CPSC 418/MATH 318 Practice Problems

Extended Euclidean Algorithm and Modular Inverses

Recall that the *Euclidean Algorithm* finds the greatest common divisor (gcd) of two integers, and the *Extended Euclidean Algorithm* produces a way to write this gcd as an integer linear combination of the two integers.

Fix a positive integer m. Recall that an integer a has a *inverse* modulo m, i.e. there exists an integer x such that $ax \equiv 1 \pmod{m}$, if and only if $\gcd(a, m) = 1$. or equivalently, $a \in \mathbb{Z}_m^*$. In this case, the extended Euclidean algorithm produces an identity of the form $ax + my = 1$, and x is a modular inverse of $a \pmod{m}$.

1. Compute $d = \gcd(a, b)$ and find integers x, y such that $ax + by = d$ for the following values of a and b:
   (a) $a = 36$, $b = 15$.
   (b) $a = 6$, $b = 70$.
   (c) $a = -356$, $b = 13$.
   (d) $a = 0$, b an arbitrary integer.
   (e) $a = 1$, b an arbitrary integer.

2. For which of the following integers a, m does a have an inverse modulo m?
   (a) $a = 637$, $m = 14$.
   (b) $a = 101$, $m = 7$.
   (c) $a = -356$, $b = 13$.

3. For those pairs (a, m) in Problem 2 for which a has an inverse modulo m, find such a modular inverse.

4. (a) Let $a, b \in \mathbb{Z}$, not both zero, such that $\gcd(a, b) = 1$.Then there exist integers x, y with $ax + by = 1$. Prove that for any $c \in \mathbb{Z}$, there exist integers X, Y such that $aX + bY = c$, and explain how to obtain X and Y from x and y.
   (b) Let m be a positive integer and $a \in \mathbb{Z}_m^*$. Use part (a) to prove that for every $c \in \mathbb{Z}$, there exists an integer $X \in \mathbb{Z}_n^*$ such that $aX \equiv c \pmod{m}$, and explain how to obtain X from the inverse of a modulo m.
   (c) Solve the congruence $101X \equiv 4 \pmod{7}$.