NUMBER THEORY AND THEIR APPLICATION IN COMPUTER SCIENCE AND CRYPTOGRAPHY

Debjeet Banerjee[1], Sagnik Dutta[2], Souvik Bhattacharyya[3], Sujan Sarkar[4], Sneha Rakshit[5], Raktim Chakraborty[6].

[1,2,3,4,5,6]*Institute of Engineering & Management,*
Salt Lake Electronics Complex
Kolkata-700091. India
Email: whokilleddb@gmail.com, duttasagnik1234@gmail.com

Abstract

Here we have briefly discussed the various applications of number theory in the fields of Computation with special emphasis on Encryption algorithms.We have laid special emphasis on prime numbers and briefly touched upon their importance in modern day Cryptography , especially in RSA Encryption which is the most widely used encryption technique nowadays.

Keywords: *Number theory, encryption, algorithm, prime numbers, cryptography, RSA encryption.*

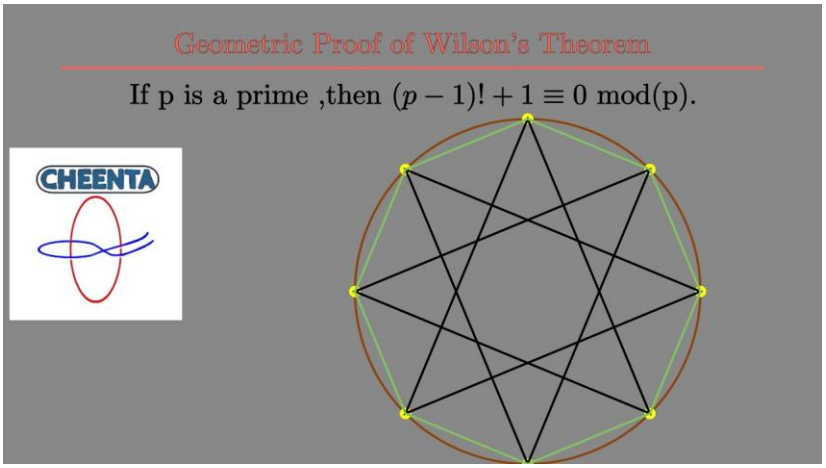
INTRODUCTION

With recent advancement in computation , the field of Number Theory is expanding it's domains of applicability from beyond theoretical results to real life applications in the various fields of Technology. It's a fundamental tool which forms the basis of modern cryptography techniques forming the base line for Key Generation used to secure connections nowadays.Besides that , there are various other spheres where number theory is used like Pseudorandom number generator, locating grid points on a plane at specified distances and many more. We have also touched upon various theorems used for the verification and generation of primes and the uses of modulus operator in this field.

THEOREMS

Wilson's theorem :

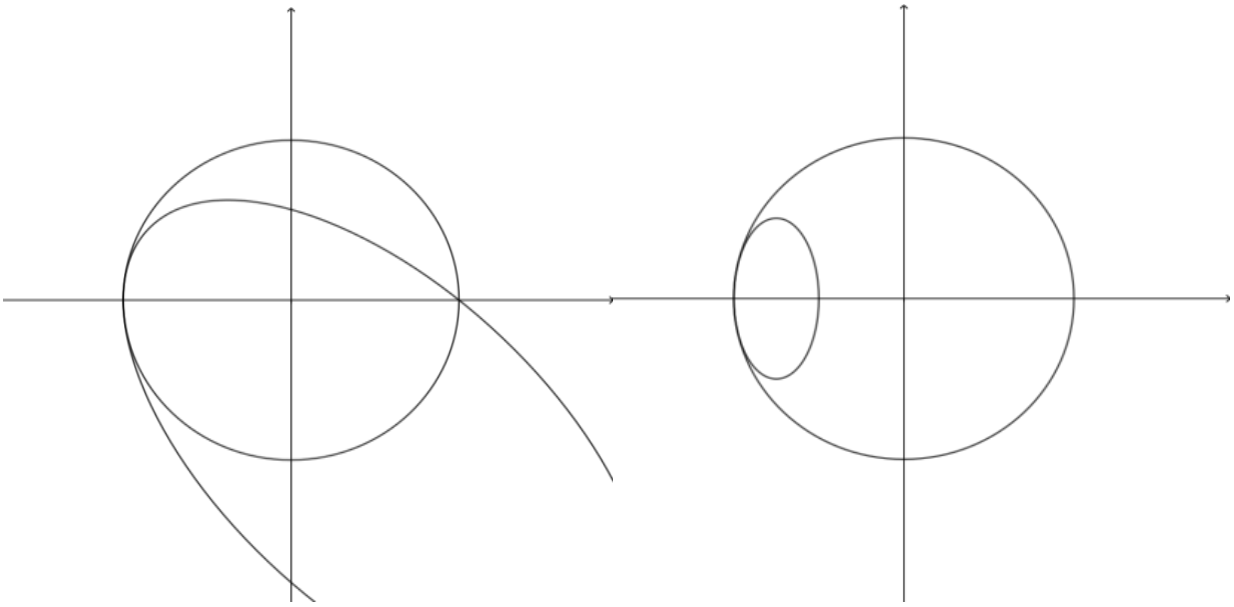
Wilson's theorem states that a natural number n > 1 is a prime number if and only if the product of all the positive integers less than n is one less than a multiple of n. That is (using the notations of modular arithmetic), the factorial satisfies exactly when n is a prime number. The converse of this theorem is also true and can be co-related to Euler's totient function which plays a key role in RSA encryption as we shall see later.



Bezout's Theorem :

Bézout's theorem is a statement in algebraic geometry which deals with the number of intersection points of two plane algebraic curves which intersect at a finite number of points only. The theorem states that the number of common points of two such curves is at most equal to the product of their degrees, and equality holds if we consider points at infinity and in the Argand plane (or more generally, coordinates from the algebraic closure of the ground field), and if each point is counted with its intersection multiplicity).

Suppose that X and Y are two plane projective curves defined over a field F that do not have a common component (this condition means that X and Y are defined by polynomials, which are not multiples of a common non constant polynomial; in particular, it holds for a pair of "generic" curves). Then the total number of intersection points of X and Y with coordinates in an algebraically closed field E which contains F, counted with their multiplicities, is equal to the product of the degrees of X and Y.



When dealing with certain problems which can be transposed to a graphical or a two dimensional domain , this theorem facilitates the use of various existing solutions to similar problems to examine the solution of the given problem. This is most commonly implemented for finding solutions of equations and graphs in time domain after converting the same to a two-dimensional spatial domain by using Fourier Transforms.

RSA

RSA (Rivest-Shamir-Adleman) is a set of computer instructions used by modern computers to turn inputs into secret code and change secret codes into readable messages. It is an asymmetric encryption method which means that there are two different keys. This is also called public key cryptography, because one of the keys (the public key) is let out on the internet which is in a public domain. The other key must be kept private. The set of computer instructions is based on the fact that finding the factors of a large composite number is very hard: when the factors are prime numbers, the problem is called most important factorization. Also , the keys so generated are always in pairs (one public key and one private key).

RSA Explained [1]:

Two large distinct primes , say p and q , are generated by the system.

Their product $N = p \; x \; q$ is calculated.

The Euler Totient Function $\phi(N)$ is calculated. As p and q are primes then the output of this function comes out to be :

$\phi(N)=(p-1) \times (q-1)$

Choose an integer e , such that $1 < e < \phi (n)$ and e is co-prime to $\phi (n)$, i.e.: e and $\phi (n)$ share no factors other than 1; $gcd(e , \phi (n))$ is released as the public key exponent. e is released as the public key exponent.

Compute d to satisfy the congruence relation $d \times e \equiv 1 (mod \phi (n))$ i.e.: $d \times e = 1 + z \phi (n)$ for some integer z. (Simply to say : Calculate $d = (1 + z \phi (n)) / e$ to be integer).d is kept as the private key exponent.

Encrypting :

Alice gives her public key (n & e) to Bob and keeps her private key secret. Bob wants to send message M to Alice.

First he turns M into a number m smaller than n by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to:

$$c = m^e \ mod \ n$$

This can be done quickly using the method of exponentiation by squaring. Bob then sends c to Alice.

Decrypting A Message :

Alice can recover m from c by using her private key d in the following procedure:

$$m = c^d \ mod \ n$$

Given m , she can recover the original distinct prime numbers, applying the Chinese remainder theorem to these two congruences yields

$$m^{(e \times d)} \equiv m \ mod \ p \times q$$

Thus,

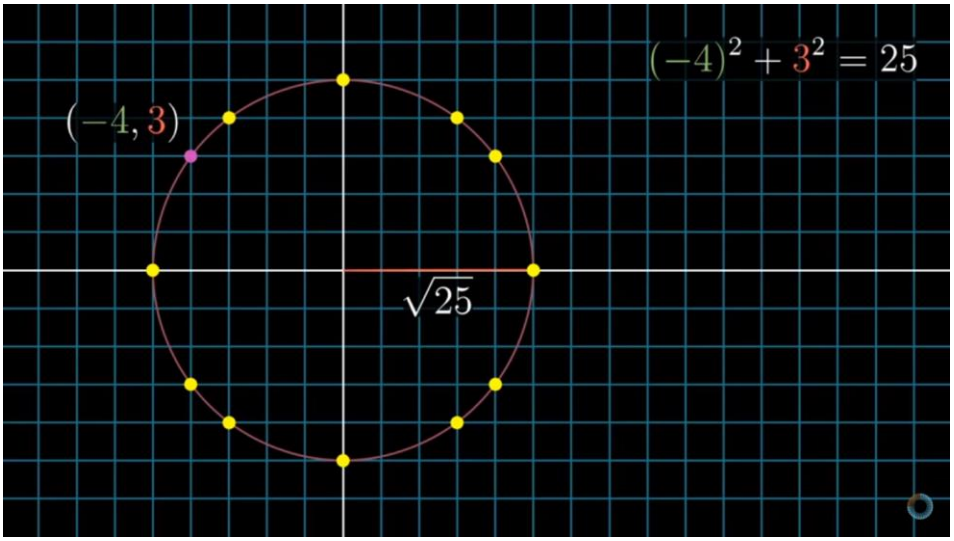
$$c^d \equiv m \ mod \ n$$

RSA encryption relies on the fact that the prime factorization of such large numbers takes an enormous amount of computational power. Even with supercomputers this would still take a long time.

CONGRUENCE

The concept of congruence can be applied to find the number of nodes at a given distance from the origin in a Cartesian system.

Transposing the Cartesian space to an Argand plane , we can graph a function which gives the output as the number of lattice points inside a system.



As we can see , numbers with property *a≡1 (mod 4)* contain exactly *12* lattice points on their circumference while numbers with *a≡3 (mod 4)* have *4* lattice points on their circumference.

This helps us to build more precise node hopping algorithms and predict the location of a point.[2]

Pseudo Randomness

Pseudo Random Number Generator(PRNG) refers to an algorithm that uses mathematical formulas to produce sequences of random numbers. PRNGs generate a sequence of numbers approximating the properties of random numbers.

With the advent of computers, programmers recognized the need for a means of introducing randomness into a computer program. However, surprising as it may seem, it is difficult to get a computer to do something by chance as the computer follows the given instructions blindly and is therefore completely predictable. It is not possible to generate truly random numbers from deterministic things like computers so PRNG is a technique developed to generate random numbers using a computer.

$Xn+1 = (aXn + c) \bmod m$

where X is the sequence of pseudo-random values

m, $0 < m$ - modulus

a, $0 < a < m$ - multiplier

c, $0 \leq c < m$ - increment

x_0, $0 \leq x_0 < m$ - the seed or start value

This is used for training for algorithms on different data sets to test the efficiency of the algorithm.

PRNGs are repetitive and can be used time and again to train different algorithms using the same data set.

CONCLUSION

Hence we can conclude that number system is extremely helpful to us and we can derive a lot of innovative and practical things from here.

Some applications are very vital such as:

- Cryptography
- Hashing
- Public key Generation
- Pseudorandomness number generation

REFERENCES

[1] https://en.wikipedia.org/wiki/RSA_(cryptosystem)
[2] https://www.youtube.com/watch?v=NaL_Cb42WyY