RP-178: A Study on Standard Quadratic Congruence of Prime Modulus having Solutions Consecutive- Integers

Prof B M Roy
Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist: Gondia, M. S., India. Pin: 441801
(Affiliated to R T M Nagpur University)

ABSTRACT
Here in this paper, the author studies on standard quadratic congruence of prime modulus whose solution-pair is consecutive integers. The author has formulated the construction of such quadratic congruence of prime modulus and also formulated the solutions of the congruence. Such congruence can now be formed and solved orally within a very short time.

This is the merit of the paper.

KEY- WORDS and PHRASES
Composite modulus, Middle-pair solutions, Prime modulus, Quadratic congruence.

INTRODUCTION
A standard quadratic congruence of prime modulus: \( x^2 \equiv a \pmod{p} \), \( p \) being an odd prime, is said to be solvable, if \( a \) is quadratic residue of \( p \) i.e. \( a \equiv b^2 \pmod{p} \) or can be written so, by adding \( kp \) to \( a \) i.e. \( b^2 = a + kp \), for some integer \( k \). Then the congruence:

\[ x^2 \equiv b^2 \pmod{p} \]

has exactly two solutions \( x \equiv \pm b \pmod{p} \) i.e. \( x \equiv b, p - b \pmod{p} \) [1], [2], [3].

These solutions may not be consecutive integers.

In this paper, the author wishes to study the standard quadratic congruence of prime modulus having solutions which are consecutive integers.

PROBLEM-STATEMENT
Here the problem is-

“To construct (frame) a standard quadratic congruence of prime modulus of the type:

\[ x^2 \equiv a \pmod{p}; \ p \text{ an odd prime} \].

LITERATURE REVIEW
Standard quadratic congruence of prime and composite modulus are generally studied in degree colleges in mathematics stream. It is a part of Elementary Number Theory [1], [2], [3]. Much has been researched on it. Even much has been remained to research.

The author has formulated many standard quadratic congruence of prime and composite modulus [4], [5], [6], [7], etc. Also has discovered three new methods of solving standard quadratic congruence of prime modulus [8], [9], [10]. In continuation of his research journey, the author has presented here in this paper a new quadratic congruence with solutions consecutive integers.
ANALYSIS & RESULTS

The analysis is done in two cases: \( p \equiv 3 \pmod{4} \) & \( p \equiv 1 \pmod{4} \).

Case-I: Let \( p \equiv 3 \pmod{4} \).

Then, \( p - 3 = 4k \), for some integer \( k \).

Adding 4 to both sides, one get:
\[
p - 3 + 4 = 4k + 4 \quad \text{i.e.} \quad p + 1 = 4(k + 1) \quad \text{i.e.} \quad \frac{p+1}{4} = k + 1, \text{an integer}.
\]

The non-zero residue system of \( p \) is the set: \( \{1, 2, 3, 4, ..., \frac{p-1}{2}, \frac{p+1}{2}, ..., ..., (p - 1)\} \).

The pair \( \left(\frac{p-1}{2}, \frac{p+1}{2}\right) \) is the middle- pair and consecutive integers. Also every member of the above set is a solution of any quadratic congruence of prime modulus \( p \).

Then, for the solutions: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod{p} \), the corresponding standard quadratic congruence is seen to be:
\[
x^2 \equiv \left(\frac{p-1}{2}\right)^2 \pmod{p} \\
\equiv \frac{p^2-2p+1}{4} \pmod{p} \\
\equiv \frac{1}{4} \pmod{p} \\
\equiv \frac{p+1}{4} \pmod{p}
\]

Thus, if \( p \equiv 3 \pmod{4} \), then the required quadratic congruence is:
\[
x^2 \equiv \left(\frac{p+1}{4}\right)^2 \pmod{p} \text{ with the solutions: } x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod{p}.
\]

Case-II: Let \( p \equiv 1 \pmod{4} \).

Then, \( p - 1 = 4k \), for an integer \( k \). Multiplying by 3 to both sides, one get
\[
3p - 3 = 12k
\]

Adding 4 to both sides one get \( 3p - 3 + 4 = 12k + 4 \quad \text{i.e.} \quad \frac{3p+1}{4} = 3k + 1, \text{an integer}.
\]

The non-zero residue system of \( p \) is as before: \( \{1, 2, 3, 4, ..., \frac{p-1}{2}, \frac{p+1}{2}, ..., ..., (p - 1)\} \).

The pair \( \left(\frac{p-1}{2}, \frac{p+1}{2}\right) \) is the middle- pair and consecutive integers. Also every member of the above set is a solution of any quadratic congruence of prime modulus \( p \).

Then, for the solutions: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod{p} \), the corresponding standard quadratic congruence is seen to be:
\[
x^2 \equiv \left(\frac{p-1}{2}\right)^2 \pmod{p} \\
\equiv \frac{p^2-2p+1}{4} \pmod{p} \\
\equiv \frac{1}{4} \pmod{p} \\
\equiv \frac{3p+1}{4} \pmod{p}
\]

Thus, if \( p \equiv 1 \pmod{4} \), then the required quadratic congruence is:
\[ x^2 \equiv \frac{3p+1}{4} \pmod p \text{ with the solutions } x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod p. \]

**RESULTS**

The results can be stated as:

For every odd prime, there exists a standard quadratic congruence of prime modulus whose solutions are consecutive integers.

**ILLUSTRATIONS**

**Example-1**) Consider a prime \( p = 19 \).

It is of the type: \( p = 19 \equiv 3 \pmod 4 \).

Then the quadratic congruence having solutions consecutive integers is:

\[ x^2 \equiv \frac{3p+1}{4} \pmod p \]
\[ \equiv \frac{19+1}{4} \pmod 19 \]
\[ \equiv 5 \pmod 19 \]

Therefore, \( x^2 \equiv 5 \pmod 19 \) has solutions which are consecutive integers.

These solutions are: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \equiv 9, 10 \pmod 19 \).

**Example-2**) Consider a prime \( p = 17 \).

It is of the type: \( p = 17 \equiv 1 \pmod 4 \).

Then the quadratic congruence having solutions consecutive integers is:

\[ x^2 \equiv \frac{3p+1}{4} \pmod p \]
\[ \equiv \frac{51+1}{4} \pmod 17 \]
\[ \equiv 13 \pmod 17 \]

Therefore, \( x^2 \equiv 13 \pmod 17 \) has solutions which are consecutive integers.

These solutions are: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \equiv 8, 9 \pmod 17 \).

**Example-3**) Consider a prime \( p = 41 \).

It is of the type: \( p = 41 \equiv 1 \pmod 4 \).

Then the quadratic congruence having solutions consecutive integers is:

\[ x^2 \equiv \frac{3p+1}{4} \pmod p \]
\[ \equiv \frac{123+1}{4} \pmod 41 \]
\[ \equiv 31 \pmod 41 \]

Therefore, \( x^2 \equiv 31 \pmod 41 \) has solutions which are consecutive integers.

These solutions are: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \equiv 20, 21 \pmod 41 \).

**Example-4**) Consider a prime \( p = 503 \).

It is of the type: \( p = 503 \equiv 3 \pmod 4 \).

\[ x^2 \equiv \frac{3p+1}{4} \pmod p \]
Then the quadratic congruence having solutions consecutive integers is:

\[ x^2 \equiv \frac{p+1}{4} \pmod{p} \]
\[ \equiv \frac{503+1}{4} \pmod{503} \]
\[ \equiv 126 \pmod{503} \]

Therefore, \( x^2 \equiv 126 \pmod{503} \) has solutions which are consecutive integers.

These solutions are: \( x \equiv \frac{p-1}{2}, \frac{p+1}{2} \equiv 251, 252 \pmod{503} \).

**CONCLUSION**

Therefore, it can be concluded that if \( p \equiv 3 \pmod{4} \), then the congruence having solutions which are consecutive integers is

\[ x^2 \equiv \frac{p+1}{4} \pmod{p} \]

and the solutions are the integers

\[ x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod{p} \].

Also, if \( p \equiv 1 \pmod{4} \), then the congruence having solutions which are consecutive integers is

\[ x^2 \equiv \frac{3p+1}{4} \pmod{p} \]

and the solutions are the integers

\[ x \equiv \frac{p-1}{2}, \frac{p+1}{2} \pmod{p} \].

**REFERENCES**


