WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 27

June 20, 2024

Primitive Roots

- Primitive roots modulo n are frequently used in cryptography, particularly in the Diffie-Hellman key exchange protocol, which is commonly used to securely transmit cryptographic keys over a public channel. This protocol's security is based on the complexity of the discrete logarithm problem, which is itself based on primitive root properties.
- Primitive roots are also employed in digital signature algorithms and public key cryptosystems, including the Digital Signature Algorithm (DSA) and the ElGamal encryption technique. Both rely on the mathematical properties of primitive roots to provide security and functionality.

- Primitive roots have well-defined mathematical properties, which are used to create strong cryptographic protocols. Understanding these properties enables cryptographers to develop and analyze secure systems.

Definition 1

Let $a > 1$ and $\gcd(a, n) = 1$. The smallest positive integer g such that $a^g \equiv 1 \bmod n$ is known as the order of a modulo n, denoted by $|a| = g$. If $|a| = \phi(n)$, a becomes a primitive root modulo n.

- Definition 1 says that if a is a unit modulo n and if the order of a is $\phi(n)$ then a is a primitive root modulo n.

No. of primitive $\phi(\phi(n))$.

$\phi(6) = 2$

Example 1

- For $n = 7$ we have $\phi(7) = 6$. Therefore, the unitary group $U(7) = \{1, 2, 3, 4, 5, 6\}$. Let us find the orders of each element in $U(7)$.

$1^1 \equiv 1$

$2^1 \equiv 2 \quad 2^2 \equiv 4 \quad 2^3 \equiv 1$

$3^1 \equiv 3 \quad 3^2 \equiv 2 \quad 3^3 \equiv 6 \quad 3^4 \equiv 4 \quad 3^5 \equiv 5 \quad 3^6 \equiv 1$

$4^1 \equiv 4 \quad 4^2 \equiv 2 \quad 4^3 \equiv 1$

$5^1 \equiv 5 \quad 5^2 \equiv 4 \quad 5^3 \equiv 6 \quad 5^4 \equiv 2 \quad 5^5 \equiv 3 \quad 5^6 \equiv 1$

$6^1 \equiv 6 \quad 6^2 \equiv 1$

- From the above table, $|1| = 1$, $|2| = 3$, $|3| = 6$, $|4| = 3$, $|5| = 6$ and $|6| = 2$. Therefore, the primitive roots of modulo 7 are $\{3, 5\}$.

- Thus, a primitive root modulo n generates $U(n)$. For instance, if $n = 7$, the primitive roots 3 and 5 generate $U(7) = \{1, 2, 3, 4, \cdots, 6\}$.

Example 2

Compute the order of $2, 3$ and 5 modulo 23. Which of these 3 are primitive roots modulo 23?

$2^1 = 2$
$2^2 = 4$
$2^3 = 8$
$2^4 = 16$
$2^5 = 2^4 \times 2 = 32 = 9$
$2^6 = 18$
$2^7 = 13$
$2^8 = 3$
$2^9 = 6$
$2^{10} = 12$
$2^{11} = 1$

$|2| = 11 \neq \phi(23)$

$\phi(23) = 22$

$\therefore$ 2 is not a primitive root mod 23

Solution

$2^1 = 2$	$3^1 = 3$	$5^1 = 5$	$5^{12} = 18$
$2^2 = 4$	$3^2 = 9$	$5^2 = 2$	$5^{13} = 21$
$2^3 = 8$	$3^3 = 4$	$5^3 = 10$	$5^{14} = 13$
$2^4 = 16$	$3^4 = 12$	$5^4 = 4$	$5^{15} = 19$
$2^5 = 9$	$3^5 = 13$	$5^5 = 20$	$5^{16} = 3$
$2^6 = 18$	$3^6 = 16$	$5^6 = 8$	$5^{17} = 15$
$2^7 = 13$	$3^7 = 2$	$5^7 = 17$	$5^{18} = 6$
$2^8 = 3$	$3^8 = 6$	$5^8 = 16$	$5^{19} = 7$
$2^9 = 6$	$3^9 = 18$	$5^9 = 11$	$5^{20} = 12$
$2^{10} = 12$	$3^{10} = 8$	$5^{10} = 9$	$5^{21} = 14$
$2^{11} = 1$	$3^{11} = 1$	$5^{11} = 22$	$5^{22} = 1$

From the above table we note that $|2| = 11$, $|3| = 11$ and $|5| = 22$.

Thus 5 is a primitive root modulo 23. Notice that 5 generates $U(23)$.

Revision Questions

a) Find the orders of $2, 3, 9$ modulo 10. Which of the three is a primitive root.

b) Find the orders of $5, 7, 8$ modulo 18. Which of the three is a primitive root.

c) Find the orders of $5, 7, 8$ modulo 22. Which of the three is a primitive root.

d) Find the orders of 3 and 15. Which of them is a primitive root?

Solution

$$\phi(10) = 2 \times 5$$
$$\left((1-1/2) \times (1-1/5)\right) \times 10$$

Solution

$2, 3, 9 \mod 10$

$\phi(10) = 4$

$2^1 = 2$

$2^2 = 4$

$2^3 = 8$

$2^4 = 6$

$2^5 = 2$

$2^6 = 4$

$2^7 = 8$

$2^8 = 6$

$2^9 = 2$

$3^1 = 3$

$3^2 = 9$

$3^3 = 7$

$3^4 = 1$

Solution

$9^1 = 9$

$9^2 = 1$

$5, 7, 8 \mod 18$

$\phi(18) = \left(1 - \frac{1}{2}\right)\left(\frac{-1}{3}\right) 18$

Solution

$$\phi(18) = \frac{1}{2} \times \frac{2}{3} \times 18$$

$$\phi(18) = 6$$

$5^1 = 5$

$5^2 = 7$

$5^3 = 17$

$5^4 = 13$

$5^5 = 11$

$5^6 = 1$

$|5| = 6$

Solution

$7^1 \equiv 7$

$7^2 \equiv 13$

$7^3 \equiv 1$

$|7| = 3$

7 is not a primitive root

Solution

$8^1 = 8$

$8^2 = 10$

$8^3 = 8$

$= 5$ is the primitive w-root of 18

Solution

$\phi 22 = 2 \times 11$

$= \phi 10$

$5^1 = 5$ ✓ $\quad 5^{5-1}$! ✓

$5^2 = 3$ ✓

$5^3 = 15$ ✓ $\quad |51| = 5$

$5^4 = 9$ ✓

Solution

$7^1 = 7$ ✓

$7^2 = 5$ ✓

$7^3 = 13$ ✓

$7^4 = 3$ ✓

$7^5 = 21$ ✓

$7^6 = 15$ ✓

$7^7 = 17$ ✓

$7^8 = 9$ ✓

$7^9 = 19$ ✓

$7^{10} = 1$ ✓

Solution

2, 3 mod 15

$\phi 15 = 3, 5$

1 $\quad$ 9 15 = 8

$2^1 = 2 \quad 2^4 = 1$

$2^2 = 4$

$2^3 = 8 \quad |2| = 4$

3

- Number of primitive roots of a number n is given by $\phi(\phi(n))$. For instance, number of primitive roots modulo 22 is given by $\phi(\phi(22)) = \phi(10) = 4$ primitive roots while the number of primitive roots modulo 23 is given by $\phi(\phi(23)) = \phi(22) = 10$ primitive roots.

1.1 Easy method to compute primitive roots

- According to definition 1, a number is considered a primitive root modulo n if it is relatively prime to n. Furthermore, its order must be equal to $\phi(n)$.
- It is important to note that the possible orders of numbers that are relatively prime to n must divide n.
- So, to determine whether a number is a primitive root modulo n, consider its possible orders, as illustrated below.

Example 3

Find the primitive roots modulo 10

Solution

First, the number of primitive roots modulo 10 are $\phi(\phi(10)) = \phi(4) = 2$

The possible primitive roots are numbers relatively prime to 10 which are $1, 3, 7, 9$. Only two of these are primitive roots.

The possible orders of the primitive roots must divide $\phi(10) = 4$.

So the possible orders are $1, 2, 4$.

So we find the orders of $1, 3, 7, 9$.

Obviously, the order of 1 is 1 and so 1 is not a primitive root.

Now,

$3^1 = 3,\ 3^2 = 9,\ 3^4 = 1,$ so, 3 is a primitive root since $|2| = \phi(10)$

$7^1 = 7,\ 7^2 = 9,\ 7^4 = 1$ so, 7 is a primitive root since $|7| = \phi(10)$

$9^1 = 9,\ 9^2 = 1$ so, 9 is not a primitive root since $|9| \neq \phi(10)$

Example 4

Find all primitive roots modulo 9

Solution

Here, $\phi(9) = 6$

There are $\phi(\phi(9)) = \phi(6) = 2$ primitive roots.

The possible primitive roots are $1, 2, 4, 5, 7, 8$ (must be relatively prime to 9)

The possible orders (must divide $\phi(9) = 6$) are $1, 2, 3, 6$.

We test the above possible primitive roots with the possible orders to see which ones have orders equal to $\phi(9) = 6$.

Clearly, 1 is not a primitive root since $|1| = 1 \neq \phi(9)$

Let us test for 2.

$2^1 = 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^6 = 1$ and so $|2| = 6 = \phi(9)$. Hence 2 is a primitive root.

Solution (conti...)

Let us test for 4

$4^1 = 4,\ 4^2 = 7,\ 4^3 = 1$ and so $|4| = 3 \neq \phi(9)$. Hence 4 is not a primitive root.

Let us test for 5

$5^1 = 5,\ 5^2 = 7,\ 5^3 = 8,\ 5^6 = 1$ and so $|5| = 6 = \phi(9)$. Hence 5 is a primitive root.

We already have the two primitive roots as $\{2, 5\}$ so there is no need of testing 7 and 8 since they will not be primitive roots.

Example 5

There is no primitive root modulo 15 since none of its units have order equal to $\phi(15) = 8$. For instance, the unit 1 (order 1), 2 (order 4), 4 (order 2), 7 (order 4), 8 (order 4), 11 (order 2), 13 (order 4) and 14 (order 2), and none of these is a primitive root.

- Primitive roots are very important in cryptography, especially for Diffie-Hellman key exchange and the RSA algorithm.
- To determine a primitive root $\bmod n$, we try $a = 2$, then $a = 3$, etc., until we find an a with order $\phi(n)$. Therefore, finding a primitive root modulo n for large n appears to be a difficult problem.

Revision Questions

Find the primitive roots modulo;

a) 10 b) 16 c) 18

d) 22 e) 19 f) 25

Solution

Mod 10

$\{1, 3, 7, 9\}$ | $\phi(10) = 4$

$\{1, 2, 4\}$

Solution

$3^1 = 3$

$3^2 = 9$

$3^4 = 1$

$|3| = 4 \equiv \phi(10)$

$3,$

$7^1 = 7$

$7^2 = 9$

$7^4 = 1$

$|7| = 4$

7

Solution

$\phi(4) \Rightarrow 2$.

$\equiv \pmod{16}$

$\{1, 3, 5, 7, 9, 11, 13, 15\}$

$\phi(16) = \frac{1}{2} \times 16 = 8$

$\{1, 2, 4, 8\}$

Solution

$3^1 = 3$ $\quad$ $5^1 = 5$

$3^2 = 9$ $\quad$ $5^2 = 9$

$3^4 = 1$ $\quad$ $5^4 = 1$

$|3| = 4$ $\quad$ $|5| = 4$

Solution

$7^1 = 7$ $9^1 = 9$ $11^1 = 11$

$7^2 = 1$ $9^2 = 1$ $11^2 = 9$

$11^4 = 1$

$17| = 2$ $19| = 2$

$111| = 4$

Solution

$13^1 = 13$

$13^2 = 9$

$13^4 = 1$

$|13| = 4$

$15^1 = 15$

$15^2 = 1$

$|15| = 2$

$\Rightarrow 16$ has no primitive roots

Solution