International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-56: Reformulation of Solutions of a Standard Quadratic Congruence of Composite Modulus- An Eighth Multiple of a Product of Two Odd Primes

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, Nagpur)

ABSTRACT

In this paper, the author considered a very general type of standard quadratic congruence of composite modulus- an eighth multiple of product of two odd primes for reformulation of its solutions. The author's first formulation was very simple but readers had to use many formulae for its solutions. Now the reformulation reduces the numbers of formulae for solutions. The discovered formula is justified and verified by using some required suitable numerical examples. The congruence is first time formulated. It is the merit of the paper. The existed method is complicated and time-consuming. Now a time-saving formulation is obtained.

KEYWORDS: *Chinese Remainder Theorem (CRT), Composite modulus, odd primes, Quadratic Congruence*

How to cite this paper: Prof B M Roy "RP-56: Reformulation of Solutions of a Standard Quadratic Congruence of Composite Modulus- An Eighth Multiple of a Product of Two Odd Primes" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.527-529, URL: www.ijtsrd.com/papers/ijtsrd33407.pdf

IJTSRD33407

INTRODUCTION

Here, a standard quadratic congruence of *composite modulus*- an eighth multiple of product of two odd primes, is considered for reformulation. It is of the type:
$x^2 \equiv a^2 (mod\ 8pq)$, p, q being positive odd prime integers. It is always solvable. Such type of standard quadratic congruence is not formulated by the earlier mathematicians.

Hence the author took the responsibility of formulating the congruence for its solutions.

The said congruence is already formulated by the author [3] but the author found one more simple and useful formulation.

LITERATURE REVIEW

No formulation is found for the said congruence. Only the use of Chinese Remainder Theorem [1], [2] is discussed. Much had been written on standard quadratic congruence of prime modulus but no formulation for quadratic congruence of composite modulus is found. A short discussion is found in the book of Thomas Koshy[1]. He used Chinese Remainder Theorem for solutions.

Knowing this, the author tried his best to formulate the congruence for solutions. The author already had formulated many standard quadratic congruence of composite modulus[3], [4], [5], [6]. In this sequence of formulation, the author found this present quadratic congruence unformulated and hence it is considered for formulation.

PROBLEM-STATEMENT

Here the problem is-
"To reformulate the solutions of the standard quadratic congruence of composite modulus of the type:$x^2 \equiv a^2 (mod\ 8pq)$ with p, qareodd primes in two cases:
Case-I: a is an odd prime,
Case-II: a is an even prime.

ANALYSIS & RESULTS

Solution by Existed Method
The congruence under consideration can be split into three individual congruence as:

$x^2 \equiv a\ (mod\ 8) \dots\dots\dots\dots\dots..(1)$

$x^2 \equiv a\ (mod\ p) \dots\dots\dots\dots\dots\dots(2)$

$x^2 \equiv a\ (mod\ q) \dots\dots\dots\dots\dots\dots.(3)$

The congruence (1) has four solutions, if $a \equiv 1\ (mod\ 8)\ i.e. if\ a\ is\ odd\ positive$

$integer$ [2] but has exactly two solutions if a is even positive integer.The congruence (2)& (3)have exactly two-two solutions.

So, the congruence under consideration must have sixteen solutions, if $a \equiv 1\ (mod\ 8)$ and has eight solutions, if a is even positive integer.

These solutions can be obtained by solving the individual congruence separately and the common solutions are obtained using CRT.

Author's Formulation of Solutions

Consider the congruence:$x^2 \equiv a(mod\ 8pq)$.

If $a = b^2$, then the congruence reduces to: $x^2 \equiv b^2 (mod\ 8pq)$.

Case-I: Let a be an odd positive integer.Then b is also an odd positive integer.

Let $x \equiv 2pqk \pm b\ (mod\ 8pq)$.

Then $x^2 \equiv (2pqk \pm b)^2\ (mod\ 8pq)$

$\equiv (2pqk)^2 \pm 2.2pqk + b^2\ (mod\ 8pq)$

$\equiv 4p^2q^2k^2 \pm 4pqk.b + b^2\ (mod\ 8pq)$

$\equiv 4pqk\ (pqk \pm b) + b^2\ (mod\ 8pq)$

$\equiv 4pqk\{2t\} + b^2 (mod\ 8pq)$.

Therefore, $x \equiv 2pqk \pm b\ (mod\ 8pq)$ satisfies the congruence and hence it is a solution.

But for $k = 4$, the solutions reduces to

$x \equiv 2pq.4 \pm b\ (mod\ 8pq)$

$\equiv 8pq \pm b\ (mod\ 8pq)$

$\equiv 0 \pm b\ (mod\ 8pq)$.

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

Therefore, the eight solutions are given by $x \equiv 2pqk \pm b\ (mod\ 8pq); k = 0, 1,2,3$.

For the remaining eight solutions, consider $x \equiv \pm(2pk \pm b)\ (mod\ 8pq)$.

Then $x^2 \equiv (2pk \pm b)^2\ (mod\ 8pq)$

$\equiv (2pk)^2 \pm 2.2pk + b^2\ (mod\ 8pq)$

$\equiv 4p^2k^2 \pm 4pk.b + b^2\ (mod\ 8pq)$

$\equiv 4pk\ (pk \pm b) + b^2 (mod\ 8pq); if\ k(pk \pm b) = 2qt$.

$\equiv 4p\{2qt\} + b^2 (mod\ 8pq)$

$\equiv 8pqt + b^2\ (mod\ 8pq)$

$\equiv b^2\ (mod\ 8pq)$

Thus, $x \equiv \pm(2pk \pm b)\ (mod\ 8pq)$ gives the solutions $if\ k(pk \pm b) = 2qt$.

Case-II: Let a be an even positive integer.

Let$x \equiv 4pqk \pm b\ (mod\ 8pq)$.

Then $x^2 \equiv (4pqk \pm b)^2\ (mod\ 8pq)$

$\equiv (4pqk)^2 \pm 2.4pqk + b^2\ (mod\ 8pq)$

$\equiv 16p^2q^2k^2 \pm 8pqk.b + b^2\ (mod\ 8pq)$

$\equiv 8pqk\ (2pqk \pm b) + b^2\ (mod\ 8pq)$

$\equiv 8pqk\{t\} + b^2 (mod\ 8pq)$.

Therefore, $x \equiv 4pqk \pm b\ (mod\ 8pq)$ satisfies the congruence and hence it is a solution.

But for $k = 2$, the solutions reduces to

$x \equiv 4pq.2 \pm b\ (mod\ 8pq)$

$\equiv 8pq \pm b\ (mod\ 8pq)$

$\equiv 0 \pm b\ (mod\ 8pq)$.

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

Therefore, the four solutions are given by $x \equiv 4pqk \pm b\ (mod\ 8pq); k = 0, 1$.

For the remaining four solutions, consider $x \equiv \pm(4pk \pm b)\ (mod\ 8pq)$.

Then $x^2 \equiv (4pk \pm b)^2\ (mod\ 8pq)$

$\equiv (4pk)^2 \pm 2.4pk + b^2\ (mod\ 8pq)$

$\equiv 16p^2k^2 \pm 8pk.b + b^2\ (mod\ 8pq)$

$\equiv 8pk\ (2pk \pm b) + b^2 (mod\ 8pq); if\ k(2pk \pm b) = qt$.

$\equiv 8p\{qt\} + b^2 (mod\ 8pq)$

$\equiv 8pqt + b^2\ (mod\ 8pq)$

$\equiv b^2\ (mod\ 8pq)$

Thus, $x \equiv \pm(4pk \pm b)\ (mod\ 8pq)$ gives the solutions $if\ K(2pk \pm b) = qt$.

ILLUSTRATIONS

Example-1: consider the congruence: $x^2 \equiv 49\ (mod 120)$.

It can be written as $x^2 \equiv 7^2\ (mod 8.5.3)$

It is of the type: $x^2 \equiv b^2 (mod\ 8pq)$

$with\ p = 5, q = 3, b = 7, an\ odd\ positive\ integer$.

Therefore, it has sixteen solutions, eight are given by

$x \equiv 2pqk \pm b\ (mod\ 8pq)$.

$\equiv 2.5.3k \pm 7\ (mod\ 8.5.3)$

$\equiv 30k \pm 7\ (mod\ 120); k = 0, 1, 2, 3$.

$\equiv 0 \pm 7; 30 \pm 7; 60 \pm 7; 90 \pm 7\ (mod\ 120)$

$\equiv 7, 113; 23, 37; 53, 67; 83, 97\ (mod\ 120)$.

The remaining eight solutions are given by

$x \equiv \pm(2pk \pm b)(mod\ 8pq), if\ k(pk \pm b) = 2qt$.

$\equiv \pm(2.5k \pm 7)(mod\ 120), if\ k(5k\ \pm 7) = 2.3t$

$\equiv \pm(10k \pm 7)(mod\ 120), if\ k(5k \pm 7) = 6t$.

But for $k = 1, we\ have\ 1.(5.1 + 7) = 6t\ i.e. 5 + 7 = 12 = 6t$

The corresponding solutions are

$x \equiv \pm(10.1 + 7)\ (mod\ 120)$

$\equiv \pm 17\ (mod\ 120)$

$\equiv 17, 103 (mod\ 120)$.

Also for $k = 2, we\ have\ 2.(5.2 - 7) = 6 = 6t$

The corresponding solutions are

$x \equiv \pm(10.2 - 7)\ (mod\ 120)$

$\equiv \pm 13\ (mod\ 120)$

$\equiv 13, 107\ (mod\ 120)$.

Also for $k = 4, we\ have\ 4.(5.4 + 7) = 108 = 6t$

The corresponding solutions are
$x \equiv \pm(10.4 + 7)\ (mod\ 120)$
$\equiv \pm 47\ (mod\ 120)$
$\equiv 47, 73\ (mod\ 120).$

Also for $k = 5, we\ have\ 5.(5.5 - 7) = 5.18 = 6t$

The corresponding solutions are
$x \equiv \pm(10.5 - 7)\ (mod\ 120)$
$\equiv \pm 43\ (mod\ 120)$
$\equiv 43, 77\ (mod\ 120).$

Therefore all the sixteen solutions are
$x \equiv 7, 113; 23, 37; 53, 67; 83, 97;\ 13, 107;$
$17, 103; 47, 73; 43, 77\ (mod\ 120).$

Example-2: Consider the congruence: $x^2 \equiv 4\ (mod 120)$.

It can be written as $x^2 \equiv 2^2\ (mod 8.5.3)$

It is of the type: $x^2 \equiv b^2 (mod\ 8pq)$
$with\ p = 5, q = 3, b = 2, an\ even\ positive\ integer.$

It has eight solutions, four are given by $x \equiv 4pqk \pm b\ (mod\ 8pq)$.
$\equiv 4.5.3k \pm 2\ (mod\ 8.5.3)$
$\equiv 60k \pm 2\ (mod\ 120); k = 0, 1.$
$\equiv 0 \pm 2; 60 \pm 2\ (mod\ 120)$
$\equiv 2, 118; 58, 62\ (mod\ 120).$

The remaining four solutions are given by
$x \equiv \pm(4pk \pm b)(mod\ 8pq), if\ k(2pk \pm b) = qt.$
$\equiv \pm(4.5k \pm 2)(mod\ 120), if\ k(2.5k\ \pm 2) = 3t$
$\equiv \pm(20k \pm 2)(mod\ 120), if\ K(10k \pm 2) = 3t.$

But for $k = 1, we\ have\ 1.(10.1 + 2) = 3t\ i.e. 10 + 2 = 12 = 3t$

The corresponding solutions are
$x \equiv \pm(20.1 + 2)\ (mod\ 120)$
$\equiv \pm 22\ (mod\ 120)$
$\equiv 22, 98\ (mod\ 120).$

Also for$k = 2, we\ have\ 2.(10.2 - 2) = 36 = 3t$
The corresponding solutions are
$x \equiv \pm(20.2 - 2)\ (mod\ 120)$
$\equiv \pm 38\ (mod\ 120)$
$\equiv 38, 82\ (mod\ 120).$

Therefore all the eight solutions are given by
$x \equiv 2, 118; 58, 62; 22, 98; 38, 82\ (mod\ 120).$

CONCLUSION

Therefore it is concluded that the said congruence: $x^2 \equiv b^2 (mod\ 8pq)$ with b an odd positive integer, has sixteen incongruent solutions; eight solutions are given by
$x \equiv 2pqk \pm b\ (mod\ 8pq)\ with\ k = 0, 1, 2, 3.$

The remaining eight solutions are given by
$x \equiv \pm(2pk \pm b)(mod\ 8pq),$
$if\ k(pk \pm b) = 2qt.$

But if b is an even positive integer, then the said congruence has exactly eight incongruent solutions; the four solutions are given by $x \equiv 4pqk \pm b\ (mod\ 8pq)$ with $k = 0, 1$.The remaining four solutions are given by $x \equiv \pm(4pk \pm b)(mod\ 8pq), if\ k(2pk \pm b) = qt.$

MERIT OF THE PAPER

The said congruence under consideration is first time formulated for its solutions. The readers get formulation for its solutions. It is time – saving & simple. It is also labour-saving. This is the merit of the paper.

REFERENCE

[1] Thomas Koshy, *(2009) Elementary Number Theory with Applications*, Academic Press (An Imprint of Elsevier), ISBN: 978-81-312-1859-4.

[2] Zuckerman H. S., Niven I., Montgomery H. L., (2008) "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.

[3] oy B M, *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, Vol-04, Issue-04, July-18.

[4] Roy B M, *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, Vol-02, Issue-02, June-18.

[5] Roy B M, *Formulation of solutions of standard quadratic congruence of even composite modulus*, International Journal of Research science and management (IJRSM), ISSN: 2243-7789, Vol-05, Issue-05, May-18.

[6] Roy B M, *Formulation of solutions of solvable standard quadratic congruence of odd composite modulus as a product of two different odd primes and also a product of twin-primes*, International Journal of Current Research (IJCR), ISSN: 0975-833X, Vol-10, Issue-05, May-18.