# A Book of Abstract Algebra | (2nd Edition)

Chapter 23, Problem 1EF

Bookmark

Show all steps: ON

## Problem

Prove part:

If gcd ($a$, $n$) = 1, the solution modulo $n$ of $ax \equiv b$ (mod $n$) is $x \equiv a^{\phi(n)-1}b$ (mod $n$).

## Step-by-step solution

**Step 1** of 3

Consider any two relatively prime numbers $a$ and $n$, that is,

$\gcd(a, n) = 1$.

Objective is to prove that solution modulo $n$ of $ax \equiv b(\bmod n)$ is

$x \equiv a^{\phi(n)-1}b(\bmod n)$.

The $x \equiv a^{\phi(n)-1}b(\bmod n)$ will be a solution of congruence $ax \equiv b(\bmod n)$, if it satisfies this congruence relation.

Comment

**Step 2** of 3

To check this, assume that this $x$ is solution, then

$$\begin{aligned} ax &= a\left(a^{\phi(n)-1}b\right) \\ &= a^{\phi(n)}b. \end{aligned}$$

Since $\gcd(a, n) = 1$, then by Euler's theorem,

$a^{\phi(n)} \equiv 1(\bmod n)$.

Therefore,

$$\begin{aligned} ax &= a^{\phi(n)}b \\ &\equiv 1 \cdot b \pmod{n} \\ &\equiv b \pmod{n}. \end{aligned}$$

Comment

**Step 3** of 3

Hence, $x \equiv a^{\phi(n)-1}b \pmod{n}$ will be the solution of $ax \equiv b \pmod{n}$.

Comment