us that

$$196 = 7 \cdot 28 + 0,$$

so $7|196$. We can write $q_3 = 28, r_3 = 0$. Therefore, $\gcd(196, 7) = 7$, so $\gcd(994, 399) = 7$.

Altogether, it took us 3 Euclidean divisions to reach our final answer. A Euclidean division requires a fair amount of work, but not much more work than simply testing whether a number divides another number. In particular, notice that this method of calculating gcds is probably faster than trying to list all the factors of the initial two numbers 994 and 399. And if a, b are really large (like tens or hundreds of digits long), then a computer can still calculate gcds really quickly, but will take a long time (unless you are lucky) to calculate all the factors of a, b.

3. 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 terms of a, b, and some other integers. 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

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

Well, this isn't exactly what we want, since we have a r_{n-3}, r_{n-2}, and q_{n-1}. 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

$$r_{n-1} = \gcd(a, b) = r_{n-3} - q_{n-1}(r_{n-4} - q_{n-2} r_{n-3}).$$

This looks more messy (in a way, it is), but it expresses r_{n-1} 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-3}, r_{n-4} to one involving r_{n-4}, r_{n-5}. 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, an example should make things 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*. But 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. □