iJETRM
International Journal of Engineering Technology Research & Management

RP-39: FORMULATION OF SOLUTIONS OF A CLASS OF STANDARD QUADRATIC CONGRUENCE OF COMPOSITE MODULUS- A PRODUCT OF TWO POWERED ODD PRIMES AND EIGHT, IN TWO SPECIAL CASES

Prof B M Roy
Head, Department of Mathematics
Jagat Arts, Commerce & IHP Science College, Goregaon
Dist - Gondia, M. S., India.
Pin: 441801

ABSTRACT
In this paper, the author has formulated a class of standard quadratic congruence of composite modulus- a product of two different powered odd primes and eight in two special cases. This congruence has already been formulated by the author in two general cases only.
The current two cases were not considered then for formulation. Two different formulations is derived here for the solutions of the congruence under consideration. The formulations are tested and verified true using different numerical examples.

Key-words:
Composite modulus, Formulation, Quadratic congruence.

INTRODUCTION

The author has formulated many standard quadratic congruence of prime & composite modulus. Even some remains unformulated. One of such unformulated quadratic congruence is considered here for study and formulation of solutions in two special cases. It is of the type: $x^2 \equiv a^2 \ (mod\ 8\ p^m q^n)$ with p, q different odd primes.
The two cases are already formulated and published for odd & even positive integer a.

PROBLEM-STATEMENT

Here the problem is "To formulate the standard quadratic congruence of composite modulus of the type: $x^2 \equiv a^2 \ (mod\ 8p^m q^n)$ in two cases as:
Case-I: If $a = p$;
Case-II: If $a = q$. "

LITERATURE-REVIEW

In the literature of mathematics, there's found no formulation or any method to find the solutions of the standard quadratic congruence of composite modulus under consideration**.**
Only the author's formulations of different types of standard quadratic congruence of composite modulus are seen [4], [5], [6]. First time some formulations are going to discovered. Even one can use the Chinese Remainder Theorem (CRT) to find the solutions. But it is very complicated and difficult to use CRT.

iJETRM
International Journal of Engineering Technology Research & Management

EXISTED METHOD

In the existed method (CRT method) [1], [2], [3], the original congruence is split into individual congruence and then find their solutions. Here lies the difficulty, because every quadratic congruence of prime modulus cannot be solved easily. The actual solutions of the congruence are obtained using CRT method. It is time-consuming.

$e.g.$ *Consider the congruence*: $x^2 \equiv 13^2 \ (mod\ 13^3)$. It has exactly 26 incongruent solutions. But it is time-consuming using CRT method.

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv a^2 \ (mod\ 8p^m q^n); p, q$ odd primes.

Case-I: Let $a = p$.

Then the congruence becomes $x^2 \equiv p^2 \ (mod\ 8p^m q^n)$.

For solutions, let $x \equiv 2p^{m-1}q^n k \pm p \ (mod\ 8p^m q^n)$.

Then, $x^2 \equiv (2p^{m-1}q^n k \pm p)^2 \ (mod\ 8p^m q^n)$

$\equiv (2p^{m-1}q^n k)^2 \pm 2.2p^{m-1}q^n k.p + p^2\ 8p^m q^n$

$\equiv 4p^m q^n k\ (p^{m-2}q^n k \pm 1) + p^2\ (8p^m q^n)$

$\equiv 0 + p^2 \ (mod\ 8p^m q^n)$

$\equiv p^2 \ (mod\ 8p^m q^n)$

Therefore, $x \equiv 2p^{m-1}q^n k \pm p \ (mod\ 8p^m q^n)$ is a solution of the said congruence.

But for $k = 4p$, the solution reduces to $x \equiv 2p^{m-1}q^n.4p \pm p \ (mod\ 8p^m q^n)$

$\equiv 8p^m q^n \pm p \ (mod\ 8p^m q^n)$

$\equiv 0 \pm p \ (mod\ 8p^m q^n)$

It is the same solution as for $k = 0$.

Similarly, for $k = 4p + 1, 4p + 2, \ldots\ldots$ the solutions repeats as for $k = 1, 2, \ldots.$

Thus, $x \equiv 2p^{m-1}q^n k \pm p \ (mod\ 8p^m q^n)$ gives all the solutions for $k = 0, 1, 2, \ldots\ldots, 4p - 1$.

This gives $8p$ −solutions of the said congruence.

Case-II: Let $a = q$.

Then the congruence becomes $x^2 \equiv q^2 \ (mod\ 8p^m q^n)$.

For solutions, let $x \equiv 2p^m q^{n-1}k \pm q \ (mod\ 8p^m q^n)$.

Then, $x^2 \equiv (2p^m q^{n-1}k \pm q)^2 \ (mod\ 8p^m q^n)$

$\equiv (2p^m q^{n-1}k)^2 \pm 2.2p^m q^{n-1}k.q + q^2 \ (mod\ 8p^m q^n)$

$\equiv 4p^m q^n k\ (p^m q^{n-2}k \pm 1) + q^2 \ (mod\ 8p^m q^n)$

$\equiv 0 + q^2 \ (mod\ 8p^m q^n)$

$\equiv q^2 \ (mod\ 8p^m q^n)$

Therefore, $x \equiv 2p^m q^{n-1}k \pm q \ (mod\ 8p^m q^n)$ is a solution of the said congruence.

But for $k = 4q$, the solution reduces to $x \equiv 2p^m q^{n-1}.4q \pm q \ (mod\ 8p^m q^n)$

$\equiv 8p^m q^n \pm q \ (mod\ 8p^m q^n)$

$\equiv 0 \pm q \ (mod\ 8p^m q^n)$

It is the same solution as for $k = 0$.

Similarly, for $k = 4q + 1, 4q + 2, \ldots\ldots$ the solutions repeats as for $k = 1, 2, \ldots.$

Thus, $x \equiv 2p^m q^{n-1}k \pm q \ (mod\ 8p^m q^n)$ gives all the solutions for $k = 0, 1, 2, \ldots\ldots, 4q - 1$.

iJETRM
International Journal of Engineering Technology Research & Management

This gives $8q$ −solutions of the said congruence.

ILLUSTRATIONS

Example-I: Consider the congruence: $x^2 \equiv 25\ (mod\ 1800)$.
The congruence can be written as $x^2 \equiv 5^2\ (mod\ 8.5^2.3^2)$
It is of the type: $x^2 \equiv p^2\ (mod\ 8p^mq^n)$.
Therefore, the congruence has exactly $8p = 8.5 = 40$ solutions, given by
$x \equiv 2p^{m-1}q^nk \pm p\ (mod\ 8p^mq^n);\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (4p-1).$
$\equiv 2.5^{2-1}.3^2k \pm 5\ (mod\ 8.5^2.3^2);\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots, 19.$
$\equiv 2.5.9k \pm 5\ (mod\ 8.25.9)$
$\equiv 90k \pm 5\ (mod\ 1800);\ k = 0, 1, 2, 3, \ldots\ldots\ldots, 19.$
$\equiv 0 \pm 5; 90 \pm 5; 180 \pm 5; 270 \pm 5; \ldots\ldots\ldots\ldots\ldots; 1710 \pm 5\ (mod\ 1800).$
$\equiv 5, 1795; 85, 95; 175, 185; 265, 275; \ldots\ldots\ldots\ldots; 1705, 1715\ (mod\ 1800)$
These are the required forty solutions of the congruence.

Example-II: Consider the congruence: $x^2 \equiv 9\ (mod\ 1800)$.
The congruence can be written as $x^2 \equiv 3^2\ (mod\ 8.5^2.3^2)$
It is of the type: $x^2 \equiv q^2\ (mod\ 8p^mq^n)$.
Therefore, the congruence has exactly $8q = 8.3 = 24$ Solutions.
These solutions are given by
$x \equiv 2p^mq^{n-1}k \pm q\ (mod\ 8p^mq^n);\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (4q-1).$
$\equiv 2.5^2.3^{2-1}k \pm 3\ (mod\ 8.5^2.3^2);\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots, 11.$
$\equiv 2.25.3k \pm 3\ (mod\ 8.25.9)$
$\equiv 150k \pm 3\ (mod\ 1800);\ k = 0, 1, 2, 3, \ldots\ldots\ldots, 11.$
$\equiv 0 \pm 3; 150 \pm 3; 300 \pm 3; 450 \pm 3; \ldots\ldots\ldots\ldots\ldots; 1650 \pm 3\ (mod\ 1800).$
$\equiv 3, 1797; 147, 153; 297, 303; 447, 453; \ldots\ldots\ldots\ldots; 1647, 1653\ (mod\ 1800)$
These are the required twenty four solutions of the congruence.

CONCLUSION

Therefore, it is concluded that the congruence under consideration
$x^2 \equiv a^2\ (mod\ 8p^mq^n)$ has $8p - solutions$: $x \equiv 2p^{m-1}q^nk \pm p\ (mod\ 8p^mq^n);$
$k = 0, 1, 2, \ldots\ldots, 4p-1$, if $a = p$.
And it also has $8q - solutions$: $x \equiv 2p^mq^{n-1}k \pm q\ (mod\ 8p^mq^n);$
$k = 0, 1, 2, \ldots\ldots, 4q-1,$ if $a = q$.

MERIT OF THE PAPER

A direct formula is established for solutions**.** Using this formula, the solutions can be obtained orally. Therefore, formulation of solutions is the merit of the current paper.

REFERENCE

iJETRM
International Journal of Engineering Technology Research & Management

[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
[6]Roy B M, *Formulation of solutions of a class of Solvable standard quadratic congruence of composite modulus- A prime positive integer multiple of eight*, (IJMTT), ISSN: 2231-5373, Vol-61, Issue-04, Oct-18.