3 Diophantine equations

Diophantine equations are usual equations but we are only interested in integer solutions.

Example 39. Find a solution to the diophantine equation $15x + 28y = 1$.

Solution. Note that $\gcd(15, 28) = 1$. Hence, we can use the Euclidean algorithm to find a solution to $15x + 28y = 1$. Indeed, as in the previous example:

$$\underbrace{\gcd(15, 28)}_{28 = 1\cdot 15 + 13} = \underbrace{\gcd(13, 15)}_{15 = 1\cdot 13 + 2} = \underbrace{\gcd(2, 13)}_{13 = 6\cdot 2 + 1} = \gcd(1, 2) = 1$$

Trace back: $1 = 13 - 6\cdot \underbrace{2}_{2 = 15 - 13} = -6\cdot 15 + 7\cdot \underbrace{13}_{13 = 28 - 15} = 7\cdot 28 - 13\cdot 15$

In other words, we have found the solution $x = -13$ and $y = 7$.

Are there other solutions? **Yes!** For instance, $22\cdot 28 - 41\cdot 15 = 1$ or $37\cdot 28 - 69\cdot 15 = 1$.

What is the **general solution**?

Solution. Note that, $x = 28t$, $y = -15t$ is an obvious solution (for any integer t) to the **homogeneous equation** $15x + 28y = 0$. We can add these solutions to any **particular solution** to $15x + 28y = 1$ to obtain the general solution to $15x + 28y = 1$. Here, the general solution to

Example 40. Find the general solution to the diophantine equation $6x + 15y = 10$.

Solution. This equation has no (integer) solution because the left-hand side is divisible by $\gcd(6, 15) = 3$ but the right-hand side is not divisible by 3.

Lemma 41. Let $a, b \in \mathbb{Z}$ (not both zero). The diophantine equation $ax + by = c$ has a solution if and only if c is a multiple of $\gcd(a, b)$.

The fact that there is a solution if c is a multiple of $\gcd(a, b)$ is a consequence of Bezout's identity.

We can therefore focus on the diophantine equation $ax + by = c$ with $\gcd(a, b) = 1$.

(Just divide both sides by $\gcd(a, b)$.)

Theorem 42. The diophantine equation $ax + by = c$ with $\gcd(a, b) = 1$ has the general solution

$$x = x_0 + bt, \quad y = y_0 - at,$$

where $t \in \mathbb{Z}$ is a parameter, and x_0, y_0 is any particular solution.

How to find a particular solution? Since $\gcd(a, b) = 1$, we can find integers x_1, y_1 such that $ax_1 + by_1 = 1$ (this is Bezout's identity). Multiply both sides with c, to see that we can take $x_0 = cx_1$ and $y_0 = cy_1$.

Proof. First, let us consider the case of any real solutions. The general solution of $ax + by = c$ (which describes a line!) can be described as

$$x = x_0 + bt, \quad y = y_0 - at.$$

Since $\gcd(a, b) = 1$, this solution will be integers if and only if t is an integer. □

Example 43. Determine all integer solutions to the diophantine equation $56x + 72y = 40$.

Solution. Since $\gcd(56, 72) = \gcd(16, 56) = \gcd(8, 16) = 8$, this equation simplifies to $7x + 9y = 5$.

Since $\gcd(7, 9) = 1$, we can find $x, y \in \mathbb{Z}$ (for instance using the Euclidean algorithm) such that $7x + 9y = 1$. Indeed, $x = 4$ and $y = -3$ work. Multiplying this with 5, we find that a particular solution to is $7x + 9y = 5$ is provided by $x_0 = 4\cdot 5 = 20$, $y_0 = -3\cdot 5 = -15$.

In conclusion, the general solution is $x = 20 + 9t$, $y = -15 - 7t$.

Armin Straub
straub@southalabama.edu