International Journal of Physics and Mathematics
www.physicsjournal.net
Online ISSN: 2664-8644, Print ISSN: 2664-8636
Received: 15-07-2021; Accepted: 30-07-2021; Published: 16-08-2021
Volume 3, Issue 2, 2021, Page No. 01-02

Formulation of solutions of a special standard quadratic congruence modulo an even prime integer raised to the power n

B M Roy[1], A A Qureshi[2*]
[1] Head, Department of Mathematics, Jagat Arts, Commerce and IHP Science, Goregaon, District Gondia, Maharashtra, India
[2] Head, Department of Mathematics, D R B Sindhu Mahavidyalaya, Nagpur, Maharashtra, India

Abstract
In this paper, authors have formulated solutions of special type of a standard quadratic congruence $x^2 \equiv 0\ (mod\ 2^n)$ of composite modulus. This congruence was not formulated by the earlier mathematicians, so the present authors studied it rigorously and attempted to formulate the solutions of this congruence. The authors have presented the formula for the solutions of the said quadratic congruence here and obtained nonzero solutions.

Keywords: 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 and k is some positive integer.

Theorem-2: 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 and k is some positive integer.

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

$$\text{If } k = 2^{\frac{n}{2}} + 1, \text{then } x \equiv 2^{\frac{n}{2}}.(2^{\frac{n}{2}} + 1)\ (mod\ 2^n)$$
$$\equiv (2^n + 2^{\frac{n}{2}})\ (mod\ 2^n)$$
$$\equiv 0 + 2^{\frac{n}{2}}\ (mod\ 2^n)$$
$$\equiv 2^{\frac{n}{2}}(mod\ 2^n).$$

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 nonzero solutions are given by

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

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

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

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

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

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

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

Also, the congruence $x^2 \equiv 0\ (mod\ 2^n)$has nonzero solutions $x \equiv 2^{\frac{n+1}{2}}k\ (mod\ 2^n); k = 1, 2, 3, \dots.., 2^{\frac{n-1}{2}}$, if n is an odd positive integer.

References

1. Niven I, Zuckerman HS, Montgomery HL. (1960, Reprint 2008), “An Introduction to The Theory of Numbers”, 5/e, Wiley India (Pvt) Ltd, problem-11, 2008, 148.
2. Roy BM. Discrete Mathematics & Number Theory, Das Ganu Prakashan, Nagpur, India, ISBN: 978-93-84336-12-7, 2016.
3. Roy BM. 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, 2018, 4(3).
4. Roy BM. 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, 2018, 2(2).
5. Roy BM. 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, 2018, 4(4).
6. Roy BM. 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, 2018, 3(5).
7. Roy BM. 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, 2018, 3(7).
8. Roy BM. 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, 2018, 3(8).
9. Roy BM. 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, 2018, 4(6).
10. Roy BM. Formulation of a Class of Solvable Standard Quadratic Congruence of Even Composite Modulus, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, 2019, 4(3).
11. Roy B M, Qureshi A A. 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, 2019, 2(2).
12. Roy B M, Qureshi A A. Solving some special classes of standard congruence of prime modulus of higher degree, International Journal of Physics and Mathematics (IJPM), ISSN: 2664-8644,2021:3(1):31-34.