1 Modular Potpourri

Note 6

Prove or disprove the following statements:

(a) There exists some $x \in \mathbb{Z}$ such that $x \equiv 3 \pmod{16}$ and $x \equiv 4 \pmod{6}$.

(b) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{12}$.

(c) $2x \equiv 4 \pmod{12} \iff x \equiv 2 \pmod{6}$.

2 Modular Inverses

Note 6

Recall the definition of inverses from lecture: let $a, m \in \mathbb{Z}$ and $m > 0$; if $x \in \mathbb{Z}$ satisfies $ax \equiv 1 \pmod{m}$, then we say x is an **inverse of a modulo m**.

Now, we will investigate the existence and uniqueness of inverses.

(a) Is 3 an inverse of 5 modulo 10?

(b) Is 3 an inverse of 5 modulo 14?

(c) Is each $3 + 14n$ where $n \in \mathbb{Z}$ an inverse of 5 modulo 14?

(d) Does 4 have inverse modulo 8?

(e) Suppose $x, x' \in \mathbb{Z}$ are both inverses of a modulo m. Is it possible that $x \not\equiv x' \pmod{m}$?

3 Modular Practice

(a) Calculate $72^{316} \pmod{7}$.

(b) Solve the following system for x:

$$\begin{aligned} 3x &\equiv 4 + y && \pmod{5} \\ 2(x-1) &\equiv 2y && \pmod{5} \end{aligned}$$

(c) Let n, x be positive integers. Prove that x has a multiplicative inverse modulo n if and only if $\gcd(n,x) = 1$. (Hint: Remember an iff needs to be proven both directions. The gcd cannot be 0 or negative.)