INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X

Impact factor: 4.295

(Volume 4, Issue 2)

Available online at: www.ijariit.com

Formulation of solutions of a special type of standard congruence of prime modulus of higher degree

B. M. Roy

roybm62@gmail.com

Jagat College, Gondia, Maharashtra

ABSTRACT

In this paper, a special type of congruence of prime modulus of higher degree is considered. A direct formula for solutions is established. Formula is well-tested by solving suitable examples.

A comparison is made with the method established by Eugen Vedral and the method presented here in this paper and the method is proved to be a generalization of Eugen Vedral's method.

It is proved more useful than the method suggested by Eugen Vedral.

Keywords: *Congruence of higher degree, Fermat's Little Theorem, Inverse number modulo a prime, prime modulus.*

1. INTRODUCTION

Many mathematicians tried their best to find method to solve a congruence of prime modulus of higher degree. These methods are found in mathematics literature. Eugen Vedral [1] is one of such mathematician. He proposed two methods to find the "solutions of some classes of congruence" of prime modulus of higher degree. But when I have gone through the literature presented by E. Vedral and I found that the method proposed is limited. In this paper, I have tried to generalize the idea of Eugen Vedral in some other way.

2. EUGEN VEDRAL'S IDEA

Consider a congruence $x^k \equiv a \ (mod\ p)$, p odd prime positive integer and k$\neq lp$, for some positive integer $l \geq 1$.

If $p = kl + 2, then$ the congruence can be reduced to a linear congruence and can be solved easily. Consider a positive odd prime $p = 41$. It can be expressed in two different ways such as

$$41 = 3.13 + 2 \ \ \& \ \ 41 = 13.3 + 2.$$

Thus, E. Vedral's method can be applied to two congruence only for a particular prime p:

$(i)\ \ x^3 \equiv a \ (mod\ 41)$

$(ii)\ \ x^{13} \equiv a \ (mod\ 41)$

for the particular prime $p = 41$.

But in this paper, this method is modified to use in the following congruence of the same modulus such as

$(1)\ \ x^3 \equiv a \ (mod\ 41)$

$(2)\ \ x^{13} \equiv a \ (mod\ 41)$

$(3)\ \ x^9 \equiv a \ (mod\ 41)$

$(4)\ \ x^{27} \equiv a \ (mod\ 41)$

(5) $x^{11} \equiv a\ (mod\ 41)$

(6) $x^{7} \equiv a\ (mod\ 41)$

(7) $x^{23} \equiv a\ (mod\ 41)$, And many more.

3. DEMERIT OF E. VEDRAL'S METHOD

From the above discussion it is clear that Eugen Vedral's method has limited use.

4. PROBLEM STATEMENT

Consider the congruence $x^k \equiv a\ (mod\ p)$, p an odd prime positive integer, $k \neq lp$, for positive integer l, $1 \leq a \leq p-1\ with\ (k,\ p-1) = 1$.

Here the problem is to formulate the solutions of the congruence under consideration in two cases:

(i) $mk = n(p-1)+1$,

(ii) $mk = n(p-1)-1$, For some positive integers m & n.

Here it will be shown that in both the cases, the congruence will reduce to a linear congruence.

Also, a direct formula for solution will be obtained.

5. ANALYSIS and RESULT

Consider the congruence $x^k \equiv a\ (mod\ p)$ with the conditions as mentioned above.

If there exist positive integer's m & n such that $mk = n(p-1)+1$, then the congruence can be written as:

$$x^k \equiv a\ (mod\ p)$$

$$i.e.\ \ x^{mk} \equiv a^m\ (mod\ p)$$

$$i.e.\ \ x^{n(p-1)+1} \equiv a^m (mod\ p)$$

$$i.e.\ \ x^{n(p-1)}.x^1 \equiv\ a^m\ (mod\ p)$$

$$i.e.\ \ 1.x \equiv a^m\ (mod\ p),\quad by\ Fermat's\ little\ theorem,$$

$$i.e.\quad x \equiv a^m\ (mod\ p).$$

Thus, if $mk = n(p-1)+1$, then the congruence $x^k \equiv a\ (mod\ p)$ has a unique solution

$$x \equiv a^m (mod\ p).$$

If there exist positive integers m & n such that $mk = n(p-1)-1$, then the congruence can be written as

$$x^{mk} \equiv a^m\ (mod\ p)$$

$$i.e.\ \ x^{n(p-1)-1} \equiv a^m (mod\ p)$$

$$i.e.\ \ x^{n(p-1)} \equiv a^m x\ \ (mod\ p)$$

$$i.e.\ \ 1 \equiv\ a^m x\ (mod\ p),\ \text{by Fermat's little theorem[4]}$$

$$i.e.\quad a^m x \equiv 1\ (mod\ p),\ \text{which is a linear congruence,}$$

$$i.e.\ x \equiv \overline{a^m}\ (mod\ p),\ \ where\ \overline{a^m}\ \text{is the inverse of}\ a^m\ \text{modulo p.}$$

Thus, if $mk = n(p-1)-1$, then the congruence $x^k \equiv a\ (mod\ p)$ reduces to a linear

Congruence of prime modulus and has a unique solution, given by

$$x \equiv \overline{a^m} (mod\ p).$$

6. EXAMPLES

Consider the example: $x^9 \equiv 2\ (mod\ 41)$.

Here, we see that $9.9 = 2.(41-1)+1 = 2.40+1\ \&\ (9\ ,40) = 1$.

Then above congruence can be written as: $x^{9.9} \equiv 2^9\ (mod\ 41)\ i.e.\ x^{81} \equiv 20\ (mod\ 41)$

as $2^9 \equiv 20\ (mod\ 41)$. It can be written as: $x^{2.40+1} \equiv 20\ (mod\ 41)\ \ i.e. x \equiv 20\ (mod\ 41)$.

This is the only solution.

By using the formula developed, the solution is $x \equiv a^m \ (mod\ p)$.

In this case $m = 9,\ \ a = 2,\ p = 41.$

Therefore, $x \equiv 2^9 \ (mod\ 41) \quad i.e.\ \ x \equiv 20 \ (mod\ 41).$

The proposed method can also be applied to solve the congruence

$x^3 \equiv 3 \ (mod\ 41);\ \ x^{27} \equiv 4 \ (mod\ 41)$

But E. Vedral's method can't.

Consider another example: $x^{13} \equiv 3 \ (mod\ 41)$

Here, we see that $13.3 = 1.40 - 1\ \ \&\ \ (13\ ,40) = 1.$

Then above congruence can be written as: $x^{13.3} \equiv 3^3 \ (mod\ 41)$

$i.e.\ x^{39} \equiv 27 \ (mod\ 41)$ as $3^3 \equiv 27 \ (mod\ 41)$.

It can be written as: $x^{1.40-1} \equiv 27 \ (mod\ 41)\ \ i.e. 27\ x \equiv 1 \ (mod\ 41)$

$i.e.\ 81\ x \equiv 3 \ (mod\ 41)\ \ i.e. -x \equiv 3 \ (mod\ 41)\ \ i.e.\ x \equiv -3 \equiv 38 \ (mod\ 41)$

This is the only solution.

By using the formula developed, the solution is $x \equiv \overline{a^m} \ (mod\ p)$.

In this case $m = 3,\ \ a = 3,\ p = 41.$

Therefore, $x \equiv \overline{3^3} \ (mod\ 41) \quad i.e.\ \ x \equiv \overline{27} \ (mod\ 41)$

$i.e.\ x \equiv 38 \ (mod\ 41),\ as\ 38.27 = 1026 \equiv 1 \ (mod\ 41).$

7. MERIT OF THE METHOD

This method can be used to find the solutions of many standard

Congruence of higher degree. Formulae are developed to find solutions directly. It saves time in finding solutions.

8. CONCLUSION

Thus, in this paper, the solutions of a special type of congruence of higher degree is considered and discussed. Its solutions are formulated. The direct formula for solutions is the merit of this paper. It saves the time of calculation for solution. There is no other method to find solutions of these types of congruence.

9. REFERENCES

[1] Vedral Eugen, 'Solutions of Some Classes of Congruence' from the Journal "Teaching of Mathematics", 2006, Vol. IX, PP. 41-44.
[2] Koshy, Thomas; *Elementary Number Theory with Applications*; 2/e; Academic press.
[3] Niven. I.; Zuckerman H S.; Montgomery H L.; *an Introduction to the Theory of Numbers*; 5/e; WSE.
[4] B. M. ROY, Discrete Mathematics & Number Theory, 1/e, Das Ganu Prakashan. Nagpur (M S).

