JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

RP-180: Formulation of Solutions of a Special Standard Quadratic Congruence Congruent to zero modulo a powered Even Prime

[1] Prof B M Roy
[1]Head, Department of Mathematics
[1] Jagat Arts, Commerce & I H P Science Nagpur
Dist- Gondia, M. S., India.
(Affiliated to R T M Nagpur University)

[2]Prof A. A. Qureshi
[2]Head, Department of Mathematics
[2]D. R. B. Sindhu Mahavidyalaya, Goregaon.
Dist-Nagpur, M.S., India.
(Affiliated to R T M Nagpur University)

ABSTRACT

The paper presented here, is a very special type of a standard quadratic congruence of composite modulus. It is considered for study and formulation of its solutions. The problem is studied rigorously and correctly formulated. It was found not formulated by the earlier mathematicians. So, the present authors attempted to establish a formulation of the solutions of the said congruence. The authors considered the problem, studied it and formulated the solutions. The authors have provided a formula for the solutions of the said quadratic congruence and presented here.

Key-words: Composite Modulus, Quadratic Congruence, Formulation.

INTRODUCTION

In the book of Number Theory by Zuckerman [1], the congruence: $x^2 \equiv a \ (mod\ 2^n); n \geq 3$, is found formulated with four incongruent solutions for $a \equiv 1 \ (mod\ 8)$; the same problem is also found in the book of Thomas Koshy , similarly formulated [2] but no discussion is found about the congruence: $x^2 \equiv 0 \ (mod\ 2^n)$ nowhere. The authors have found that such types of congruence have many nonzero solutions. Hence, the authors considered the said congruence for formulation of its solutions.

The authors already have formulated the congruence and got published in different international journals [3], [4], [5], [6], [7], [8], [9], [10], [11], [12].

PROBLEM-STATEMENT

The problem of study is stated here in the form of two theorems**:**

Theorem-1: The solutions of the standard quadratic congruence: $x^2 \equiv 0 \ (mod\ 2^n)$ has exactly $2^{n/2}$ nonzero solutions given by $x \equiv 2^{\frac{n}{2}}k \ (mod\ 2^n), if\ n$ is an even positive integer & k some positive integer.

Theorem-1: The solutions of the standard quadratic congruence: $x^2 \equiv 0\ (mod\ 2^n)$ has exactly $2^{\frac{n-1}{2}}k$ nonzero solutions given by $x \equiv 2^{\frac{n+1}{2}}k\ (mod\ 2^n), if\ n$ is an odd positive integer & k some positive integer.

ANALYSIS & RESULTS

Proof of Theorem -1:

Let n be even positive integer**.**

The congruence under consideration is: $x^2 \equiv 0\ (mod\ 2^n)$. It is always solvable.

For its solutions, consider $x \equiv 2^{\frac{n}{2}}\ k\ (mod\ 2^n), if\ n\ is\ an\ even\ positive\ integer.$

Then, $x^2 \equiv \left(2^{\frac{n}{2}}\ k\right)^2 \equiv 2^n k.k \equiv 0\ (mod\ 2^n)$.

Hence, $x \equiv 2^{\frac{n}{2}}\ k\ (mod\ 2^n); k = 1, 2, 3, \dots ....$ gives the solutions of the congruence.

If $k = 2^{\frac{n}{2}} + 1$, then $x \equiv 2^{\frac{n}{2}}.(2^{\frac{n}{2}} + 1)\ (mod\ 2^n)$

$$\equiv 2^n + 2^{\frac{n}{2}}\ (mod\ 2^n)$$

$$\equiv 0 + 2^{\frac{n}{2}}\ (mod\ 2^n)$$

$$\equiv 2^{\frac{n}{2}}\ (mod\ 2^n).$$

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

Also it is seen that for $k = 2^{\frac{n}{2}} + 2$, the solution is the same for $k = 2$.

Therefore, all the solutions are given by

$$x \equiv 2^{\frac{n}{2}}\ k\ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n}{2}}.$$

Proof of Theorem-2:

Let n be an odd positive integer.

The congruence under consideration is: $x^2 \equiv 0\ (mod\ 2^n)$. It is always solvable.

For the solutions, consider $x \equiv 2^{\frac{n+1}{2}}\ k\ (mod\ 2^n), if\ n\ is\ an\ odd\ positive\ integer.$

Then, $x^2 \equiv \left(2^{\frac{n+1}{2}}\ k\right)^2 \equiv 2^{n+1}k.k \equiv 2^n k.2k \equiv 0\ (mod\ 2^n)$.

Hence, $x \equiv 2^{\frac{n+1}{2}}\ k\ (mod\ 2^n); k = 1, 2, 3, \dots.., 2^{\frac{n-1}{2}}$ gives the solutions of the congruence.

If $k = 2^{\frac{n-1}{2}} + 1$, then $x \equiv 2^{\frac{n+1}{2}}.(2^{\frac{n-1}{2}} + 1)\ (mod\ 2^n)$

$$\equiv 2^n + 2^{\frac{n+1}{2}}\ (mod\ 2^n)$$

$$\equiv 0 + 2^{\frac{n+1}{2}}\ (mod\ 2^n)$$

$$\equiv 2^{\frac{n+1}{2}}\ (mod\ 2^n).$$

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

Also it is seen that for $k = 2^{\frac{n-1}{2}} + 2$, the solution is the same for $k = 2$.

Therefore, all the solutions are given by

$x \equiv 2^{\frac{n-1}{2}} k \ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n-1}{2}}.$

ILLUSTRATIONS

Example-1: Consider the congruence: $x^2 \equiv 0\ (mod\ 256)$.

It can be written as: $x^2 \equiv 0\ (mod\ 2^8)$.

It is of the type: $x^2 \equiv 0\ (mod\ 2^n)\ with\ n = 8, an\ even\ positive\ integer$.

Its solutions are given by:

$x \equiv 2^{\frac{n}{2}} k\ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n}{2}}.$

$\equiv 2^4 k\ (mod\ 2^8); k = 1, 2, 3, \dots \dots \dots, 2^4.$

$\equiv 16k\ (mod\ 256); k = 1, 2, 3, \dots \dots \dots, 16.$

$\equiv 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240, 256\ (mod\ 256).$

These are the sixteen nonzero solutions of the congruence.

Example-2: Consider the congruence: $x^2 \equiv 0\ (mod\ 128)$.

It can be written as: $x^2 \equiv 0\ (mod\ 2^7)$.

It is of the type: $x^2 \equiv 0\ (mod\ 2^n)\ with\ n = 7, an\ odd\ positive\ integer$.

Its solutions are given by:

$x \equiv 2^{\frac{n+1}{2}} k\ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n-1}{2}}.$

$\equiv 2^4 k\ (mod\ 2^7); k = 1, 2, 3, \dots \dots \dots, 2^3.$

$\equiv 16k\ (mod\ 128); k = 1, 2, 3, \dots \dots \dots, 8.$

$\equiv 16, 32, 48, 64, 80, 96, 112, 128\ (mod\ 128).$

These are the eight nonzero solutions of the congruence.

CONCLUSION

The congruence $x^2 \equiv 0\ (mod\ 2^n)$ has nonzero solutions:

$x \equiv 2^{\frac{n}{2}} k\ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n}{2}}$, if n is an even positive integer.

Also, the congruence $x^2 \equiv 0\ (mod\ 2^n)$ has nonzero solutions:

$x \equiv 2^{\frac{n+1}{2}} k\ (mod\ 2^n); k = 1, 2, 3, \dots \dots, 2^{\frac{n-1}{2}}$, if n is an odd positive integer.

MERIT OF THE PAPER

The solutions of the present quadratic congruence is formulated successfully by formulating in two different cases. A single formula gives all the solutions of the congruence. Therefore it can be said that the formulation of solutions is the merit of the paper.

REFERENCES

1. Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, page-148, problem-11.

2. Roy B M, 2016, *Discrete Mathematics & Number Theory*, Das Ganu Prakashan, Nagpur, India, ISBN: 978-93-84336-12-7.
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.*
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 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.
8. 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.
9. Roy B M, 2018, *An Algorithmic 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.
10. 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.
11. Roy B M, Qureshi A A; 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.
12. Roy B M, Qureshi A A, 2021; Solving some special classes of standard congruence of prime modulus of higher degree, International Journal of Physics and Mathematics (IJPM), ISSN: 2664-8644, Vol-03, Issue-01, Jun-21, Pages: 31-34.