Extended Euclidean Algorithm

Prove Bézout's identity.
Bézout's Identity: Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that $ax + by = d$. Moreover, the integers of the form $az + bt$ are exactly the multiples of d.

This theorem can be reworded as: there exist integers x and y such that $ax + by = d$, where d is the greatest common divisor of a and b. Then, we prove from left to right.

Let $a, b \in \mathbb{Z}$. Define $S = \{ax + by \mid x, y \in \mathbb{Z} \text{ and } ax + by > 0\}$.

S is non-empty. If $a < 0$, it contains $-a = a * -1 + b * 0$. Otherwise, it contains $a = a * 1 + b * 0$.

The set must have a minimum element; let d (of the form $as + bt$) be this element.

The division of a by d can be represented as $a = dq + r$, where $q \in \mathbb{Z}$ and $0 \leq r < d$. This means $r = a - dq$, which can be rewritten as $r = a - (as + bt)q = a - asq + btq = a(1 - sq) + btq$. Thus, r also takes the form $ax + by$. Therefore, $r \in \{0\} \cup S$.

d is the minimum element of S. Therefore, there is no element in S that is less than d.
$r < d \Rightarrow r \notin S \Rightarrow r \in \{0\} \Rightarrow r = 0$.

Thus, $a = dq$, so d is a divisor of a. A similar line of reasoning can be used to show that d is a divisor of b, so d is a common divisor of a and b.

Let c be a common divisor of a and b, so $a = cu$ and $b = cv$. $d = as + bt = cus + cvt = c(us + vt)$. Thus, c is a divisor of d. Because $d > 0$, this means $c \leq d$. Thus, d is the greatest common divisor of a and b.

Because d is a common divisor of a and b, $a = dq$ and $b = dp$. Thus, $az + bt = dqz + dpt = d(qz + pt)$, so every integer of the form $az + bt$ is a multiple of d.

Explain why there can be no integer solutions to $ax + by = 1$ if a and b are not relatively prime.

If a and b are not relatively prime, then $gcd(a, b) = d$ where $d > 1$. Because $d > 1$, there is no integer n for which $dn = 1$. Every integer of the form $ax + by$ is a multiple of d, but no multiple of d can be 1, so $ax + by$ can never equal 1.

Show that if a and b are relatively prime, then the equation $ax + by = c$ has an integer pair solution for any c.

If a and b are relatively prime, then $gcd(a, b) = 1$, so there exist integers x and y such that $ax + by = 1$. Thus, $acx + bcy = c$. c is an integer, so cx and cy are also integers and form the integer pair solution.

Write a Python program which takes three inputs: a, b, and c. It should solve the equation $ax + by = c$ if it has integer solutions; if $ax + by = c$ has no integer pair solution, your program should return "no solution". Use your program to solve the following equations.

1. $1402x + 1969y = 1 \rightarrow 1402 * 889 + 1969 * -633 = 1 \rightarrow x = 889, y = -633$
2. $994x + 399y = 8 \rightarrow 994 * -2 + 399 * 5 = 7 \rightarrow x = -2, y = 5$
3. $60x + 18y = 97 \rightarrow$ no solution

These tests leaves out situations where c is a multiple of $\gcd(a, b)$. However, the program still works: $1402x + 1969y = 3$ returns $x = 2667$, $y = -1899$.