International Journal of Scientific Research and Engineering Development-– Volume 3 - Issue 5, Sep - Oct 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-146: Formulation of Solutions of Standard Quadratic Congruence of Composite Modulus Modulo A Product of Square of An Odd Prime & Four

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 has formulated the solutions of a standard quadratic congruence of composite modulus modulo a product of square of an odd prime & four. Such type of congruence always has $2p$ incongruent solutions, where p is the prime in the modulus. Various numerical examples are solved using the established formula; solutions are tested true. The solutions can also be obtained orally. This is the merit of the paper.

Keywords: Composite modulus, Formulation, Quadratic congruence.

Introduction

The author first time has attempted to formulate some special type of standard quadratic congruence of composite modulus. In this connection, in continuation of the previous formulation, one more standard quadratic congruence of such type is considered here for formulation the congruence $x^2 \equiv p^2 (mod\ 4p^2), p\ an\ odd\ prime$.It is found that it has a different type of formulation. No special method or formulation is found in the literature of mathematics.

Problem-Statement

Here the problem is – "To formulate the standard quadratic congruence of the type:

$$x^2 \equiv p^2 (mod\ 4p^2), p\ an\ odd\ prime".$$

Literature-Review

The author already has formulated many standard quadratic congruence of composite modulus [1], [2], [3], [4].

No literature of mathematics, except the book of Koshy [5] discusses the standard quadratic congruence of composite modulus. In this book, the method of solving the congruence:

$x^2 \equiv a\ (mod\ p^n), n \geq 1, p$an odd prime, is discussed. It is an iterative method which takes a long time. No formulation is given for solutions. But the book remains silent about the present congruence. Hence, the author wishes to formulate the congruence.

Analysis & Result

Consider the congruence: $x^2 \equiv p^2(mod\ 4p^2), p\ an\ odd\ prime.$

For the solutions, let $x \equiv 4pk \pm p\ (mod\ 4p^2)$.

Then, $x^2 \equiv (4pk \pm p)^2\ (mod\ 4p^2)$

$$\equiv (\ 4pk)^2 \pm 2.4pk.p + p^2\ (mod\ 4p^2)$$

$$\equiv 16p^2k^2 \pm 8pk + p^2(\ (mod\ 4p^2)$$

$$\equiv 8pk(2pk \pm 1) + p^2(mod\ 4p^2)$$

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

Therefore, $x \equiv 4pk \pm p\ (mod\ 4p^2)$ satisfies the said congruence and hence it must be consider as solutions of the congruence. But $if\ k = p$, the solution formula reduces to the form, $x \equiv 4p.p \pm p\ (mod\ 4p^2)$

$$\equiv 4p^2 \pm p\ (mod\ 4p^2)$$

$$\equiv 0 \pm p\ (mod\ 4p^2).$$

These are the same solutions as for $k = 0$.

Also for $k = p + 1$, the solution formula reduces to the form: $x \equiv 4p \pm p\ (mod\ 4p^2)$.

These are the same solutions as for $k = 1$.

Therefore, all the solutions are given by:

$x \equiv 4pk \pm p\ (mod\ 4p^2); k = 0, 1, 2, \ldots\ldots, (p-1)$.

These are $2p -$ incongruent solutions as for a single value of k, it has exactly two solutions.

Illustrations

Example-1: Consider the congruence $x^2 \equiv 49\ (mod\ 196)$.

It can be written as $x^2 \equiv 7^2(mod\ 4.7^2)$.

It is of the type $x^2 \equiv p^2(mod\ 4.p^2)\ with\ p = 7$.

It has $2p = 2.7 = 14$ incongruent solutions given by

$x \equiv 4pk \pm p\ (mod\ 4p^2); k = 0, 1, 2, \ldots\ldots, (p-1)$.

$$\equiv 4.7k \pm 7\ (mod\ 4.49); k = 0, 1, 2, 3, 4, 4, 6.$$

$$\equiv 28k \pm 7\ (mod\ 196); k = 0, 1, 2, 3, 4, 5, 6.$$

$$\equiv 0 \pm 7; 28 \pm 7; 56 \pm 7; 84 \pm 7; 112 \pm 7; 140 \pm 7; 168 \pm 7\ (mod\ 196).$$

$$\equiv 7, 189; 21, 35; 49, 63; 77, 91; 105, 119; 133, 147; 161, 175\ (mod\ 196).$$

These are the fourteen solutions of the congruence.

Example-2: Consider the congruence $x^2 \equiv 9\ (mod\ 36)$.

It can be written as $x^2 \equiv 3^2(mod\ 4.3^2)$.

It is of the type $x^2 \equiv p^2(mod\ 4.p^2)\ with\ p = 3$.

It has $2p = 2.3 = 6$ incongruent solutions given by

$x \equiv 4pk \pm p\ (mod\ 4p^2); k = 0, 1, 2, \ldots\ldots, (p-1)$.

$$\equiv 4.3k \pm 3\ (mod\ 4.9); k = 0, 1, 2.$$

$$\equiv 12k \pm 3\ (mod\ 36); k = 0, 1, 2\ .$$

$$\equiv 0 \pm 3; 12 \pm 3; 24 \pm 3\ (mod\ 36).$$

$$\equiv 3, 33; 9, 15; 21, 27\ (mod\ 36).$$

$$\equiv 3, 9, 15, 21, 27, 33\ (mod\ 36).$$

These are the six solutions of the congruence.

Conclusion

Therefore, the congruence $x^2 \equiv p^2(mod\ 4.p^2)$ has 2p-incongruent solutions given by

$x \equiv 4pk \pm p\ (mod\ 4p^2); k = 0, 1, 2, \ldots\ldots, (p-1)$.

These solutions are tested by trial and error method and found true.

MERIT OF THE PAPER

A formula is established for solutions of the said congruence. Now it becomes possible to find the solutions directly. Formulation of the congruence is the merit of the paper.

Reference

[1] Roy B M, *Formulation of solutions of a very special standard quadratic congruence of prime-power modulus*, (IJTSRD), ISSN: 2456-6470, vol-04, Issue-05, July-20.

[2] Roy B M, *Formulation of a very special type of standard quadratic congruence of composite modulus modulo a product of a powered odd prime integer and four*, (IJSDR), ISSN: 2455-2631, vol-05, Issue-07, July-20.

[3] Roy B M, *Formulation of solutions of a very special type of standard quadratic congruence of composite modulus – an eighth multiple of an odd prime-power integer*, (IJSDR), ISSN: 2455-2631, vol-05, Issue-08, Aug-20.

[4] Roy B M, *Formulation of solutions of a class of standard quadratic congruence of composite modulus modulo double of a squared odd prime*, (IJSDR), ISSN: 2455-2631, vol-05, Issue-10, Oct-20.

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

…….xxx……..

