Volume 1, Issue 3, July-2018: 27-29
International Journal of Current Innovations in Advanced Research ISSN: 2636-6282

Solutions of a Class of Congruence of Multiple of Prime-Power Modulus of Higher Degree

Prof. B. M. Roy

Head, Dept. of Mathematics, Jagat Arts, Commerce and I. H. P. Science College, Goregaon, (Gondia), M. S., India, Pin-441801
Corresponding author E-mail: roybm62@gmail.com

Abstract: In this paper, a formula to find the solutions of a congruence of prime power modulus of higher degree the type $x^p \equiv b^p \pmod{ap^n}$, where p is an odd positive prime integer and $n \geq 2$, 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 $b^p \equiv b \pmod{ap^n}$ and each congruence has exactly p solutions and in total, there are (p-1) such congruence.
Keywords: Binomial Expansion, Fermat's Theorem, Prime-power modulus

Citation: Roy, B.M. 2018. Solutions of a Class of Congruence of Multiple of Prime-Power Modulus of Higher Degree. International Journal of Current Innovations in Advanced Research, 1(3): 27-29.

Introduction

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

Need of this Research

Even then there remains much work to 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 my best to formulate the congruence and my effort is presented in this paper.

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" (Koshy Thomas, 2009). 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, $n \geq 1$ any positive integer, (p, a) =1 has exactly two incongruent solutions" (Ivan Niven *et al.,* 2008).

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

Problem Statement

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

The congruence $x^p \equiv b^p \ (mod\ ap^n)$ is always solvable and $x \equiv b \ (mod\ ap^n)$ is one of the solution. All solutions are given by $x \equiv b + ap^{n-1}k \ (mod\ ap^n); n \geq 2$ where $k = 0, 1, 2, \dots\dots, (p-1)$. There are (p-1) such congruence and each congruence has exactly p solutions.

Analysis and Result

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

For $x = b, we\ have\ x^p = b^p \ (mod\ ap^n)$.

So, $x \equiv b \ (mod\ ap^n)$ is a solution.

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

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

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

$$= b^p + \{\cdots\cdots\cdots\cdots\cdots\}.ap^n$$

$$\equiv b^p \ (mod\ ap^n)$$

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

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

$x \equiv b + kp^n \ (mod\ ap^n)$

$i.e.\ x \equiv b \ (mod\ ap^n)$, which is same as for $k = 0$. Similar results for $k = p+1, p+2, \dots$

Result of Analysis

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

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

We illustrate the formula established by giving two examples below.

Illustration

Consider $x^7 \equiv 128 \ (mod\ 147)$. Here 147=3.49=$3.7^2$

It can be written as:$x^7 \equiv 128 \ (mod\ 3.7^2)\ i.e.\ x^7 \equiv 128 \equiv 2^7 \ (mod\ 3.7^2)$

It is of the type $x^p \equiv b^p \ (mod\ ap^n)\ with\ b = 2,\ p = 7,\ n = 2, a = 3.$

Hence the congruence is solvable and has 7-solutions with

$x \equiv 2 \ (mod\ 3.49) is\ one\ of\ the\ solution.$

All the solutions are giving by

$$x \equiv 2 + 3.7^{2-1}.k \ (mod\ 3.7^2) \ \ with\ k = 0,1,2,3,4,5,6.$$
$$i.e.\ x \equiv 2 + 3.7^{2-1}k$$
$$i.e.\ x \equiv 2 + 3.7k$$
$$i.e.\ x \equiv 2 + 21k \ \ for\ k = 0,1,2,3,4,5,6\ .$$
$$i.e.\ x \equiv 2, 2+21, 2+42, 2+63, 2+84, 2+105, 2+126 \quad (mod\ 147)$$
$$i.e.\ x \equiv 2, 23, 44, 65, 86, 107, 128\ (mod\ 147)$$

These are the required solutions obtained. These solutions are tested true.
Let us consider one more example:

Consider $x^5 \equiv 7\ (mod\ 150)\ i.e.\ x^5 \equiv 7\ (mod\ 6.5^2)$
It is of the type $x^p \equiv b\ (mod\ ap^n)\ \ with\ a = 6,\ \ p = 5,\ \ n = 2, b = 7.$
Now, $7^5 = 16807 \equiv 7\ (mod\ 6.5^2)\ .$

Hence the congruence is solvable and has 5-solution.
All the solutions are giving by

$$x \equiv b + ap^{n-1}k\ (mod\ ap^n)\ \ with\ k = 0,1,2,3,4.$$
$$i.e.\ x \equiv 7 + 6.p^{2-1}k$$
$$i.e.\ x \equiv 7 + 30k\ for\ k = 0,1,2,3,4$$
$$i.e.\ x \equiv\ 7, 37, 67, 97, 127 (mod\ 150).$$

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

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 formula found in literature.

Conclusion

Therefore, we can conclude that $x \equiv b + ap^{n-1}k\ \ (mod\ ap^n)\ \ with\ \ n \geq 2,$
$k = 0, 1, 2, \ldots\ldots, (p-1)$ are the p- solutions of the congruence of the type $x^p \equiv b^p\ (mod\ ap^n)$, with p an odd positive prime integer.

References

1. Ivan Niven, Harbert S. Zuckerman and Hugh L. Montgomery, 2008. An Introduction to the Theory of Numbers. 5th Edition, Wiley, India.

2. Koshy Thomas, 2009. Elementary Number Theory with Applications. 2nd Edition, Academic Press.