Diophantine equations.

A Diophantine equation is a linear equation with integer coefficients requiring integer solutions.

The Diophantine equation \( ax + by = c \) has an integer solution if and only if \( \gcd(a, b) \) divides \( c \).

To find one solution to the Diophantine equation \( ax + by = c \) follow the steps below.

1. First check that \( \gcd(a, b) \mid c \), to make sure that this equation has in fact integer solutions.

2. Divide the equation by \( \gcd(a, b) \) to obtain \( \frac{a}{\gcd(a, b)} x + \frac{b}{\gcd(a, b)} y = \frac{c}{\gcd(a, b)} \). We will just write \( a' = \frac{a}{\gcd(a, b)}, b' = \frac{b}{\gcd(a, b)}, c' = \frac{c}{\gcd(a, b)} \). So our new equation is \( a'x + b'y = c' \) where \( \gcd(a', b') = 1 \).

Note that any solution to \( ax + by = c \) is also a solution to \( a'x + b'y = c' \) and vice versa.

3. Use the Euclidean algorithm to write the \( \gcd(a', b') = 1 \) as a linear combination of \( a' \) and \( b' \). Say \( a'x_0 + b'y_0 = 1 \).

4. Finally multiply this last expression by \( c' \) to get

\[
a' (c' x_0) + b' (c' y_0) = c'
\]

then \( x = c' x_0 \) and \( y = c' y_0 \) is your solution.

To get all solutions to the Diophantine equation \( ax + by = c \) we actually find all solutions to the equation \( a'x + b'y = c' \) as follows.

5. Find one solution (using the four steps above or guessing it). Say \( x_1 \) and \( y_1 \).

6. Then for any integer \( k \) we have

\[
a' (x_1 + b'k) + b' (y_1 - a'k) = c'.
\]

Therefore all solutions to the equation \( a'x + b'y = c' \) have the form

\[
x = x_1 + b'k, \\
y = y_1 - a'k,
\]

where \( k \) is any integer number.