The Proof of the Formula for the General Solution of the Diophantine Equation

$$mx + ny = c$$

Theorem 5. Let $m, n, c \in \mathbb{Z}$ be non-zero integers and suppose that

$$g := \gcd(m, n) \mid c.$$

Then the general integer solution (x, y) of the equation

(1) $$mx + ny = c$$

is given by the formula

(2) $$\left.\begin{aligned} x &= \tfrac{c}{g}x_0 + \tfrac{n}{g}t \\ y &= \tfrac{c}{g}y_0 - \tfrac{m}{g}t \end{aligned}\right\} \text{ where } t \in \mathbb{Z},$$

and $x_0, y_0 \in \mathbb{Z}$ are (any) integers satisfying the equation

(3) $$mx_0 + ny_0 = g.$$

Proof of the Theorem

The theorem consists of two separate assertions:

1) Every (x, y) defined by (2) is a solution of (1).

2) Every solution (x, y) of (1) is of the form (2).

Proof of 1): Check that (2) is a solution of equation (1).

Proof of 2): Suppose that (x, y) is an integer solution of (1); i.e. we have

$$mx + ny = c. \tag{4}$$

Now since (x_0, y_0) is a solution of (3), it follows that $(x', y') := \frac{c}{g}(x_0, y_0)$ is also a solution of (1):

$$mx' + ny' = m\frac{c}{g}x_0 + n\frac{c}{g}y_0 = c. \tag{5}$$

Thus, subtracting (5) from (4) yields

$$mx'' + ny'' = m(x - x') + n(y - y') = 0,$$

where we have put $x'' = x - x'$ and $y'' = y - y'$. Dividing this equation by g gives

$$\frac{m}{g}x'' = -\frac{n}{g}y''. \tag{6}$$

Thus $\frac{n}{g}|\frac{m}{g}x''$, and so by Euclid's Lemma,

$$\frac{n}{g}|x'' \quad \text{or} \quad x'' = \frac{n}{g}t, \text{ for some } t \in \mathbb{Z}. \tag{7}$$