Math 250: Number Theory and Mathematical Reasoning
Valente

Section 2.1: Linear Diophantine Equations

Definition 2.1 Let a, b, and c be integers with a and b non-zero. Then the equation $aX + bY = c$ is called a linear diophantine equation .

Theorem 2.2 Let $aX + bY = c$ be a linear diophantine equation. This equation will have a solution if and only if $(a, b)|c$.

Further, let x_0 and y_0 denote one solution pair, $a = (a, b)a'$, and $b = (a, b)b'$. With this, the integers x and y form a solution to the equation if and only if

$$x = x_0 + b't \quad \text{and} \quad y = y_0 - a't$$

for some integer t.

NB. Using Theorem 2.2 together with the Euclidean Algorithm, one can find a complete set of solutions to any linear diophantine equation.