The Mathematics Education ISSN 0047-6269
Volume - LVIII, No. 2, June 2024
Journal website: www.internationaljournalsiwan.com
ORCID Link: https://orcid.org/0009-0006-7467-6080
Google Scholar: https://scholar.google.com/citations?hl=en&user=UOfM8B4AAAAJ
Refereed and Peer-Reviewed Quarterly Journal

Quadratic residues, Non-residues and Some Consequences

by **Ram Babu Singh,** *Research Scholar,*
P.G. Department of Mathematics,
Jai Prakash University, Chapra - 841301, India

(Received: May 28, 2024; Accepted: June 18, 2024; Published Online: June 28, 2024)

Abstract:

Here we shall discuss the quadratic congruence in one variable. The general form of quadratic congruence is $ax^2 + bx + c \equiv 0 \pmod{n}$.

Where a is not divisible by n, and a, b, c are integers.

For Quadratic residues and non-residues, we can reduce the above equation in the form

$$x^2 \equiv a \pmod{p} \quad \text{(i)}$$

Where p is a odd prime, a is an integer which is Co-prime to p i.e $(a, p) = 1$ or $p \nmid a$.

The congruence of the above form (i) has two solutions. Let us try to solve, the congruence.

Let x_0 be the solution, then

$$x_0^2 \equiv a \pmod{p} \tag{ii}$$

Also $(p - x_0)$ satisfy the congruence

$$\Rightarrow (p - x_0)^2 \equiv a \pmod{p} \qquad [\because (p - x_0)^2 \equiv (-x_0)^2 \pmod{p}]$$

implies x_0 and $(p - x_0)$ are two solutions of the above congruence.

If possible, let x_1 be the third solution of the above congruence, then from (i)

$$x_1^2 \equiv a \pmod{p} \tag{iii}$$

using (ii),

$$x_1^2 \equiv x_0^2 \pmod{p}$$

$$\Rightarrow p \text{ divides } (x_1 - x_0) \text{ or } (x_1 + x_0)$$

In first case

$x_1 \equiv x_0 \pmod{p}$, and in the 2nd case

$x_1 \equiv p - x_0 \pmod{p}$

x_1 is the same, not distinct solution our assumption is wrong. In fact, we have exactly two solutions.

Now for the Quadratic residues and non-residues of the above equation (i)

(a) If the equation (i) is solvable, then 'a' is quadratic residue mod p.

(b) If the above equation (i) has no solution then 'a' is quadratic non-residue mod p.

Example: The quadratic residues mod 5 are 1 and 4 whereas 2 and 3 are non-residues.

In case of quadratic residues and non-residues, we have some fundamental problems arise here.

Problem (i): For a given prime number p, we have to determine in which 'a' are quadratic residues or non-residues of prime p.

Problem (ii): For a given number 'a' we have to determine those prime p for which 'a' is a quadratic residues and those for which 'a' is a quadratic non-residues.

For solving problem (i), we give some methods. For this let us try to find out the quadratic residues of prime $p = 13$.

Let us consider the squares as

$$1^2 = 1,\ 2^2 = 4,\ 3^2 = 9,\ 4^2 = 3,\ 5^2 = 12,\ 6^2 = 10$$

and the next half of the squares are congruent to the numbers in reverse order.

$$7^2 = 10,\ 8^2 = 12,\ 9^2 = 3,\ 10^2 = 9,\ 11^2 = 4,\ 12^2 = 1$$

therefore, quadratic residues of 13 are

1, 4, 9, 3, 12, 10, after arranging,

1, 3, 4, 9, 10, 12 as $12^2 \equiv 1 \pmod{13}$

and the Quadratic non-residues are

2, 5, 6, 7, 8, 11

Both are equal in number.

Illustration:

The above example illustrate the following theorems.

Theorem 1: In reduced system of odd prime p there are exactly $\frac{1}{2}(p-1)$ quadratic residue of p and other $\frac{1}{2}(p-1)$ integers are the quadratic non-residue of p and the quadratic residues belong to the system containing the squares

$$1^2, 2^2, 3^2, \ldots, (p-1)^2$$

Proof: Suppose p is an odd prime and the congruence $x^2 \equiv a \pmod{p}$, $p \nmid a$, is solvable, then its solution must be congruence modulo p to some integer of reduced residue system $\pm 1, \pm 2, ..., \pm(p-1)$ of p, then any integer congruent to one of the following integers

$1^2, 2^2, 3^2, ..., \left(\frac{p-1}{2}\right)^2$ is a quadratic residue of p. It is clear that the reduced residue system of p, except the integers congruent to one of the integers, are all quadratic non-residue of p. But no two of the number, are congruent to each other mod p, for if $i^2 \equiv j^2 \pmod{p}$ with $1 \le i \le \frac{p-1}{2}$, $1 \le j \le \frac{p-1}{2}$

then $i^2 - j^2 \equiv \pmod{p}$

$\Rightarrow (i+j)(i-j) \equiv 0 \pmod{p}$. So either

$i+j \equiv 0 \pmod{p}$, $\quad i-j \equiv 0 \pmod{p}$.

It is impossible as $i+j$ and $i-j$ both are numerically less than p.

Since $(p-k)^2 \equiv k^2 \pmod{p}$, every quadratic residue is congruent mod p to exactly one of the numbers.

Proved.

Theorem 2: If p is an odd prime, and a is an integer where $(a, p) = 1$, then either $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$

Proof: Applying Fermat's little theorem, we have

$$a^{p-1} \equiv 1 \pmod{p}$$

$$\Rightarrow \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod{p}$$

then either p divides $\left(a^{\frac{p-1}{2}} - 1\right)$ or p divides $\left(a^{\frac{p-1}{2}} + 1\right)$, but can not divide both, as in the case $\left(a^{\frac{p-1}{2}} + 1\right) - \left(a^{\frac{p-1}{2}} - 1\right) = 2$, which is divisible by p. But it is impossible.

Example: Find the quadratic residues and non-residues of 13.

Solution: As (2, 13) = 1

Also $2^{\frac{13-1}{2}} = 2^6 = 64$

But $64 \equiv 12 \pmod{13}$

$\equiv -1 \pmod{13}$

2 is the quadratic non-residue of 13.

Also (3, 13) = 1

But $3^{\frac{13-1}{2}} = 3^6 = (3^3)^2 = (27)^2$

But $(27)^2 \equiv 1^2 \pmod{13}$

$\equiv 1 \pmod{13}$

3 is a quadratic residue of 13.

Proved.

Some Consequences:

If two integers a and b are relatively prime with an odd integer p i.e. $(a, p) = 1$, $(b, p) = 1$.

We have

(1) a and b are both quadratic residues or both are quadratic non-residues of p, then the product of a and b i.e. $a\,b$ is a quadratic residue of p.

(2) When one of a, b is a quadratic residues of p and other is a non-residue, then $a\,b$ is quadratic non-residue of p.

References:

1. George E. Andews : Number theory, Hindustan Publication Corp, N. Delhi, 1984.

2. T.M. Apostal : An Introduction to analytic number theory, Narosa Publishing House, New Delhi.

3. H. Rade Macher : Lecture on elementary number theory, Blais dell, New York, 1964.