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-185: To find Solutions of a special standard quadratic congruence of composite modulus modulo a multiple of an odd prime and a powered 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 research paper, the author has considered for his study, a very special type of standard quadratic congruence of composite modulus modulo an odd prime multiple of a powered even prime. After a rigorous study of the problem, a simple formulation of the solutions is established. It finds the solutions very easily with less effort. The method proved time-saving and simple to find the solutions. Formulation of solutions is the merit of the paper.

KEY- WORDS: Composite modulus, Formulation, Prime multiple, Quadratic congruence.

INTRODUCTION

Congruence is a topic in the book of Number Theory. Discussions on Linear and quadratic congruence are found in those books.

A standard quadratic congruence is defined mathematically as: $x^2 \equiv a\ (mod\ d)$ *and* the values of x that satisfies the congruence are called solutions of it $i.e.$ *to find* those values of x, whose square when divided by m, gives the remainder as a.

In this paper, some special types of a & m are considered $i.e. a = 2^{2m}, d = 2^{2m-2}.p$, p being an odd prime positive integer. Then the congruence under consideration becomes:

$$x^2 \equiv 2^{2m}\ (mod\ 2^{2m-2}.p).$$

PROBLEM-STATEMENT

Here the problem of study is:

To find the solutions of the congruence

$$x^2 \equiv 2^{2m}\ (mod\ 2^{2m-2}.p); p\ an\ odd\ prime\ positive\ integer.$$

LITERATURE REVIEW

The present standard quadratic congruence considered for formulation of its solutions, is neither be formulated nor discussed anywhere in the literature of mathematics. Zuckerman et el [1], Thomas Koshy [2], David M Burton [3] all have discussed the standard quadratic congruence of prime and composite modulus but nothing is found reported for the present problem. The author has already formulated many such standard quadratic congruence of composite modulus [4], [5], [6], [7]. Previously the author has formulated the following quadratic congruence of composite modulus as:

(1) $x^2 \equiv 2^{2m} \ (mod\ 2^{2m}.p); p\ an\ odd\ prime\ positive\ integer;$
(2) $x^2 \equiv 2^{2m} \ (mod\ 2^{2m+1}.p); p\ an\ odd\ prime\ positive\ integer.$

In continuation, the author has considered the said problem under consideration for formulation of solutions.

ANALYSIS & RESULTS

Consider the congruence: $x^2 \equiv 2^{2m} \ (mod\ 2^{2m-2}.p); p\ an\ appropriate\ odd\ prime.$

Then it reduces to the form: $x^2 \equiv 2^{2m} \ (mod\ 2^{2m-2}.p).$

For its solutions, let $x \equiv 2^{m-1}.pk \pm 2^m (mod\ 2^n.p)$

Then, $x^2 \equiv (2^{m-1}.pk \pm 2^m)^2 \ (mod\ 2^{2m-2}.p)$

$$\equiv (2^{m-1}.pk)^2 \pm 2.2^{m-1}.pk.2^m + 2^{2m} (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{m-1}pk(2^{m-1}.pk \pm 2.2^m) + 2^{2m} (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{m-1}pk.2^{m-1}(pk \pm 2.2) + 2^{2m} \ (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{2m-2}.pk(pk \pm 4) + 2^{2m} \ (mod\ 2^{2m-2}.p)$$

$$\equiv 0 + 2^{2m} \ (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{2m} \ (mod\ 2^{2m-2}.p)$$

Therefore, the formulation satisfies the congruence and hence it can be considered as solutions of the said congruence for different values of positive integer k.

But for $k = 2^{m-1}$**, the solutions formula reduces to the form:**

$$x \equiv 2^{m-1}.p.2^{m-1} \pm 2^m (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{2m-2}.p \pm 2^m (mod\ 2^{2m-2}.p)$$

$$\equiv 0 \pm 2^m \ (mod\ 2^{2m-2}.p)$$

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

Also, for $k = 2^{m-1} + 1$**, the solutions formula reduces to the form:**

$$x \equiv 2^{m-1}.p.(2^{m-1} + 1) \pm 2^m (mod\ 2^{2m-1}.p)$$

$$\equiv 2^{2m-2}.p + 2^{m-1}.p \pm 2^m (mod\ 2^{2m-2}.p)$$

$$\equiv 0 + 2^{m-1}.p \pm 2^m (mod\ 2^{2m-2}.p)$$

$$\equiv 2^{m-1}.p \pm 2^m \ (mod\ 2^{2m-2}.p)$$

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

Therefore, all the solutions are given by

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

This gives $2.2^{m-1} = 2^m$ incongruent solutions as for each value of k gives exactly two solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 2^6\ (mod\ 2^4.5)$

It can be written as: $x^2 \equiv 2^{2.3}\ (mod\ 2^4.5)$

It is of the type $x^2 \equiv 2^{2m}\ (mod\ 2^{2m-2}.p)\ with\ m = 3, p = 5$.

It has exactly $2^{m+1}\ incongruent\ solutions$.

Its solutions are given by

$$x \equiv 2^{m-1}.pk \pm 2^m (mod\ 2^{2m-2}.p)$$
$$\equiv 2^2.5k \pm 2^3\ (mod\ 2^4.5)$$
$$\equiv 2^2.5k \pm 2^3\ (mod\ 2^4.5)$$
$$\equiv 20k \pm 8\ (mod\ 80); k = 0, 1, 2, 3.$$
$$\equiv 0 \pm 8; 20 \pm 8; 40 \pm 8; 60 \pm 8\ (mod\ 80)$$

≡8, 72; 12, 28; 32, 48; 52, 68 (mod 80)

These are the eight solutions.

Example-2: Consider the congruence $x^2 \equiv 2^8\ (mod\ 2^6.5)$

It can be written as: $x^2 \equiv 2^{2.4}\ (mod\ 2^6.5)$

It is of the type $x^2 \equiv 2^{2m}\ (mod\ 2^{2m-2}.p)\ with\ m = 4,\ p = 5$.

Its solutions are

$$x \equiv 2^{m-1}.pk \pm 2^m (mod\ 2^{2m-2}.p)$$
$$\equiv 2^3.5k \pm 2^4\ (mod\ 2^6.5)$$
$$\equiv 2^3.5k \pm 2^4\ (mod\ 2^6.5)$$
$$\equiv 40k \pm 16\ (mod\ 320); k = 0, 1, 2, 3, 4, 5, 6, 7.$$
$$\equiv 0 \pm 16; 40 \pm 16; 80 \pm 16; 120 \pm 16; 160 \pm 16; 200 \pm 16;$$
$$240 \pm 16; 280 \pm 16\ (mod\ 320)$$

≡16, 304; 24, 56; 64, 96; 104, 136; 144, 176; 184, 216; 224, 256; 264, 296 (mod 320)

These are the sixteen solutions.

CONCLUSION

Therefore, it is concluded that the congruence under consideration:

$x^2 \equiv 2^{2m}\ (mod\ 2^{2m-2}.p)$ has $2.2^{m-1} = 2^m$ Incongruent solutions given by

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

as for one value of k, the formula gives exactly two solutions of the quadratic congruence under consideration.

Merit of the paper

The present congruence under consideration is successfully formulated. It has a lot of solutions. All the solutions can be obtained at a time. Formulation provides all the solutions. These are the merit of the paper.

REFERENCES

[1] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.

[2] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley India (P) Ltd, 2008, ISBN: 978-81-265-1811-1.

[3] Burton David M., *Elementary Number Theory*, seventh edition, Mc Graw Hill education (India), 2017. ISBN: 978-1-25-902576-1.

[4] B M Roy, *A Study on Standard Quadratic Congruence of Prime Modulus having Solutions Consecutive- Integers*, Journal of Emerging Technologies and Innovative Research (JETIR),ISSN: 2349-5162, Vol-08, Issue-07, July-21.

[5] B M Roy, A A Qureshi, *Formulation of Solutions of a Special Standard Quadratic Congruence modulo an Even Prime Integer raised to the power n*, International Journal of Physics and Mathematics (IJPM), ISSN: 2664-8644, Vol-03, Issue-02, Aug-21.

[6] B M Roy, *Formulation of Standard Quadratic Congruence of Even Composite Modulus modulo an even prime raised to the power n*, International Journal of Research in Applied Science & Engineering Technology (IJRASET), ISSN: 2321-9653, Vol-09, Issue-09, Aug-21.

[7]B M Roy, *Solving special standard quadratic congruence of composite modulus modulo an odd prime multiple of powered even prime*, Journal of Emerging Technologies and Innovative Research (JETIR), ISSN: 2349-5162, Vol-08, Issue-09,Sep-21.