International Journal of Mathematical Archive-12(1), 2021, 20-23
Available online through www.ijma.info ISSN 2229 – 5046

A DISCUSSION ON SOLVING STANDARD QUADRATIC CONGRUENCE OF EVEN COMPOSITE MODULUS MODULO A SPECIAL EVEN MULTIPLE OF AN ODD 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.
(Affiliated to R T M Nagpur University)**

(Received On: 27-12-20; Revised & Accepted On: 04-01-21)

ABSTRACT

In this paper, the author discussed the solutions of the standard quadratic congruence of composite modulus modulo a special even multiple of an odd prime in two cases. It is found that in the first case, the congruence has eight incongruence solutions while in the second case, it has sixteen incongruent solutions. The author established different formulae for the solutions for the congruence for both the cases. Formulation of solutions is the merit of the paper.

Key-Words: *Composite Modulus, Chinese Remainder Theorem, Odd Prime, Quadratic Residues, Quadratic congruence.*

INTRODUCTION

A standard quadratic congruence of composite modulus is a congruence of the type: $x^2 \equiv a\ (mod\ m)$, m being a composite positive integer, $a$any integer. This congruence is solvable if$a$ is quadratic residue of m i.e. $r^2 \equiv a\ (mod\ m),\ r\ being\ a\ residue\ of\ m$. Here the author considers $m = 2^n.p;\ p\ odd\ prime\ and\ n\ positive\ integer$. So, the congruence under consideration is

$$x^2 \equiv a\ (mod\ 2^n.p) \tag{1}$$

PROBLEM STATEMENT

Here the problem is-"To discuss the solutions of the congruence:

$$x^2 \equiv a\ (mod\ 2^n.p),\ \ p\ odd\ prime, n\ positine\ integer\ in\ two\ cass.$$

LITERATURE REVIEW

Such types of congruence are not formulated earlier by earlier mathematicians. The literature of mathematics is nearly silent to provide any type of formulation for its solutions. Readers are compelled to use Chinese Remainder theorem [1]. This is the only existed method.

EXISTED METHOD

In [2], only standard quadratic congruence of prime modulus are discussed while in [3], congruence of composite modulus are also discussed, but using Chinese Remainder Theorem.

The congruence in the problem stated can be solved using Chinese Remainder Theorem by spliting into two individual congruence:

$$x^2 \equiv a\ (mod\ p) \tag{2}$$
$$x^2 \equiv a\ (mod\ 2^n) \tag{3}$$

Corresponding Author: Prof B M Roy
Head, Department of Mathematics,
Jagat Arts, Commerce & I H P Science College, Goregaon,
Dist-Gondia, M. S., INDIA, Pin: 441801.
(Affiliated to R T M Nagpur University)

Congruence (2) has exactly two incongruent solutions [2] while the congruence (3) has exactly four incongruent solutions, if $a \equiv 1\ (mod\ 8)\ i.e.\ a\ is\ an\ odd\ positive\ integer$ [2]. But if a is a perfect square even positive integer, then the congruence has exactly eight incongruent solutions [4]. Hence it can be easily said that the congruence under consideration (1) must have eight or sixteen incongruent solutions. Sometimes, the congruence (1) takes a long time to find its two solutions. There is no method to find the solutions found in the literature of mathematics except the author's Middle- pair solutions formulation [5].The author already has formulated the same congruence with $m = 2$ & 3 [6], [7].

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv a\ (mod\ 2^n.p),\ p\ odd\ prime.$
It is a standard quadratic congruence of composite modulus.
Such types of congruence are only solvable if a is a quadratic residue of p.

So, a can always be expressible as b^2 by adding $k.p.2^n\ \ to\ a\ \ i.e.\ a = b^2\ \ or\ \ a + k.p.2^n = b^2$, for some suitable k.
Then the congruence is written as: $x^2 \equiv b^2 (mod\ 2^n.p)$.

Case-I: Let a be an odd positive integer such that $a \equiv 1\ (mod\ 8)$.

For solutions, consider $x \equiv 2^{n-1}pk \pm b\ (mod\ 2^n.p)$
Then, $x^2 \equiv (2^{n-1}pk \pm b)^2 (mod\ 2^n.p)$
$\equiv (2^{n-1}pk\ )^2 \pm 2.2^{n-1}pk.b + b^2\ (mod\ 2^n.p)$
$\equiv 2^{2n-2}p^2k^2 \pm 2^n.pkb + b^2\ (mod\ 2^n.p)$
$\equiv 2^n pk(2^{n-2}pk \pm b) + b^2\ (mod\ 2^n.p)$
$\equiv b^2\ (mod\ 2^n.p)$.

Thus, $x \equiv 2^{n-1}pk \pm b\ (mod\ 2^n.p)$ are the solutions of the congruence.

But for $k = 2$, the solutions formula reduces to: $x \equiv 2^{n-1}p.2 \pm b\ (mod\ 2^n.p)$
$\equiv 2^n p \pm b\ (mod\ 2^n.p)$
$\equiv 0 \pm b\ (mod\ 2^n.p)$
These are the same solutions as for $k = 0$.

Also for$k = 3 = 2 + 1$, the solutions formula reduces to: $x \equiv 2^{n-1}p.(2 + 1) \pm b\ (mod\ 2^n.p)$
$\equiv 2^n.p + p.2^{n-1} \pm b\ (mod\ 2^n.p)$
$\equiv\ 2^{n-1}.p \pm b\ (mod\ 2^n.p)$
These are the same solutions as for $k = 1$.

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

This gives only four of the eight solutions.

For the remaining four solutions, consider $x \equiv \pm(2pk \pm b)(mod\ 2^n.p)$.
Then, $x^2 \equiv (2pk \pm b)^2 (mod\ 2^n.p)$
$\equiv (2pk\ )^2 \pm 2.2pk.b + b^2\ (mod\ 2^n.p)$
$\equiv 4p^2k^2 \pm 4.pkb + b^2\ (mod\ 2^n.p)$
$\equiv 4pk(pk \pm b) + b^2\ (mod\ 2^n.p)$
$\equiv 4p.2^{n-2}t + b^2 (mod\ 2^n.p),\ if\ k(pk \pm b) = 2^{n-2}t.$
$\equiv b^2 (mod\ 2^n.p)$.
These gives the remaining four solutions of the congruence.

Therefore, the congruence in the problem has exactly eight incongruent solutions.

Case-II: Let b be an even perfect square.
Consider $x \equiv 2^{n-3}.pk \pm b\ (mod\ 2^n.p)$.
Then, $x^2 \equiv (2^{n-3}pk \pm b)^2 (mod\ 2^n.p)$
$\equiv (2^{n-3}pk\ )^2 \pm 2.2^{n-3}pk.b + b^2\ (mod\ 2^n.p)$
$\equiv 2^{2n-6}p^2k^2 \pm 2^{n-2}.pkb + b^2\ (mod\ 2^n.p)$
$\equiv 2^{n-2}pk(2^{n-4}pk \pm b) + b^2\ (mod\ 2^n.p)$
$\equiv 2^{n-2}pk(2^{n-4}pk \pm 4t) + b^2 (mod\ 2^n.p) as\ b\ is\ even\ perfect\ square.$
$\equiv 2^n pk(2^{n-6}pk \pm t) + b^2\ (mod\ 2^n.p)$
$\equiv b^2\ (mod\ 2^n.p)$.
Thus, $x \equiv 2^{n-3}pk \pm b\ (mod\ 2^n.p)$ are the solutions of the congruence.

But for $k = 8$, the solutions formula reduces to: $x \equiv 2^{n-3}p.8 \pm b\ (mod\ 2^n.p)$
$\equiv 2^n p \pm b\ (mod\ 2^n.p)$
$\equiv 0 \pm b\ (mod\ 2^n.p)$
These are the same solutions as for $k = 0$.

Also for$k = 9 = 8 + 1$, the solutions formula reduces to: $x \equiv 2^{n-3}p.(8+1) \pm b\ (mod\ 2^n.p)$
$\equiv 2^n.p + 2^{n-3}.p \pm b\ (mod\ 2^n.p)$
$\equiv\ 2^{n-3}.p \pm b\ (mod\ 2^n.p)$
These are the same solutions as for $k = 1$.

Therefore, the solutions are given by:$x \equiv 2^{n-3}pk \pm b\ (mod\ 2^n.p);\ k = 0, 1, 2, 3, 4, 5, 6, 7.$

These gives the sixteen incongruent solutions of the congruence.

ILLUSTRATIONS

Example-1: Consider the congruence$x^2 \equiv 9\ (mod\ 80)$.
It can be written as $x^2 \equiv 3^2 (mod\ 2^4.5)$.
It is of the type $x^2 \equiv b^2 (mod\ 2^n.p)\ with\ p = 5, n = 4, b = 3, an\ odd\ positive\ integer.$
It has exactly eight incongruent solutions.
The four of the eight solutions are given by $x \equiv 2^{n-1}.pk \pm a\ (mod\ 2^n.p)$.
$\equiv 2^3.5k \pm 3\ (mod\ 2^4.5)$
$\equiv 40k \pm 3\ (mod\ 80), k = 0, 1.$
$\equiv 0 \pm 3; 40 \pm 3\ (mod\ 80).$
$\equiv 3, 80-3; 40-3, 40+3\ (mod\ 80)$
$\equiv 3, 77; 37, 43\ (mod\ 80).$

The other four solutions are given by: $x \equiv \pm(2pk \pm b\ )\ (mod\ 2^n.p), if\ (pk \pm b) = 2^{n-2}t$
$\equiv \pm(2.5k \pm 3)\ (mod\ 2^4.5), if\ (5k \pm 3) = 2^{4-2}t.$
$\equiv \pm(10k \pm 3)(mod\ 80), if\ (5k \pm 3) = 4t$
$\equiv \pm(10k \pm 3)\ (mod\ 5.16), if\ (5k \pm 3) = 4t$
$\equiv \pm(10k \pm 3)\ (mod\ 80)$

But for $k = 1, (5.1 + 3) = 8 = 4.2$
So, $x \equiv \pm(10.1 + 3)\ (mod\ 5.2^4)$
$\equiv \pm 13\ (mod\ 80)$
$\equiv 13, 67\ (mod\ 80).$

Also, for $k = 3, (5.3 - 3) = 12 = 4.3$
So, $x \equiv \pm(10.3 - 3)\ (mod\ 5.2^4)$
$\equiv \pm 27\ (mod\ 80)$
$\equiv 27, 53\ (mod\ 80).$

Therefore, all the eight solutions are $x \equiv 3, 77; 13, 67;\ 27, 53;\ 37, 43\ (mod\ 80).$

Example-2: Consider the congruence$x^2 \equiv 49\ (mod\ 160)$.
It can be written as $x^2 \equiv 7^2 (mod\ 2^5.p)$.
It is of the type $x^2 \equiv b^2 (mod\ 2^n.p)\ with\ p = 5, n = 5, b = 7,\ \ an\ odd\ positive\ integer.$
It has exactly eight incongruent solutions given by $x \equiv 2^{n-1}.pk \pm a\ (mod\ 2^n.p)$.
$\equiv 2^4.5k \pm 7\ (mod\ 2^5.5)$
$\equiv 80k \pm 7\ (mod\ 160), k = 0, 1.$
$\equiv 0 \pm 7; 80 \pm 7\ (mod\ 160).$
$\equiv 7, 153; 73,\ 87\ (mod\ 160).$

The other four solutions are given by: $x \equiv \pm(2pk \pm b\ )\ (mod\ 2^n.p), if\ (pk \pm b) = 2^{n-2}t$
$\equiv \pm(2.5k \pm 7)\ (mod\ 2^5.5), if\ (5k \pm 7) = 2^{5-2}t.$
$\equiv \pm(10k \pm 7)(mod\ 32.5), if\ (5k \pm 7) = 8t$
$\equiv \pm(10k \pm 3)\ (mod\ 160.), if\ (5k \pm 7) = 8t$
$\equiv \pm(10k \pm 7)\ (mod\ 160)$

But for $k = 3, (5.3 - 7) = 8 = 8.1$
So, $x \equiv \pm(10.3 - 7)\ (mod\ 2^5.5)$
$\equiv \pm 23\ (mod\ 160)$
$\equiv 23, 137\ (mod\ 160).$

Also, for $k = 5, (5.5 + 7) = 32 = 8.4$

So, $x \equiv \pm(10.5 + 7)\ (mod\ 2^5.5)$
$\equiv \pm 57\ (mod\ 160)$
$\equiv 57, 103\ (mod\ 160)$.
Therefore, all the eight solutions are $x \equiv 7, 153; 73, 87;\ 23, 137;\ 57, 103\ (mod\ 160)$.

Example-3: Consider the congruence$x^2 \equiv 36\ (mod\ 160)$.
It can be written as $x^2 \equiv 6^2 (mod\ 2^5.5)$.
It is of the type $x^2 \equiv b^2 (mod\ 2^n.p)\ with\ p = 5, n = 5, b = 6,\ \ an\ even\ positive\ integer$.
It has exactly sixteen incongruent solutions given by

$x \equiv 2^{n-3}.pk \pm a\ (mod\ 2^n.p)$.
$\equiv 2^2.5k \pm 6\ (mod\ 2^5.5)$
$\equiv 20k \pm 6\ (mod\ 160), k = 0, 1.$
$\equiv 0 \pm 6; 20 \pm 6; 40 \pm 6\ ; 60 \pm 6; 80 \pm 6; 100 \pm 6; 120 \pm 6; 140 \pm 6\ (mod\ 160)$.
$\equiv 6, 154; 14, 26; 34, 46;\ 54, 66; 74, 86; 94, 106; 114, 126; 134, 146\ \ (mod\ 160)$.

These are the sixteen incongruent solutions.

CONCLUSION

Therefore, it can be concluded that the congruence under consideration: $x^2 \equiv a\ (mod\ 2^n.p),\ p\ odd\ prime$, has exactly eight incongruent solutions, if $a \equiv 1\ (mod\ 8)$
$i.e.\ a\ is\ some\ special\ odd\ positive\ integer$; it has exactly sixteen incongruent solutions if a is an even perfect square.

MERIT OF THE PAPER

The congruence under consideration can be solved very easily and sometimes orally also using the author's formulation established. This is the merit of the paper.

REFERENCE

1. Roy B M, 2016, *Discrete Mathematics & Number Theory*, Das GanuPrakashan, Nagpur, India, 1/e, ISBN: 978-93-84336-12-7.
2. Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.
3. Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Delhi, India, ISBN:978-81-312-1859-4.
4. Roy B M,*Reformulation of a special standard quadratic congruence of even composite modulus*, International Journal of Management Research and social science (IJMRSS), ISSN: 2394-6415, Vol-07, Issue-2A, Mar-20.
5. Roy B M, *A New Method of Finding Solutions of a Class of Standard Quadratic Congruence of Prime Modulus*, International Journal Of Advanced Research, Ideas, Innovation in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-06, Nov-Dec-18.
6. Roy B M,*Formulation of a class of standard quadratic congruence of composite modulus- a positive prime multiple of four*, International Journal of science and Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-11, Nov-18.
7. Roy B M, *Reformulation of solutions of a class of standard quadratic congruence of composite modulus-a product of an odd prime and eight*, International Journal for research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-05, Issue-08, Aug-20.

Source of support: Nil, Conflict of interest: None Declared.