Diophantine Equations

Reading

Section 5.1

Practice Problems

5.1 2, 3, 4, 11, 18, 20
Challenge 5.1 (optional) 12, 13, 14, 15
Fun 5.1 1

Notes

Diophantine equations have the form:

$$ax + by = c$$

where all numbers are integers.

We in general are interested in three questions:

1. Does it have any solutions?
2. Can we *find* a solution?
3. How *many* solutions does it have?
4. Under what conditions on a, b, c do those answers change?

Case of 1 variable

Let us start with the simplest case:

$$ax = c$$

1. If $a = 0$, then there is a solution only if $c = 0$, and in that case we have infinitely many solutions.
2. If $a \neq 0$, then there is a solution if and only if a divides c, and in that case there is exactly one solution, the quotient $x = c/a$.

Now let's look at the case of two variables.

Case of 2 variables

First, a necessary condition:

> For $ax + by = c$ to have a solution, we must have that $\gcd(a, b)|c$.

This is easy to see. The interesting thing is that the converse is also true:

> If $\gcd(a, b)|c$, then the equation $ax + by = c$ has a solution.

This is also easy to see.

- Suppose $d = \gcd(a, b)$ and $c = dk$.
- We saw already that the gcd is an integer combination of a, b, so there must be some m, n so that: $d = am + bn$.
- But then $c = dk = amk + bnk$. So we found a solution $x = mk$, $b = nk$.

Here is a special case of this result:

> The equation $ax + by = 1$ has a solution if and only if $\gcd(a, b) = 1$.

This follows as the only way $\gcd(a, b)$ would divide 1 is if it were actually equal to 1.

In the next segment, we will see how the Euclidean Algorithm can help us find a solution.