Lecture 3

Recall that we say an integer d *divides* an integer n if there exists an integer m such that $n = md$. If d divides n we write $d|n$, but if d does not divide n (i.e., there is no integer m such that $n = md$) we write $d \nmid n$.

Given two integers m and n, there may be several *common divisors*, integers d such that $d|m$ and $d|n$. For example, the common divisors of 90 and 150 are

1, 2, 6, 10, 15, and 30

The largest common divisor of m and n is called the *greatest common divisor* of m and n and is denoted $\gcd(m,n)$. For example, $\gcd(90,150) = 30$.

While in principle it is possible to write down all common divisors of two numbers and then select the largest, in practice this is very difficult — even on a very fast computer this process is excruciatingly slow. Despite this, there is a fast algorithm for determining the gcd of two numbers which goes back to the

time of Euclid. Before describing this procedure for computing the gcd, we recall one preliminary fact known as the division algorithm

Theorem (The Division Algorithm)
For any two natural numbers m and n, there exists a pair of unique non-negative integers q and r such that

$$m = nq + r$$

and $0 \leq r < n$.

Pf
First we need to show such a q and r exist, and then we need to show q and r are unique.

Let S be the set of all non-negative integers of the form $m - nx$, where x is a non-negative integer. Notice $S \neq \emptyset$ because we may take $x = 0$ — at the very least, $m \in S$.

Now let y be the smallest element of S — so, $y = m - nx$ for some non-negative integer x. Let $q = x$.

Notice that $y = m - nq$ is less than n. If this was not the case, then

$$m - nq \geq n$$
$$\Rightarrow m - nq - n \geq 0$$
$$\Rightarrow m - n(q+1) \geq 0$$

But $m - nq$ is supposed to be the smallest element of S, and $m - nq - n$ is an even smaller value. This is a contradiction, and so it must be that $m - nq < n$.

Let $r = m - nq$, so $0 \leq r < 0$. Note

$$nq + r = nq + m - nq$$
$$= m$$

Thus we have shown there exists an q and r with $m = nq + r$ and $0 \leq r < 0$. It remains to show q and r are unique, and this is left as an exercise. □

Exercise

Show the q and r guaranteed to exist above are unique. Hint suppose there are two such pairs:

$$m = nq_1 + r_1 \quad \text{and} \quad m = nq_2 + r_2$$

Show $r_1 = r_2$ and then show $q_1 = q_2$.

Now we're ready to describe Euclid's gcd algorithm:

The Euclidean Algorithm

To calculate gcd(m,n), use the division algorithm to write

$$m = nq_1 + r_1$$

If $r_1 = 0$, then n is the gcd.
If $r_1 \neq 0$, apply the division algorithm to n and r_1:

$$n = r_1 q_2 + r_2$$

If $r_2 = 0$, then r_1 is the gcd. If $r_2 \neq 0$, apply the division algorithm to r_1 and r_2:

$$r_1 = r_2 q_3 + r_3$$

Repeat this procedure until there is a zero remainder:

$$\begin{aligned}
m &= nq_1 + r_1 \\
n &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
r_2 &= r_3 q_4 + r_4 \\
&\vdots \\
r_{t-2} &= r_{t-1} q_t + r_t \\
r_{t-1} &= r_t q_{t+1} + 0
\end{aligned}$$

The last non-zero remainder, r_t, is the gcd.

So, why does this algorithm work? Let's first notice that this algorithm always terminates. By the division algorithm we know $0 \leq r_1 < n$; and $0 \leq r_2 < r_1$; and $0 \leq r_3 < r_2$; and so on. We have a strictly decreasing sequence of non-negative sequence of integers: $r_1 > r_2 > r_3 > \dots \geq 0$. Such a sequence must stop, and so the algorithm will always stop.

Now observe $r_t | n$ and $r_t | m$. To see this we work backwards. The last line,

$$r_{t-1} = r_t q_{t-1}$$

tells us $r_t | r_{t-1}$. The line above this may be rewritten as

$$\begin{aligned} r_{t-2} &= r_t q_{t+1} q_t + r_t \\ &= r_t (q_{t+1} q_t + 1) \end{aligned}$$

so $r_t | r_{t-2}$. The line above this,

$$r_{t-3} = r_{t-2} q_{t-1} + r_{t-1}$$

But $r_t | r_{t-2}$ and $r_t | r_{t-1}$, so $r_t | r_{t-3}$ as well. Continuing like this gives that $r_t | r_i$ for $1 \leq i \leq t-1$. Thus, as $n = r_1 q_2 + r_2$ we have $r_t | n$; since $m = n q_1 + r_1$, $r_t | m$.

To show r_t is the <u>greatest</u> common divisor, suppose d is any common divisor of m and n.

Writing

$$r_1 = m - nq_1$$

tells us that $d | r_1$. Writing

$$r_2 = n - r_1 q_2$$

then gives that $d | r_2$. Writing

$$r_3 = r_1 - r_2 q_3$$

gives that $d | r_3$. Continuing like this means $d | r_t$. If $d | r_t$, though, then $d \leq r_t$, and so r_t is in fact the greatest common divisor. (Note too that this means all common divisors of m and n must divide $\gcd(m,n)$.)

Example

Calculate the gcd of 1050 and 325

$$1050 = 325 \cdot 3 + 75$$

$$325 = 75 \cdot 4 + 25$$

$$75 = 25 \cdot 3 + 0$$

So $\gcd(1050, 325) = 25$.

Exercises for Ch. 5: 5.3 and 5.4

Now we apply gcd's to study the following problem: Suppose a and b are integers. Are there any integers x and y such that

$$ax + by = c?$$

If we considered all possible values we could obtain from $ax+by$ by plugging integers in for x and y, we might notice that each one is a multiple of the gcd of a and b. This isn't hard to see: Let $d = \gcd(a,b)$, and say $a = \alpha d$, $b = \beta d$. Then

$$\begin{aligned} ax + by &= \alpha d x + \beta d y \\ &= d(\alpha x + \beta y) \end{aligned}$$

Now, how does this help us solve equations of the form $ax+by=c$? Well, if c is not a multiple of $\gcd(a,b)$, then it's clear there's no solution to the equation.

But if c is a multiple of $\gcd(a,b)$, is there guaranteed to be a solution? Note that if we could solve

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

Then we could solve $ax+by=c$ where c is any multiple of $\gcd(a,b)$.

If $c = m \cdot \gcd(a,b)$ and if x and y solve $ax + by = \gcd$, then mx and my solve $ax + by = c$:

$$\begin{aligned} amx + bmy &= m(ax + by) \\ &= m \cdot \gcd(a,b) \\ &= c \end{aligned}$$

So we really need to figure out if

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

always has a solution or not.

To study this equation, let's again consider the Euclidean algorithm for calculating $\gcd(a,b)$:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ r_2 &= r_3 q_4 + r_4 \\ &\vdots \\ r_{t-3} &= r_{t-2} q_{t-1} + r_{t-1} \\ r_{t-2} &= r_{t-1} q_t + r_t \\ r_{t-1} &= r_t q_{t+1} \end{aligned}$$

where $r_t = \gcd(a,b)$. Now let's solve each equation for the remainder:

$$
\begin{aligned}
r_1 &= a - bq_1 \\
r_2 &= b - r_1 q_2 \\
r_3 &= r_1 - r_2 q_3 \\
r_4 &= r_2 - r_3 q_4 \\
&\vdots \\
r_j &= r_{j-2} - r_{j-1} q_j \\
&\vdots \\
r_{t-1} &= r_{t-3} - r_{t-2} q_{t-1} \\
r_t &= r_{t-2} - r_{t-1} q_t
\end{aligned}
$$

Let's notice the first equation has the form

$$r_1 = ax_1 + by_1 \qquad (x_1 = 1,\ y_1 = -q_1)$$

Plugging this into the second equation gives

$$
\begin{aligned}
r_2 &= b - r_1 q_2 \\
&= b - (ax_1 + by_1) q_2 \\
&= a(-x_1 q_2) + b(1 - y_1 q_2)
\end{aligned}
$$

So we could write

$$r_2 = ax_2 + by_2 \qquad (x_2 = -x_1 q_2,\ y_2 = 1 - y_1 q_2)$$

Plugging these into the third equation yields

$$
\begin{aligned}
r_3 &= r_1 - r_2 q_3 \\
&= ax_1 + by_1 - (ax_2 + by_2) q_3 \\
&= a(x_1 - x_2 q_3) + b(y_1 - y_2 q_3)
\end{aligned}
$$

So we can write

$$r_3 = ax_3 + by_3$$

Continuing like this gives

$$r_t = a x_t + b y_t$$

As $r_t = \gcd(a,b)$, we thus know that

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

always has a solution, and so

$$ax + by = c$$

has a solution if and only if c is a multiple of $\gcd(a,b)$.

In particular, if a and b are relatively prime (also called coprime), meaning $\gcd(a,b) = 1$, then $ax + by = c$ has a solution for every c.

These solutions above are not unique. Suppose $\gcd(a,b) = 1$ and that (x_1, y_1) solve

$$ax + by = 1$$

Note for any $k \in \mathbb{Z}$,

$$ax_1 + by_1 + kab - kab = 1$$
$$\Rightarrow a(x_1 + kb) + b(y_1 - ka) = 1$$

and so we get a new solution (x_2, y_2) to the equation $ax + by = 1$ by setting $x_2 = x_1 + kb$, $y_2 = y_1 - ka$.

Can all the solutions be obtained in this way? Again, suppose (x_1, y_1) is some solution to $ax + by = 1$. Let (x', y') be any other solution.

$$ax_1 + by_1 = 1$$
$$ax' + by' = 1$$

Note

$$ax_1y' + by_1y' = y'$$
$$ax'y_1 + by'y_1 = y_1$$
$$\Rightarrow (ax_1y' + by_1y') - (ax'y_1 + by'y_1) = y' - y_1$$
$$\Rightarrow ax_1y' - ax'y_1 = y' - y_1$$
$$\Rightarrow a(x_1y' - x'y_1) = y' - y_1$$
$$\Rightarrow y' = y_1 + a(x_1y' - x'y_1) = y_1 - a(x'y_1 - x_1y')$$

Similarly

$$ax_1x' + by_1x' = x'$$
$$ax'x_1 + by'x_1 = x_1$$
$$\Rightarrow (ax_1x' + by_1x') - (ax'x_1 + by'x_1) = x' - x_1$$
$$\Rightarrow b(y_1x' - y'x_1) = x' - x_1$$
$$\Rightarrow x' = x_1 + b(y_1x' - y'x_1)$$

Thus $(x', y') = (x_1 + kb, y_1 - ka)$ where $k = x'y_1 - y'x_1$. So, given one solution to $ax + by = 1$, we can easily produce all solutions.

Suppose now that a and b are not relatively prime. Setting $a' = \frac{a}{\gcd(a,b)}$ and $b' = \frac{b}{\gcd(a,b)}$ makes a' and b' relatively prime. Notice if x_1, y_1 solve

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

then they also solve

$$a'x + b'y = 1$$

and vice versa — any solution (x_2, y_2) to $a'x + b'y = 1$ is also a solution to $ax + by = \gcd(a,b)$. But we know how to generate all the solutions to $a'x + b'y = 1$, and so we can generate all the solutions to $ax + by = \gcd(a,b)$.

Exercise

Fill in the gaps above to show that if (x_1, y_1) solve $ax + by = \gcd(a,b)$, then every solution to $ax + by = \gcd(a,b)$ has the form $\left(x_1 + k \cdot \frac{b}{\gcd(a,b)}, y_1 - k\frac{a}{\gcd(a,b)}\right)$ for some $k \in \mathbb{Z}$.