Formulation of Solutions of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- a Prime Positive Integer Multiple of Five

Prof. B M Roy

Head, Dept. Of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist. Gondia (M S), INDIA 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 five, 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.**

***Keywords*: Chinese Remainder Theorem, Composite modulus, Quadratic Congruence.**

INTRODUCTION

In this study, a solvable standard quadratic congruence of **composite modulus**- an odd positive prime integer multiple of five, 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 $x^2 \equiv a^2 \ (mod\ 5p)$, p being a positive prime integer.

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 is found **[3].** A very short discussion is found in the book of Thomas Koshy **[4].** He used Chinese Remainder Theorem for solutions. No one had attempted to do anything for the students' sake. This pained me very much.

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 must get rid of such method and should 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.

PROBLEM-STATEMENT

Here, the problem is to formulate the standard quadratic congruence

$x^2 \equiv a^2 (mod\ 5p), p \neq 5$, p being an odd positive prime integer.

Such congruence always has four solutions **[3]**. Here, I must try my best to find the formulae for solutions of the said congruence.

ANALYSIS & RESULT (Formulation)

Consider the congruence $x^2 \equiv a^2 \ (mod\ 5p); p \neq 5, (a^2, 5p) = 1.$

It is always solvable and the two obvious solutions are: $x \equiv 5p \pm a = a, 5p - a \ (mod\ 5p).$

Sometimes, we may have the congruence of the type: $x^2 \equiv b \ (mod\ 5p).$

It can be written as $x^2 \equiv b + k.5p = a^2 \ (mod\ 5p)$ for some positive integer k **[2].**

Then its two obvious solutions are $x \equiv 5p \pm a = a, 5p - a \ (mod\ 5p).$

We search for other two solutions as under:

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

Then, $x^2 = (p \pm a)^2 = p^2 \pm 2pa + a^2 = a^2 + p(p \pm 2a) = a^2 + p.5m,\ \ if\ p \pm 2a = 5m$

Therefore, **two other solutions are:** $\boldsymbol{x \equiv \pm(p \pm a)(mod\ 5p),\ \ if\ p \pm 2a = 5m}$.

Also, consider $x = \pm(2p \pm a)$

Then, $x^2 = (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) = a^2 + 4p.5m,\ \ if\ p \pm a = 5m$

Thus, other two solutions are: $\boldsymbol{x \equiv \pm(2p \pm a)\ (mod\ 5p)}$, **if** $\boldsymbol{p \pm a = 5m}$.

There is no other possibility found.

But, if $(a, 5p) \neq 1$, then the congruence has only two obvious solutions. Because then,

$b = 5k\ and\ ultimately, p \pm a \neq 5m; p \pm 2a \neq 5m$. Hence, the second pair of solutions is not possible. And the said congruence must have the obvious pair of solutions.

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 1\ (mod\ 55)$

It can be written as $x^2 \equiv 1 = 1^2\ (mod\ 5.11)\ with\ p = 11\ \&\ a = 1$.

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 5p)$

Then $x \equiv 5p \pm a = 55 \pm 1\ (mod\ 55) \equiv 1, 54\ (mod\ 55)$ are the two obvious solutions.

Also, $(a^2, 5p) = (1, 55) = 1$. So, other two solutions exist.

For these two solutions consider

$p - a = 11 - 1 = 10 = 5.2 = 5m$

Thus, $x \equiv \pm(2p - a) = \pm(2.11 - 1) = \pm 21 = 21, 34\ (mod\ 55)$ are the other two solutions.

Therefore, the said congruence under considerations has four solutions

$\boldsymbol{x \equiv 1, 54;\ 21, 34\ (mod\ 55)}$.

Consider one more example**:** $x^2 \equiv 16\ (\text{mod } 85)$.

It can be written as $x^2 \equiv 4^2\ (\text{mod } 5.17)$

It is of the type $x^2 \equiv a^2\ (mod\ 5p) with\ p = 17\ \&\ a = 4$.

Its two obvious solutions are $x \equiv 5p \pm a = 85 \pm 4 = \boldsymbol{4, 81}\ \boldsymbol{(mod\ 85)}$.

Also for other two solutions, we see that

$(a^2, 5p) = (16, 85) = 1\ and\ p + 2a = 17 + 8 = 25 = 5.5$

Hence other two solutions exist.

Those solutions are $x \equiv \pm(P + a) \equiv \pm(17 + 4) \equiv \pm 21$

$\equiv 21, 85 - 21 \equiv\ 21, 64\ (mod 85)$.

Consider one more congruence as per need: $x^2 \equiv 5\ (mod\ 95)$

It can be written as $x^2 \equiv 5 + 95 = 100 = 10^2\ (mod\ 5.19)\ with\ p = 19$.

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 5p)$.

Then $x \equiv 5p \pm a = 95 \pm 10\ (mod\ 95) \equiv 10, 85\ (mod\ 95)$ are the two obvious solutions

For the other two solutions, we see that $(a^2, 5p) = (100, 95) \neq 1$.

Thus, the congruence has no other solution.

Therefore, the above congruence has only two obvious solutions

$$\boldsymbol{x \equiv 10, 85 \ (mod \ 95)}.$$

CONCLUSION

Therefore, we conclude that the congruence under consideration $x^2 \equiv a^2 (mod\ 5p)$, p$\neq$ 5, with $(a^2, 5p) = 1,$ has four congruent solutions given by:

Two obvious solutions are $\boldsymbol{x \equiv 5p \pm a = a, 5p - a \ (mod\ 5p)}$

And other two solutions are given in the followings ways:

If p $\boldsymbol{\pm 2a = 5m, then \ x \equiv \pm (p \pm a) \ mod \ (5p)}$ **are the other two solutions.**

If $\boldsymbol{p \pm a = 5m, \ then \ x \equiv \pm (2p \pm a)}$ **are the other two solutions.**

But if $\boldsymbol{(a^2, 5p) \neq 1, then \ the \ congruence \ have \ only \ two \ obvious \ solutions}$.

MERIT OF THE PAPER

In this paper, a class of solvable standard quadratic congruence is formulated which was not formulated earlier. First time, formulae are established. No need to use Chinese Remainder Theorem. This is the merit of the paper.

REFERENCE

[1] Burton David M, *Elementary Number Theory*, Seventh Indian edition, Mc Graw Hill(Pvt) Ltd.
[2] Roy B M , *Discrete Mathematics & Number Theory*, First edition, Das Ganu Prakashan, Nagpur (INDIA)
[3] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, 2008.
[4] Koshy Thomas, *Elementary Number Theory with Applications*, second edition,Indian Print, 2009.