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

Solution:

(a) Impossible.

Suppose there exists an x satisfying both equations.

From $x \equiv 3 \pmod{16}$, we have $x = 3 + 16k$ for some integer k. This implies $x \equiv 1 \pmod{2}$.

From $x \equiv 4 \pmod{6}$, we have $x = 4 + 6l$ for some integer l. This implies $x \equiv 0 \pmod{2}$.

Now we have $x \equiv 1 \pmod{2}$ and $x \equiv 0 \pmod{2}$. Contradiction.

(b) False, consider $x \equiv 8 \pmod{12}$.

The reason we can't eliminate the 2 in the first equation to get the second equation is because 2 does not have a multiplicative inverse modulo 12, as 2 and 12 are not coprime.

(c) True. We can write $2x \equiv 4 \pmod{12}$ as $2x = 4 + 12k$ for some $k \in \mathbb{Z}$. Dividing by 2, we have $x = 2 + 6k$ for the same $k \in \mathbb{Z}$. This is equivalent to saying $x \equiv 2 \pmod{6}$.

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 $x \not\equiv x' \pmod{m}$?

Solution:

(a) No, because $3 \cdot 5 = 15 \equiv 5 \pmod{10}$.

(b) Yes, because $3 \cdot 5 = 15 \equiv 1 \pmod{14}$.

(c) Yes, because $(3 + 14n) \cdot 5 = 15 + 14 \cdot 5n \equiv 15 \equiv 1 \pmod{14}$.

(d) No. For contradiction, assume $x \in \mathbb{Z}$ is an inverse of 4 modulo 8. Then $4x \equiv 1 \pmod{8}$. Then $8 \mid 4x - 1$, which is impossible.

(e) No. We have $xa \equiv x'a \equiv 1 \pmod{m}$. So

$$xa - x'a = a(x - x') \equiv 0 \pmod{m}.$$

Multiply both sides by x, we get

$$\begin{aligned} xa(x - x') &\equiv 0 \cdot x \pmod{m} \\ \implies x - x' &\equiv 0 \pmod{m}. \\ \implies x &\equiv x' \pmod{m} \end{aligned}$$

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.)

Solution:

(a) Notice that $72 \equiv 2 \pmod{7}$. Also notice that $2^3 = 8 \equiv 1 \pmod{7}$. Then

$$72^{316} \equiv 2^{316} \equiv 2 \cdot 2^{315} \equiv 2 \cdot (2^3)^{105} \equiv 2 \cdot 1^{105} \equiv 2 \pmod{7}$$

(b) Solving the system we get $2x \equiv 3 \pmod 5$. At this point, the student must remember that he/she cannot divide by 2 and must find the inverse. We can multiply both sides by $2^{-1} \pmod 5$. Since $2 * 3 \equiv 1 \pmod 5$, we multiply 3 on both sides of the second equation to get $x - 1 \equiv 6y \pmod 5$, which can be simplified to $x - 1 \equiv y \pmod 5$. (Note that division by 2 in normal arithmetic is the same as multiplying by 2^{-1} in modular arithmetic.) Our final solution is $x = 4$.

(c) If x has a multiplicative inverse modulo n, then $\gcd(n, x) = 1$.

Given that x has a multiplicative inverse modulo n, we can proceed as follows:

Assume for the sake of contradiction that the gcd, d, is greater than 1.

$$
\begin{aligned}
xa &\equiv 1 \pmod n \\
xa &= bn + 1 \\
\frac{xa}{d} &= \frac{bn + 1}{d} \\
\frac{xa}{d} &= \frac{bn}{d} + \frac{1}{d}
\end{aligned}
$$

We've reached a contradiction because xa/d and bn/d must both be integers, however, $1/d$ is not. Therefore we've reached a contradiction, and because the gcd cannot be 0 or negative, it must be 1.

If $\gcd(n, x) = 1$, then x has a multiplicative inverse modulo n. The proof is as follows:

We know $\exists\, a, b \in \mathbb{Z}$ such that

$$
\begin{aligned}
an + bx &= 1, \\
bx &\equiv 1 \pmod n.
\end{aligned}
$$

Thus, x has a multiplicative inverse b.