ISSN No:-2456-2165

RP-27: Formulation of Solutions of a Class of Congruence of Prime-Power Modulus of Higher Degree.

B. M. Roy
Head, Dept. of Mathematics
Jagat Arts, commerce & I. H. P. Science College, Goregaon(Gondia), M. S., India.
Pin-441801

Abstract:- In this paper, a formula to find the solutions of a congruence of prime power modulus of higher degree the type $x^p \equiv a \pmod{p^n}$, where p is an odd positive prime integer and n≥ 2,is any positive integer, is established. The formula is of great merit and of time-saving in calculation.The method found in the Mathematics literature is time-consuming. It is also found that such a congruence is solvable if $a^p \equiv a \pmod{p^n}$ and each congruence has exactly p solutions and in total, there are (p-1) such congruence.

***Key-words**:- Binomial Expansion; Fermat's Theorem Prime-power modulus.*

I. INTRODUCTION

Many mathematicians worked on number theory and improved the theory. Many more theorems and methods are developed to make the theory interesting and computationally easy. Euler, Lagrange& Fermat are such mathematicians who improved Number Theory the most. They proposed methods to find solutions of congruence of prime & composite modulus.

II. NEED OF THIS RESEARCH

Even then there remains much workto do. Going through those previous works presented in the literature, some results insist me to write this paper. It is found that no formulation is done to find the solutions of the congruence. Then a class of congruence appeared in my mind which is not yet formulated. I tried to do so, here.

III. LITERATURE REVIEW

We have a corollary of Lagrange's Theorem in Number Theory that "if p is an odd prime and d|(p-1), then the congruence $x^d \equiv 1 \ (mod\ p)$ has exactly d incongruent solutions modulo p"[1].Also we have a Theorem in Number Theory that "The congruence $x^2 \equiv a \ (mod\ p^n)$ with p an odd positive prime integer, n≥ 1 any positive integer, (p, a) =1 has exactly two incongruent solutions"[2].

Then a congruence of the type $x^p \equiv a \ (mod\ p^n)$appeared in my mind. I tried my best to formulate the solutions of the congruence. What I found, is placed in this paper.

IV. PROBLEM STATEMENT

Consider the congruence$x^p \equiv a \ (mod\ p^n)$ with $n \geq 2, p\ bieng$ appositive prime.

The congruence $x^p \equiv a \ (mod\ p^n)$ is solvable, if $a^p \equiv a \ (mod\ p^n)$and $x \equiv a \ (mod\ p^n)$ is one of the solution. All solutions are given by $x \equiv a + p^{n-1}k \ (mod\ p^n); n \geq 2,$

$k = 0, 1, 2, \dots\dots, (p-1)$. There are (p-1) such congruence each has exactly p solutions.

V. FORMULATION OF SOLUTION (ANALYSIS)

Let us consider the congruence $x^p \equiv a \ (mod\ p^n)$ with the condition: $a^p \equiv a \ (mod\ p^n)$, p being odd positive prime integer and n≥ 2, any positive integer.

For $x = a, we\ have\ x^p = a^p \equiv a \ (mod\ p^n)\ by\ Fermat'Little\ Theorem.$

So, $x \equiv a \ (mod\ p^n)$ is a solution of$x^p \equiv a \ (mod\ p^n)$.

Consider now that$x = a + p^{n-1}k\ \ for\ k = 0, 1, 2, \dots\dots, (p-1)$.

Then, $x^p = (a + p^{n-1}k)^p$

$$= a^p + p.a^{p-1}p^{n-1}k + \frac{p(p-1)}{2!}a^{p-2}p^{2n-2}k^2 + \cdots\dots\dots\dots\dots + (p^{n-1}k)^p$$

$$= a^p + \left\{ a^{p-1}k + \frac{p(p-1)}{2!} a^{p-2}k^2 p^{n-2} + \cdots \ldots \ldots \ldots \ldots \ldots \right\} . p^n$$

$$\equiv a^p \ (mod\ p^n)$$

$\equiv a\ (mod\ p^n), \quad if \quad a^p \equiv a\ (mod\ p^n).$

So, for $x \equiv a + p^{n-1}k\ (mod\ p^n)$, we always have $x^p \equiv a\ (mod\ p^n)$.

If we take $k = p,\ then\ x \equiv a + p^{n-1}.k\ (mod\ p^n)$ becomes

$$x \equiv a + p^n\ (mod\ p^n)$$

$i.e.\ x \equiv a\ (mod\ p^n)$, which is same as for $k = 0$.s

VI. RESULT OF ANALYSIS

A congruence of the type $x^p \equiv a\ (mod\ p^n)$ is made easy to find its solutions by using theestablished formula. It is found that

$x \equiv a + p^{n-1}k\ (mod\ p^n)fork = 0, 1, 2, 3, \ldots \ldots, (p-1)$are the p-solutions of the congruence $x^p \equiv a\ (mod\ p^n)$. And there is no other possibilities. These must give all the possible solutions.

We illustrate the formula established by giving two examples below:

VII. ILLUSTRATION

Consider $x^7 \equiv 18\ (mod\ 49)$.

It can be written as:$x^7 \equiv 18\ (mod\ 7^2)$.

It is of the type $x^p \equiv a\ (mod\ p^n)\ \ with\ a = 18,\ \ p = 7,\ \ n = 2.$

Now, $18^7 = 612220032 \equiv 18\ (mod\ 7^2)\ which\ implies\ that\ a^p \equiv a\ (mod\ p^n)$.

Hence the congruence is solvable and has 7-solutions with

$$x \equiv 18\ (mod\ 49) is\ one\ of\ the\ solution.$$

All the solutions are giving by

$$x \equiv a + p^{n-1}k\ (mod\ p^n)\ \ with\ k = 0, 1, 2, 3, 4, 5, 6.$$

$$i.e.\ x \equiv 18 + p^{2-1}k$$

$$i.e.\ x \equiv 18 + 7k$$

$$i.e.\ x \equiv 18, 18+7, 18+14, 18+21, 18+28, 18+35, 18+42 \quad (mod\ 49)$$

$$i.e.\ x \equiv 18, 25, 32, 39, 46, 53, 60\ \ (mod\ 49)$$

$$i.e.\ x \equiv 4, 11, 18, 25, 32, 39, 46\ (mod\ 49).$$

These are the required solutions obtained. These solutions are tested true.

Let us consider one more example:

Consider $x^5 \equiv 7\ (mod\ 25)$.

It is of the type $x^p \equiv a\ (mod\ p^n)\ \ with\ a = 7,\ \ p = 5,\ \ n = 2.$

Now, $7^5 = 16807 \equiv 7\ (mod\ 5^2)\ which\ implies\ that\ a^p \equiv a\ (mod\ p^n)$.

Hence the congruence is solvable.

All the solutions are giving by

$$x \equiv a + p^{n-1}k\ (mod\ p^n)\ \ with\ k = 0, 1, 2, 3, 4.$$

$$i.e.\ x \equiv a + p^{2-1}k$$

$$i.e.\ x \equiv 2 + 5k$$

$$i.e.\ x \equiv 2, 7, 12, 17, 22\ \ (mod\ 25)$$

These are the required solutions obtained. These solutions are tested true.

VIII. MERIT OF THE PAPER

In this paper, a formula is established to find all the possible solutions of the given congruence. It saves time in calculation. The method found in the literature, is time-consuming. There is no such formulae found in literature.

IX. CONCLUSION

Therefore, we can conclude that$x \equiv a + p^{n-1}k\ \ (mod\ p^n)\ \ withn \geq 2,$

$k = 0, 1, 2, \ldots \ldots, (p-1)$are the p- solutions of the congruence of the type $x^p \equiv a\ (mod\ p^n)$, with p being odd positive prime integer when $a^p \equiv a\ (mod\ p^n)$.

REFERENCES

[1]. Koshy Thomas,"Elementary Number Theory with Applications", 2/e, Academic Press,2009.

[2]. Niven, Zuckerman, Montgomery,"An Introduction to The Theory of Numbers"; 5/e;Wiley India, 2008.

[3]. Burton David M., "Elementary Number Theory", 7/e,McGraw Hill, 2011.