iJETRM
International Journal of Engineering Technology Research & Management

RP-34: FORMULATION OF SOLUTIONS OF A STANDARD QUADRATIC CONGRUENCE OF COMPOSITE MODULUS- A PRODUCT OF TWO DIFFERENT POWERED ODD PRIMES AND EIGHT

Prof B M Roy
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- Gondia, M. S., India. Pin: 441801
(Affiliated to R T M Nagpur University)

ABSTRACT
In this paper, the author has formulated a standard quadratic congruence of composite modulus- a product of two different powered odd primes and eight. The solutions can be obtained very easily using this formulation. No such formulation is available in the literature of mathematics. These congruence have sixteen incongruent solutions for an odd positive integer but have eight incongruent solutions for an even positive integer mentioned in the congruence.

Keywords: Composite modulus, Chinese Remainder Theorem (CRT), Quadratic Congruence.

INTRODUCTION

The congruence of the type $x^2 \equiv a\ (mod\ m), m\ any\ composite\ positive\ integer$, is a standard quadratic congruence of composite modulus. If a is a quadratic residue of m, it is solvable. If it is solvable, then it can be written as: $x^2 \equiv a^2\ (mod\ m)$[1].
In this paper, the author wishes to take $m = 8p^m q^n; p, q$ are different positive odd primes and m, n are positive integers.

PROBLEM-STATEMENT

The problem is "To formulate the solutions of the standard quadratic congruence
$x^2 \equiv a^2\ (mod\ 8p^m q^n), p, q\ are\ odd\ primes\ with\ a \neq p,\ a \neq q.$

LITERATURE REVIEW

The method of finding solutions of the stated quadratic congruence or any type of formulation is not found in the literature of mathematics except the author's formulation of some of standard quadratic congruence [4]. Even the readers can use the
Familiar Chinese Remainder Theorem (CRT) [2]. The author found the clue of this quadratic congruence in the book of Koshy [3].

ANALYSIS & RESULTS

Consider the congruence under consideration: $x^2 \equiv a^2\ (mod\ 8p^m q^n)$, p, q odd primes.
Case-I: Let a be an odd positive integer.
Then for solutions consider $x \equiv 2p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1, 2, \ldots..$
So, $x^2 \equiv (2p^m q^n k \pm a\ )^2\ (mod\ 8.p^m q^n)$
$\equiv (2p^m q^n k\ )^2 \pm 2.2p^m q^n k.a + a^2\ (mod\ 8.p^m q^n)$

iJETRM
International Journal of Engineering Technology Research & Management

$\equiv 4p^m q^n k(\, p^m q^n k \pm a) + a^2 \ \ (mod\ 8.p^m q^n)$
$\equiv 4p^m q^n k\ (\, 2t) + a^2\ (mod\ 8.p^m q^n)$
$\equiv a^2 (mod\ 8.p^m q^n)$.

Therefore, $x \equiv 2p^m q^n k \pm a\ (mod\ 8.p^m q^n)$ **are the solutions of the congruence.**

But for $k = 4$**, the solutions reduces to** $x \equiv 2p^m q^n.4 \pm a\ (mod\ 8.p^m q^n)$
$\equiv 8p^m q^n \pm a\ (mod\ 8p^m q^n)$
$\equiv \pm a\ (mod\ 8p^m q^n)$.

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

Also the solutions repeat for $k = 5, 6, 7 \ldots \ldots$ **as for** $k = 1, 2, 3 \ldots$

Thus, the eight solutions are given by

$x \equiv 2p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1, 2, 3.$

For the remaining eight solutions, consider $x \equiv \pm(2p^m k \pm a)\ (mod\ 8p^m q^n)$.

$x^2 \equiv (2p^m k \pm a\ )^2\ (mod\ 8p^m q^n)$
$\equiv (2p^m k\ )^2 \pm 2.2p^m k.a + a^2\ (mod\ 8p^m q^n)$
$\equiv 4p^m k\ (\, p^m k \pm a) + a^2\ (mod\ 8p^m q^n)$
$\equiv 4p^m k(\, 2q^n t) + a^2\ (mod\ 8p^m q^n)$
$\equiv a^2\ (mod\ 8p^m q^n)$**, if** $k(p^m k \pm a) = 2q^n t$.

For different values of k**, this gives the remaining eight solutions of the congruence.**

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

Then for solutions consider $x \equiv 4p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1, 2, \ldots\ldots$

So, $x^2 \equiv (4p^m q^n k \pm a\ )^2\ (mod\ 8.p^m q^n)$
$\equiv (4p^m q^n k\ )^2 \pm 2.4p^m q^n k.a + a^2\ (mod\ 8.p^m q^n)$
$\equiv 8p^m q^n k(2\, p^m q^n k \pm a) + a^2\ \ (mod\ 8.p^m q^n)$
$\equiv 4p^m q^n k\ (\, t) + a^2\ (mod\ 8.p^m q^n)$
$\equiv a^2 (mod\ 8.p^m q^n)$.

Therefore, $x \equiv 4p^m q^n k \pm a\ (mod\ 8.p^m q^n)$ **are the solutions of the congruence.**

But for $k = 2$**, the solutions reduces to** $x \equiv 2p^m q^n.4 \pm a\ (mod\ 8.p^m q^n)$
$\equiv 8p^m q^n \pm a\ (mod\ 8p^m q^n)$
$\equiv \pm a\ (mod\ 8p^m q^n)$.

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

Also the solutions repeat for $k = 3, 4 \ldots \ldots$ **as for** $k = 1, 2, \ldots$

Thus, the four solutions are given by: $x \equiv 4p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1.$

For the remaining four solutions, consider $x \equiv \pm(2p^m k \pm a)\ (mod\ 8p^m q^n)$.

$x^2 \equiv (2p^m k \pm a\ )^2\ (mod\ 8p^m q^n)$
$\equiv (2p^m k\ )^2 \pm 2.2p^m k.a + a^2\ (mod\ 8p^m q^n)$
$\equiv 4p^m k\ (\, p^m k \pm a) + a^2\ (mod\ 8p^m q^n)$
$\equiv 4p^m k(\, 2q^n t) + a^2\ (mod\ 8p^m q^n)$
$\equiv a^2\ (mod\ 8p^m q^n)$**, if** $k(p^m k \pm a) = 2q^n t$.

For different values of k**, this gives the remaining four solutions of the congruence.**

iJETRM
International Journal of Engineering Technology Research & Management

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 1\ (mod\ 1800)$.

Here, $1800 = 8.25.9 = 8.5^2.3^2$ **and** $1 = 1^2$.

So, the congruence can be written as $x^2 \equiv 1^2\ (mod\ 8.5^2.3^2)$.

It is of the type $x^2 \equiv a^2\ (mod\ 8.p^m.q^n)\ \ with\ a = 1, p = 5, q = 3$.

Therefore, it has sixteen solutions.

The eight solutions are given by

$x \equiv 2p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1, 2, 3.$

$\equiv 2.5^2.3^2 k \pm 1\ (mod\ 8.5^2.3^2)$

$\equiv 450k \pm 1\ (mod\ 1800)$

$\equiv 0 \pm 1; 450 \pm 1;\ 900 \pm 1; 1350 \pm 1\ (mod\ 81800)$

$\equiv 1, 1799;\ 449, 451; 899, 901; 1349, 1351\ (mod\ 1800)$

The remaining eight solutions are given by

$x \equiv \pm(\ 2p^n k \pm a)\ (mod\ 8p^m q^n)$**, if** $k(p^m k \pm a) = 2q^n t.$

$\equiv \pm(2.5^2 k \pm 1)\ (mod\ 8.5^2.3^2),\ \ if\ \ K(5^2 k \pm 1) = 2.3^2 t$

$\equiv \pm(50k \pm 1)\ (mod\ 1800)\ if\ k(25k \pm 1) = 18t.$

But for $k = 4, 5, 13, 14$**, it is seen that**

$4(25.4 - 1) = 18t;\ 5(125 + 1) = 18t;\ \ 13(325 - 1) = 18t;\ \ 14(350 + 1) = 18t.$

Therefore the required solutions are

$x \equiv \pm(50.4 - 1) = \pm 199 = 199, 1601\ (mod\ 1800).$

$x \equiv \pm(50.5 + 1) = \pm 251 = 251, 1549\ (mod\ 1800).$

$x \equiv \pm(50.13 - 1) = \pm 649 = 649, 1151\ (mod\ 1800).$

$x \equiv \pm(50.15 + 1) = \pm 701 = 701, 1099\ (mod\ 1800).$

Therefore, all the sixteen solutions are

$x \equiv 1, 1799; 449, 451; 899, 901; 1349, 1351;$

$199, 1601; 251, 1549; 649, 1151; 701, 1099 (mod\ 1800)$

Example-2: Consider the congruence $x^2 \equiv 4\ (mod\ 1800)$.

Here, $1800 = 8.25.9 = 8.5^2.3^2$ **and** $4 = 2^2$.

So, the congruence can be written as $x^2 \equiv 2^2\ (mod\ 8.5^2.3^2)$.

It is of the type $x^2 \equiv a^2\ (mod\ 8.p^m.q^n)\ \ with\ a = 2, p = 5, q = 3$.

Therefore, it has eight solutions.

The four solutions are given by

$x \equiv 4p^m q^n k \pm a\ (mod\ 8.p^m q^n); k = 0, 1.$

$\equiv 4.5^2.3^2 k \pm 1\ (mod\ 8.5^2.3^2)$

$\equiv 900k \pm 2\ (mod\ 1800)$

$\equiv 0 \pm 2;\ 900 \pm 1\ (mod\ 1800)$

$\equiv 2, 1798; 898, 902\ (mod\ 1800)$

The remaining four solutions are given by

$x \equiv \pm(\ 2p^n k \pm a)\ (mod\ 8p^m q^n)$**, if** $k(p^m k \pm a) = 2q^n t.$

$\equiv \pm(2.5^2 k \pm 1)\ (mod\ 8.5^2.3^2),\ \ if\ \ K(5^2 k \pm 1) = 2.3^2 t$

$\equiv \pm(50k \pm 1)\ (mod\ 1800)\ if\ k(25k \pm 1) = 18t.$

But for $k = 8, 10$ **it is seen that**

iJETRM
International Journal of Engineering Technology Research & Management

$4(25.4-1)=18t;\ 5(125+1)=18t;\ \ 13(325-1)=18t;\ \ 14(350+1)=18t.$

Therefore the required solutions are

$x\equiv\pm(50.8-2)=\pm398=398,1402\ (mod\ 1800).$

$x\equiv\pm(50.10+2)=\pm502=502,1298\ (mod\ 1800).$

Therefore, all the eight solutions are

$x\equiv 2,1798;898,902;398,1402;502,1298\ (mod\ 1800)$**.**

CONCLUSION

Therefore it can be concluded that the congruence under consideration: $x^2\equiv a^2\ (mod\ 8.p^m.q^n)\ \ with\ p,q$ **odd primes has exactly sixteen solutions; the eight are given by** $x\equiv 2p^mq^nk\pm a\ (mod\ 8.p^mq^n);k=0,1,2,3$ **and the remaining eight are given by** $x\equiv\pm(\ 2p^nk\pm a)\ (mod\ 8p^mq^n)$**, if** $k(p^mk\pm a)=2q^nt,\ \ if\ a\ is\ an\ odd\ prime\ integer.$

Also, the said congruence has exactly eight solutions; the four are given by

$x\equiv 4p^mq^nk\pm a\ (mod\ 8.p^mq^n);k=0,1$ **and the remaining four are given by**

$x\equiv\pm(\ 2p^nk\pm a)\ (mod\ 8p^mq^n)$**, if** $k(p^mk\pm a)=2q^nt,\ \ if\ a\ is\ an\ even\ prime\ integer.$

MERIT OF THE PAPER

The congruence under consideration is formulated and solutions can be obtained very easily. This is the merit of the paper.

REFERENCE

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

[2] 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).

[3]] Koshy Thomas, ***Elementary Number Theory with Applications*****, Academic Press, an Imprint of Elsevier, second edition, Indian Reprint, 2009, ISBN: 978-81-312-1859-4.**

[4] Roy 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, Jun-Jul-18.**

[5]Roy B M, ***Formulation of solutions of a standard quadratic congruence of even composite modulus-a product of a powered odd prime with eighth multiple of another odd prime*****, International Journal of Scientific Research and Engineering development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-03, Jun-Jul-20**

ISSN: 2456-9348
Impact Factor: 4.520

iJETRM
International Journal of Engineering Technology Research & Management