RP-145: Formulation of solutions of a class of standard quadratic congruence of composite modulus modulo double of a squared odd prime.

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist - Gondia, M. S., INDIA. Pin: 441801.

***Abstract*: In this paper, the author considered a special type of standard quadratic congruence of composite modulus modulo double of square of an odd prime for formulation of its solutions.**

In the literature of mathematics, no formulation of solutions of such congruence is found.

The author has successfully formulated the solutions and established a very simple formula.

The formula is tested and verified by solving some numerical examples. Formulation is the merit of the paper

***Keywords*: Composite modulus, Formulation, Quadratic congruence,**

INTRODUCTION

A congruence of the type $x^2 \equiv a \ (mod\ m)$, m being a composite integer, is a standard quadratic congruence of composite modulus. Such types of congruence are already has been formulated and published by the author.

Yet he has formulated the congruence: $x^2 \equiv p^2 \ (mod\ 2p^n); n \geq 3 \ \ p\ an\ odd\ prime$. It is found that it has exactly $2p$ incongruent solutions. The paper has been published in [1]. Here, in this paper, the author wishes to formulate the same congruence for $n = 2$. It is also seen that this congruence has a different formulation and a different number of solutions.

PROBLEM-STATEMENT

Here the problem is "To formulate the solutions of the congruence

$x^2 \equiv p^2 \ (mod\ 2p^2), \ \ p\ an\ odd\ prime$"

LITERATURE-REVIEW

The author already has published many standard quadratic congruence of composite modulus such as [2], [3].

The literature of mathematics suggests a book: "Elementary Number Theory with Applications [4] in which a new method is described to find the solutions of the said congruence. That is an iterated method. It takes a long time. Also no one knows how to solve the individual congruence. Here lies the difficulty to apply the above method mentioned. In the literature of mathematic no formulation is found. There standard quadratic congruence of prime modulus is discussed [5], [6]. The author has started formulating such congruence.

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv p^2 \ (mod\ 2p^2)$; p an odd prime.

For solution, consider $x \equiv 2pk + p \ (mod\ 2p^2)$.

Then, $x^2 \equiv (2pk + p)^2 \ (mod\ 2p^2)$

$\equiv (\ 2pk)^2 + 2.2pk.p + p^2 \ (mod\ 2p^2)$

$\equiv 4p^2k^2 + 4p^2k + p^2 \ (mod\ 2p^2)$

$\equiv 4p^2k(k + 1) + p^2 \ (mod\ 2p^2)$

$\equiv 0 + p^2 \ (mod\ 2p^2)$

$\equiv p^2 \ (mod\ 2p^2)$.

Therefore, it is seen that $x \equiv 2pk + p \ (mod\ 2p^2)$ gives solutions of the congruence. But if$k = p$, the solution formula reduces to $x \equiv 2p.p + p \ (mod\ 2p^2)$

$$\equiv 2p^2 + p(mod\ 2p^2)$$

$$\equiv 0 + p \ (mod\ 2p^2)$$

This is the solutions as for $k = 0$.

Also if $k = p + 1$, it can be seen that the solution formula reduces to

$x \equiv 2p + p \ (mod\ 2p^2)$.

This is the solution as for $k = 1$.

Therefore, all the solutions are given by $x \equiv 2pk + p \ (mod\ 2p^2); k = 0, 1, 2, \dots\dots, (p-1)$.

ILLUSTRATIONS

Example-1: consider the congruence $x^2 \equiv 25 \ (mod\ 50)$.

It can be written as $x^2 \equiv 5^2 (mod\ 2.5^2)\ with\ p = 5$.

It has exactly $p = 5$ incongruent solutions.

These solutions are given by $x \equiv 2pk + p \ (mod\ 2p^2); k = 0, 1, 2 \dots\dots, (p-1)$.

$$\equiv 2.5k + 5 \ (mod\ 2.5^2); k = 0, 1, 2, 3, 4.$$

$$\equiv 10k + 5 \ (mod\ 50)$$

$$\equiv 0 + 5, 10 + 5, 20 + 5, 30 + 5, 40 + 5 \ (mod\ 50)$$

$$\equiv 5, 15, 25, 35, 45 \ (mod\ 50).$$

Example-2: consider the congruence $x^2 \equiv 49 \ (mod\ 98)$.

It can be written as $x^2 \equiv 7^2 (mod\ 2.7^2)\ with\ p = 7$.

It has exactly $p = 7$ incongruent solutions.

These solutions are given by

$x \equiv 2pk + p \ (mod\ 2p^2); k = 0, 1, 2 \dots\dots, (p-1)$.

$\equiv 2.7k + 7 \ (mod\ 2.7^2); k = 0, 1, 2, 3, 4, 5, 6.$

$\equiv 14k + 7 \ (mod\ 50)$

$\equiv 0 + 7, 14 + 7, 28 + 7, 42 + 7, 56 + 7, 70 + 7, 84 + 7 \ (mod\ 50)$

$\equiv 7, 21, 35, 49, 63, 77, 91 \ (mod\ 98)$.

Example-3: consider the congruence $x^2 \equiv 9 \ (mod\ 18)$.

It can be written as $x^2 \equiv 3^2 (mod\ 2.3^2)\ with\ p = 3$.

It has exactly $p = 3 = 6$ incongruent solutions.

These solutions are given by

$x \equiv 2pk + p \ (mod\ 2p^2); k = 0, 1, 2 \dots\dots, (p-1)$.

$\equiv 2.3k + 3 \ (mod\ 2.3^2); k = 0, 1, 2.$

$\equiv 6k + 3 \ (mod\ 18)$

$\equiv 0 + 3, 6 + 3, 12 + 3 \ \ (mod\ 50)$

$\equiv 3, 9, 15\ (mod\ 18)$.

Example-4: Consider the congruence $x^2 \equiv 361\ (mod\ 722)$.

It can be written as $x^2 \equiv 19^2 (mod\ 2.19^2)\ with\ p = 19$.

It has exactly $p = 19$ incongruent solutions.

These solutions are given by

$x \equiv 2pk + p\ (mod\ 2p^2); k = 0, 1, 2 \dots \dots, (p-1)$.

$\equiv 2.19k + 19\ (mod\ 2.19^2); k = 0, 1, 2 \dots \dots \dots \dots \dots, 17, 18$.

$\equiv 38k + 19\ (mod\ 722)$

$\equiv 0 + 3, 6 + 3, 12 + 3\ \ (mod\ 722)$

$\equiv 19,\ 57,\ 95,\ 133, 171, \dots \dots \dots \dots, 665, 703\ \ (mod\ 722)$.

These are the nineteen incongruent solutions.

CONCLUSION

Therefore, it is concluded that the standard quadratic congruence considered as:

$x^2 \equiv p^2 (mod\ 2p^2)$ has exactly p- incongruent solutions given by

$x \equiv 2pk \pm p\ (mod\ 2p^2); k = 0, 1, 2, \dots . (p-1)$.

MERIT OF THE PAPER

Therefore it is concluded that the standard quadratic congruence:

$x^2 \equiv p^2 (mod\ 2p^2)$, p an odd prime is formulated. Solutions are obtained by the established formula. So, formulation is the merit of the paper.

REFERENCES

[1] Roy B M, Formulation of a class of standard quadratic congruence of composite modulus modulo double of a powered odd prime, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-05, Issue-10, oct-20.

[2] Roy B M, *Formulation of solutions of a very special standard quadratic congruence of prime-power modulus*, International Journal of Trends in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-05, July-20.

[3]Roy B M, *An algorithmic formulation of solving standard quadratic congruence of prime power modulus*, International Journal of Advanced Research, Ideas and Innovation in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-06, Dec-18.

[4] Koshy Thomas, 2009, *Elementary Number Theory with Applications, Second edition, Academic Press*, ISBN: 978-81-312-1859-4.

[5] Zuckerman H. S., Niven I., Montgomery H. L., 2008, "*An Introduction to The Theory of Numbers*", fifth edition, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.

[6] Burton D. M, 2012, *Elementary Number Theory*, Indian edition, Mc Graw Hill Publication, ISBN: 978-1-25-902576-1.