iJETRM
International Journal of Engineering Technology Research & Management

RP-130: FORMULATION OF SOLUTIONS OF A CLASS OF STANDARD QUADRATIC CONGRUENCE MODULOA MULTIPLE OF POWER OF AN ODD PRIME

Prof B M Roy
M. Sc. (Maths), Hon. Ph. D., Hon. D. Sc.
Head, department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- GONDIA, M. S., INDIA. Pin: 441801

ABSTRACT
Herein this study, the solutions of a class of standard quadratic congruence of a multiple of prime-power modulus is considered for study and also for formulation. The solutions of the congruence are formulated successfully. These types of congruence have many solutions. Using the formulation Solutions can be obtained easily. This formulation of solutions of the congruence is the merit of the paper.

Key-words: Composite modulus, Formulation, Prime-power modulus, Quadratic congruence.

INTRODUCTION

The congruence of the type: $x^2 \equiv a \ (mod\ m)$, m being a Prime or Composite integer is called standard quadratic congruence of prime or composite modulus. The values of x that satisfy the congruence are called its solutions. A standard quadratic congruence of prime modulus has exactly two solutions [1];*but if it is a quadratic congruence of composite modulus, then it may have more than two solutions [2]. Here in this paper, the author formulated the solutions of the congruence of the type* $x^2 \equiv (mp)^2 (mod\ b.p^n)$; *p*$\geq 2$, *a positive prime integer and b, m are positive integer.*

PROBLEM-STATEMENT

Here the problem is-

"To formulate the solutions of the standard quadratic congruence:

$x^2 \equiv (mp)^2 (mod\ b.p^n);\ b\ , m, n\ \ are$ Positive integers, p odd prime and $n \geq 2, b \neq lp$".

LITERATURE-REVIEW

The standard quadratic congruence of prime modulus is a prominent part in the literature of mathematics. It is fully discussed but no discussion is found on quadratic congruence of prime-power modulus.

It is found that if $(a, p) = 1$, then $x^2 \equiv a\ (mod\ p^n)$*has exactly two solutions [2]. But no formulation is seen.* The author's successful efforts for formulation of the congruence is presented here. He (the author) already formulated many standard quadratic congruence of prime and composite modulus [3] to [13].

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv (mp)^2 (mod\ b.p^n);\ b, m\ are$ positive integers, $b \neq lp; n \geq 2$.

Let us consider that $x \equiv b.p^{n-1}k \pm mp \ \ (mod\ b.p^n)$.

Then $x^2 \equiv (b.p^{n-1}k \pm mp)^2$ (mod b. p^n)

iJETRM
International Journal of Engineering Technology Research & Management

$$\equiv (b.p^{n-1}k)^2 \pm 2.b.p^{n-1}k.mp + (mp)^2 \ (mod\ b.p^n)$$

$\equiv b.p^n k(b\ p^{n-2}k + 2m) + (mp)^2 \ \ (mod\ b.p^n)$

$\equiv 0 + mp^2 \ (mod\ b.p^n)$.

$\equiv mp^2 \ (mod\ b.p^n)$.

Thus, $x \equiv b.p^{n-1}k \pm mp \ \ (mod\ b.p^n)$is a solution of the congruence

$x^2 \equiv (mp)^2(mod\ b.p^n);\ b,m\ are$ Positive integers, $n \geq 2$.

But, if we consider $k = p$, then $x \equiv b.p^{n-1}.p \pm mp \ \ (mod\ b.p^n)$

$$\equiv b.p^n \pm mp \ \ (mod\ b.p^n)$$

$$\equiv 0 \pm mp \equiv \pm mp \ (mod\ b.p^n)$$

Which is the same solution as for $k = 0$.

Similarly, for higher values of k, the solutions repeats as for $k = 1, 2, 3, \ldots\ldots, (p-1)$.

Therefore, all the required solutions are given by

$$x \equiv b.p^{n-1}k \pm mp \ (mod\ b.p^n); k = 0, 1, 2, \ldots\ldots\ldots (p-1).$$

These are $2p$ incongruent solutions for all values of k as the congruence has two solutions for every value of k and k has p different values.

In particular, if $b = 1, then$ one get the solutions

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

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 196\ (mod\ 1715\ )$.

It can be written as $x^2 \equiv 14^2(mod\ 5.7^3)$.

It is of the type $x^2 \equiv (mp)^2(mod\ b.p^n);\ \ with\ p = 7, n = 3, m = 2, b = 5$.

The solutions are

$$x \equiv b.p^{n-1}k \pm mp \ (mod\ b.p^n); k = 0, 1, 2, \ldots\ldots\ldots (p-1).$$

$$\equiv 5.7^{3-1}k \pm 14\ (mod\ 5.7^3); k = 0, 1, 2, \ldots\ldots\ldots\ldots.., 7-1.$$

$$\equiv 245k \pm 14\ (mod\ 1715); k = 0, 1, 2, 3, \ldots\ldots.6.$$

$$\equiv 0 \pm 14; 245 \pm 14; 490 \pm 14; 735 \pm 14; 980 \pm 14; 1225 \pm 14; 1470 \pm 14\ (mod\ 1715$$

$$\equiv 14, 1701; 231, 259; 476, 504; 721, 749; 966, 994; 1211, 1239; 1456, 1484\ (mod\ 1715).$$

There are 14 solutions of the congruence.

Consider $the\ congruence\ x^2 \equiv 225\ (mod\ 625)$.

iJETRM
International Journal of Engineering Technology Research & Management

It is of the type $x^2 \equiv 15^2 (mod\ 5^4)\ with\ p = 5, n = 4.$

The solutions are $x \equiv p^{n-1}k \pm mp (mod\ p^n); k = 0, 1, 2, \dots \dots \dots (p - 1).$

$$\equiv 5^{4-1}k \pm 15\ (mod\ 5^4); k = 0, 1, 2, \dots \dots \dots (5 - 1).$$

$$\equiv 125k \pm 15\ (mod\ 625); k = 0,1, 2, 3,4.$$

$$\equiv 0 \pm 15; 125 \pm 15; 250 \pm 15; 375 \pm 15; 500 \pm 15\ (mod\ 625).$$

$$\equiv 5, 610; 110, 140; 235, 265; 360, 390; 485, 515\ (mod\ 625).$$

There are 10 solutions of the congruence.

Consider the congruence$x^2 \equiv 100\ (mod\ 500).$

It is of the type $x^2 \equiv 10^2 (mod\ 4.5^3)\ with\ p = 5, n = 2.$

The solutions are $x \equiv b. p^{n-1}k \pm mp (mod\ b. p^n); k = 0, 1, 2, \dots \dots \dots (p - 1).$

$$\equiv 4. 5^{3-1}k \pm 10\ (mod\ 4. 5^3); k = 0, 1, 2, \dots \dots \dots (5 - 1).$$

$$\equiv 100k \pm 10\ (mod\ 500); k = 0,1, 2, 3,4.$$

$$\equiv 0 \pm 10; 100 \pm 10; 200 \pm 10; 300 \pm 10; 400 \pm 10\ (mod\ 500).$$

$$\equiv 10, 490; 90, 110; 190, 210; 290, 310; 390, 410\ (mod\ 500).$$

There are 10 solutions of the congruence.

CONCLUSION

Therefore, it is concluded that the congruence $x^2 \equiv (mp)^2 (mod\ b. p^n); n \geq 2$, has 2p incongruent solutions $x \equiv b. p^{n-1}k \pm mp\ (mod\ b. p^n); k = 0, 1, 2, \dots \dots . (p - 1).$

But if $b = 1, then\ the\ congruence\ reduces\ to\ x^2 \equiv p^2\ (mod\ p^n)$and also has 2p incongruent

Solutions given by $x \equiv p^{n-1}k \pm p\ (mod\ p^n); k = 0, 1, 2, \dots \dots . (p - 1).$

MERIT OF THE PAPER

In this current paper, a class of standard quadratic congruence of multiple of prime-power modulus is formulated. Formulation is the merit of the paper.

REFERENCE

1. H S Zuckerman at el, 2008, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.
2. Thomas Koshy, 2009, "*Elementary Number Theory with Applications*", 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.
3. Roy B M, 2018, *A new method of finding solutions of a solvable standard quadratic congruence of comparatively large prime modulus,* International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-3, May-Jun-18.
4. Roy B M, 2018, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & four, International Journal of Recent Innovations In Academic Research (IJRIAR), ISSN:2635-3040, Vol-2, Issue-2, Jun-18.*

iJETRM
International Journal of Engineering Technology Research & Management

5. Roy B M, 2018, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & eight,* International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-4, July-18.
6. Roy B M, 2018, *Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime-power integer by two or four, International Journal for Research Trends and Innovations*(IJRTI), ISSN:2456-3315, Vol-3, Issue-5, May-18.
7. Roy B M, 2018, *Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime-power integer by two or four,* International Journal for Research Trends and Innovations(IJRTI), ISSN:2456-3315, Vol-3, Issue-5, May-18.
8. Roy B M, 2018, *Formulation of Standard Quadratic Congruence of Composite modulus as a product of prime-power integer and eight,* International Journal of Science & Engineering Development Research (IJSDR),ISSN: 2455-2631, Vol-3, Issue-7, Jul-18.
9. Roy B M, 2018, *Formulation of solutions of a class of standard quadratic congruence of even composite modulus,* International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-3, Issue-8, Jul-18.
10. Roy B M, 2018, *AnAlgorithmic Formulation of solving Standard Quadratic Congruence of Prime-power Modulus*, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-6, Dec-18.
11. Roy B M, 2019, *Formulation of a Class of Solvable Standard Quadratic Congruence of Even Composite Modulus,* International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-4, Issue-3, Mar-19.
12. Roy B M, 2019,*Formulation of Some Classes of Solvable Standard Quadratic Congruence modulo a Prime Integer - Multiple of Three & Ten,* International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-2, Issue-2, Mar-19.
13. Roy B M, *Formulation of solutions of a class very special standard quadratic congruence of multiple of prime-power modulus,*International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-2, Issue-6, Nov-Dec-19.