Linear diophantine equations

Marlon Mendes

1 Problem statement

Given integers a, b, c find integers x, y such that $ax + by = c$.

2 Existence of a solution

Let $d = gcd(a, b)$ be the greatest common divisor between integers a, b. We know that $a = dr$, $b = ds$, so $ax + by = drx + dsy = c$. That last equation states that c must be a multiple of d, otherwise there's no solution, because:

$$ax + by = drx + dsy = c$$
$$d(rx + sy) = c$$

Now we have to prove that if d divides c, than there is a solution. Using Bézout's Lemma, we can write $d = ax_0 + by_0$. Also, d divides c, so $c = dt$.

$$ax + by = c$$
$$ax + by = dt$$
$$ax + by = (ax_0 + by_0)t$$
$$ax + by = ax_0t + by_0t$$
$$ax + by = a(x_0t) + b(y_0t)$$

So we found a solution where $x = x_0t$ and $y = y_0t$.

3 Zero or infinity solutions

We proved that if $gcd(a, b) \nmid c$ there's no solution, however if $gcd(a, b) \mid c$ then we showed how to find one solution. The next theorem states that if we find any solution, we can build infinitely many others from that one.

Let (x_0, y_0) be the solution we found, we're interested in finding another solution (x', y').

$$
\begin{aligned}
ax_0 + by_0 &= c \\
ax_0 + by_0 &= ax' + by' \\
a(x' - x_0) &= b(y_0 - y')
\end{aligned}
$$

We can divide both a, b by their gcd $d = gcd(a, b)$, making $a = dr$ and $b = ds$, so:

$$
\begin{aligned}
a(x' - x_0) &= b(y_0 - y') \\
dr(x' - x_0) &= ds(y_0 - y') \\
r(x' - x_0) &= s(y_0 - y')
\end{aligned}
$$

From now we know that $r \mid (y_0 - y')$ because $gcd(r, s) = 1$, so there exists some $t : (y_0 - y') = rt$. Substituting, we obtain:

$$
\begin{aligned}
r(x' - x_0) &= srt \\
x' - x_0 &= st \\
x' &= x_0 + st \\
(y_0 - y') &= rt \\
y' &= y_0 - rt
\end{aligned}
$$

Note that $r = \left(\frac{a}{d}\right), s = \left(\frac{b}{d}\right)$, so:

$$
\begin{aligned}
x' &= x_0 + \left(\frac{b}{d}\right) t \\
y' &= y_0 - \left(\frac{a}{d}\right) t
\end{aligned}
$$

We can manipulate both of the above equations to show that satisfy the original diophantine equation regardless of the choice of the integer t:

$$
\begin{aligned}
ax' + by' &= a\left[x_0 + \left(\frac{b}{d}\right) t\right] + b\left[y_0 - \left(\frac{a}{d}\right) t\right] \\
&= ax_0 + a\left(\frac{b}{d}\right) t + by_0 - b\left(\frac{a}{d}\right) t
\end{aligned}
$$

$$\begin{aligned} &= ax_0 + by_0 + a\left(\frac{b}{d}\right)t - b\left(\frac{a}{d}\right)t \\ &= c + \left(\frac{ab}{d} - \frac{ab}{d}\right)t \\ &= c + 0t \\ &= c \end{aligned}$$

Which proves that there infinitely many choices for t, and each choice of t gives one new solution to the diophantine equation.

4 Conclusion

Given integers a, b, c we can find integers x, y such that $ax + by = c$ if and only if $d = gcd(a, b) \mid c$. If $d \mid c$ we can find one solution using Bézout's Lemma.

Let $d = ax_0 + by_0$ and $c = dt, t = \left(\frac{c}{d}\right)$.

$$\begin{aligned} ax + by &= c \\ &= dt \\ &= (ax_0 + by_0)t \\ ax + by &= a(x_0 t) + b(y_0 t) \end{aligned}$$

So, $x = (x_0 t)$ and $y = (y_0 t)$ is a valid solution. We can now build other solutions using the following equations:

$$x' = x_0 + \left(\frac{b}{d}\right)v$$

$$y' = y_0 - \left(\frac{a}{d}\right)v$$

Where v is any arbitrary integer.

5 References

- Elementary Number Theory, David M. Burton.
- github.com/edsomjr/TEP/blob/master/Matematica/text/Divisibilidade.md