Finding all Solutions to Diophantine Equations

Reading

- Section 5.4

Practice Problems

5.4 ~

Challenge 5.4 (Optional)

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.

Before proceeding, we will need a lemma:

> The $lcm(a, b)$ divides all other common multiples of a, b.

This is actually easy to see, and once again boils down to Euclidean Division:

- Say $m = lcm(a, b)$ and M is another common multiple.
- Divide m into M: $M = qm + r$, $0 \leq r < m$.
- Then $m - r$ is a common multiple, and $0 < m - r \leq m$.
- It must be the case that $r = 0$. So $m|M$.

Let us return to our main topic. Here is a theorem that tells us how to find other solutions:

> Suppose $ax_1 + by_1 = c$, $m = lcm(a, b)$ and d_1, d_2 are such that $ad_1 = bd_2 = m$.
> Then $a(x_1 - kd_1) + b(y_1 + kd_2) = c$ for all integers k.
> Moreover, all solutions to $ax + by = c$ have this form.

We have already seen that other solutions (x_2, y_2) have to relate to the original $(x1, y1)$ 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).

Let $d = \gcd(a, b)$ and a', b' are such that

$$a = da', \quad b = db'$$

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.