WEB3CLUBS FOUNDATION LIMITED

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

Foundational Mathematics for Web3 Builders

Lecture 6

May 2,2024

Exercise 6

a) Write a program to compute $\phi(n)$, the value of Euler's phi function. You should compute $\phi(n)$ by using a factorization of n into primes, not by finding all the a's between 1 and n that are relatively prime to n.

2 Primitive Roots and Discrete logarithm Problem

2.1 Primitive Roots

Definition 17

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

Theorem 17 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.

For instance, 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 66

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

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.

2.2 Easy method to compute primitive roots

From theorem 17, a number a is a primitive root modulo n if a is relatively prime to n. Further, its order must equal to $\phi(n)$. Note that the possible orders of numbers relatively prime to n must divide n. So to check if a number is a primitive root modulo n, it is easier to check their possible orders as shown below.

Example 67

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 68

Find all primitive roots modulo 19

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 69

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 quite useful in number theory, particularly in the context of cryptographic algorithms like the Diffie-Hellman key exchange and the RSA algorithm.

To actually find a primitive root $\bmod n$ in practice we try $a = 2$, then $a = 3$, etc., until we find an a that has order $\phi(n)$ and so finding a primitive root modulo n for large n seems to be a difficult problem.

Theorem 18

If a is a primitive root modulo p for p an odd prime, then a is a primitive root modulo p^2 if $a^{p-1} \not\equiv 1 \bmod p^2$. If $a^{p-1} \equiv 1 \bmod p^2$ then $a + p$ is a primitive root modulo p^2. Furthermore, if b is a primitive root modulo p^2, then b is a primitive root modulo p^k for each $k \geq 3$. If b is odd then b is also primitive root modulo $2p^k$, and if b is even then $b + p^k$ is a primitive root modulo $2p^k$.

Example 70

Find the primitive root modulo 11, modulo 11^2, modulo $2 \cdot 11^2$, and modulo 11^{100}.

Solution

First, we find primitive root modulo 11. Though there are $\phi(\phi(11)) = 4$ primitive roots, we are only interested with the least of them all.

The possible primitive roots are $1, 2, 3, 4, \cdots, 10$. The possible orders are $1, 2, 5, 10$. Let us use trial to find the first primitive root.

Clearly, 1 is not a primitive root.

$2^1 = 2,\ 2^2 = 4, 2^5 = 10,\ 2^{10} = 1$ and so 2 is a primitive root modulo 11. From theorem 18, we see that $2^{10} = 1024 = 56 \not\equiv 1 \bmod 11^2$. Thus, 2 is a primitive root modulo 11^2. Similarly, 2 is a primitive root modulo 11^k for $k \geq 2$ hence for $k = 100$.

From theorem 18, since 2 is even, $2 + 11^2 = 123$ s a primitive root modulo 11^2.

A primitive root exists if and only if n is $1, 2, 4, p^k$ or $2p^k$, where p is an odd prime and $k > 0$. These are essentially all the cases in which primitive roots exist. There is no primitive root modulo the prime power 2^3, and hence none $\mod 2^n$ for $n \geq 3$.

Example 71

Find a primitive root modulo 54.

Solution

We have $54 = 2 \cdot 3^3$ and so a primitive root modulo 54 exists.

To make our work easy we use theorem 18 to find the primitive root modulo 3 and 3^3.

The primitive root modulo 3 is 2.

Since $2^{3-1} = 4 \not\equiv 1 \mod 3^2$ we have that 2 is a primitive root modulo $3^2 = 9$ and 2 is also a primitive root modulo $3^3 = 27$.

Since 2 is even, we have that $2 + 3^3 = 29$ is a primitive root modulo 54.

Theorem 19

If p is an odd prime and a is a unit with $a^{(p-1)/q} \not\equiv 1 (\mathrm{mod}\, p)$ for any prime divisor q of $p-1$, then a is a primitive root modulo p.

The point is that, by Fermat's little theorem the order of a divides $p-1$, and if the order of a were smaller than $p-1$ then $a^{(p-1)/q}$ would be congruent to 1 for at least one prime divisor q of $p-1$.

Example 72

Find a primitive root modulo $p = 647$.

Solution

First we factor $p - 1 = 646 = 2 \cdot 17 \cdot 19$ using a factorization algorithm.

Now search for residues a such that none of $a^{(p-1)/2}$, $a^{(p-1)/17}$, $a^{(p-1)/19}$ is congruent to 1 modulo p.

Solution (conti...)

Let us check $2, 3, 5, 7, 9, 10$ as shown in the table below

	$a^{(p-1)/2}$	$a^{(p-1)/17}$	$a^{(p-1)/19}$
$a = 2$	1	293	544
$a = 3$	1	573	55
$a = 5$	-1	300	104
$a = 7$	1	67	55
$a = 9$	1	300	437
$a = 10$	646	555	287

From the table, $a = 5$ is a primitive root since none of $a^{(p-1)/2}$, $a^{(p-1)/17}$, $a^{(p-1)/19}$ is congruent to 1 modulo p. The other primitive root from the table is $a = 10$.

Example 73

Find a primitive root modulo $p = 2394863$.

Solution

First we factor $p - 1 = 2394862 = 2 \cdot 37 \cdot 32363$ using a factorization algorithm. Now search for residues a such that none of $a^{(p-1)/2}$, $a^{(p-1)/37}$, $a^{(p-1)/32363}$ is congruent to 1 modulo p.

Let us check $2, 3, 5, 7, 9$ as shown in the table below

	$a^{(p-1)/2}$	$a^{(p-1)/37}$	$a^{(p-1)/32363}$
$a = 2$	1	14871	23729
$a = 3$	1	50374	2128656
$a = 5$	2394862	2184105	929101
$a = 7$	-1	819245	996833
$a = 9$	1	1379959	2170679

From the table, $a = 5$ is a primitive root since none of $a^{(p-1)/2}$, $a^{(p-1)/37}$, $a^{(p-1)/32363}$ is congruent to 1 modulo p. The other primitive root from the table is $a = 7$.

We have already seen examples that agree with the following theorem.

Theorem 20 (Primitive Root Theorem)

Every prime p has a primitive root. More precisely, there are exactly $\phi(p-1)$ primitive roots modulo p.

Although the Primitive Root Theorem tells us that there are lots of primitive roots modulo p, in fact, precisely $\phi(p-1)$ of them, it doesn't give us any information at all about which specific numbers are primitive roots.

Exercise 7

1. Find all the primitive roots if they exist.

   a) modulo 8 b) modulo 10 c) modulo 23

2. a) Find all primes less than 20 for which 3 is a primitive root.

   b) If you know how to program a computer, find all primes less than 100 for which 3 is a primitive root

3. Write a program to compute order of a modulo p which is the smallest positive power k such that $a^k \equiv 1(\mathrm{mod}p)$.(Use the fact that if $a^k \not\equiv 1(\mathrm{mod}\ p)$ for all $1 \leq k < \frac{p}{2}$, then the order of a modulo p is automatically $p-1$).

4. Write a program that finds the smallest primitive root for a given prime p. Make a list of all primes between 100 and 200 for which 2 is a primitive root.

2.3 Discrete logarithm problem

In designing public-key cryptosystems, two problems dominate the designs: the integer factorization problem and the discrete logarithm problem.

Discrete logarithms have a natural extension into the realm of elliptic curves and hyperelliptic curves. The Elliptic ElGamal has proved to be a strong cryptosystem using elliptic curves and discrete logarithms.

The discrete logarithm problem involves finding an integer x such that

$$g^x \equiv b \bmod n$$

where g, b and n are given integers. Here, g is a generator (a primitive root of n) of the unitary group $U(n)$. The number x is called discrete logarithm of b with respect to base g modulo n and we write $x = \log_g b$.

The term discrete logarithm is commonly used in cryptography although the generalized multiplicative order is sometimes used. In number theory the term index is generally used. This problem is computationally difficult to solve efficiently, especially for large prime numbers n, which is the basis for some cryptographic algorithms, such as the Diffie-Hellman key exchange and the Digital Signature Algorithm (DSA).

The security of these cryptographic systems relies on the difficulty of solving the discrete logarithm problem efficiently, particularly in cases where n is a large prime number.

The discrete logarithm can also be solved for an additive cyclic group. For instance, take the cyclic group $\mathbb{Z}/n\mathbb{Z}$, computing $\log g^x$ is really solving the congruence

$$mg \equiv x \bmod n$$

for some m which can be done easily essentially using the Euclid's algorithm.

It is very easy to compute discrete logarithms in the additive group since all we need to do is compute the multiplicative inverse of g modulo n and multiply by m.

Example 74

Take $G_1 = \mathbb{Z}/100\mathbb{Z}$ and $G_2 = U(101)$. These two groups are both cyclic groups of order 100 generated by 3. Let us compute $\log_3 17$ in G_1 and G_2.

In G_1, let $\log_3 17 = n \Rightarrow 3^n \equiv 17 \bmod 100$. So, in G_1 we solve $3n \equiv 17 \bmod 100$ by first getting $3^{-1} \bmod 100 = 67$. Then multiply on both sides by 67 to get

$n \equiv 17 \cdot 67 \bmod 100 \equiv 39 \bmod 100$.

In G_2, to solve $3^n \equiv 17 \bmod 101$ is much harder. One way to achieve this is by trial and error, where we compute each power of $3 \bmod 101$ till we find our target 17. Doing this gives $n = 70$.

Example 75

Solve $\log_2 9 \bmod 11$

Solution

Let $\log_2 9 \bmod 101 \equiv x$. To find x, we write $\log_2 9 = x$ in index form as $2^x \equiv 9 \bmod 11$.

To find x, try integers $1, 2, 3, \cdots, 10$ to see which one satisfies $2^x \equiv 9 \bmod 11$.

$2^1 = 2 \not\equiv 9$

$2^2 = 4 \not\equiv 9$

$2^3 = 8 \not\equiv 9$

$2^4 = 5 \not\equiv 9$

$2^5 = 10 \not\equiv 9$

$2^6 = 9 \not\equiv 9$

$2^7 = 7 \equiv 9$

$2^8 = 3 \not\equiv 9$

$2^9 = 6 \not\equiv 9$

$2^{10} = 1 \not\equiv 9$

Thus $x = 6$

Example 76

Using the same reasoning as from example 75, find the discrete logarithms of each unit modulo 11 to the base 2

Solution

After working out $2^0,\ 2^1,\ 2^2,\ \cdots,\ 2^{10} \bmod 11$, we come up with the following table.

x	1	2	3	4	5	6	7	8	9	10
$\log_2 x$	0	1	8	2	4	9	7	3	6	5

Example 77

Solve $\log_3 x \bmod 101 \equiv 24$

Solution

To find x we solve $3^{24} = x \bmod 101$

Using the fast powering algorithm we get

$3^1 = 3$ $\qquad$ $3^8 = 97$

$3^2 = 9$ $\qquad$ $3^{16} = 16$

$3^4 = 81$

Therefore, $3^{24} = 3^{16+8}$

$= 3^{16} \times 3^8$

$= 16 \times 97$

$= 37 \bmod 101$

Hence $x \equiv 37 \bmod 101$

Some of the algorithms that can be used to compute discrete logarithms are:

a) Baby-step-giant-step (BSGS) algorithm

b) Pohlig-Hellman algorithm

c) Pollard-ρ Algorithm