NUMBER THEORY AND CRYPTOGRAPHY

Akhlak Ansari

December 4, 2022

Department of Mathematics and Statistics

Fall' 2022-23

Role of Number Theory in Cryptography

Number theory has an important role in Cryptographic foundation.To produce secret messages an send securely and secretly to the recepient in this technological era through internet, we must have knowledge of behaviour of numbers, which is summurize in the branch of mathematics called **Number Theory**.i.e what a number means and what kind of manipulation allows to do with numbers and all other kind of stuffs to encrypt the messages and make their secrecy. So In order to make an intuitive idea of **Cryptography**, we must have a deep knowledge of **Number Theory**.

Pre-Requisites :

1. Integers
2. Divisor
3. Division Algorithm
4. Greatest Common Divisor / gcd(a,b)
5. Least Common Multiple / lcm(a,b)
6. Euler totient function / Euler ϕ - function
7. Congruency
8. Encryption
9. Decryption

Let's discuss briefly about pre-requisites -

1.Integers:

The integers is the set of positive and negative counting numbers including zero. It is represented by $\mathbb{Z}$.i.e

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

2.Divisor:

If an integer n can be eritten as a product $k \cdot d = n$ of two integers k and d , then
we say that d divides n, or that n is divisible by d, or that d is a **divisor** of n. i.e

$$n = k.d \implies d|n. \; ; \; \forall \; n, k, d \in \mathbb{Z}$$

eg. $2|8$, $6|24$, $3|27$ etc.

We occassionaly choose the term **proper divisor** to denote a positive divisor n which is not n. When $n = 8$, we see the that $1, 2, 4$ are all proper divisors.

3.Division Algorithm:

For $a, b \in \mathbb{Z}$ and $b > 0$, we can always write $a = q \cdot b + r$ with $0 \leq r < b$ and q an integer. Moreover, given a, b there is only one pair q, r which satisfies these constraints.We call the first element q the quotient and the second one r the remainder.

eg. $35 = 6 \cdot 5 + 5$

4.Greatest Common Divisor:

If we consider the various divisors of two numbers a and b , we say that d is a **common divisor** of a and b if $d|a$ and $d|b$. If d is the bigger such common divisor, it is called the **greatest common divisor**, or gcd of a and b and written as

$$d = gcd(a, b)$$

eg. $gcd(3, 10) = 1$

5.Least Common Multiple:

Let a and b any two integers not both zero,then an integer $m \geq 1$ is called a **least common multiple** of a and b, if the following properties holds,

- $a|m$ and $b|m$
- For any integer n, if $a|n$ and $b|n$ then $m|n$.

eg. $lcm(168, 490) = 5880$.

6.Euler ϕ - function:

In number theory, Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter ϕ as $\phi(n)$ and may also be called Euler's phi function. In other words, it is the number of integers k in the range $1 \leq k \leq n$ for which the greatest common divisor $gcd(n, k)$ is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

$$\phi(n) = \{1 \leq k \leq n;\ gcd(n, k) = 1;\ \forall k, n \in \mathbb{Z}\}$$