**CS3031 – Telecommunications**

**Cryptography Notes**

**Euler’s Function:**

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

***Rule 1:*** If p is prime then:

e.g

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

e.g

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

e.g

**Extended Euclidean Algorithm (EEA):**

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

*What is modulo 11?*

*Solve for x*

**Fermat’s Little Theorem:**

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

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

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

Compute :

**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***

**Finite Groups:**

integers i=0,1,… where **gcd(i, n) =1**

🡪 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:

*Determine the order of a=3 in*

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

Therefore the order of a=3 in is 5.

**Cyclic Groups:**

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

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

*Q) Check if a=2 is a primitive root of in*

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

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

Therefore, **ord(a) = 4**. Now let us calculate |

|

Therefore , as a result we can say that is a cyclic group.

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

* The number of primitive roots of G is
* If G is prime then all elements are primitive.

*Q) Find the number of primitive roots in*

Given that 11 is prime we know that is a finite cyclic group. As a result we can infer that the number of primitive roots of is:

Therefore, the number of primitive roots in is 4.