Formulation of Solutions of a Solvable Standard Quadratic Congruence of Composite Modulus- an Odd Positive Prime Integer Multiple of Nine

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 nine, 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 are 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].

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]. 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.

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: $x^2 \equiv a^2 \pmod{9p}$,

where p is an odd positive prime integer.

Consider the congruence in two different cases: $(a, p) = 1$ and $a = p$ i.e. Formulation is the need of this paper.

ANALYSIS AND RESULT (Formulation)

Let us consider the congruence: $x^2 \equiv a^2 \pmod{9p}$, where p is an odd positive prime integer with (a, p) =1.

Such type of quadratic congruence is always solvable. It has exactly four solutions [3].

Consider the congruence $x^2 \equiv a^2 \pmod{9p}$.

Two obvious solutions are given by $x \equiv \pm a \pmod{9p} = a, 9p - a \pmod{9p}$.

Other two solutions are obtained in the following cases:

Case-I: For other two solutions, consider $x \equiv \pm(p \pm a)$.

Then $x^2 \equiv (p \pm a)^2 = p^2 \pm 2pa + a^2 = a^2 + p(p \pm 2a) = a^2 + p.9m$,

if $p \pm 2a = 9m$ i.e. $x^2 \equiv a^2 \pmod{9p}$.

Thus, if $p \pm 2a = 9m$, then $x \equiv \pm(p \pm a) \pmod{9p}$ are the two other solutions.

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

Then $x^2 \equiv (2p \pm a)^2 = 4p^2 \pm 4pa + a^2 = a^2 + 4p(p \pm a) = a^2 + p.9m$,

if $p \pm a = 9m$ i.e. $x^2 \equiv a^2 \pmod{9p}$.

Thus, $x \equiv \pm(2p \pm a)$ are the two other solutions, if $p \pm a = 9m$.

Case-III: For the other two solutions, consider $x \equiv \pm(3p \pm a)$

Then $x^2 \equiv (3p \pm a)^2 = 9p^2 \pm 6pa + a^2 = a^2 + 3p(3p \pm 2a) = a^2 + 3p.3m$, if $3p \pm 2a = 3m$ i.e. $x^2 \equiv a^2 \pmod{9p}$.

Thus, $x \equiv \pm(3p \pm a)$ are the two other incongruent solutions, if $3p \pm 2a = 3m$.

Case-IV: For the other two solutions, consider $x \equiv \pm(4p \pm a) \pmod{9p}$.

Then $x^2 \equiv (4p \pm a)^2 = 16p^2 \pm 8pa + a^2 = a^2 + 8p(2p \pm a) = a^2 + p.9m$, if $2p \pm a = 9m$ i.e. $x^2 \equiv a^2 \pmod{9p}$.

Thus, $x \equiv \pm(4p \pm a)$ are the two other solutions, if $2p \pm a = 9m$.

Sometimes, the congruence can be given by: $x^2 \equiv b \pmod{9p}$.

It can be written as $x^2 \equiv b + k.9p = a^2 \pmod{9p}$ for some positive integer k [2].

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

ILLUSTRATIONS

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

1] Consider the congruence $x^2 \equiv 22 \pmod{99}$.

It can also be written as $x^2 \equiv 22 + 99 = 121 \pmod{99}$[2].

i.e. $x^2 \equiv 11^2 \pmod{9.11}$. Here, $99 = 9.11$ with $p = 11$.

It can be written as $x^2 \equiv 11^2 \pmod{9.11}$.

It is of the type $x^2 \equiv a^2 \pmod{9p}$

Two obvious solutions are $x \equiv \pm a \pmod{9p}$ i.e. $x \equiv a, 9p - a \pmod{9p}$.

i.e. $x \equiv 11, 99 - 11 \equiv 11, 88 \pmod{99}$ as $a = 11$.

Also, $(a, p) = (11, 11) = 11$ i.e. $a = p = 11$.

For other two solutions, we see that $p \pm a = 11 \pm 11 = 11 - 11 = 0 = 9.0$

Hence, the two solutions are $x \equiv \pm(2p - a) = \pm(22 - 11) = \pm 11 = 11, 88 \pmod{99}$.

Thus, the required solutions are $x \equiv 11, 88; 11, 88 \pmod{99}$. Hence, the congruence has only two incongruent solutions $x \equiv 11, 88 \pmod{99}$.

2] Consider the congruence $x^2 \equiv 9 \pmod{104}$ i.e. $x^2 \equiv 3^2 \pmod{9.13}$; $104 = 9.13$ & $p = 13$.

It can be written as $x^2 \equiv 3^2 \pmod{9.13}$.

It is of the type $x^2 \equiv a^2 \pmod{9p}$.

Two obvious solutions are $x \equiv \pm a \pmod{9p}$ i.e. $x \equiv a, 9p - a \pmod{9p}$.

i.e. $x \equiv 3, 104 - 3 \equiv 3, 101 \pmod{104}$.

Also, $(a, p) = (3, 13) = 1$. So other two incongruent solutions exist.

For the other two solutions, we see that $3p \pm a = 39 \pm 3 = 39 - 3 = 36 = 9.4$.

Hence, the two solutions are $x \equiv \pm(6p - a) = \pm(78 - 3) = \pm 75 = 75, 29 \pmod{104}$.
Thus, the required solutions are $x \equiv 3, 101; 29, 75 \pmod{104}$.
3] Consider the congruence $x^2 \equiv 36 \pmod{99}$. Here, $99 = 9.11$ with $p = 11$.
It can be written as $x^2 \equiv 6^2 \pmod{9.11}$.
It is of the type $x^2 \equiv a^2 \pmod{9p}$.
Two obvious solutions are $x \equiv \pm a \pmod{9p}$ i.e. $x \equiv a, 9p - a \pmod{9p}$.

$$\text{i.e. } x \equiv 6, 99 - 6 \equiv 6, 93 \pmod{99} \text{ as } a = 6.$$

Also, $(a, p) = (6, 11) = 1$. So, other two incongruent solutions exist.

For the other two solutions, we see that $3p \pm 2a = 3.11 \pm 2.6 = 33 + 12 = 45 = 9.5$

Hence, the two solutions are $x \equiv \pm(3p + a) = \pm(33 + 6) = \pm 39 = 39, 60 \pmod{99}$.

Thus, the required solutions are $x \equiv 6, 93; 39, 60 \pmod{99}$.

4] Consider the congruence $x^2 \equiv 9 \pmod{99}$. Here, $99 = 9.11$ with $p = 11$.

It can be written as $x^2 \equiv 3^2 \pmod{9.11}$.

It is of the type $x^2 \equiv a^2 \pmod{9p}$.

Two obvious solutions are $x \equiv \pm a \pmod{9p}$ i.e. $x \equiv a, 9p - a \pmod{9p}$.

$$\text{i.e. } x \equiv 3, 99 - 3 \equiv 3, 96 \pmod{99} \text{ as } a = 3.$$

For the other two solutions, we see that $3p \pm 2a = 3.11 \pm 6 = 33 - 6 = 27 = 9.3$

Hence, the two solutions are $x \equiv \pm(3p - a) = \pm(33 - 3) = \pm 30 = 30, 69 \pmod{99}$.

Thus, the required solutions are $x \equiv 3, 96, 30, 69 \pmod{99} \equiv 3, 30, 69, 96 \pmod{99}$.

CONCLUSION

Thus, it can be concluded that the congruence under consideration

i.e. $x^2 \equiv a^2 \pmod{9p}$, with $(a, p) = 1$, p being an odd positive prime integer has exactly four solutions. These solutions are given by:

$x \equiv \pm a \pmod{9p} = a, 9p - a \pmod{9p}$ are the two obvious solutions.

Other two solutions are given by any one of the following cases:

Case-I: If $p \pm 2a = 9m$, then $x \equiv \pm(p \pm a) \pmod{9p}$ are the other two solutions.

Case-II: If $p \pm a = 9m$, then $x \equiv \pm(2p \pm a)$ are the two other solutions.

Case-III: If $3p \pm 2a = 3m$, then $x \equiv \pm(3p \pm a)$ are the two other solutions.

Case-IV: If $2p \pm a = 9m$, then $x \equiv \pm(4p \pm a)$ are the two other solutions.

MERIT OF THE PAPER

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

REFERENCE

[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.