Formulation of Solutions of a Solvable Standard Quadratic Congruence of Composite Modulus- an Odd Prime Multiple of Four

Prof. B. M. Roy

Head, Department of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon
Dist. Gondia, M S, (INDIA) Pin: 441801

***Abstract*: In this paper, a solvable standard quadratic congruence of composite modulus- an odd positive prime integer multiple of four, is formulated. The formulae are tested true by solving different examples and found correct. Formulation is the merit of this paper. No need to use Chinese Remainder Theorem.**

***Keywords*: Chinese Remainder Theorem, Quadratic congruence, composite modulus.**

INTRODUCTION

I have formulated many solvable standard quadratic congruence of prime and composite modulus. Some of the congruence of higher degree are also successfully formulated. Even some congruence is remained to formulate. Here, in this paper, one such congruence is considered for the formulation. It was not formulated earlier by the mathematicians. First time an attempt has been made to find the solutions without using Chinese Remainder Theorem [3].It works like a magic.

LITERATURE REVIEW

In the literature of mathematics, quadratic congruence of prime modulus is discussed in detailed [3] and a very little discussion on the solutions of quadratic congruence of composite modulus is found [1].Thomas Koshy had made an insufficient attempt to consider the congruence of composite modulus for discussion [4]. It seems that no one cared for quadratic congruence of composite modulus. In this paper, a solvable standard quadratic congruence of composite modulus is considered for formulation.

NEED OF MY RESEARCH

Students / readers find it difficult to use Chinese Remainder Theorem for the solutions of congruence as it takes a long time; to get rid of the said method, formulation is very necessary. I have tried my best to establish formulae for these solutions. This is the need of my research.

PROBLEM STATEMENT

The problem for this paper is to find the solutions of solvable standard quadratic congruence of the type $x^2 \equiv a^2 \pmod{4p}$, where p is an odd positive prime integer, in two different cases: $a = p$ & $a \neq p$.

ANALYSIS AND RESULT (Formulation)

Let us consider the congruence $x^2 \equiv a^2 (\text{mod } 4p)$, where p is an odd positive prime integer witha $\neq$ p. Such type of quadratic congruence is always solvable. It must have exactly four solutions [3].

Consider the congruence $x^2 \equiv a^2 \pmod{4p}$.

Its two obvious solutions are given by $x \equiv \pm a \pmod{4p}$

$$= 4p \pm a \pmod{4p}$$

$$= a, 4p - a \pmod{4p}.$$

For the other two solutions, consider $x \equiv (2p \pm a)$

Then $x^2 \equiv (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) \equiv a^2 (\text{mod } 4p)$.

i.e. $x^2 \equiv a^2 \pmod{4p}$ is satisfied.

Thus, $x \equiv 2p \pm a \pmod{4p}$ are the two other solutions.

Sometimes, the congruence can be given by: $x^2 \equiv b \pmod{4p}$.

It can be written as $x^2 \equiv b + k.4p = a^2 \pmod{4p}$ for some positive integer k [2].

Then the four solutions are as in above.

If $a = p$, then the congruence has only two solutions. In this case, the other two solutions do not exist. It can be seen as:

Solutions are $x \equiv 4p \pm a; 2p \pm a \pmod{4p}$.

As $a = p$, hence solutions are given by $x \equiv 4p \pm p; 2p \pm p \pmod{4p}$

$$\equiv p, 3p\, ; p, 3p \pmod{4p}$$

$$\equiv p, 3p \pmod{4p}.$$

Therefore, we see that in this case the congruence has exactly two incongruent solutions.

ILLUSTRATIONS

Let us solve some of the congruence of the said type to check the established formulae.

1] Consider the congruence $x^2 \equiv 5 \pmod{76}$.

It can also be written as $x^2 \equiv 5 + 76 = 81 \pmod{76}$[2].

i.e. $x^2 \equiv 9^2 \pmod{4.19}$. Here, $76 = 4.19$ with $p = 19$ & $a = 9$.

It is of the type $x^2 \equiv a^2 \pmod{4p}$.

Two obvious solutions are $x \equiv \pm a \pmod{4p}$ i.e. $x \equiv a, 4p - a \pmod{4p}$.

$$\text{i.e. } x \equiv 9, 76 - 9 \equiv 9, 67 \pmod{76} \text{ as } a = 9.$$

Also, $a \neq p$, other two solutions exist.

The other two solutions are $x \equiv (2p \pm a) = (38 \pm 9) = 47, 29 \pmod{76}$.

Thus, the required solutions are $x \equiv 9, 67; 47, 29 \pmod{76}$.

Hence, the congruence has four incongruent solutions $x \equiv 9, 67; 47, 29 \pmod{76}$.

2] Consider the congruence $x^2 \equiv 16 \pmod{68}$ i.e. $x^2 \equiv 4^2 \pmod{4.17}$;

$68 = 4.17$ & $p = 17$.

It can be written as $x^2 \equiv 4^2 \pmod{4.17}$.

It is of the type $x^2 \equiv a^2 \pmod{4p}$.

Two obvious solutions are $x \equiv 4p \pm a \pmod{4p}$ i.e. $x \equiv a,\ 4p - a \pmod{4p}$.

$$\text{i.e. } x \equiv 4, 68 - 4 \equiv 4, 64 \pmod{68}.$$

Also, $a \neq p$. So other two incongruent solutions exist.

Hence, other two solutions are $x \equiv (2p \pm a) = (34 \pm 4) = 30, 38 \pmod{68}$.

Thus, the required solutions are $x \equiv 4, 64; 30, 38 \pmod{68}$.

Consider the congruence $x^2 \equiv 5 \pmod{20}$

It can be written as $x^2 \equiv 5 + 20 = 25 = 5^2 \pmod{4.5}$

Two obvious solutions are $x \equiv \pm 5 = 5, 20 - 5 = 5, 15 \pmod{20}$.

As$a = p$, hence it has exactly two incongruent solutions as can be seen below:

The other two solutions are $x \equiv (2p \pm a) = (10 \pm 5) = 15, 5 \pmod{20}$

which are the same as above.

Thus, the congruence has exactly two incongruent solutions $x \equiv 5, 15 \pmod{20}$.

CONCLUSION

Thus, it can be concluded that the congruence under consideration

$\text{i.e.} \;\; x^2 \equiv a^2 \pmod{4p}$, with $a \neq p$, p being an odd positive prime integer has exactly four solutions. These solutions are given by:

$x \equiv 4p \pm a \pmod{4p} = a, 4p - a \pmod{4p}$ are the two obvious solutions.

Other two solutions are given by $x \equiv (2p \pm a)$ are the two other solutions.

But if $a = p$, then the congruence has exactly two incongruent solutions.

MERIT OF THE PAPER

In this paper, a solvable standard quadratic congruence of composite modulus- an odd prime integer multiple of four is formulated. The formula is tested true. Formulation of solutions of the solvable standard quadratic congruence is the merit of the paper.

REFERENCES

[1]Burton David M, Elementary Number Theory, Seventh Indian edition, Mc Graw Hill (Pvt) Ltd., 2012.
[2] Roy B M , Discrete Mathematics & Number Theory, First edition, Das Ganu Prakashan, Nagpur, INDIA, 2016.
[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 Application, second edition, Academic press, 2007.