Formulation of a class of standard congruence of higher degree modulo an odd prime-square integer

Prof. B M Roy

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

***Abstract*: In this paper, a class of standard congruence of higher degree modulo a prime-square integer is formulated. Formula is tested and found true by solving different examples. No formulation is found in the literature of mathematics for the congruence under consideration. Formulation is the merit of the paper.**

***Keywords*: Binomial theorem, Prime-power residues,**

INTRODUCTION

Number Theory is a special branch of pure mathematics. Congruence is the stream of blood running throughout. So, no one can neglect it. But now-a-days, it is seldom known to the teachers/ readers. All are running behind the theory of relativity. Thus the most of the researches are carried out on relativity. The number theory is a poor and neglected branch of mathematics though it is the building- block of modern industries. It must be enriched with new formulae and method to find the solutions of the congruence. There is vast scope of research. The author understood the same and tried his best to improve this branch of mathematics. The author formulated a lot of congruence. Here is the congruence under consideration for formulation of the type: $x^p \equiv a \ (mod\ p^2)$, p being an odd prime positive integer.

LITRATURE-REVIEW

The congruence under consideration is $x^p \equiv a \ (mod\ p^2), p\ being\ a\ prime$. No method or formulation is found for the said congruence in the literature of mathematics. Modern mathematicians are not paid heed to the said branch. It is very pathetic that still today the readers are studied the Euler's / Fermat's method. No one attempted to find a simple formula / a method to solve the problems of congruence. It seems that the branch of mathematics- The Number Theory- is very unfortunate.

NEED OF RESEARCH

The author tried his best to formulate the congruence and presented his effort in this paper. To establish a formulation of the congruence is the need of the research.

PROBLEM-STATEMENT

The congruence of the type:$x^p \equiv a \ (mod\ p^2), (a,p) = 1,\ p\ being\ an\ odd\ prime$, is the congruence considered for formulation; also, the solvability condition of the said congruence is to find.

ANALYSIS & RESULT

Consider the congruence:$x^p \equiv a \ (mod\ p^2), p\ being\ an\ odd\ prime\ integer.$

Such congruence is solvable, if a is p^{th}- power residue of p and always has p solutions.

To find those solutions, consider $x \equiv pm + a \ (mod\ p^2)$.

Then $x^p = (pm + a)^p$

Expanding using binomial theorem, it is seen that

$$x^p = (pm + a)^p$$

$$\equiv a^p \equiv a \ (mod\ p^2), \qquad if\ a^p \equiv a \ (mod\ p^2).$$

Thus, $x = pm + a$ satisfies the said congruence and hence it can be considered as solutions of the congruence. As it has p solutions, all solutions can be obtained by putting different values of m such as: $m = 0, 1, 2, \ldots\ldots\ldots\ldots, (p-1)\ \ldots\ \ldots$
If $m = p$, then $x \equiv p.p + a \equiv p^2 + a \equiv a \ (mod\ p^2)$ which is the same for $m = 0$.

It is also seen that for $m = p + 1,\ p + 2, \ldots\ldots, p + (p - 1)$, the result repeats as for

$m = 1, 2, \ldots\ldots (p - 1)$. Thus, $m = 0, 1, 2, \ldots\ldots, (p - 1)$.

The condition $a^p \equiv a\ (mod\ p^2)$ can be considered as the condition of solvability of the said congruence.

ILLUSTRATION

Let us consider the congruence $x^5 \equiv 4\ (mod\ 25)$.

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

At first solvability condition is to be tested. As per the solvability condition, 4 must be fifth-power residue of 5.

The residues of 5 are 0, 1, 2, 3, 4.

Their fifth-power residues modulo 25 are 0, 1, 7, 18 & 24. It is seen that 4 is not fifth-power residue of 5 modulo 25. Thus, as per the condition said, the congruence is not solvable. It is also tested true.

Consider one more example.

Consider $x^7 \equiv 30\ (mod\ 49)$.

It can be written as $x^7 \equiv 30\ (mod\ 7^2)\ \ with\ p = 7; a = 30$.

The residues of 7 are 0, 1, 2, 3, 4, 5, 6.

Their seventh powers congruent to 49 are: 0, 1, 30, 31, ...

Thus 30 is a seventh-power residue of 7 modulo 49.

Therefore, the congruence is solvable and has seven incongruent solutions.

These are given by the formula $x \equiv pm + a\ (mod\ 49);\ m = 0, 1, 2, 3, 4, 5, 6$.

$$\equiv 7m + 30(mod\ 49)$$

$$\equiv 30, 37, 44, 51, 58, 65, 72\ (mod\ 49)$$

$$\equiv 30, 37, 44, 2, 9, 16, 23\ (mod\ 49)$$

$$\equiv 2, 9, 16, 23, 30, 37, 44\ (mod\ 49).$$

One more examples is $x^5 \equiv 1\ (mod\ 25)$.

It can be written as $x^5 \equiv 1\ (mod\ 5^2)\ \ with\ p = 5; a = 30$.

The residues of 5 are 0, 1, 2, 3, 4.

Their fifth- powers modulo 25 are: 0, 1, 7, 18 & 24.

Thus 1 is fifth-power residue of 5.

Therefore, the congruence is solvable and has five incongruent solutions.

These are given by the formula $x \equiv pm + a\ (mod\ 25); m = 0, 1, 2, 3, 4$.

$$\equiv 5m + 1(mod\ 5^2)$$

$$\equiv 1, 6, 11, 16, 21\ (mod\ 5^2)$$

$$\equiv 1, 6, 11, 16,\ \ 21\ (mod\ 5^2).$$

CONCLUSION

Thus, it is concluded that the congruence under consideration $i.e.x^p \equiv a\ (mod\ p^2)$ has exactly p-solutions given by $x \equiv pm + a\ (mod\ p^2) with\ m = 0, 1, 2, 3, \ldots\ldots, (p-1)$ and $a^p \equiv a\ (mod\ p^2)$ is the solvability condition of the said congruence.

MERIT OF THE PAPER

A formula to find the solutions directly of the said congruence is established. This is the merit of the paper.

REFERENCE

[1] Burton D M, "*Elementary Number Theory*", 2/e, 2003, Universal Book Stall.
[2] Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.
[3] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.
[4] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.