Computational Number Theory
Programming HW 2

Due Date: 07/09/2022

1. **Arithmetic in $\mathbb{Z}_n$** Write functions for the following; for (b), (c), (d), you may reuse code/invoke functions from your first assignment.

   (a) Input: $a \in \mathbb{Z}_n$ and $b \in \mathbb{N}$; output: $a^b \in \mathbb{Z}_n$.

   (b) Input: $a \in \mathbb{Z}_n$; output: True if $a \in \mathbb{Z}_n^*$ and False otherwise.

   (c) Input: $a \in \mathbb{Z}_n$; output: $b \in \mathbb{Z}_n$ such that $ab = gcd(a, n)$. This can be thought of as a generalized inverse: when $a \in \mathbb{Z}_n^*$, the value returned is a^{-1}.

   (d) Input: $a \in \mathbb{Z}_n$; output: if $a \in \mathbb{Z}_n^*$, then $b \in \mathbb{Z}_n$ such that $ab = 1$; else output an error message.

2. **Chinese Remainder Theorem** Write a function that accepts four integers a, b, m, n with $m, n > 0$ and returns the least positive integer x such that x simultaneously satisfies: $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. If no solution exists, you may output an error message. You may reuse code/invoke functions from your first assignment.