RP-68: Solutions of a Special Standard Congruence of Prime modulus of higher degree

Prof. B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon (GONDIA)
M. S., INDIA. Pin: 441801
(Affiliated to R T M Nagpur University)

***Abstract*: In this paper, a congruence of higher degree of prime modulus is considered for its solutions. A technique is developed and proved true, solving different examples. It is seen that the reduced residues are the solutions of the congruence under consideration. Finding the reduced residues of a prime, using Euler's Criterion, is not a time-saving method. A new method is in an urgent need.**

***Keywords*: Fermat's Little Theorem, Prime modulus, Quadratic residues, Reduced Residues.**

INTRODUCTION

In this paper, the author, wishes to find the solutions of a special type of standard congruence of higher degree of prime modulus. They are having solutions related to p only. Some has solutions as quadratic residues of p and some has non-quadratic residues of p [1]. Quadratic residues are the positive integers such that if a is a residues (least remainder when the integer is divided by prime p) of P, then $a^2 \equiv b\ (mod\ p)$ is a quadratic residues of p [3].

PROBLEM-STATEMENT

The problem is-

"To find the solutions of the congruence of higher degree of the types:

$x^{\frac{p-1}{2}} \equiv a\ (mod\ p); where$ p an odd positive prime, and (a, p)=1".

LITERATURE REVIEW

A very little literature is found for the congruence of higher degree of prime and composite modulus except the author's research papers published in different international journals [5], [6], ……, [10].

In the book of Number Theory, Euler's criterion is given for finding reduced residues of a prime p [2], [3]. It is not practicable. It takes a long time and not easy. No direct formulation is found in the literature of mathematics.

NEED OF RESEARCH

In continuation of author's research, he found one more congruence to discuss for its solutions. This congruence also creates difficulty to the readers. A lot of labour is required to find the solutions of the said congruence. To lessen the labour of the readers, the author takes the opportunity to search an easy way to find the solutions of the congruence under consideration. This is the need of the research.

ANALYSIS & RESULT

Consider the congruence $x^{\frac{p-1}{2}} \equiv a\ (mod\ p); (a,p) = 1; p\ odd\ positive\ prime.$

Let $x \equiv u\ (mod\ p) be\ a\ solution.$

Then, $u^{\frac{p-1}{2}} \equiv a\ (mod\ p)$

$i.e.\ u^{p-1} \equiv a^2\ (mod\ p)\ i.e.\ \boldsymbol{a^2 \equiv 1\ (mod\ p)}$, by Fermat's Little Theorem.

$\boldsymbol{i.e.\ a \equiv \pm 1\ (mod\ p)}$.

So, $\boldsymbol{a^2 \equiv 1\ (mod\ p)}$ can be considered as a **solvability condition** of the said congruence.

And, $a \equiv \pm 1\ (mod\ p)$ shows that there are two solvable congruence which are

$x^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ & $x^{\frac{p-1}{2}} \equiv -1 (mod\ p)\ i.e.\ x^{\frac{p-1}{2}} \equiv p-1 (mod\ p)$.

Therefore, the other congruence $x^{\frac{p-1}{2}} \equiv a\ (mod\ p)\ with\ a = 2, 3, 4, \ldots\ldots\ldots, (p-2)$

are not solvable.

Consider the congruence $x^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$.

Let r be a reduced residue of p, then (r, p) =1.

So, $r^{\frac{p-1}{2}} \equiv$ a (mod p) $i.e.\ r^{p-1} \equiv a^2\ (mod\ p)$

But by Fermat's Little Theorem,

$r^{p-1} \equiv 1\ (mod\ p)\ \ i.e. (r^2)^{p-1/2} \equiv 1\ (mod\ p)$.

Thus, r^2 is a solutions of the said congruence but r is a residue of p.

Therefore, $r^2\ is\ a\ quadratic\ residue\ of\ p.$

Hence, every quadratic residue is a solution of the congruence.

Consider the congruence $x^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$.

Then, quadratic residues are not the solutions of the congruence. Therefore, quadratic non-residues are the solutions. Its solutions are the quadratic non-residues of p [4].

ILLUSTRATIONS

Consider the congruence $x^5 \equiv 1\ (mod\ 11)$. Here p =11, an odd prime positive integer.

It can be written as $x^{\frac{11-1}{2}} \equiv 1\ (mod\ 11); hence\ is\ of\ the\ type\ x^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$.

It is always solvable and solutions are the quadratic residues of p.

The reduced residues of 11 are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.

Then the required quadratic residues are: 1, 4, 9, 5, 3, 5, 9, 4, 1 $i.e.\ 1, 3, 4, 5, 9\ (mod\ 11)$.

The required solutions are $x \equiv 1, 3, 4, 5, 9\ (mod\ 11)$.

Consider the congruence $x^5 \equiv 10\ (mod\ 11)$.

It can be written as $x^{\frac{11-1}{2}} \equiv -1\ (mod\ 11) and\ of\ the\ type\ x^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$.

Its solutions are the quadratic non-residues of p = 11.

As the quadratic residues are 1, 3, 4, 5, 9 (mod 11) hence the non-residues are 2, 6, 7, 8, 10.

The solutions of the congruence are $x \equiv 2, 6, 7, 8, 10\ (mod\ 11)$.

Consider the congruence $x^6 \equiv 10\ (mod\ 13)$.

It can be written as $x^{\frac{13-1}{2}} \equiv 10\ (mod\ 13)$.

It is of the type $x^{\frac{p-1}{2}} \equiv a\ (mod\ p)$. As $a \neq \pm 1$, hence it is not solvable.

So, the congruence has no solution.

CONCLUSION

The congruence $x^{\frac{p-1}{2}} \equiv a\ (mod\ p)$ is only solvable if $a^2\ \equiv 1\ (mod\ P)$

$i.e. a \equiv \pm 1\ (mod\ p)$.

For $a = 1$, the solutions of the congruence: $x^{\frac{p-1}{2}} \equiv 1\ (mod\ p)$ are the quadratic residues of P while for $a = -1$, the solutions of $x^{\frac{p-1}{2}} \equiv -1\ (mod\ p)$ are the quadratic non-residues of p.

MERIT OF THE PAPER

In this paper, it is found that there two congruence of higher degree under consideration are solvable. The solvability condition is obtained. This is the merit of the paper.

REFERENCES

[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.
[5] Roy B M, *Formulation of solutions of a special type of standard congruence of prime modulus of higher degree,* International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-02, Mar-Apr-18.
[6] Roy B M, *Formulation of solutions of a class of standard congruence of prime-power modulus of higher degree,* International Journal of Innovative Science and Research Technology *(IJISRT),*ISSN: 2456-2165,vol-03, Issue-04, April-18.
[7] Roy B M, *Formulation of solutions of two special congruence of prime modulus of higher degree, International Journal of Science and Engineering Development Research (IJSDR), ISSN: 2455-2631, vol-03,Issue-05,May-18.*
[8] Roy B M, *Solutions of two special types of congruence of higher degree,* (IJRULA), Vol-01, Issue-07, July-18.
[9] Roy B M, *Solving Three special types of standard congruence of prime modulus of higher degree,* (IJTSRD), vol-03, Issue-03, April-19.
*[10]*Roy B M, *Solving Two special types of standard congruence of prime modulus of higher degree,* (IJTSRD), vol-03, Issue-03, April-19.