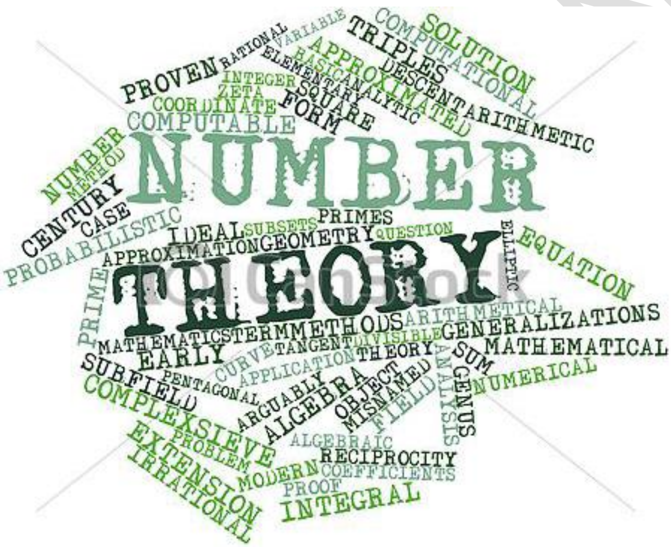
MODULE-1 Modular Arithmetic and Number

Vidyalankar Institute of Technology

Accredited A+ by NAAC



Prepared by Prof. Amit K. Nerurkar

Module 1 Number Theory

Number Theory

Prime number is a positive integer > 1 whose only factors are 1 and itself. It cannot be divided by any number other than 1 and itself. Examples: 2, 3, 5, 7, 11.

Two numbers are **relatively prime** whey they have no factors in common other than 1. If the Greatest Common Divisor (GCD) of a and n is 1, it is written as GCD(a, n)=1. As we will note that the numbers 21 and 44 are relatively prime (because they have no factors in common), but the numbers 21 and 45 are not (because they have a factor 3 in common).

Euclid's algorithm

One of the basic techniques of number theory is the Euclidean algorithm, which is a simple procedure for determining the greatest common divisor of two posit ive integers. First, we need a simple definition: Two integers are **relatively prime** if their only common positive integer factor is 1.

The Euclidean algorithm is based on the following theorem: For any nonnegative integer a and any positive integer b,

$$\gcd(a, b) = \gcd(b, a \bmod b)$$

E.g. Find gcd (105,80) using Euclid's algorithm also tell whether 105 and 90 are relatively prime

Solution:

We know gcd(a,b)=gcd(b,a mod b)

So, gcd(105,80)= gcd(80, 105 mod 80)=gcd(80,25)

= gcd(25, 80 mod 25)=gcd(25,5)

=gcd(5, 25 mod 5)=gcd(5,0)

Since y=0, so gcd=x

i.e. gcd=5

Two integers are relatively prime when there are no common factors other than 1. This means that no other integer could divide both numbers evenly.

Two integers a,b are called relatively prime to each other if gcd(a,b)=1.

For example, 7 and 20 are relatively prime

105 and 80 are not relatively prime

Example:

GCD(20, 3) = GCD(3, 20 MOD 3) = GCD(3, 2)
= GCD(2, 3 MOD 2)
= GCD(2, 1)
= GCD(1, 2 MOD 1)
= GCD(1, 0)=1

GCD(34, 6) = GCD(6, 34 MOD 6) = GCD(6, 4)
= GCD(4, 6 MOD 4)
= GCD(4, 2)
= GCD(2, 4 MOD 2)
= GCD(2, 0)
= 2

Euler Totient Function (Ø(n))

This function is written as Ø(n), where Ø(n) is the number of positive integers less than n and relatively prime to n.

Example 1: if n=6, the positive integers less than n are 1, 2, 3, 4 and 5. Of these, only 1 and 5 do not have any factors common with 6. Thus, Ø(n)=Ø(6)=2.

Example 2: if n=7. Hence, all the positive integer preceding it (ie., 1 to 6) are relatively prime to it. Thus, Ø(n)=Ø(7)=6.

Euler's theorem:

It says that every a and n that are relatively prime. So, a^Ø(n) mod n≡ 1.

Example 1: If a=3, n=10 then Ø(n)=Ø(10)=4 (4 numbers are 1, 3, 7 and 9).
So, a^Ø(n) = 3^4 = 81 mod 10 = 1.

Example 2: If a=2, n=11 then Ø(n)=Ø(11)=10 (10 numbers are 1 to 10).
So, a^Ø(n) = 2^10 = 1024 mod 11 = 1.

References

1. https://binaryterms.com/network-security-model.html
2. https://www.summaryplanet.com/information-technology/OSI-security-architecture.html
3. https://www.geeksforgeeks.org/active-and-passive-attacks-in-information-security/
4. https://www.geeksforgeeks.org/caesar-cipher-in-cryptography/
5. https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_multiplicative_cipher.htm
6. https://www.javatpoint.com/vigenere-cipher
7. https://www.geeksforgeeks.org/hill-cipher/
8. https://www.educative.io/edpresso/what-is-the-hill-cipher
9. https://sangonok.wordpress.com/2014/12/04/keyed-transposition-cipher/
10. https://www.101computing.net/the-rail-fence-cipher/
11. https://www.edureka.co/blog/steganography-tutorial