Diophantine Equations and the Euclidean Algorithm

Reading

- Section 5.2
- Section 5.3

Practice Problems

5.2 2-7, 11, 13
Challenge 5.2 (Optional) 14
5.3 1, 2-5, 12, 15
Challenge 5.3 (Optional) 25

Notes

Case of c=gcd

The Euclidean Algorithm allows us to find a solution to the equation

$$ax + by = c$$

where $c = d = \gcd(a, b)$. We can then use this to find a solution for any c divisible by $d = \gcd(a, b)$.

Let us take a look at the first few steps in the Euclidean Algorithm:

$$a = q_1 b + r_1$$

$$b = q_2 r_1 + r_2$$

$$r_1 = q_3 r_2 + r_3$$

We will show that all r_1, r_2, r_3 are explicit linear combinations of a and b. For r_1 this is clear, as:

$$r_1 = a - q_1 b$$

For r_2 we would use this fact, so we would have:

$$r_2 = b - q_2 r_1 = b - q_2(a - q_1 b) = (1 + q_1 q_2)b - q_2 a$$

Similarly we can write r_3 as an explicit compination of a and b by using its equation along with the fact that we already have a way to write r_1 and r_2.

This continues:

> In the Euclidean Division algorithm, each remainder r_n is an *explicit* integer linear combination of a and b.

Since the last step is the $\gcd(a, b)$, we now have a way of writing $\gcd(a, b)$ in an explicit way as an integer linear combination of a and b.

Case of other c's

We already know two things:

- How to find an explicit solution to $ax + by = \gcd(a, b)$
- That the only way that $ax + by = c$ has a solution is if $\gcd(a, b)|c$

We now want to find an explicit solution in the case where $\gcd(a, b)|c$. To do that:

- Write $c = d \gcd(a, b)$, where d is an integer.
- Write $ax + by = \gcd(a, b)$ for some integers x, y.
- Then we have $a(xd) + b(yd) = \gcd(a, b)d = c$ and we have our solution.

So every solution to the $c = \gcd$ case can scale up to a solution of the c case for all those c for which there is a solution in the first place.