NUMBER THEORY

PROJECT SUBMITTED BY-*PRADIP GHOSH*

Registration No-202001020434 OF 2020-21

Roll No-200313700007

Semester- VI

GOVERNMENT GENERAL DEGREE COLLEGE AT KALNA-1

Under guidance of *Dr. Krishnendu Dutta,*

Professor of Mathematics,GGDCK-1

UNIVERSITY OF BURDWAN

IN PARTRIAL FULFILMENT OF THE REQUIREMENT FOR THE ***BACHELOR DEGREE OF SCIENCE IN MATHEMATICS.***

CERTIFICATE

This is to certify that the project report title "NUMBER THEORY" submitted by PRADIP GHOSH Towards partial fulfillment of the requirements of degree of bachelor degree of science in mathematics is a bonafide work carried out by them during the academic year 2019-20.

Project supervisor-.....................

Signature Of Guide -.........................

DEPARTMENT OF MATHEMATICS

DECLARATION

We hereby declare that this project entitled ”NUMBER THEORY’ is an original work done by me under the supervison and guidance of Prof. (Dr.) KRISHNENDU DUTTA ,principal of Government general degree college of bachelor degree of science under Burdwan university .I further declare that this project is not partly or wholly submitted for any other purpose and the data included in project is collected from various sources and true to the best of my knowledge.

Pradip Ghosh

Place:GGDCK-1

PRADIP GHOSH

ACKNOWLEDGEMENT

We express our heart fit gratitude to our project supervisor Mr. Krishnendu Dutta ,principal of GGDCK-1,for providing me necessary stimulus for the preparation of this project .

CONTENTS

CHAPTER-1

INTRODUCTION *:The theory of numbers is one of the oldest branches of mathematics ;an enthusiast ,by stretching a point here and there ,could extend its roots back to surprisingly remote date .Although it seems proable that the Greeks were largely indebted to the Babylonians and ancient Egyptians for a core of information about the properties of the natural numbers ,the rudiment of an actual theory are generally credited to Pythagoras and his disciples .another approach to divisibility question is through the arithmetic of remainders ,or the theory of congruence's as it's now commonly known .The concept and the notation that makes it such a powerful tool, was first introduced by the German mathematician CARL FRIEDRICH GAUSS (1777-1855) in his 'Disquisitions Arithmetical ' , this monumental work ,which appeared in 1801 when Gauss was 24 year old ,laid the foundations of modern number theory ."It is really astonishing" ,said Kronecker ,"to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline."*

CHAPTER-2

DIVISIBILITY : When dividing an integer by a second nonzero integer ,the quotient may or may not be an integer.

For example , $\frac{12}{3} = 4$ *while* $\frac{9}{4} = 2.25$.

This issue of divisibility is addressed in the following definition.

Definition : if a and b are integers with $a \neq 0$,we say that a divides b if there exists an integer c such that $b = ac$ .when a divides b we say that a is a factor of b and that b is multiple of a.The notation $a|b$ *denotes* a divides b and $a \nmid b$ denotes a does not divide b. back to the above examples ,we see that 3 divides 112, denoted as 3|12,and 4 does not divide 9,denoted as $4 \nmid 9$.

Divisibility properties :

1. If $a|b$ and $a|c$ then $a|(b + c)$;
2. If $a|b$ *then* $a|bc \; \forall$ *integers* c ;
3. If $a|b$ *and* $b|c$ *then* $a|c$.

CHAPTER-3

Modular Arithmetic :

Definition : If a and b are integers and m is a positive , then a congruent to b modulo m if m divides $(a-b)$.

We use notation $a \equiv b(mod\ m)$ if this is case , and $a \not\equiv b(mod\ m)$,otherwise.

Theorem 1: Let a and b be integers and let m be a positive integer. Then $a \equiv b(mod\ m)$ if and only if $a\ (mod\ m\ ) = b\ (mod\ m)$.

Example : 10 and 26 are congruent modulo 8, since their difference is 16 or -16, which is divisible by 8.when dividing 10 and 26 by 8 we get $10 = 1 \times 8 + 2\ and\ 26 = 4 \times 6 + 2$. so $10\ (mod\ 8) = 2 = 16\ (mod\ 8)$.

THEOREM-2 : Let m be a positive integer .the integers $a\ and\ b\ are\ congruent\ modulo\ m$ if and only if there is an integer k such that $a = b + km$.

THEOREM-3: Let m be a positive integer. If $a \equiv b(mod\ m) and\ c \equiv d(mod\ m)$, then $a + c = b + d\ and\ ac \equiv bd\ (mod\ m)$.

Chapter-4

PRIMES :

Definition : A positive integer $p > 1$ is called prime if the only positive factors of p are 1 and p.A positive integer that is greater than one and is not prime is called composite .

An integer n is complete if and only if there exits an integer a such that $a|n \ and \ 1 < a < n$. Prime numbers 2,3,5,7,11,13, etc.for the following composite numbers n provide a proof it is composite ,that is,give a divisor a ,with $1 < a < n$:

Composite numbers :4,6,8,10,12,14,15,etc.

THEOREM(The fundamental theorem of arithmetic) :

Every positive integer greater than 1 can be written uniquely as a prime or as the product of non-decreasing size.

The proof uses strong induction ,so we will delay it until the next topic.

Examples :

$$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$$

$$641 = 614$$

$$333 = 3 \times 3 \times 37 = 3^2 \times 37$$

$64=2\times 2 \times 2 \times 2 \times 2 \times 2 =2^6$

Theorem : There are infinitely many primes.

Fermat's little theorem : If p is a prime and a is an integer not divisible by p then, $a^{p-1} \equiv 1(mod\ p)$.further more , for every integer a we have $a^p \equiv a(mod\ p)$.

Example : $p = 5$ verify that the theorem works for $a = 1,2,3,4$: for 1 is trivial, $2^4 = 16 \equiv 1(mod\ 5), 3^4 = 81 \equiv 1(mod\ 5), 4^4 = 256 \equiv 1(mod\ 5)$.

CHAPTER-5

Number theoretic function :

THE MOBIUS INVERSION FORMULA : We introduce another naturally defined function on the positive integers , the $mobius\ \mu\ funtion.$

Definition : For a positive integer n , define μ by the rules

$$\mu(n) = \begin{cases} 1 \ if \ n = 1 \\ 0 \ if \ p^2 | n \ for \ some \ prime \ p \\ (-1)^r \ if \ n = \ p_1 p_2 ... p_r, where \ p_i \ are \ distinct \ primes \ . \end{cases}$$

It states that $\mu(n\ ) = 0 \ if \ n$ is not a free integer ,whereas $\mu(n) = (-1)^r$,if n is square free with r prime factors .

For example : $\mu(30)$ =$\mu(2 \times 3 \times 5) = (-1)^3 = -1.$ the first values of μ are $\mu(1) = 1 \times \mu(2) = -1 \times \mu(3) = 1 \times \mu(4) = 0 \times \mu(5) = -1 \times \mu(6) = \cdots$

If p be a prime number,it is clear that$\mu(p) = -1; in \ addition \ , \mu(p^k) = 0 \ for \ k \geq 2.$

Theorem :

Let $F \ and \ f$ be two number theoretic function related by the formula $F(n) = \sum_{d|n} f(d)$ then $f(n) = \sum_{d|n} \mu\left(d\right) F(\frac{n}{d}) = \sum_{d|n} \mu\left(\frac{n}{d}\right) F\left(d\right)$.

Theorem :

if F is a multiplicative function and $F(n) = \sum_{d|n} f(d)$ then f is also multiplicative.

CHAPTER-6

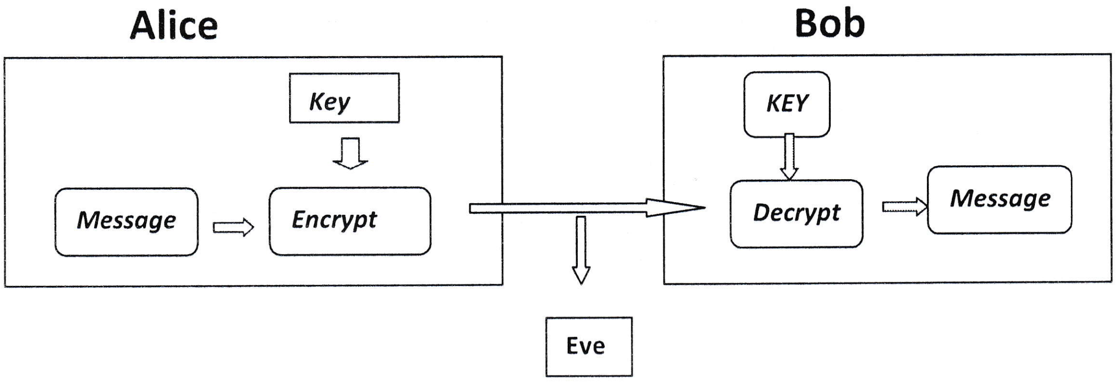
Application :

Cryptography : Application of number theory allow the development of mathematical algorithms that can make information (data) unintelligible to everyone except for intended users . In addition , mathematical algorithms can provide real physics security to data – allowing only authorized users to delete or update data. One of the problems in developing tools to crack encryption code involves finding ways to factor very large numbers . Advances in application of number theory , along with significant improvements in the power of computers , have made factoring large numbers less daunting.

Public key cryptography and RSA cryptosystem :

Public key cryptography and RSA cryptosystem two people , Alice and bob ,would like to exchange secret message ; however , eve is eavesdropping :

One technique would be to use an encryption technique based on an encryption key , but this poses a challenge : how do they exchange the encryption key without eve receiving it?



RSA Cryptosystem : The most common form of public key cryptosystem is RSA , which stands for Rivest ,Shamir , Adleman , who invented it. It based on modular arithmetic and large primes , its security comes from the computational difficulty of factoring large numbers.

The idea is as follow : select p and q to be large primes (at least several hundred digits) ; the degree of security is dependent of the size of p and q .Take $n = pq$. then the public key is a pair $k = (n, e)$ such that $\gcd(e, (p-1)(q-1)) = 1$.

The encoding function is : $f(m, k) \equiv m^e (mod\ n)$.

This assumes that the message can be represented by an integer $m < n$ with $\gcd(m, p) = \gcd(m, q) = 1$, if not we can break m down into smaller pieces and encode each individually.

The private key is a pair $k' = (n, d)$ such that $de \equiv 1(mod(p-1)(q-1))$.

The decoding function is :

$g(c,k') = c^d\ (mod\ n)$. the security of the algorithm lies in challenge of prime factorization : in order to calculate d , it is necessary to factor n to get $p\ amd\ q$, which is very difficult (exponential in the number of digits in $p\ and\ q$.

Theorem ;

Let $p\ and\ q$ be primes with $n = pq$ and let e be an integer such that $\gcd(e,(p-1)(q-1)) = 1, with\ ed = 1(mod(p-1)(q-1)$. let m be an integer with $m < n$ and $\gcd(m,p) = \gcd(m,q) = 1$.

Define $k = (n,e) and\ k' = (n,d)$, and the functions :

$f(m,k) = m^d(\ mod\ n)$.

$g(c,k) = c^e\ (mod\ n)$.

Then we claim that : $g(f(m,k),k') = m$.

Proof :

We have that

$$g(f(m,k),k') = (m^e\ mod\ n)^d\ mod\ n = m^{ed}\ mod\ n.$$

By the choice of e and d ,we have that : $ed \equiv 1(mod\ (p-1)(q-1))$.

Or, equivalently , for some integer s ,$ed = 1 + s(p-1)(q-1)$.

By Fermat's theorem ,$m^{p-1} \equiv 1\ (mod\ p)$ and $m^{q-1} \equiv 1\ (mod\ q)$, giving

$$m^{ed} \equiv m^{1+s(p-1)(q-1)} \equiv m \cdot (m^{p-1})^{s(q-1)} \equiv m \cdot 1^{s(q-1)} \equiv m\ (mod\ p).$$

Similarly ,$m^{ed} \equiv m \ (mod\ q)$. since $\gcd(p,q) = 1$ by Chinese remainder theorem ,$m^{ed} = m \ (mod\ pq)$ as required .

Note that we can apply the same argument to show that :

$$f(g(m,k'),k) = m\ .$$

Thus the owner of the private key can encrypt a message m using the private key, which can then be decrypted by anyone using the public key, and prove that only the private key owner could have encrypted it. This is basis of ***digital signature system.***

Example : Bob wants to receive message from Alice , so he selects two primes ,say $p = 43, q = 59$.(we choose small prime for feasibility of the examples ; in reality , they would be vastly larger.)then $n = pq = 2537\ and\ (p-1)(q-1) = 2436$. Then he picks $e = 13$, which has the property that : $\gcd(e,(p-1)(q-1)) = \gcd(13{,}2436) = 1$.

Bob then calculates $d = 937$, the inverse of $e\ mod\ 2436$

$$de \equiv 937 \times 13 \equiv 12181 \equiv 5 \times 2436 + 1 \equiv 1\ (mod\ 2436).$$

Bob publishes the public key $k = (2537{,}13)$.

Alice wants to send message “STOP” to bob using the *RSA* . she encodes this S→18, T→ 19, O→14, P→15 ,i.e,1819 1415 grouped into blocks of 4 . thus ,$m = m_1m_2 = 18191415$. Each block encrypted :

$$1819^{13}\ mod\ 2537 = 2081$$

$$1451^{13}\ mod\ 2537 = 2182$$

Then the encrypted message is 20812182. Bob has private key $k' = (2537{,}937)$, and computes ;

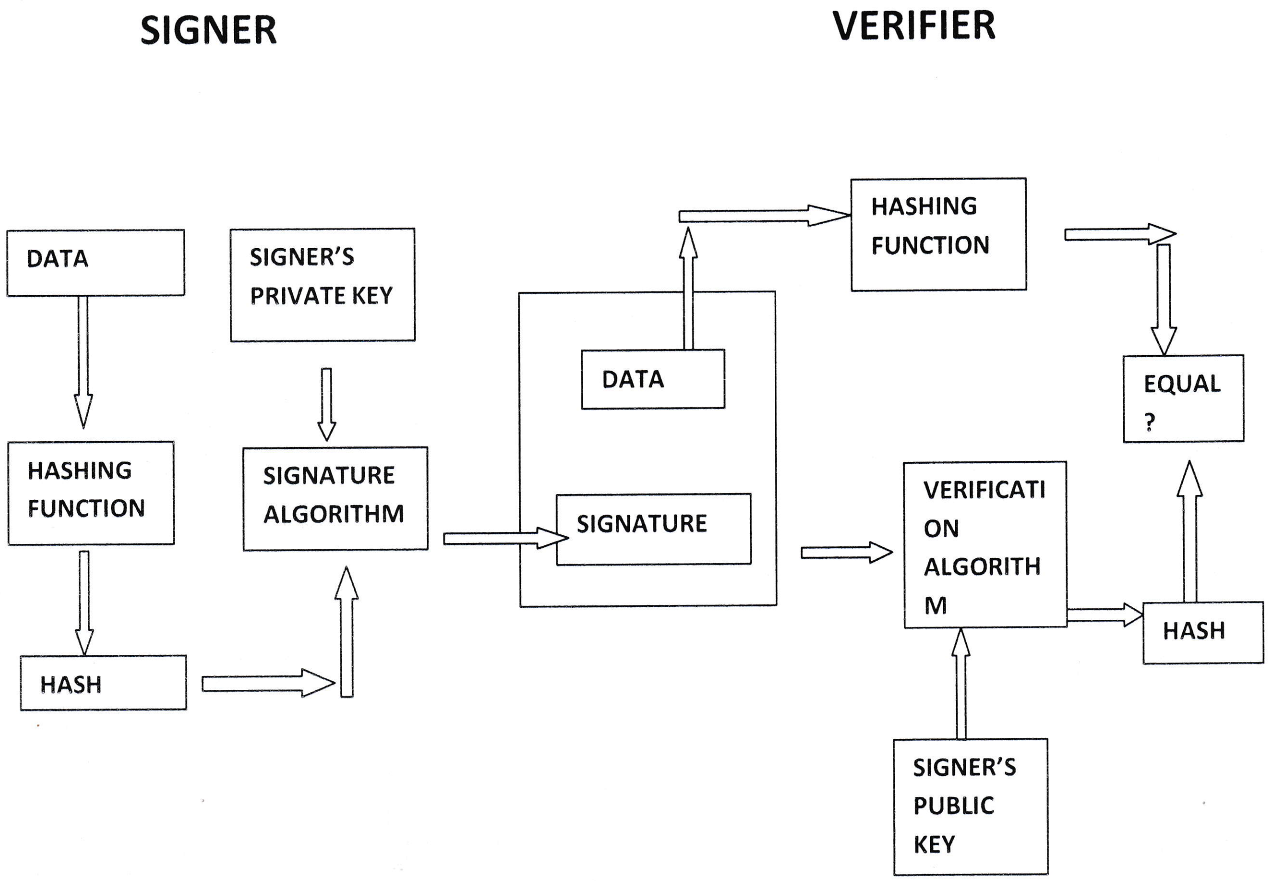
$$2081^{937} mod\ 2537 = 1819 \rightarrow ST$$

$$2812^{937}\ mod\ 2537 = 1415 \rightarrow OP$$

Thus , the original message was “STOP”.

Digital signature standard :

The DSA works in the frame work of public key cryptosystems and is based on the algebraic properties of modular exponentiation , together with the discrete problem , which is considered to be computationally intractable . The algorithm uses a key pair consisting of a public key and a private key . the private key is use to generate a digital signature for a message , and such a signature can be verified by using the signer’s corresponding public key. The digital signature provides message authentication (the receiver can verify the origin of the message),integrity (the receiver can verify that the message has not been modified since it was signed) and non-reputation (the sender cannot falsely claim that they have not signed the message).


SIGNER
VERIFIER
DATA
SIGNER'S PRIVATE KEY
HASHING FUNCTION
SIGNATURE ALGORITHM
HASH
DATA
SIGNATURE
HASHING FUNCTION
EQUAL ?
VERIFICATI ON ALGORITH M
HASH
SIGNER'S PUBLIC KEY

CONCLUSION

Number theory (or arithmetic or higher arithmetic in older usage)is a branch of pure mathematics devoted primarily to the study of the integers and integer – valued functions. German mathematician Carl Friedrich Gauss (1777-1855) said : “Mathematics is the queen of the sciences – and number theory is the queen of mathematics.”

Number theory has always fascinated amateurs as well as professional mathematicians . in contrast to other branches of mathematics ,many of the problems and theorems of number theory can be understood by Laypersons , although solutions to the problems and proofs of the theorems often require a sophisticated mathematical background.

REFERENCE

- GOOGLE
- WIKIPEDIA
- CHATGPT
- Math.brown.edu
- Site.uottawa.ca
- Etc.

THANK YOU