International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 6, Nov-Dec 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-149: Formulation of Solutions of Special Standard Quadratic Congruence of Composite Modulus Modulo A Power of Even 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 solutions of a special type of standard quadratic congruence of composite modulusis formulated. The congruencemodulo a power of an even prime in a special case is formulated for its solutions. Such type of congruence was already formulated by the earlier mathematicians but the formulation was incomplete. The formulation was only for some special odd positive integers. But no discussion was found on even perfect squares. Here the author consider the case for formulation of solutions and presented the formulation in this paper. It is found that in this special case, the congruence has exactly eight solutions. Formulation is the merit of the paper.

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

Introduction

Standard quadratic congruence of composite modulus in comparison to the congruence of prime modulus is less studied and a very less study material is available in the literature. The author wishes to consider the congruence for formulation of its solutions and wants to formulatethe solutionsof the standard quadratic congruence of even composite modulus in a special case.

Problem-Statement

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

$$x^2 \equiv a \ (mod\ 2^n); a\ being\ an\ even\ perfect\ square\ but\ a \neq 2^{2m}\ ".$$

Literature Review

The above problem is discussed in the book of Zuckerman and others [1], Thomas Koshy [2], David M Burton [3]. There they considered $'a'$ in the problem odd and $a \equiv 1\ (mod\ 8)$.

Then the congruence has exactly four solutions given by $x_0, -x_0, 2^{n-1} + x_0, 2^{n-1} - x_0$, if x_0 is any solution of the said congruence but how to find x_0 is not mentioned.

The author now wishes to formulated the said congruence when a iseven perfect square.In this case the author wishes to show that the congruence has different number of solutions, if $a$even is a perfect square.

Analysis & Results

Consider the congruence: $x^2 \equiv a\ (mod\ 2^n); a\ being\ an\ even\ perfect\ square$. Then it can also be written as: $x^2 \equiv b^2 (mod\ 2^n), b\ an\ even\ positive\ integer$.

 ©IJSRED:All Rights are Reserved

For its solutions, consider: $x \equiv 2^{n-2}k \pm b \ (mod\ 2^n)$.

$$x^2 \equiv (2^{n-2}k \pm b)^2 \ (mod\ 2^n)$$

$$\equiv (2^{n-2}k)^2 \pm 2.2^{n-2}k.b + b^2 \ (mod\ 2^n)$$

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

$$\equiv 2^{n-1}k\{\ 2^{n-3}k \pm b\} + b^2 \ (mod\ 2^n)$$

$$\equiv 2^{n-1}k\{2^{n-3}k \pm 2t\} + b^2 (mod\ 2^n) \ \ as\ \ b\ is\ even\ \&\ hence\ b = 2t.$$

$$\equiv 2^n k\{\ 2^{n-4}k \pm t\} + b^2 \ (mod\ 2^n)$$

$$\equiv b^2 (mod\ 2^n), if\ n \geq 4.$$

But for $k = 2^2 = 4$, the solutions formula reduces to: $x \equiv 2^{n-2}.2^2 \pm b \ (mod\ 2^n)$.

$$\equiv 2^n \pm b \ (mod\ 2^n)$$

$$\equiv \pm b \ (mod\ 2^n)$$

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

Also for $k = 5 = 4 + 1$, the solutions formula reduces to: $x \equiv 2^{n-2}.(2^2 + 1) \pm b \ (mod\ 2^n)$.

$$\equiv (2^n + 2^{n-2}) \pm b \ (mod\ 2^n)$$

$$\equiv 2^{n-2} \pm b \ (mod\ 2^n).$$

This is the same solutions s for $k = 1$.

Therefore, all the solutions are given by:$x \equiv 2^{n-2}.k \pm b \ (mod\ 2^n)$;k=0, 1, 2, 3, 4.

These are the eight solutions of the congruence as for each value of k, two solutions exist.

If $a = 0, then\ b = 0, (even\ positive\ integer)$, and the congruence reduces to

$x^2 \equiv 0 \ (mod\ 2^n)$.Then it can be easily seen that $x \equiv 8k \ (mod\ 2^n); k = 0, 1, 2, 3, \ldots\ldots\ldots$ are the eight solutionsof the congruence $i.e.\ all\ positive\ integer\ divisible\ by\ 8$ but less than 2^n.

Thus it can be easily seen that for odd positive integer b, there would be 2^{n-3} congruence, each having four solutions and so total number of solutions would be $2^{n-3}.4 = 2^{n-1}$.

There remains another $2^{n-1}\ solutions$ for even positive integer a. But all mathematicians consider zero (o) as even integer and has exactly eight solutions, hence there remains only $(2^{n-1} - 8)$ solutions for nonzero even positive integer. And each congruence have exactly eight solutions. This is only possible whenever $'a'$ is perfect square.

Thus, in the case when a is an even positive integer, the congruence is only solvable if $'a'$ is perfect square.

Illustrations

Example-1: Consider the congruence: $x^2 \equiv 36 \ (mod\ 64)$.

It is of the type: $x^2 \equiv a \ (mod\ 2^n)\ with\ a = 36$, an even perfect square.

 ©IJSRED:All Rights are Reserved

It has exactly eight incongruent solutions.

It can be written as: $x^2 \equiv 6^2 (mod\ 2^6)$.

It is of the type: $x^2 \equiv b^2 (mod\ 2^n)$ with $n = 6$ & $b = 6$, an even positive integer.

These solutions are given by: $x \equiv 2^{n-2}k \pm b\ (mod\ 2^n)$; k=0, 1, 2, 3.

$$\equiv 2^{6-2}k \pm 6\ (mod\ 2^6); k = 0, 1, 2, 3.$$

$$\equiv 2^4 k \pm 6\ (mod\ 64)$$

$$\equiv 16k \pm 6\ (mod\ 64)$$

$$\equiv 0 \pm 6;\ 16 \pm 6; 32 \pm 6;\ 48 \pm 6\ (mod\ 64).$$

$$\equiv 6, 58; 10, 22; 28, 38; 42, 54\ (mod\ 64).$$

These are the required eight incongruent solutions of the above congruence.

Example-2: Consider the congruence: $x^2 \equiv 16\ (mod\ 64)$.

It is of the type: $x^2 \equiv a\ (mod\ 2^n)\ with\ a = 4$, an even perfect square.

It can be written as: $x^2 \equiv 4^2 (mod\ 2^6)$.

It is of the type: $x^2 \equiv b^2 (mod\ 2^n)$ with $n = 6$ & $b = 4$, an even positive integer.

It has exactly eight incongruent solutions.

These solutions are given by: $x \equiv 2^{n-2}k \pm b\ (mod\ 2^n)$; k=0, 1, 2, 3.

$$\equiv 2^{6-2}k \pm 4\ (mod\ 2^6); k = 0, 1, 2, 3.$$

$$\equiv 2^4 k \pm 4\ (mod\ 64)$$

$$\equiv 16k \pm 4\ (mod\ 64)$$

$$\equiv 0 \pm 4;\ 16 \pm 4; 32 \pm 4; 48 \pm 4\ (mod\ 64).$$

$$\equiv 4, 60; 12, 20; 28, 36; 44, 52\ (mod\ 64).$$

These are the required eight incongruent solutions of the above congruence.

Example-3: Consider the congruence: $x^2 \equiv 36\ (mod\ 1024)$.

It is of the type: $x^2 \equiv a\ (mod\ 2^n)\ with\ a = 36$, an even perfect square.

It has exactly eight incongruent solutions.

It can be written as: $x^2 \equiv 6^2 (mod\ 2^{10})$.

It is of the type: $x^2 \equiv b^2 (mod\ 2^n)$ with $n = 10$ & $b = 6$, an even positive integer.

The solutions are given by: $x \equiv 2^{n-2}k \pm b\ (mod\ 2^n)$; k=0, 1, 2, 3.

$$\equiv 2^{10-2}k \pm 6\ (mod\ 2^{10}); k = 0, 1, 2, 3.$$

$$\equiv 2^8 k \pm 6\ \ (mod\ 1024)$$

$$\equiv 256k \pm 6\ \ (mod\ 1024)$$

 ©IJSRED:All Rights are Reserved

$$\equiv 0 \pm 6; 256 \pm 6; 512 \pm 6; 768 \pm 6 \ (mod\ 1024).$$

$$\equiv 6, 1018; 250, 262; 506, 518; 762, 774 \ (mod\ 1024).$$

These are the required eight incongruent solutions of the above congruence.

Conclusion

Thus, it can be conclude that the standard quadratic congruence of even composite modulus of the type: $x^2 \equiv b^2 (mod\ 2^n)$, $n \geq 4$ has exactly eight solutions given by:

$$x \equiv 2^{n-2}k \pm b \ (mod\ 2^n); k = 0, 1, 2, 3.$$

MERIT OF THE PAPER

A formula is established for the solutions of the said congruence. Formulation made it easy to find the solutions of the congruence. Solutions can be obtained orally. This is the merit of the paper.

References

[1]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.

[2]Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press (India), Second Edition, ISBN: 978-81-312-1859-4.

[3] David M Burton, 2012, Elementary Number Theory, McGraw Hill Education (India) Private Limited, New Delhi, Seventh Edition, ISBN: 978-1-25-902576-1.

……..xxx……..

 ©IJSRED:All Rights are Reserved