Finding all Solutions to Diophantine Equations

Reading

- Section 5.4

Practice Problems

5.4 1-4, 10-12, 20, 21, 22
Challenge 5.4 (Optional) 18, 19

Notes

Now that we know how to find one solution, the question naturally arises if we can find more, preferably if we can find them all.

Let us think about this for a minute. Suppose we did have another solution, so:

$$ax_1 + by_1 = c = ax_2 + by_2$$

Then we should be able to say:

$$a(x_1 - x_2) = b(y_2 - y_1)$$

So there is some relation between these solutions and a *common multiple* of a and b. Let's make it more precise:

> If $ax_1 + by_1 = c$ is a solution.
>
> Then every other solution can be obtained as
>
> $$x_2 = x_1 - k_1, \quad y_2 = y_1 + k_2$$
>
> where (k_1, k_2) are such that $ak_1 = bk_2$.

This is easy to see. So the solutions to the diophantine equations are in 1-1 correspondence with these pairs of numbers.

Before we see the main theorem, let us have some definitions and a key result:

> Let $d = \gcd(a, b)$ and $m = lcm(a, b)$. Further let $a'd = a$ and $b'd = b$. Then:
>
> - a', b' are relatively prime.
> - $a'b = ab' = m$.
> - $dm = ab$.

To see this:

- Any common factor of a' and b' would, when multiplied by d, provide a common divisor of a and b. d is the largest such divisor, so that common factor can only be 1. So a', b' must be relatively prime.
- The other two parts say the same thing, so we only need to show one of them. We will show the last one, that $dm = ab$.
  - First, notice that $\frac{ab}{d}$ is an integer that is a common multiple of a and b. Therefore $\frac{ab}{d} \geq m$, so $ab \geq md$.
  - Second, notice that since d is the gcd we can write $d = ax + by$. Multiplying by m gives us: $md = amx + bmy$.
  - Since m is a multiple of b, and also a mupltiple of a, it follows that the two terms in the right hand side are both multiples of ab.
  - So that equation becomes $md = K \times ab$. But this says $md \geq ab$.
  - Hence $md = ab$.

Here is the main theorem that tells us how to find other solutions:

> Suppose $ax_1 + by_1 = c$, $m = lcm(a, b)$ and a', b' are as above.
>
> Then $a(x_1 - kb') + b(y_1 + ka') = c$ for all integers k.
>
> Moreover, all solutions to $ax + by = c$ have this form.

To see this:

- We have already seen that other solutions (x_2, y_2) have to relate to the original (x_1, y_1) via:

$$x_1 - x_2 = k_1$$

$$y_2 - y_1 = k_2$$

  where k_1 and k_2 are such that

$$ak_1 = bk_2$$

- All we need to do now is find all such pairs (k_1, k_2). This will be done in the next theorem.

> Let $d = \gcd(a, b)$ and a', b' are as before.
>
> Then for any pair (k_1, k_2) with $ak_1 = bk_2$ there is an integer k such that
>
> $$k_1 = kb', \quad k_2 = ka'$$

Let us prove this:

- First of all, note that numbers (k_1, k_2) that have this form (kb', ka') do satisfy the needed equation $ak_1 = bk_2$. So this does in fact give us all such pairs of numbers.
- For proving the other direction, suppose $ak_1 = bk_2$.
- Note that a' and b' are relatively prime: $\gcd(a', b') = 1$.
- Since $a = da'$ and $b = db'$, it follows that $a'k_1 = b'k_2$.
- We claim that b' must divide k_1.
  - If we believe that for a minute, we can finish the proof: $k_1 = b'k$
  - Therefore the previous equation becomes $a'b'k = b'k_2$, or $a'k = k_2$.
- The fact that b' must divide k_1 will follow from the following more general statement:

  If $\gcd(a, b) = 1$ and $b|ac$, then it must be the case that $b|c$.

To prove this:

- We start with the equation $ax + by = 1$, which we know must have a solution since a, b are relatively prime.
- We multiply both sides by c. We then get $acx + bcx = c$.
- Since b divides both terms on the left side, it must also divide the right hand side c.