Formulation of Solutions of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- an Odd Prime Positive 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) Pin-441801, (Affiliated to R T M Nagpur University, Nagpur)

Abstract

In this study, a class of solvable standard quadratic congruence of composite modulus- an odd positive prime integer multiple of eight, is formulated. Formulae are established successfully and are tested true with suitable examples. No need to use Chinese Remainder Theorem. Formulation is the merit of the paper.

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

I. INTRODUCTION

In this paper, a solvable standard quadratic congruence of composite modulus- an odd positive prime integer multiple of eight, is considered for formulation. I have formulated a lot of standard quadratic congruence earlier. I have tried my best to formulate all those quadratic congruence successfully; even some quadratic congruence remains to formulate. Here I shall consider one such standard quadratic congruence of composite modulus yet not formulated. It is of the type $x^2 \equiv a^2 \ (mod\ 8p)$, p being a positive prime integer.

II. LITERATURE REVIEW

Going through different books on Number Theory and also peeping into the literature of mathematics, 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. A very short discussion is found in the book of Thomas Koshy [2]. He used Chinese Remainder Theorem for solutions. No one had attempted to do anything for the students' sake.

III. NEED OF MY RESEARCH

The use of Chinese Remainder Theorem is a very lengthy procedure. It is not a fare method for students in the examination. It takes a long time. Students / readers try to get rid of such method and want to feel comfortable in solving such quadratic congruence. It is only possible if the problem is formulated. I have tried my best to formulate the problem. This is the need of my research.

IV. PROBLEM-STATEMENT

The problem is to formulate the standard quadratic congruence: $x^2 \equiv a^2 (mod\ 8p)$,with p an odd positive prime integer. Such congruence always has eight solutions [4]. Here, I must try my best to find the formulae for solutions of the said congruence.

V. ANALYSIS & RESULT (Formulation)

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

It is always solvable and the four obvious solutions are:

$x \equiv 8p \pm a;\ \ 4p \pm a \ (mod\ 8p) \equiv a, 8p - a; 4p - a, 4p + a \ (mod\ 8p),$ as they satisfy the congruence.

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

We search for other four solutions as under:

Consider $x = \pm(2p \pm a)$

Then, $x^2 = (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) = a^2 + 4p.2m,\ \ if\ p \pm a = 2m.$

Therefore, two other solutions are:

$$x \equiv \pm(2p \pm a)(mod\ 8p),\ \ if\ p \pm a = 2m\ i.e. if\ a\ is\ an\ odd\ positive\ integer.$$

But if $a\ is\ an\ even\ integer, then\ p \pm a \neq 2m\ \ and\ hence\ \ x \equiv \pm(2p \pm a)(mod\ 8p)$ cannot be the other solutions. There is no other possibility found.

Thus, it also reveals that if $a\ is$ an even integer, then the congruence has only four obvious solutions.

Sometimes, it happens that $a = p$, then $p \pm a = 2p$, the congruence would be of the type $x^2 \equiv a^2\ (mod\ 8p^2)$ which is not the congruence under consideration. Thus, the congruence has only four solutions.

VI. ILLUSTRATIONS

Consider the congruence $x^2 \equiv 1\ (mod\ 88)$

It can be written as $x^2 \equiv 1 = 1^2\ (mod\ 8.11)\ with\ p = 11\ \&\ a = 1$, which is an odd integer.

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 8p)$ and the congruence has exactly eight solutions.

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

$i.e.\ \ x \equiv 88 \pm 1; 44 \pm 1\ (mod\ 88) \equiv 1, 87; 43, 45\ (mod\ 88)$.

For the other four solutions, consider $p \pm a = 11 \pm 1 = 10, 12 = 2m.$

Thus, $x \equiv \pm(2p \pm a) = \pm(2.11 \pm 1) = \pm(22 \pm 1) = \pm 21, \pm 23\ (mod\ 88)$ are the other four solutions.

Therefore, the said congruence under considerations has eight solutions as under:

$$x \equiv 1{,}87; 43, 45; 21, 67; 23{,}65\ (mod\ 88).$$

Consider one more example: $x^2 \equiv 16\ (\text{mod } 104)$.

It can be written as $x^2 \equiv 4^2\ (\text{mod } 8.13)$

It is of the type $x^2 \equiv a^2\ (mod\ 8p) with\ p = 13\ \&\ a = 4.$

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

$i.e.\ \ 104 \pm 4; 52 \pm 4 (mod\ 104) = 4, 100; 48, 56\ (mod\ 104)$.

Also for other solutions, $(a^2, 8p) = (16, 104) \neq 1$.

We see that $p \pm a = 13 \pm 4 \neq 2m$; Hence, $x \equiv \pm(2p \pm a)(mod\ 104)$ are not the solutions.

Other solutions do not exist.

Therefore, the above congruence has only four obvious solutions $x \equiv 4, 100; 56, 48\ (mod\ 104)$.

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

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

It can be seen that as $p + a = 11 + 11 = 22 = 2.m$

Then the solutions are given by

$$x \equiv \pm(p \pm a) = \pm(22 \pm 11) = \pm 33;\ \pm 11 = 33, 55\ ; 11, 77\ (mod\ 88).$$

We can see that these four solutions are repeated solutions as before.

VI. CONCLUSION

Therefore, it can be concluded that the congruence under consideration $x^2 \equiv a^2 (mod\ 8p)$ has eight incongruent solutions are given by:

Four obvious solutions are $x \equiv 8p \pm a;\ \ 4p \pm a = a, 8p - a; 4p - a, 4p + a\ (mod\ 8p).$

And other four solutions are given in the followings ways:

If $\mathrm{p} \pm a = 2m\ \ for\ odd\ a\ , then\ \ x \equiv\ \pm(\ p \pm a\ )\ \ mod\ \ (8p)$ are the other four solutions.

But $for\ an\ even\ a, the\ congruence\ have\ only\ four\ obvious\ solutions.$

If $a = p$, then also the solutions are the same as obvious solutions because the next four solutions are repeated.

VII. MERIT OF THE PAPER

In this paper, a class of solvable standard quadratic congruence of composite modulus- a prime multiple of eight is formulated. It is tested true using examples. No need to use Chinese Remainder Theorem. Formulation is the merit of the paper.

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.