CS3031 – Telecommunications
Cryptography Notes

Euler's ϕ Function:

$\phi(n)$- The number of integers between 1 and n where gcd(n, x) = 1

Rule 1: If p is prime then:

$$\phi(p) = p - 1$$

e.g $\phi(11) = 11 - 1 = 10$

Rule 2: If a can be represented as p^n with p prime then:

$$\phi(a) = \phi(p^n)$$
$$\phi(p^n) = p^n - p^{n-1}$$

e.g $\phi(32) = \phi(2^5)$
$\phi(2^5) = 2^5 - 2^4 = 16$

Rule 3: If gcd(m,n)=1 then:

$$\phi(mn) = \phi(m) * \phi(n)$$

e.g $\phi(35) = \phi(7 * 5)$
$\phi(7 * 5) = \phi(7) * \phi(5)$
$= (7 - 1) * (5 - 1)$
$= 24$

Extended Euclidean Algorithm (EEA):

This algorithm is useful for modulo arithmetic for inverse of numbers:

What is 4^{-1} modulo 11?

$x \equiv 4^{-1} \, mod \, 11$
$\boldsymbol{4 * x \equiv 1 \, mod \, 11}$

Solve for x

$4 * 3 \equiv 1 \, mod \, 11$
$\boldsymbol{x = 3}$

Fermat's Little Theorem:

For Fermat's Little theorem everything is stated in terms of mod p where p is prime:

- $a^p \equiv a \ (mod \ p)$
- $a^{p-1} \equiv 1 \ (mod \ p)$
- $a * a^{p-2} \equiv 1 \ (mod \ p)$

Somewhat the most important derivation of Fermat's Little Theorem can be derived as follows:

- $a * a^{p-2} \equiv 1 \ (mod \ p)$

$$\boldsymbol{a^{-1} \equiv a^{p-2} \ (mod \ p)}$$

Some examples. Given p=7 and a=3, verify FLT:

$$a^p \equiv a \ (mod \ p)$$
$$3^7 \equiv 3 \ (mod \ 7)$$
$$2187 \equiv 3 \ (mod \ 7)$$

Compute $4^{-1} \ mod \ 11$:

$$a^{-1} \equiv a^{p-2} \ (mod \ p)$$
$$4^{-1} \equiv 4^{11-2} \ (mod \ 11)$$
$$4^{-1} \equiv 4^9 \ (mod \ 11)$$
$$4^{-1} \equiv 262144 \ (mod \ 11)$$
$$4^{-1} \equiv 3 \ (mod \ 11)$$

Square And Multiply Algorithm:

This is used for performing modulo arithmetic on large numbers. The method involves breaking the exponent into it's binary form, then converting the 1's to decimal and re-writing the exponent in terms of these decimal numbers:

Calculate $\boldsymbol{3^{133}\ mod\ 7}$

$$133_{10} = 1000\ 0101_2 = 128 + 4 + 1$$

$$\begin{aligned} \therefore 3^{133} &= 3^{128+4+1} \\ &= 3^{128} * 3^4 * 3^1 \end{aligned}$$

$$3^{128}\ mod\ 7 = 2$$
$$3^4\ mod\ 7 = 4$$
$$3^1\ mod\ 7 = 3$$

$$\begin{aligned} \therefore 3^{133}\ mod\ 7 &= 3^{128} * 3^4 * 3^1\ mod\ 7 \\ &= 2 * 4 * 3\ mod\ 7 \\ &= 24\ mod\ 7 \\ &= 3 \end{aligned}$$

Finite Groups:

$\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$

$\mathbb{Z}^*{}_n$ integers i=0,1,… where **gcd(i, n) =1**

$|\mathbb{Z}^*{}_n| = \phi(n)$ → The number of elements **relatively prime to n**

The order – **ord(a)** – of an element a of a group (G, *) is the smallest possible integer k such that:

$a^k = a * a * \dots * a = 1$

Determine the order of a=3 in $\mathbb{Z}^*{}_{11}$

We keep computing the powers of a until we obtain the identity element (1):

- $a^1 = 3^1 = 1 \equiv 3\ mod\ 11$
- $a^2 = 3^2 = 9 \equiv 9\ mod\ 11$
- $a^3 = 3^3 = 27 \equiv 5\ mod\ 11$
- $a^4 = 3^4 = 15 * 3 \equiv 4\ mod\ 11$
- $\mathbf{a^5 = 3^4 = 4 * 3 \equiv 1\ mod\ 11}$

Therefore the order of a=3 in $\mathbb{Z}^*{}_{11}$ is 5.

Cyclic Groups:

A group G which contains an element a with **maximum order** is said to be cyclic, i.e if:

$$\boldsymbol{ord(a) = |G|}$$

Elements with maximum order are called **primitive roots/generators** of G.

Q) Check if a=2 is a primitive root of in $\mathbb{Z}^*{}_5$

In order for a to be a primitive root it must satisfy:

$$\boldsymbol{ord(a) = |G|}$$

First, let us calculate ord(a=2):

- $a^1 = 2^1 = 2 \equiv 2 \; mod \; 5$
- $a^2 = 2^2 = 4 \equiv 4 \; mod \; 5$
- $a^3 = 2^3 = 8 \equiv 3 \; mod \; 5$
- $\mathbf{a^4 = 2^4 = 16 \equiv 1 \; \boldsymbol{mod} \; 5}$

Therefore, **ord(a) = 4**. Now let us calculate $|\mathbb{Z}^*{}_5|$

$\mathbb{Z}^*{}_5 = \{1,2,3,4\}$
$|\mathbb{Z}^*{}_5| = 4$

Therefore $\boldsymbol{ord(a) = 4} = |\mathbb{Z}^*{}_5|$, as a result we can say that $\mathbb{Z}^*{}_5$ is a cyclic group.

Let G be a finite cyclic group, then it holds that:

- The number of primitive roots of G is $\phi(|G|)$
- If G is prime then all elements $a \neq 1 \in G$ are primitive.

Q) Find the number of primitive roots in $\mathbb{Z}^*{}_{11}$

Given that 11 is prime we know that $\mathbb{Z}^*{}_{11}$ is a finite cyclic group. As a result we can infer that the number of primitive roots of $\mathbb{Z}^*{}_{11}$ is:

$$\mathbb{Z}^*{}_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$$

$$\begin{aligned}\phi(|\mathbb{Z}^*{}_{11}|) &= \phi(10) \\ &= 2 * 5 \\ &= (2^1 - 2^0) * (5^1 - 5^0) \\ &= 1 * 4 \\ &= 4\end{aligned}$$

Therefore, the number of primitive roots in $\mathbb{Z}^*{}_{11}$ is 4.