WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 13

May 20, 2024

1.5 Modular arithmetic

There are many applications of modular arithmetic in computer science. Some of the applications include the construction of pseudo-random number generators, hashing Functions and Cryptology.

Definition 8

Let m be a positive integer. We say that the integers a and b are congruent modulo m (or $\mathrm{mod} m$) if $m \mid (a-b)$ and we write $a \equiv b (\mathrm{mod}\ m)$. If $m \nmid (a-b)$, then we write $a \not\equiv b (\mathrm{mod}\ m)$.

The relation $a \equiv b (\mathrm{mod}\ m)$ is a congruence relation, or simply, a congruence. The number m is called the modulus of the congruence. Two numbers are are said to be incongruent with respect to a given modulus m if they are not congruent with respect to that modulus m.

Example 22

a) $10 \equiv 4 \pmod 3$ since $3 \mid (10 - 4)$

b) $10 \equiv 1 \pmod 3$ since $3 \mid (10 - 1)$

c) $15 \not\equiv -5 \pmod 3$ since $3 \nmid (15 - -5)$ or $3 \nmid 20$

d) $22 \not\equiv 4 \pmod 5$ since $5 \nmid 18$

Given $a, b, m \in \mathbb{Z}$ with $m > 0$, we also say that b is congruent to $a \bmod m$ if $b = a + mt$ for some integer t.

Example 23

Which numbers are congruent to $3 \bmod 7$?

Solution

From above, $a \equiv 3 \bmod 7$ if $a = 3 + 7t$ for some integer t. Taking $t = \cdots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \cdots$ we get
$\{\cdots, -25, -18, -11, -4, 3, 10, 17, 24, 31, \cdots\}$
Notice that all these numbers leave a remainder of 3 on division by 7.

Definition 9

Given integers a and m, with $m > 0$, $a \bmod m$ is defined to be the remainder when a is divided by m.

Example 24

a) $14 \bmod 5 = 4$

b) $139 \bmod 10 = 9$

c) $-14 \bmod 5 = 1$

d) $1148 \bmod 5 = 3$

e) $-4 \bmod 9 = 5$

f) $(17 + 23) \bmod 5 \equiv 2 + 3 = 0$

g) $(18 + 23) \bmod 4 \equiv 2 + 3 = 1$

h) $(19 \times 288) \bmod 5 \equiv 4 \times 3 \equiv 12 \bmod 5 = 2$

i) $(11^2 \times 13^3) \bmod 4 \equiv (3^2 \times 1^3) \bmod 4 \equiv 1 \times 1 = 1$

Example 25

Calculate the remainder of 35^{2024} on division by 17.

Solution

First reduce $35 \mod 17 = 1 \mod 17$.

Thus $35^{2024} \mod 17 = 1^{2024} \mod 17 = 1$.

So when 35^{2024} is divided by 17 the remainder is 1.

Example 26

Find $27^{1001} \mod 14$

Solution

First, $27 \mod 14 \equiv 13 \mod 14 \equiv -1 \mod 14$.

Therefore, $27^{1001} = (-1)^{1001} = -1 \mod 14$

Since $-1 \equiv 13 \mod 14$, the remainder is 13.

Example 32

Solve the following linear congruence equations.

a) $5x \equiv 3 \pmod{8}$

b) $6x \equiv 4 \pmod{9}$

c) $6x \equiv 8 \pmod{10}$

d) $3x + 2 \equiv 8 \pmod{10}$

e) $6x - 3 \equiv 5 + 2x \pmod{10}$

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

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.