Study of Prime, Pseudoprime and applications of Pseudoprime

A. Ananth Maria Pushpa[a], and Dr.S.Subramanian[b]

[a] Department of Mathematics, PRIST Deemed to be University,
Thanjavur -613403.

[b]Head of the Department, School of Arts and Science, PRIST Deemed to be University,Thanjavur-613403.

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: The entire research paper is based on pseudoprime and their properties in the field of mathematics as well as the other fields.

In this paper we will discuss about the properties and results of numbers and some of the applications of pseudoprime in computer application,Cryptography .

Keywords: gcd,prime,pseudoprime,Fermat pseudoprime,cryptography.

1. Introduction

Number system plays an very important role not only in Mathematics but also in practical life.So only we define

"Mathematics is the queen of sciences and Theory of numbers is the queen of Mathematics".

Prime numbers are the very special one.A prime number is a natural number which is greater than 1 which has only two divisors 1 and itself.A number which is not prime is called the composite number.

Here, we see another number pseudoprime, also called Fermat's pseudoprime which is look like prime number but it satisfies the conditions of composite number.Consider 341 is look like prime ,but it has divisors like composite number.

ie)341=11 × 31.

By using Fermat's Little Theorem and Chinese Remainder Theorem,

We have the proof $2^{340} \equiv 1(mod\ 341)$.

This method of factorizing big digit numbers into small numbers used in encrypt the messages in cryptography.

Definition: Divisibility

An integer b is divisible by an integer a$\neq 0$ if there is an integer x such that b=ax,and we write a/b.

In case b is not divisible by a,we write a $\nmid$b.

Theorem:

1) a/b implies a/bc for any integer c .
2) a/b and b/c imply a/c.
3) a/b and a/c imply a/(bx+cy),for any integer x and y.
4) a/b and b/a imply . $a = \pm b$
5) a/b,a>0,b>0,imply $a \leq b$.
6) If $m \neq 0$,a/b implies and is implied by ma/mb.

Theorem: Division Algorithm

Given integers a and b with b>0 there exists unique integers q and r satisfying a=qb+r, $0 \leq r \prec b$.

The integers q and r are called ,the quotient and remainder respectively in the division of a by b.

Definition: Greatest Common Divisor

Let a and b be given integers,with atleast one of them different from zero.The greatest common divisor of a and b,denoted by gcd(a,b),is the positive integer d satisfying the following

i. d/a and d/b.
ii. If c/a and c/b then $c \leq d$.

Example:

gcd of 12 and 36

ie) gcd(12,36):

The positive common divisor of 12 and 36 are

1,2,3,4,6,12.

Here highest common divisor is 12.

$\therefore$ gcd(12,36)=12.

Definition: Relatively Prime

Two integers a and b, not both of which are zero,are said to be relatively prime whenever gcd(a,b)=1.

Example:

(i) gcd (8,11)=1.

Here there is no common divisors except 1,for 8 and 11.

(ii)gcd(7,15)=1.

Here also there is no common divisors except 1,for 7 and 15.

Euclid's lemma:

If a/bc ,with gcd(a,b)=1,then a/c.

Definition: Least Common Multiple

The least common multiple of two non zero integers a and b,denoted by lcm(a,b),is the positive integer m satisfying the followimg:

i. a/m and b/m.

ii. If a/c and b/c ,with $c \succ 0$,then $m \le c$.

Example:

i) lcm(15,20)=60.

The factors of 15 =$1 \times 3 \times 5$

And 20=$1\times 2 \times 2 \times 5$.

$\therefore$ $\mathrm{lcm}(15{,}20) = 2 \times 2\times 3 \times 5 = 60$

ii) lcm(3,12)=12.

The factors of 3 = 1×3 and

12=$1 \times 2 \times 2 \times 3$.

$\therefore$ lcm(3,12)=12.

Theorem:

For positive integers a and b, gcd(a,b) lcm(a,b) = ab.

Definition: Prime Number

An integer p>1,is called a prime number or simply a prime ,if it can be divided exactly only by 1 and itself.

Example:

2,3,5 and 7 are the prime numbers below 10.

Note:

i) The integer 1 plays a special role, being neither prime nor composite.

ii) The integer 2 is the only even prime.

iii) 4,6,8 and 9 are the composite numbers below 10.

Theorem:

Fundamental Theorem of Arithmetic

[Unique Factorization Theorem]

Every positive integer n>1 is either a prime or a product of primes,this representation is unique,apart from the order in which the factors occur.

Definition: a is congruent to b modulo m

If an integer m,not zero,divide the difference a-b,we say that a is congruent to b modulo m and write $a \equiv b(\bmod m)$.

If a-b is not divisible by m,we say that a is not congruent to b modulo m, and we write

$\mathrm{a} \not\equiv \mathrm{b}(\mathrm{mod\ m})$.

Example:

a=10, b=1, m=3.

Here, $10 \equiv 1(\bmod 3)$.

We say that,10 is congruent to 1.

Theorem:

Let a,b,c,d denote integers.

Then i)$\mathrm{a} \equiv \mathrm{b}\ (\mathrm{mod\ m}), \mathrm{b} \equiv \mathrm{c}(\mathrm{mod\ m})$, and $\mathrm{a} - \mathrm{b} \equiv 0(\mathrm{mod\ m})$,are equivalent statements.

ii)If $\mathrm{a}\equiv \mathrm{b}\ (\mathrm{mod\ m})$ and $\mathrm{b} \equiv \mathrm{c}\ (\mathrm{mod\ m})$, then $\mathrm{a} \equiv \mathrm{c}\ (\mathrm{mod\ m})$.

iii)If $\mathrm{a} \equiv \mathrm{b}(\mathrm{mod\ m})$ and $\mathrm{c} \equiv \mathrm{d}\ (\mathrm{mod\ m})$, then $\mathrm{a} + \mathrm{c} \equiv \mathrm{b} + \mathrm{d}\ (\mathrm{mod\ m})$.

iv)If $\mathrm{a} \equiv \mathrm{b}(\mathrm{mod\ m})$ and $\mathrm{c} \equiv \mathrm{d}(\mathrm{mod\ m})$, then $\mathrm{ac} \equiv \mathrm{bd}(\mathrm{mod\ m})$.

v)If $\mathrm{a} \equiv \mathrm{b}(\mathrm{mod\ m})$ and $\mathrm{d} / \mathrm{m}, \mathrm{d} > 0$, then $\mathrm{a} \equiv \mathrm{b}(\mathrm{mod\ d})$.

vi) $\mathrm{a} \equiv \mathrm{b}(\mathrm{mod}\ )$ then $\mathrm{ac} \equiv \mathrm{bc}(\mathrm{mod\ mc})$, for $\mathrm{c} \succ 0$.

Theorem:

The linear congruence $\mathrm{ax} \equiv \mathrm{b}(\mathrm{mod\ m})$ has a solution if and only if d / b, where $\mathrm{d} = \gcd(\mathrm{a}, \mathrm{m})$. If /b, then it has d mutually incongruent solutions modulo m.

Example:

The problem posed by sun-Tsu corresponds to the system of three congruences,

$x \equiv 2(\text{mod } 3)$

$x \equiv 3(\text{mod } 5)$

$x \equiv 2(\text{mod } 7)$.

Also ,

$n=3\times 5 \times 7 \times= 105$ and

$N_1 = \frac{n}{3} = 35$

$N_2 = \frac{n}{5} = 21$

$N_3 = \frac{n}{7} = 15$.

Now the linear congruences,

$35x \equiv 1(\text{mod } 3)$

$21x \equiv 1(\text{mod } 5)$

$15x \equiv 1(\text{mod } 7)$ are satisfy by

$x_1 = 2, x_2 = 1, x_3 = 1$,respectively.

Thus a solution of the system is given by, $x = 2.35.2 \ + 3.21.1 \ + 2.15.1$.

Corollary:

If gcd(a,m)=1,then the linear congruence $ax \equiv b(\text{mod m})$ has a unique solution modulo m.

Theorem:

Chinese Remainder Theorem

Let $m_1, m_{2,} ..., m_r$ be positive integers such that

$\gcd(m_i, m_j) = 1$,for $i \neq j$.

Then the system of linear congruences

$x \equiv a_1 (\text{mod } m_1)$

$x \equiv a_2 (\text{mod } m_2)$

.

.

.

, $x \equiv a_r (\text{mod } m_r)$,

has a simultaneous solution,which is unique modulo the integer $m_1, m_{2,} ..., m_r$.

Fermat's Little Theorem

Let p be a prime and suppose that p ∤a.Then $a^{p-1} \equiv 1(mod\ p)$.

Note:

i)Converse of Fermat's Little Theorem is not true.

Ii)Every prime number satisfies Fermat's Little Theorem,not every number that satisfies Fermat's Little Theorem is prime.

Corollary:

If p is prime,then $a^p \equiv a(mod\ p)$, for any integer a .

Lemma:

If p and q are distinct primes with $a^p \equiv a(mod\ q)\ and\ a^q \equiv a(mod\ p)$,then $a^{pq} \equiv a(mod\ pq)$.

Pseudoprimes

A composite or nonprime number n that fulfills a mathematical condition that most other composite numbers fail.The best known of these numbers are the Fermat pseudoprimes.

Or simply,pseudoprime is a probable prime that means it is not a actually prime but a partially prime.

Definition: Pseudoprime

We say that, n is a base a pseudoprime if $a^{n-1} \equiv 1(mod\ n)$.

Example:

Base 2 pseudoprime

561=3 × 11 × 17 is a base 2 pseudoprime.

$2^{561-1} = 2^{560} \equiv (2^2)^{280} \equiv 1 \text{ (mod 3)}$

$2^{560} \equiv (2^{10})^{56} \equiv 1(\text{mod } 11)$

$2^{560} \equiv (2^{16})^{15} \equiv 1(\text{mod } 17)$.

$\therefore \quad 2^{560} \equiv 1(\text{mod } 3.11.17)$.

$\therefore \quad 2^{560} \equiv 1(\text{mod } 561).$

Note:

i) When a=2,n is said to be a pseudoprime.

ii) Pseudoprime is a composite number n such that $\mathrm{n}/2^{\mathrm{n}} - 2$,and every prime number also has this property.

Examples:

i. 91 is the smallest pseudoprime to the base 3.

ii. 217 is the smallest pseudoprime to the base 5.

There are infinitely many pseudoprimes to any given base.

Result:

i) The smallest four pseudoprimes are 341,561,645,1105.

ii) There are only 247 pseudoprimes smaller than one million,in comparison with78498 primes.

iii) The first example of even pseudoprimes,namely the number,

161038=2.73.1103 was found in 1950.

Fermat Pseudoprimes

In number theory the Fermat pseudoprime make up the most important class of pseudoprimes that come from Fermat's little Theorem.

Definition:

Fermat's little theorem states that, if p is prime and a is coprime to p then $a^{p-1} -1$ is divisible by p.

For an integer a>1,if a composite integer x divides $a^{x-1} - 1$, then x is called a Fermat pseudoprime to base a.

Problem:

Is the number 1729 is a pseudoprime?

Solution:

The required condition is, $\mathrm{n}/2^{\mathrm{n}} - 2$.

x≡ 1 (mod 19),i.e)$2^{n} \equiv 2(mod\ n)$

$2^{n-1} \equiv (mod\ n)$

and gcd (2,n)=1.

We want to show that, $2^{1728} \equiv 1\ (mod\ 1729)$

Now,

1729=7$\times$ 13 $\times$ 19.

Using Chinese Remainder Theorem,we've

x ≡ 1 (mod 7)

x ≡ 1 (mod 13)

$\mathbf{x \equiv 1(mod\ 19)}$

and that x is a solution of mod 1729.

Buy using Fermat's Theorem,

$2^{6} \equiv 1\ (mod\ 7)$

$2^{12} \equiv 1\ (mod\ 13)$

$2^{18} \equiv 1(mod\ 19)$

$\therefore 2^{1728} \equiv 1\ (mod\ 7.13.19).$

Thus,

$$\mathrm{x} \equiv 2^{1728}, \text{is a solution to the system m.}$$

$\therefore 2^{1728} \equiv 1(\text{mod } 1729).$

Applications of Pseudoprime

Pseudoprimes are playing an important role in public-key cryptography,which makes use of the difficulty of factoring large numbers into their prime factors.

What is Cryptography?

In practical life cryptography contains a range of situation like email and file storage using pretty Good privacy(PGP),free ware,Cash withdrawl from an ATM,pay TV,secure web browsing,and use of a GSM mobile phone

Definition: Cryptography

Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.

Cryptography is the study about secure informations techniques that allow only the sender and intended recipient of a message to view its hidden contents.

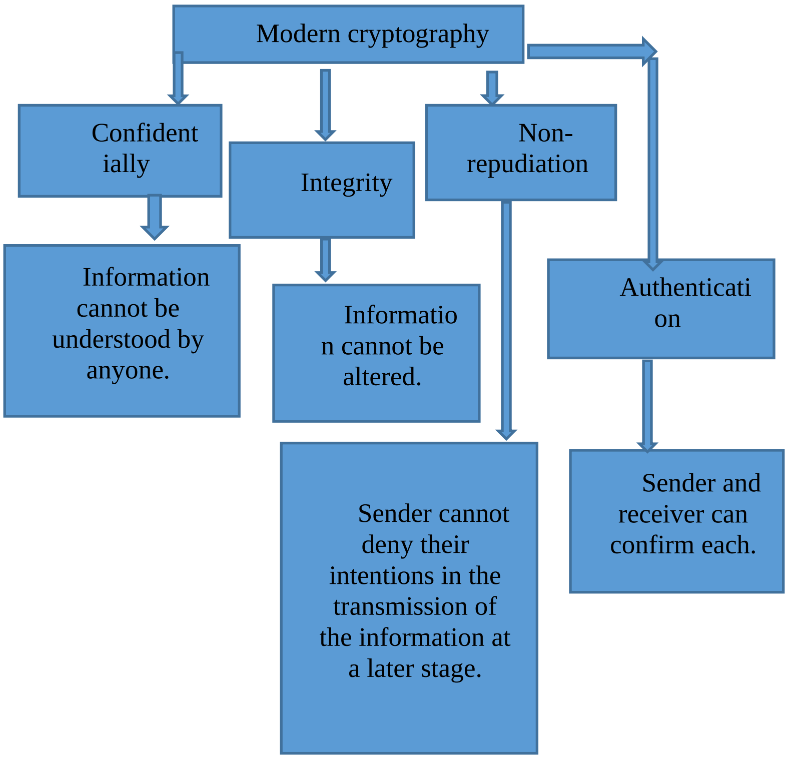
Here ,data is encrypted using a secret key,and then both the encoded messages and

Secret keys are sent to the recipient for decryption.

Uses of Cryptography

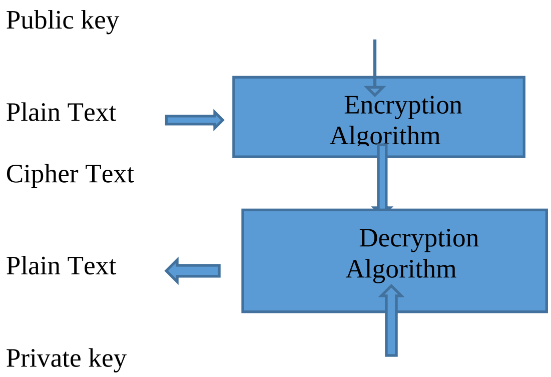
1. Cryptography has been an important technique of warfare for a long time.It is a way a military can securely transmit messages without its
enemies interceting the messages.Even if the enemy intercepts the mesage,it must decrypt the messages,so it's actually suseful.
2. Cryptography can be used to protects data from theft or altertion,and also for user authentication.
3. In earlier stage cryptography was effectively synonyms with encryption but nowadays cryptography is mainly based on mathematical theory and computer science practice.

Pictorial Representation

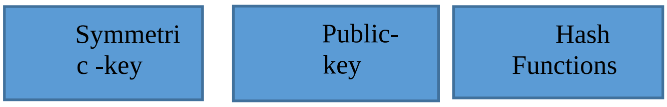

Modern cryptography
Confidentially
Integrity
Non-repudiation
Authentication
Information cannot be understood by anyone.
Information cannot be altered.
Sender cannot deny their intentions in the transmission of the information at a later stage.
Sender and receiver can confirm each.

Cryptography is commonly used in banking transactions cards,computer passwords,and e-commerce transactions.

Technique of Cryptography



Types of cryptography Techniques



Symmetric-key Cryptography:
Both the sender and receiver share a single key.The sender uses this key to encrypt plain text and send the cipher text to the receiver.The receiver also applies the same key to decrypt the message and recover the plain text.
Public-key Cryptography:

In Public- key Cryptography two related keys are used namely public and private key.Public key may be freely distributed,while its paired private key,remains secret.
The public key is used for encryption and private key is used for decryption.

Hash Functions:

No key is used in this algorithm.A fixed-length hash value is computed as per the plain text that makes it impossible for the plain text to be recovered.

Hash functions are also used by many operating systems to encrypt passwords.

Used mathematics behind the Cryptography

Examples:

i. QR code: QR code is one of the main application in Cryptography.

QR-Quick Response:They are capable of storing lots of data though they look simple.But no matter how much they contain,when scanner the QR code should allow the user to access the information instantly,that is why it is called a Quick Response Code.

ii)Bar code:

Bar code is the another example of cryptography.

A bar code encodes a sequence of digits or letters as a series of light and dark bars.The bars act like bits in a binary encoding ---- the presence of a bar is equivalent to 1,and the absence of a bar is equivalent to 0.

It contains three parts .Each part contains each information.

The first part tells us the country code where it was issued.

The second part tells us the manufacturer of the product.

The third part identifies the product itself.

Iii)ISBN numbers for published books

Consider the ISBN ,take first 9 digits and assign the values 0 to 9 from left to right .Find the sum of the product of the digits,which is congruent to modulo 11,and the final value is the valid ISBN number.

Conclusion:

In this paper we discussed about the numbers,property of numbers,Prime number,Pseudoprime and also the application of number theory in computer application .In future
we will see the detailed concept of pseudoprime,carmichael number and strong pseudoprime.

References

[1] David M. Burton:Elementary Number Theory.

[2] Ivan Niven,Herbert S.Zuckerman,Hugh L.Montgomery:An introduction to Theory of Numbers

[3] Emily Riemer,MATH0420:Pseudoprimes and Carmichael numbers.

[4] The Economic Times,E- Paper.

[5] R.LIDL and W.B.MULLER :Primality testing with lucas functions,Advances in cryptology-AUSCRYPT ‘92.