International Journal of Multidisciplinary Research and Growth Evaluation.

Evaluation of quadratic residue with the help of Legendre symbol

SP Behera [1*], S Pattnaik [2]
[1] Assistant Professor, Department of Mathematics, CV Raman Global University, Bhubaneswar, Odisha, India
[2] Student, Department of Mathematics, CV Raman Global University, Bhubaneswar, Odisha, India

* Corresponding Author: **SP Behera**

Article Info

ISSN (online): 2582-7138
Volume: 03
Issue: 02
March-April 2022
Received: 25-02-2022;
Accepted: 10-03-2022
Page No: 194-199
DOI: https://doi.org/10.54660/anfo.2022.3.2.7

Abstract
Cryptography is the study of "Mathematical Systems," which includes two types of security protocols: privacy and authentication. Quadratic residue, a mathematical notion from the discipline of number theory known as Modular arithmetic, is extremely valuable in cryptography. Cryptography is deals with huge numbers, such as integers system with millions of digits or more. In this case, the Legendre symbols may be used to determine if an integer "x" has quadratic residue modulo "p" when p is Prime.
This research article explains the mathematical ideas of quadratic residue, Fermat's little theorem, Euler's criteria, and the Legendre symbols.
The main goal of this article is to explore the calculation problem of the number of solutions for one kind congruence equation modulo p (an odd prime) using simple methods and character sum properties, and to provide some interesting identities and asymptotic formulas for it.

Keywords: Cryptography, Mathematical Systems, quadratic, Legendre

1. Introduction
The information flows between sender and receiver through an insecure network in such a way manner that the challenger (any third user) cannot understand what is being transferred is known as cryptography. The real information that the sender wishes to convey is referred to as "Plaintext," and the sender changes this plaintext into "Cipher text" (using various ways) by applying Key to it. This cypher text is extremely tough to decipher; mathematical expertise is required. This encrypted text is transformed to plaintext at the receiver by applying a key (same or different) to it, allowing the recipient to read it. The process of converting plaintext to cypher text is known as encryption, while the process of converting cypher text to plaintext is known as decryption.
A cryptosystem is a set of algorithms that transforms ordinary text to cypher text and back. The cryptosystems are of two types: symmetric cryptosystems and asymmetric cryptosystems.
In both the encryption and decryption processes, symmetric cryptosystems employ a common secret key. DES (Data Encryption Standard), AES (Advanced Encryption Standard), and Blowfish are a few examples. It has a few drawbacks, including key distribution, a compromised KDC (Key Distribution Center), random number generation, and encryption function location.
There is no requirement for a shared secret in an asymmetric cryptosystem since it employs a public key for encryption and a private key for decryption. Diffie-Hellman, RSA, and Elgamal are examples of this.
All of the strategies employed here are based on number theory and discrete logarithms. In particular, integer factorization and modular arithmetic are fundamental in number theory. The mathematical ideas of the quadratic residue, Fermat's little theorem, Euler's criteria, and Legendre and Jacobi symbol are presented in this work. On the other hand, in certain cases, the Jacobi Symbol fails to yield the proper answer, posing a restriction for estimating the quadratic residue.

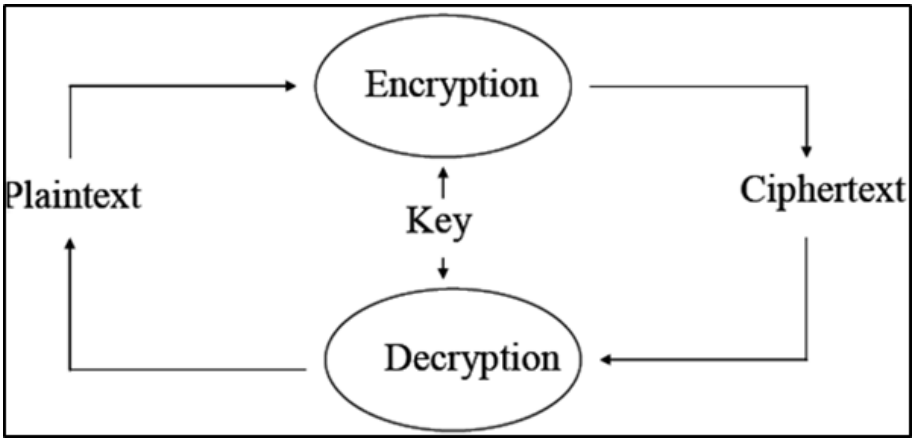

Fig 1

Let $p \geq 3$ be a prime number. The Legendre's symbol (m) modulo p is defined as follows for every integer x.

$$\frac{m}{p} = \begin{cases} 1, if\ (m,p) = 1\ and\ m\ is\ a\ quadratic\ residue\ modulo\ p \\ -1, if\ (m,p) = 1\ and\ m\ is\ a\ quadratic\ non\ residue\ modulo\ p \\ 0, if\ p|m \end{cases}$$

This arithmetic function is particularly significant in elementary number theory and analytic number theory, and it is intimately connected to many classical number theory issues, such as the least quadratic non-residue problem, the class number formula of the quadratic field, and the prime number structure. In specifically, if p is a prime and p ≡1 mod 4 is a prime, we get the identity.

$$p = \left(\sum_{x=1}^{p-1/2}\left(\frac{x+\bar{x}}{p}\right)\right)^2 + \left(\sum_{x=1}^{p-1/2}\left(\frac{x+r.\bar{x}}{p}\right)\right)^2 \equiv \alpha^2(p) + \beta^2(p)$$

In the case when r is any quadratic residue modulo p,and $x.\bar{x} \equiv 1\ mod\ p$.
The Legendre's symbol has many unique and significant qualities on its own, besides to its vast range of uses. One of these is the quadratic reciprocity law. To put it another way, for any two odd primes a and b with a ≠ b, we have the identity.

$$\left(\frac{b}{a}\right).\left(\frac{a}{b}\right) = (-1)^{(a-1)(b-1)/4}$$

In this paper, we will look at a basic number theory issue linked to the k-th residue modulo p, specifically the quadratic residue modulo p.
For every positive integer m with gcd (m, p) = 1, assume that i, j =± 1, and M(n, i, j; p) denote the number of congruence equation solutions m ≡ c + d mod p (1 ≤ c, d ≤ p − 1) such that (c/p) = i and (d/p) = j.

2. Fermat's little Theorem
Fermat's little theorem has two applications. The first version is suitable to everybody, whereas the second has limitations.
Form 1: It claims that if p is a prime number, then $x^p - x$ is an integer multiple of p for every integer x. In modular arithmetic notation, this is written as.

$$x^p \equiv x\ (mod\ p) \qquad (1)$$

Example (2.1) x=3, p=5

$x^p - x = 3^5 - 3$
$= 243 - 3$
$= 240$
$= 5 \times 48$ ← (It is p)

$x^p \equiv x\ (mod\ p)$
$3^5 mod\ 5 \equiv 3\ (mod\ 5)$
$243\ mod\ 5 \equiv 3\ (mod\ 5)$
$3 \equiv 3$ ← condition satisfy

Form 2:- $x^{p-1} - 1$ is an integer multiple of P if p does not divide x, where p is a prime number. It is written in modular arithmetic notation as

$$x^{p-1} \equiv 1 \ (mod\ p) \tag{2}$$

Example (2.2) x=3, p=5

$x^{p-1} - 1 = 3^{5-1} - 1$

$= 81 - 1$

$= 80$

$= 5 \times 16$ ↔ (It is p)

$x^{p-1} \equiv 1 \ (mod\ p)$

$3^{5-1} mod\ 5 \equiv 1 \ (mod\ 5)$

$81\ mod\ 5 \equiv 1 \ (mod\ 5)$

$1 \equiv 1$ ↔ condition satisfy

Example (2.2) x =12, p=2

form1

$x^p - x = 12^2 - 12$

$= 144 - 12$

$= 132$

$= 2 \times 61$ ↔ (It is p)

$x^p \equiv x \ (mod\ p)$

$10^2 \equiv 10 \ (mod\ 2)$

$0 \equiv 0$ ↔ Condition satisfy

form 2

$x^{p-1} - 1$

$= 12^{2-1} - 1$

$= 11$

$= Not\ possible\ to\ represented\ in\ multiples\ of\ 2$

In this problem **x/p=12/2=6,**

x mod p=12 mod 2=0

i.e. p totally divides x, so Form 2 cannot be used

3. Quadratic Residue

Assume that x ∈ N and p is an odd prime number such that gcd(p,x) = 1. If x is a perfect square modulo p, then x is termed a quadratic residue modulo p. i.e. there is a number y such that,

$$y^2 \equiv x \ (mod\ p) \tag{3}$$

If equation (1) has no solution, x is referred to as a quadratic non residue modulo p. (that is there exist no perfect square)
Example (3.1): Now to justify that 8 is a quadratic residue modulo 17.

First we find

5 mod 11 = 5

We must determine y^2 such a way that

$$y^2 \equiv 5 (mod\ 11)$$

So, we will find square of all the numbers in z_{11} set and find each square modulo 11 then we find that.

$$4^2 \equiv 5 (mod\ 11)$$

Here x=5 and p=11 and we conclude that x is quadratic residue modulo p.
Example (3.1): Let us find if 2 is quadratic residue modulo 3

First we find

2 mod 3 = 2

We have to find out y^2 such that

$$y^2 \equiv 2\ (mod\ 3)$$

So, we get the square of all the integers in the z_3 set and each square modulo 3, and we discover that there is no such thing as a perfect square. We conclude that an is quadratic non residue modulo p for a=2 and p=3.
For large integers, determining if an is quadratic residue modulo p becomes a lengthy operation. As a result, we must first determine if such a y exists that meets the requirements of $y^2 \equiv x\ (mod\ p)$
The Legendre sign can be used to do this. However, we must first comprehend Euler's criteria, which is presented in the next section.

4. Euler's Criterion
If P is an odd prime number and x is any positive integer, x is quadratic residue modulo p if and only if,$x^{(p-1)/2} \equiv 1\ (mod\ p)$
If x is a quadratic non-residue modulo p function, then

$$x^{(p-1)/2} \equiv -1\ (mod\ p)$$

x is said to be a multiple of p if the following congruence is satisfied

$$x^{(p-1)/2} \equiv 0\ (mod\ p)$$

Example (4.1): a=5, p=11

$$5^{(11-1)/2} \equiv 1\ (mod\ 11)$$
$$5^5 \equiv 1\ (mod\ 11)$$
$$1 \equiv 1$$

As a result, we may claim that x is quadratic residue modulo p.

Example (4.2): a=2, p=3

$$2^{(3-1)/2} \equiv -1\ (mod\ 3)$$
$$2^1 \equiv -1\ (mod\ 3)$$
$$2 \equiv 2$$

As a result, we may claim that x is quadratic non residue modulo p.

Example (4.3): x=14, p=7

$$14^{(7-1)/2} \equiv 0\ (mod\ 7)$$
$$14^4 \equiv 0\ (mod\ 7)$$
$$0 \equiv 0$$

As a result, we may claim that x is a multiple of p.

5. Legendre symbol
Assuming p is an odd prime number, the Legendre symbol $\frac{x}{p}$ is defined as follows for any integer x.

$$\left(\frac{x}{p}\right) = (x|p) \equiv \begin{cases} 0\ If\ p|x \\ 1\ if\ x\ is\ a\ quadratic\ residue\ modulo\ p \\ -1\ if\ x\ is\ a\ quadratic\ residue\ modulo\ p \end{cases}$$

Example (5.1): x=4, p=5

$$\left(\frac{x}{p}\right) = \left(\frac{4}{5}\right) = x^{(p-1)/2}(mod\ p) \ldots\ldots\ldots x^{(p-1)/2} \equiv 1\ (mod\ p)$$
$$= 4^{(5-1)/2}(mod\ 5)$$
$$= 4^2(mod\ 5)$$
$$= 4\ (mod\ 5)$$
$$= -1\ (mod\ p)$$

It shows that x is non-residue with modulo p.

Example (5.2): x=2, p=5

$$\left(\frac{x}{p}\right) = \left(\frac{2}{5}\right) = x^{(p-1)/2}(mod\ p) \ldots\ldots\ldots x^{(p-1)/2} \equiv -1\ (mod\ p)$$
$$= 2^{(5-1)/2}(mod\ 5)$$
$$= 2^2(mod\ 5)$$
$$= 16\ (mod\ 5)$$
$$= 1\ (mod\ p)$$

As a result, we may claim that x is an quadratic residue modulo p.

6. Conclusion

Cryptography has been developed on the mathematical notion of creating difficult problems in order to improve the efficiency of cryptographic algorithms. One such crucial notion in cryptography is quadratic residue. In this work, we show how to use the Legendre symbols to determine where an integer an is quadratic residue modulo p (p is prime). Also, using an example, we demonstrated that the findings of the Legendre Symbol do not always correspond with the real predicted results of quadratic residue

7. References

1. WP Zhang, HLLi. Elementary Number Theory, Shaanxi Normal University Press, Xi'an, China, 2013.
2. SP Behera, AC Panda. Nature Of Diophantine Equation $4^x + 12^y = z^2$, International Journal of Innovative Research in Computer Science and Technology (IJIRCST). 2021; 09(6):11-12.
3. L Chen, JY Hu. A linear recurrence formula involving cubic Gauss sums and kloosterman sums, Acta Mathematica Sinica (Chinese Series). 2018; 61:67-72.
4. WP Zhang, JY Hu. The number of solutions of the diagonal cubic congruence equation mod p, Mathematical Reports. 2018; 20:70-76.
5. BC Berndt, RJ Evans. The determination of Gauss sums, Bulletin of the American Mathematical Society. 1981; 5(2):107-130.
6. S Chowla, J Cowles, M Cowles. On the number of zeros of diagonal cubic forms, Journal of Number Theory. 1977; 9(4):502-506.
7. K Ireland, M Rosen. A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, NY, USA, 1982.