International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, July-August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Rp-135: Reformulation of Solutions of the Standard Quadratic Congruence of Composite Modulus- A Product of Odd Prime-Power Integer and Four

Prof B M Roy

Head, Department of Mathematics, Jagat Arts,
Commerce & I H P Science College, Goregaon, Maharashtra, India
(Affiliated to R T M Nagpur University)

ABSTRACT

In this paper, the author reformulated the solutions of the standard quadratic congruence of composite modulus- a product of odd prime-power integer and four. In the first formulation the solutions were obtained using different formulae. Now, a single formula is established for solutions. The formula is tested and verified using some illustrations. No need to use Chinese Remainder Theorem and solutions can now be obtained orally using the new formula. This is the merit of the paper.

KEYWORDS: *Composite modulus, Existed method, Odd prime-power integer*

How to cite this paper*:* Prof B M Roy "Rp-135: Reformulation of Solutions of the Standard Quadratic Congruence of Composite Modulus- A Product of Odd Prime-Power Integer and Four" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.1346-1347, URL: www.ijtsrd.com/papers/ijtsrd33079.pdf

IJTSRD33079

INTRODUCTION

The congruence under consideration is already formulated by the author, considering different cases [1], [2], [3]. Even the same congruence is again considered for reformulation of its solutions. After review of the previous formulation, the author found that the first formulation needs reformulation. The author wishes to find a single formula for the solutions and hence the congruence is considered for the study again.

PROBLEM-STATEMENT

Here the problem is: To reformulate the congruence: $x^2 \equiv a\ (mod\ 4p^m)$;
p *an odd prime and* $a$an even or odd perfect- square with $a \neq p$".

EXISTED METHOD

The existed method is popularly known as Chinese Remainder Theorem (CRT method). In this method the congruence under consideration is split into separate individual congruence as here:

$x^2 \equiv a\ (mod\ 4)$ ……………………………(A)

$x^2 \equiv a\ (mod\ p^m)$ …………………………(B)

After a rigorous study, it is seen that if$a \equiv 0, 1, 2\ (mod\ 4)$, the congruence (A) has exactly two solutions.These conditions on a can be assumed as the solvability condition of the original congruence.

The congruence (B) has only two solutions [5]. Hence, the congruence under consideration must have four solutions [5].

Using these solutions of the individual congruence and CRT method, the common solutions of the said congruence are obtained.

But the congruence (B) can be solved by iterative method [4].

$i.e$.at first, the congruence $x^2 \equiv a\ (mod\ p)$ is solved. Then using these solutions, the congruence $x^2 \equiv a\ (mod\ p^2)$ is solved. Proceeding in this way, at last the congruence

$x^2 \equiv a\ (mod\ p^m)$is solved. Definitely, to find the solutions of the congruence (B) is difficult, time-consuming and complicated.

NEED OF RESEARCH

Above congruence (B) is very difficult to solve using the existed method. Thomas Koshy [4]

Stated the iterative method for finding the solutions of the congruence (B). It takes a long time. To save the time in calculation, a new simple easy formulation is in an urgent need.

ANALYSIS & RESULTS

Consider the congruence: $x^2 \equiv a \ (mod\ 4p^m)$. If a is not a perfect-square, then it can be made a perfect-square as:
$x^2 \equiv a \ (mod\ 4p^m)$
$\equiv a + k.4p^m = b^2 (mod\ 4p^m)$ [6].

It is of the type: $x^2 \equiv a^2 (mod\ 4p^m)$. It is always solvable.

Consider the congruence:$x^2 \equiv a^2 (mod\ 4p^m)$.

For the solutions, consider $x \equiv 2p^m k \pm b \ (mod\ 4p^m)$

Then,
$x^2 \equiv (2p^m k \pm a\ )^2 \ (mod\ 4p^m)$
$\equiv (2p^m k)^2 \pm 2.2p^m k.a + a^2 \ (mod\ 4p^m)$
$\equiv 4p^{2m}k^2 \pm 4p^m k.a + a^2 \ (mod\ 4p^m)$
$\equiv 4p^m k(p^m k \pm a) + a^2 \ (mod\ 4p^m)$
$\equiv 0 + a^2 \ (mod\ 4p^m)$
$\equiv a^2 \ (mod\ 4p^m)$

Therefore, $x \equiv 2p^m k \pm a \ (mod\ 4p^m)$ satisfies the said congruence and hence it is a solution of the said congruence. But $for\ k = 2$, the solution reduces to
$x = 2p^m.2 \pm a \ (mod\ 4p^m)$
$\equiv 4p^m \pm a \ (mod\ 4p^m)$
$\equiv 0 \pm a \ (mod\ 4p^m)$

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

Similarly, for $k = 3$, the solutions are the same as for $k = 1$.

Therefore, all the solutions are given by $x \equiv 2p^m k \pm a \ (mod\ 4p^m); k = 0, 1$.

These are the required four solutions of the congruence.

ILLUSTRATIONS

Example-1: Consider the congruence:$x^2 \equiv 1 \ (mod\ 27436)$.
It can be written as: $x^2 \equiv 1^2 (mod\ 4.19^3) with\ p = 19, a = 1$.

It has four solutions given by
$x \equiv 2p^m k \pm a \ (mod\ 4.p^m); k = 0, 1.$
$\equiv 2.19^3 k \pm 1 \ (mod\ 4.19^3)$
$\equiv 2.6859k \pm 1 \ (mod\ 27436)$
$\equiv 13718k \pm 1 \ (mod\ 27436); k = 0, 1.$
$\equiv 0 \pm 1; 13718 \pm 1 \ (mod\ 27436).$
$\equiv 1, 27435; 13717, 13719 \ (mod\ 27436).$

Example-2: Consider the congruence:$x^2 \equiv 4 \ (mod\ 27436)$.

It can be written as: $x^2 \equiv 2^2 (mod\ 4.19^3) with\ p = 19, a = 2$, an even integer.

It has four solutions given by
$x \equiv 2p^m k \pm a \ (mod\ 4.p^m); k = 0, 1.$
$\equiv 2.19^3 k \pm 2 \ (mod\ 4.19^3)$
$\equiv 2.6859k \pm 2 \ (mod\ 27436)$
$\equiv 13718k \pm 2 \ (mod\ 27436); k = 0, 1.$
$\equiv 0 \pm 2; 13718 \pm 2 \ (mod\ 27436).$
$\equiv 2, 27434; 13716, 13720 \ (mod\ 27436).$

Example-3: Consider the congruence:
$x^2 \equiv 72 \ (mod\ 1372).$

It can be written as:
$x^2 \equiv 72 + 1372 = 1444 = 38^2 \ (mod\ 1372).$
$x^2 \equiv 38^2 (mod\ 4.7^3) with\ p = 7, a = 38.$

It has 4 solutions given by
$x \equiv 2p^m k \pm a \ (mod\ 4.p^m); k = 0, 1.$
$\equiv 2.7^3 k \pm 38 \ (mod\ 4.7^3)$
$\equiv 2.343k \pm 38 \ (mod\ 1372)$
$\equiv 686k \pm 38 \ (mod\ 1372); k = 0, 1.$
$\equiv 0 \pm 38; 686 \pm 38 \ (mod\ 1372)$
$\equiv 38, 1334; 648, 724 \ (mod\ 1372).$

These are the $four$ solutions of the congruence.

CONCLUSION

Therefore, it can be concluded that the congruence $x^2 \equiv a^2 (mod\ 4.p^m)$ with an odd prime p has exactly four solutions for a positive integer a either odd or even, has the solutions given by $x \equiv 2p^m k \pm a \ (mod\ 4.p^m); k = 0, 1.$

MERIT OF THE PAPER

Formulation is the merit of the paper. A formula for solutions is established. First time a formula is available for the readers. No need to use Iterative method and Chinese Remainder Theorem for solutions.

REFERENCE

[1] Roy B m, *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-03, Issue-05, May-18.

[2] Roy B M, *Formulation of a class of standard quadratic congruence of composite modulus- a positive prime multiple of four*, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-11, Nov-19.

[3] Roy B M, *Formulation of a very special type of standard quadratic congruence of composite modulus- a product of powered odd prime and four,*, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-07, July-20.

[4] Thomas Koshy, *Elementary Number Theory with Applications*, ISBN: 978-81-312-1859-4, Academic Press, Indian Print, second edition, 2009.

[5] Zuckerman H. S., Niven I., Montgomery H. L., "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, Page No. 136-136, Exercise-18, ISBN: 978-81-265-1811-1. (1960: Reprint 2008).

[6] Roy B M, *Discrete Mathematics & Number Theory*, ISBN: 978-93-84336-12-7, First edition, Jan-2016, Das GanuPrakashan, Nagpur, India.