# WEB3CLUBS FOUNDATION LIMITED

---

Course Instructor: DR. Cyprian Omukhwaya Sakwa
PHONE: +254723584205 Email: cypriansakwa@gmail.com

## Foundational Mathematics for Web3 Builders

**Lecture 14**

**May 21, 2024**

# 1.7 Linear Congruence

Consider the linear congruence

$$ax \equiv b(\mathrm{mod}\, m) \tag{1}$$

where $a, b, m$ are integers with $m > 0$.

By a solution of equation (1) we mean an integer $x = x_1$ for which $m \mid (ax_1 - b)$.

Note that if $x_1$ is a solution of equation (1) then $x_1 + km$ for $k \in \mathbb{Z}$ is another solution of equation (1).

**Note:** An equation $ax \equiv b(\mathrm{mod}\, m)$ has a solution if $\gcd(a, m)$ divides $b$. In this case, if $d = \gcd(a, m)$ and $d \mid b$ then the congruence equation has $d$ solutions. This congruence equation has no solution if $d \nmid b$.

**Example 32**

Solve the following linear congruence equations.

a) $5x \equiv 3 (\mod 8)$

b) $6x \equiv 4 (\mod 9)$

c) $6x \equiv 8 (\mod 10)$

d) $3x + 2 \equiv 8 (\mod 10)$

e) $6x - 3 \equiv 5 + 2x (\mod 10)$

f) $\frac{2}{3}x \equiv 4 (\mod 7)$

**Solution**

Since the moduli is relatively small, we will find solutions by testing. Later on we will see how to use extended Euclid's Algorithm to find solutions to such congruence equations.

# 1.8 Solution of Linear Congruences Using Euclid's Algorithm

**Example 33**

Find the least positive integer $x$ for which

$$53x \equiv 1 \bmod 93$$

**Solution**

First, $\gcd(93, 53) = 1$ and $1$ divides $1$ and the equation has $1$ solution.

By Euclid's algorithm algorithm we have

$$93 = 53(1) + 40$$

$$53 = 40(1) + 13$$

$$40 = 13(3) + 1$$

$$13 = 1(13) + 0$$

## Solution (conti...)

Now solve for the $\gcd$.

$$1 = 40 - 13(3) = 40 - [53 - 40(1)](3) = 40 - 53(3) + 40(3)$$

$$= -53(3) + 40(4) = -53(3) + [93 - 53(1)](4) = -53(3) + 93(4) - 53($$

$$= 93(4) + 53(-7)$$

Thus $1 = 93(4) + 53(-7)$ and therefore modulo $93$ gives $53(-7) \equiv 1 \bmod 93$.

Thus $x = -7$ is a solution. We could also give this answer as $x = 86$ since $86$ is the least positive number congruent to $-7 \bmod 93$. So, $x = 86$ is the required answer.

**Example 34**

Find integer $x$ for which $7x \equiv 13 \bmod 19$

**Solution**

$\gcd(19, 7) = 1$ and so equation has $1$ solution.

By Euclid's algorithm algorithm we have

$$19 = 7(2) + 5$$

$$7 = 5(1) + 2$$

$$5 = 2(2) + 1$$

$$2 = 1(2) + 0$$

We solve for $\gcd$

$$1 = 5 - 2(2) = 5 - [7 - 5(1)](2) = 5 - 7(2) + 5(2) = -7(2) + 5(3)$$

$$= -7(2) + [19 - 7(2)](3) = -7(2) + 19(3) - 7(6)$$

$$= 19(3) + 7(-8)$$

That is, $1 = 19(3) + 7(-8)$.

**Solution (conti...)**

Since we require $13 = 19(n) + 7(x)$ for some $n \in \mathbb{Z}$, we multiply $1 = 19(3) + 7(-8)$ by $13$ to get

$13 = 19(3 \times 13) + 7(-8 \times 13)$ which we compute $\bmod 19$ to get

$13 = 19(1) + 7(10)$

Thus, $x = 10$

**Example 35**

Solve $4043n \equiv 27 (\bmod\, 166361)$

**Solution**

Here, $\gcd(166361, 4043) = 13$ but $13 \nmid 27$. Hence the congruence has no solution.