Formulation of a Class of Standard Quadratic Congruence of Composite Modulus- a positive Prime-integer multiple of six

Prof. B M Roy

Head, Department 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 standard *quadratic congruence* of composite modulus- an odd prime-integer multiple of six, 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

Here, another standard quadratic congruence of **composite modulus**- an odd prime integer multiple of six, is considered for formulation. I have tried my best successfully to formulate many standard **quadratic congruence of prime or composite modulus**; even some remains to formulate. Here I consider one such standard quadratic congruence yet not formulated. It is of the type $x^2 \equiv a^2 \ (mod\ 6p)\ with$ p being a positive odd prime integer. Such quadratic congruence has at most four solutions [3].

LITERATURE REVIEW

I have gone through different books on Number Theory and also searched into the literature of mathematics; no formulation is found for the said congruence. Only the use of **Chinese Remainder Theorem** [1] is discussed. It is also found that Thomas Koshy had made a very small attempt to find the solutions of standard quadratic congruence of composite modulus **[4].** Most of the earlier mathematicians discussed for standard quadratic congruence of prime modulus; the standard quadratic congruence of composite modulus is found uncared. They all preferred **to** use Chinese Remainder Theorem. The use of Chinese Remainder Theorem is a very lengthy procedure. No one had attempted to do anything for the students' sake. This pained me very much. The congruence under consideration has not been formulated before by any earlier mathematicians. No one cared it.

NEED OF MY RESEARCH

The use of Chinese Remainder Theorem is not fare method for the students in examination. It takes a long time. Students are always ready to get rid of such method and want 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 and my efforts are presented in this paper. This is the need of my research.

PROBLEM-STATEMENT

The problem is to formulate the standard quadratic congruence $x^2 \equiv a^2 \ (mod\ 6p)$,

p being a positive odd prime integer. It has at most four solutions [3]. Here, I discuss the formulation for solutions of the said congruence.

ANALYSIS & RESULT (Formulation)

Consider the congruence $x^2 \equiv a^2 \ (mod\ 6p)$.

The two obvious solutions of it are $x \equiv 6p \pm a = a, 6p - a \ (mod\ 6p)$.

Sometimes the congruence may be of the form: $x^2 \equiv b \ (mod\ 6p)$.

It can be written as $x^2 \equiv b + k.6p = a^2 \ (mod\ 6p)$ for some positive integer k [2]

Then the congruence takes the form as: $x^2 \equiv a^2 \ (mod\ 6p)$.

The two obvious solutions of it are $x \equiv 6p \pm a = a, 6p - a \ (mod\ 6p)$.

We search for other two solutions as under:

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

Then, $x^2 = (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) = a^2 + 4p.3m, \ \ if\ p \pm a = 3m$

So, other two solutions are given by:

$\boldsymbol{x \equiv \pm(2p \pm a)\ (mod\ 6p), \text{if } p \pm a = 3m}$.

There is no other possibility for the existence of solutions. Thus, we conclude that the said congruence has four incongruent solutions. Some of the congruence may have only two solutions. This will depict from the example.

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 4\ (mod\ 30)$

It can be written as $x^2 \equiv 4 = 2^2\ (mod\ 6.5)\ with\ p = 5\ \&\ a = 2.$

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 6p)$

Then $x \equiv 6p \pm a = 30 \pm 2\ (mod\ 30) \equiv 2, 28\ (mod\ 30)$ are the two obvious solutions

It has four solutions. For other two solutions, we consider $p \pm a = 5 \pm 2 = 5 - 2 = 3.1$

Thus, $x \equiv \pm(2p \pm a) = \pm(10 - 2) = \pm 8 = 8, 22\ (mod\ 30)$.

Therefore, the said congruence under considerations has four solutions

$\boldsymbol{x \equiv 2, 28;\ 8, 22\ (mod\ 30)}$

Consider the congruence $x^2 \equiv 19\ (mod\ 102),\ \ with\ 102 = 6.17$

It can be written as $x^2 \equiv 19 + 102 = 121 = 11^2\ (mod\ 6.17)\ with\ p = 17;\ \ a = 11$ [2]

Thus, the congruence is of the type $x^2 \equiv a^2\ (mod\ 6p)$

Then $x \equiv 6p \pm a = 102 \pm 11\ (mod\ 102) \equiv 11, 91\ (mod\ 102)$ are the two obvious solutions

For the other two solutions, we see that $p \pm a = 17 \pm 11 = 17 - 11 = 6 = 3.2,$

Hence $x \equiv \pm(2p - a) \equiv \pm(2.17 - 11) = \pm 23 = 23, 79 (mod\ 102)$

Therefore, the said congruence under considerations has four solutions

$\boldsymbol{x \equiv 11, 91; 23, 79\ (mod\ 102).}$

Consider one more example as per need**:** $x^2 \equiv 36$ (mod 138)

It can be written as $x^2 \equiv 6^2$ (mod 6.23)

It is of the type $x^2 \equiv a^2\ (mod\ 6p) with\ p = 23\ \&\ a = 6.$

Its two obvious solutions are $x \equiv 6p \pm a = 138 \pm 6 = \boldsymbol{6, 132\ (mod\ 138)}$.

Also for other two solutions, we see that $p \pm a = 23 \pm 6 \neq 3m.$

Also, $p \pm 2a = 23 \pm 12 \neq 6m.$

Hence other two solutions do not exist and hence $x \equiv 6, 132\ (mod 138)$ are the only two solutions.

CONCLUSION

Therefore, we conclude that the congruence under consideration $x^2 \equiv a^2 (mod\ 6p)$ has at most four incongruent solutions given by:

Two obvious solutions are $x \equiv 6p \pm a = a, 6p - a \ (mod\ 6p)$

And other two solutions are:

If $p \pm a = 3m,\ then\ x \equiv \pm(2p \pm a)\ (mod\ 6p)$ **are the other two solutions**

There is no other possibility for the existence solutions.

MERIT OF THE PAPER

In this paper, a class of standard quadratic congruence is formulated which was not done previously. First time, a formula is 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.