International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 3 | Mar-Apr 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

RP-75: Formulation of two Special Classes of Standard Congruence of Prime Modulus of Higher Degree

Prof. B M Roy

Head, Department of Mathematics, Jagat Arts, commerce & I H P Science College, Gorgaon, Gondia, Maharashtra, India

How to cite this paper: Prof. B M Roy "RP-75: Formulation of two Special Classes of Standard Congruence of Prime Modulus of Higher Degree" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-3, April 2019, pp.1531-1534, URL: https://www.ijtsrd.com/papers/ijtsrd23417.pdf

IJTSRD23417

ABSTRACT

In this paper, two special classes of congruence of prime modulus of higher degree are considered for formulation. Author's sincere efforts established the corresponding formulae for solutions. The congruence were not formulated earlier. Due to this formulation, it becomes an easy task to solve the said congruence orally when p is comparatively small. Formulations of the congruence is the merit of the paper.

KEYWORDS: *Congruence of higher degree, Fermat's little theorem, Modular Inverse, Prime modulus.*

INTRODUCTION

Standard congruence of higher degree are seldom studied & discussed in the literature of mathematics. It is a neglected topic in Number Theory but is a very interesting topic of study. Even, no one cared for it. In this paper, the author wishes to formulate two interesting special classes of standard congruence of prime modulus of higher degree. Such congruence are not considered for formulation by earlier mathematicians.

LITERATURE REVIEW

A standard congruence of prime modulus of higher degree is discussed nowhere in the literature of mathematics. Author found some congruence of higher degree of prime modulus and tried his best to formulate these congruence using Fermat's Little Theorem and his own ideas. The author already formulated some standard congruence of higher degree of prime modulus [4] & [5]. Also, some cubic congruence of prime modulus [6].

PROBLEM-STATEMENT

In this paper, the Problem for discussions is:
"To formulate two special classes of standard congruence of prime modulus of higher degree of the types:

$$(1)\ x^{p-3} \equiv a\ (mod\ p),$$
$$(2)\ x^{p-4} \equiv a\ (mod\ p).$$

ANALYSIS & RESULT

Case-I: Consider the congruence $x^{p-3} \equiv a\ (mod\ p)$.

Let $x \equiv u\ (mod\ p)$ be a solution of it. Then, $u^{p-3} \equiv a\ (mod\ p)$ ..... (A)

Also, as u is a residue of p, hence, $(u, p) = 1$ & $(u^2, p) = 1$.

Multiplying (A) by u^2:

$u^2 u^{p-3} \equiv u^2 . a\ (mod\ p)$ *i.e.* $u^{p-1} \equiv au^2\ (mod\ p)$ *i.e.* $1 \equiv au^2\ (mod\ p)$.

Then, $\bar{a} \equiv u^2\ (mod\ p)$, *i.e.* $u^2 \equiv \bar{a}\ (mod\ p)$, *by fermat's Theorem* [2].

Thus, $x \equiv u \pmod p$ is a solution of the quadratic congruence: $x^2 \equiv \bar{a} \pmod p$.

Here $\bar{a}$ is the modular inverse of a *i.e.* $a\bar{a} \equiv 1 \pmod p$.
Such congruence has exactly two solutions, if it is solvable. Solvability test is found in literature in terms of Legendre's symbol [1].

If $\bar{a}$ is a quadratic residue of p, then the congruence is solvable. Thus the solvability condition is: **$\bar{a}$ is a quadratic residue of p.**
Thus, the congruence under consideration is reduced to a standard quadratic congruence of prime modulus. It can be solved easily by author's previous formulation of standard quadratic congruence of prime modulus.

Thus, the congruence $x^{p-3} \equiv a \pmod p$ is solvable if $\bar{a}$ is a quadratic residue of p.
The equivalent quadratic congruence is $x^2 \equiv \bar{a} \pmod p$.

Case-II: Consider the congruence $x^{p-4} \equiv a \pmod p$.
Let $x \equiv u \pmod p$ be a solution of the said congruence. Then, $(u, p) = 1$ & $(u^3, p) = 1$.
Then, $u^{p-4} \equiv a \pmod p$ ……(B)

Multiplying (B) by u^3:
$u^3.u^{p-4} \equiv u^3.a \pmod p$ *i.e.* $u^{p-1} \equiv au^3 \pmod p$ *i.e.* $1 \equiv au^3 \pmod p$,
i.e. $au^3 \equiv 1 \pmod p$ *i.e.* $u^3 \equiv \bar{a} \pmod p$.

Thus, $x \equiv u \pmod p$ is a solution of the cubic congruence: $x^3 \equiv \bar{a} \pmod p$.

This shows that the said congruence can be reduced to a cubic congruence of the type: $x^3 \equiv \bar{a} \pmod p$ ……(C)

Such cubic congruence of prime modulus have two types of solutions. Some has unique Solution if $p \equiv 2 \pmod 3$ and others have exactly three solutions, if $p = 1 \pmod 3$ [6].

Let us consider that $p \equiv 2 \pmod 3$.
Then, $p = 2 + 3k$ *i.e.* $p - 2 = 3k$ *i.e.* $\frac{p-2}{3} = k$.
Let $x \equiv a^{\frac{p-2}{3}} \pmod p$.

Then, from (C):
$x^3 \equiv (a^{\frac{p-2}{3}})^3 \equiv \bar{a} \pmod p$ *i.e.* $a^{p-1} \equiv a\bar{a} \equiv 1 \pmod p$.
It is true by Fermat's theorem.

Hence, $x \equiv a^{\frac{p-2}{3}} \pmod p$ is the unique solution of $x^3 \equiv \bar{a} \pmod p$, if $p \equiv 2 \pmod 3$.
Thus, the congruence is solvable for all values of a. *Let* $p \equiv 1 \pmod 3$. Then the cubic congruence has exactly three solutions .
These three solutions are the members of the residues r of p such that $r^3 \equiv \bar{a} \pmod p$ *where* $\bar{a}$ is modular inverse of a [3].

ILLUSTRATIONS
Consider $x^{10} \equiv 3 \pmod{13}$.

Here, $10 = 13 - 3$ & $a = 3$ *with* $\bar{a} = 9$ *as* $3.9 = 27 \equiv 1 \pmod{13}$.
Then the said congruence can be written as $x^{13-3} \equiv 3 \pmod{13}$.
It is of the type $x^{p-3} \equiv a \pmod p$ *and* hence, it can be reduced to: $x^2 \equiv \bar{a} \equiv 9 \pmod{13}$.
i.e. $x^2 = 3^2 \pmod{13}$, giving solutions: $x = \pm 3 = 3, 13 - 3 = 3, 10 \pmod{13}$.

Therefore, solutions of the given congruence are $x \equiv 3, 10 \pmod{13}$.
Consider $x^{38} \equiv 6 \pmod{41}$.

Here, $38 = 41 - 3$ & $a = 6$, $\bar{a} = 7$ as $6.7 = 42 \equiv 1 \pmod{41}$.

The congruence is of the type: $x^{p-3} \equiv a \pmod{p}$.

So, by author's method, it can be reduced to quadratic congruence: $x^2 \equiv \bar{a} \pmod{p}$.

The reduced congruence is then becomes $x^2 \equiv 7 \pmod{41}$.

It has exactly two solutions, if solvable.

Test of solvability states that the congruence is not solvable as $\left(\frac{7}{41}\right) = -1$.

Thus, the original congruence is not solvable.

Consider $x^{13} \equiv 4 \pmod{17}$.

Here, $p = 17 \equiv 2 \pmod{3}$ and $a = 4$. Also, $13 = 17 - 4$.

Hence, the congruence under consideration can be written as $x^{17-4} \equiv 4 \pmod{17}$.

Therefore, the congruence is of the type $x^{p-4} \equiv a \pmod{p}$ with $p \equiv 2 \pmod{3}$.

By the formulation, it has unique solution and is given by $x \equiv a^{\frac{p-2}{3}} \pmod{p}$

$$i.e.\ x \equiv 4^{\frac{17-2}{3}} \pmod{17}\ i.e.\ x \equiv 4^5 \equiv 1024 \equiv 4 \pmod{17}.$$

Consider the congruence $x^9 \equiv 5 \pmod{13}$.

Here, $p = 13 \equiv 1 \pmod{3}$ and $a = 5$. Also, $9 = 13 - 4$, and $\bar{a} = 8$.

Hence, the congruence under consideration can be written as $x^{13-4} \equiv 5 \pmod{13}$.

Therefore, the congruence is of the type $x^{p-4} \equiv a \pmod{p}$ with $p \equiv 1 \pmod{3}$.

It can be reduced to a standard cubic congruence of prime modulus of the type

$$x^3 \equiv \bar{a} \pmod{p}\ i.e.\ x^3 \equiv 8 \pmod{13}.$$

Now, it can be seen that $2^3 \equiv 8 \pmod{13}$; $5^3 \equiv 8 \pmod{13}$; $6^3 \equiv 8 \pmod{13}$.

Thus, $x \equiv 2, 5, 6 \pmod{13}$ are the three solutions of the congruence.

Consider the congruence $x^{15} \equiv 13 \pmod{19}$.

Here, $p - 19 \equiv 1 \pmod{3}$ and $a - 11$. Also, $15 - 19 - 4$, and $\bar{a} - 7$.

Hence, the congruence under consideration can be written as $x^{19-4} \equiv 11 \pmod{19}$.

Therefore, the congruence is of the type $x^{p-4} \equiv a \pmod{p}$ with $p \equiv 1 \pmod{3}$.

It can be reduced to a standard cubic congruence of prime modulus of the type

$$x^3 \equiv a \pmod{p}\ i.e.\ x^3 \equiv 7 \pmod{19}.$$

Now, it can be seen that $4^3 \equiv 7 \pmod{19}$; $6^3 \equiv 7 \pmod{19}$; $9^3 \equiv 7 \pmod{19}$.

Thus, $x \equiv 4, 6, 9 \pmod{19}$ are the three solutions of the congruence.

CONCLUSION

Thus, it can be concluded that the congruence: $x^{p-3} \equiv a \pmod{p}$ can be reduced to the Equivalent quadratic congruence: $x^2 \equiv \bar{a} \pmod{p}$.

If $\bar{a}$ Is quadratic residue of p, then it can be solved & it has exactly two solutions. It can be solved easily by existing method or Author's method.

Similarly, the congruence: $x^{p-4} \equiv a \pmod{p}$ can be reduced to the equivalent cubic congruence: $x^3 \equiv \bar{a} \pmod{p}$. It has unique solution if $p \equiv 2 \pmod{3}$ and the solution is $x \equiv a^{\frac{p-2}{3}} \pmod{p}$. If $p \equiv 1 \pmod{3}$, then the congruence has exactly three solutions which are members of residue system of p.

MERIT OF THE PAPER

The congruence under consideration are formulated successfully and tested true by solving some suitable examples. Author's formulation made the congruence easily solvable. So, formulation is the merit of the paper

REFERENCE

[1] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to the Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd

[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] Roy B M, Formulation of solutions of two special congruence of prime modulus of higher degree, International Journal of science & Engineering development and Research (IJSDR), ISSN: 2455-2631, vol-3, issue-5, May-18.

[5] Roy B M, Solutions of two special classes of congruence of prime modulus of higher degree, International Journal for Research under literal Access (IJRULA), Vol-01, Issue-04, pages: 105-107.

[6] Roy B M, Solving some special classes of standard cubic congruence of prime modulus, International Journal for Research under literal Access (IJRULA), Vol-02, Issue-02,Feb-19, pages: 85-87.