# A Comparative Study of the Existed Method and Formulation of Solutions of a Class of Standard Quadratic Congruence modulo an Odd Prime Integer Multiple of Eight

**Prof. B M Roy**

*Head, Dept. Of Mathematics*

*Jagat Arts, Commerce & I H P Science College, Goregaon, Dist. Gondia (M S)*

*(Affiliated to R T M Nagpur University, Nagpur)*

***ABSTRACT***

*In this paper, finding solutions of a class of standard quadratic congruence modulo an odd prime multiple of eight, is compared with existed method & the formulation by the author. Formulation of the solutions is proved time-saving, simple and quick than the existed method using CRT which is time-consuming. Formulation is the merit of the paper. No need to use Chinese Remainder Theorem.*

***Key-words: Chinese Remainder Theorem, Composite modulus, Quadratic Congruence.***

..........................................................................................................................................
..

## INTRODUCTION

Here, a solvable standard quadratic congruence of *composite modulus*- an odd prime integer multiple of eight, is considered for discussion. It is of the type $x^2 \equiv a^2 \ (mod\ 8p)$ , p being a positive prime integer. It is always solvable.

## LITERATURE REVIEW

In different books on Number Theory, no formulation is found for the said congruence. Only the use of Chinese Remainder Theorem [1] 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 [2]. He used Chinese Remainder Theorem for solutions.

## NEED OF RESEARCH

Chinese Remainder Theorem is a very lengthy procedure. It takes a long time. It is not a good and affordable method for students. To have remedy, formulation is necessary. This is the need of my research.

## PROBLEM-STATEMENT

The congruence under consideration is: $x^2 \equiv a^2 (mod\ 8p)$ … … … … … … … … (1)

with p an odd prime integer.

The problem is to compare the method of CRT to find the solutions of the congruence under consideration & also by formulation by the author.

Solution by Existed Method

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

It can be separated into two congruence: $x^2 \equiv a^2 \equiv b\ (mod\ 8)$ having four solutions

and $x^2 \equiv a^2 \equiv c\ (mod\ p)$ having two solutions.

Hence, the congruence (1) has eight solutions. These are obtained by using CRT.

Consider the congruence $x^2 \equiv 25\ (mod\ 152) i.e.\ x^2 \equiv 5^2\ (mod\ 8.19)$

Two separate congruence : $x^2 \equiv 25 \equiv 1\ (mod\ 8)$ and $x^2 \equiv 25 \equiv 3\ (mod 11)$.

Their solutions are: $x \equiv 1, 3, 5, 7\ (mod\ 8)\ and\ x \equiv 5, 8\ (mod\ 11) \ldots . How$?

Then using CRT, the eight common solutions can be obtained which are

$x \equiv 5, 147; 71, 81;\ 33,119; 43, 109\ (mod\ 152)$. [Tabular calculations not shown]

It takes at least 40 minutes!

Solutions by Formulation

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

It is always solvable and the four obvious solutions are given by:

$x \equiv 8p \pm a;\ \ 4p \pm a\ (mod\ 8p) \equiv a, 8p - a; 4p - a, 4p + a\ (mod\ 8p) \ldots \ldots \ldots \ldots \ldots \ldots . . (2)$

Sometimes, we may have the congruence of the type: $x^2 \equiv b\ (mod\ 8p)$.

It can be written as $x^2 \equiv b + k.8p = a^2\ (mod\ 8p)$ for some positive integer k [3].

Then its four obvious solutions are given by (2).

The other four solutions are given by: $x = \pm(2p \pm a),\ \ if\ a\ is\ odd.$

But if $a\ is\ an\ even\ integer, the\ congruence\ has\ only\ four\ obvious\ solutions.$

There is no other possibility for solutions.

But if $a = p$,then the solutions are $x \equiv p, 7p; 3p, 5p\ (mod\ 8p)$.

Thus it has only four solutions.

## ILLUSTRATIONS BY FORMULATION

Consider $x^2 \equiv 25\ (mod\ 152).\ \ Here\ 152 = 8.19\ with\ p = 19\ \&\ a = 5, an\ odd\ integer.$

So, it has exactly eight solutions.

Four are given by $x \equiv 8p \pm a; 4p \pm a\ (mod\ 8p)$

$\equiv 152 \pm 5; 76 \pm 5\ (mod 152)$

$\equiv 5, 147; 71, 81\ (mod\ 152)$.

Also, as $a = 5, an\ odd\ integer$, hence the other four solutions are:

$$x \equiv \pm(2p \pm a)\ (mod\ 8p)$$

$$\equiv \pm(38 \pm 5)\ (mod\ 8.19)$$

$$\equiv \pm 33;\ \pm 43\ (mod\ 152).$$

$$\equiv 33{,}119; 43, 109\ (mod\ 152).$$

Thus, required eight solutions are $x \equiv 5, 147; 71, 81;\ 33{,}119; 43, 109\ (mod\ 152)$.

These are the same solutions as obtained in existed method, but in a short time in at most two minutes!!

Consider the congruence: $\mathrm{x}^2 \equiv 4\ (\mathrm{mod}\ 104)$.

It can be written as $\mathrm{x}^2 \equiv 2^2\ (\mathrm{mod}\ 8.13)$

It is of the type $x^2 \equiv a^2\ (mod\ 8p) with\ p = 13\ \&\ a = 2$.

Its four obvious solutions are $x \equiv 8p \pm a; 4p \pm a\ (mod\ 8p)$

$$\equiv\ \ 104 \pm 2; 52 \pm 2 (mod\ 104)$$

$$\equiv 2, 102; 50, 54\ (mod\ 104).$$

We see that $a = 4, an\ even\ integer.$

Hence, other solutions do not exist.

Therefore, the above congruence has only four obvious solutions $x \equiv 2, 102; 50, 54\ (mod\ 104)$.

Consider another example as per need: $x^2 \equiv 33\ (mod\ 88)$.

It can be written as $x^2 \equiv 33 + 88 = 121 = 11^2\ (mod\ 88)\ \ with\ a = 11 = p.$

It has exactly four obvious solutions:

$$x \equiv 88 \pm 11;\ 44 \pm 11\ (mod\ 88).$$

$$\equiv 11, 77; 33, 55\ (mod\ 88).$$

**CONCLUSION**

In this paper, finding solutions of a class of solvable standard quadratic congruence of composite modulus- a prime multiple of eight is compared with existed method using CRT and the formulation by the author. Formulation gives solutions in less time.

**MERIT OF THE PAPER**

No need to use Chinese Remainder Theorem. Formulation is the merit of the paper. It is simple and quick.

**REFERENCE**

[1] Burton David M, *Elementary Number Theory*, Seventh Indian edition, Mc Graw Hill(Pvt) Ltd.

[2] Koshy Thomas, *Elementary Number Theory with Applications*, second edition, Indian Print, 2009.

[3] Roy B M , *Discrete Mathematics & Number Theory,* First edition, Das Ganu Prakashan, Nagpur (INDIA)

[4] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, 2008.