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-74: Solving Three Special Types 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,
Gogrgaon, Gondia, Maharashtra, India

How to cite this paper: Prof. B M Roy "RP-74: Solving Three Special Types 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.1683-1685, URL: https://www.ijtsrd.com/papers/ijtsrd23488.pdf

IJTSRD23488

ABSTRACT

In this paper, three special classes of congruence of prime modulus of higher degree are considered for formulation and author's efforts established the formulae for solutions. The congruence were not formulated by earlier mathematicians. Due to this formulation, it becomes an easy task to solve the congruence of higher degree of prime modulus reducing the congruence to their equivalent quadratic congruence of prime modulus. Formulations of the congruence is the merit of the paper.

KEYWORDS: *Fermat's little theorem, Modular Inverse, Prime modulus, Quadratic congruence.*

INTRODUCTION

A congruence of the type $x^n \equiv a^n \ (mod\ p)$ is called a standard congruence of higher degree of prime modulus. Here, n is a positive integer and p is a prime positive integer. A very little discussion is found in the literature of mathematics. It is a neglected topic in Number Theory. But it is a very interesting topic of study. Even, no one cared for it.

In this paper, the author wishes to formulate three interesting special classes of standard congruence of prime modulus of higher degree. Such congruence are not considered for formulation by earlier mathematicians. Author's formulation made the congruence easily solvable. It will be seen that the congruence under consideration can be reduced to equivalent standard quadratic congruence of prime modulus. The author already established two new method of solving such quadratic congruence of comparatively large prime modulus.

LITERATURE REVIEW

The standard congruence of prime modulus of higher degree are not discussed in the literature of mathematics. Only standard quadratic congruence are discussed [1].

Author considered some congruence of higher degree of prime modulus for formulation, not formulated earlier and tried to formulate these congruence. The author already formulated some standard congruence of prime modulus of higher degree [4], [5].

PROBLEM-STATEMENT

In this paper, the Problems for discussions are:

"To solve three special classes of standard congruence of prime modulus of higher degree of the types:

$$(1)\ x^{\frac{p+1}{2}} \equiv a\ (mod\ p),$$

$$(2)\ x^{\frac{p+1}{3}} \equiv a\ (mod\ p),$$

$$(3)\ x^{\frac{p+1}{4}} \equiv a\ (mod\ p).$$

ANALYSIS & RESULT

Consider the congruence:

$$x^{\frac{p+1}{2}} \equiv a\ (mod\ p) \ldots \ldots\ldots\ldots\ldots\ldots\ldots\ldots(A)$$

$$p\ being\ an\ odd\ prime\ positive\ integer.$$

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

Then,

$u^{\frac{p+1}{2}} \equiv a\ (mod\ p)\ \ i.e.\ u^{p+1} \equiv a^2 (mod\ p)\ \ i.e.\ u^{p-1}.u^2 \equiv a^2 (mod\ p).$

$$i.e.\ u^2 \equiv a^2\ (mod\ p), \qquad by\ Fermat's\ Little\ Theorem$$

Thus it is seen that $x \equiv u \ (mod\ p)$ is a solution of the quadratic congruence:

$$x^2 \equiv a^2 \ (mod\ p).$$

This means that the solutions of (A) are also the solutions of $x^2 \equiv a^2 \ (mod\ p)$.

So, one has to solve this quadratic congruence and test for (A).

It can also be said that the congruence under consideration can be reduced to an equivalent quadratic congruence of prime modulus of the type: $x^2 \equiv a^2 \ (mod\ p)$. It is always solvable and has exactly two solutions [1], [2].

Now consider the congruence:

$$x^{\frac{p+1}{3}} \equiv a \ (mod\ p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(B)}$$

Let $x \equiv u \ (mod\ p)$ be a solution of the above congruence.

Then,

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

$i.e. \ \ u^2 \equiv a^3 \ (mod\ p) \ by\ Fermat's\ Little\ Theoren$

Thus u satisfies the quadratic congruence

$$x^2 \equiv a^3 \ (mod\ p).$$

This means that the solutions of (B) are also the solutions of $x^2 \equiv a^3 \ (mod\ p)$

So, the congruence under consideration **(B)** can be reduced to a standard quadratic congruence of prime modulus. It has exactly two solutions [1], [2]. So, a^3 must be a quadratic residue of p. Hence it must be the condition of solvability that: $a^3 \equiv b^2 \ (mod\ p)$.

Hence solutions are: $x \equiv \pm b \equiv b, p-b \ (mod\ p)$.

Let us now consider the congruence

$$x^{\frac{p+1}{4}} \equiv a \ (mod\ p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\text{(C)}$$

Let $x \equiv u$ be a solution of the above congruence.

Then, $u^{\frac{p+1}{4}} \equiv a \ (mod\ p)$

$i.e. \ \ u^{p+1} \equiv a^4 \ (mod\ p) \ \ i.e. \ \ u^2 \equiv a^4 \ (mod\ p).$

It is a standard quadratic congruence of prime modulus. Thus the solutions of (C) are also the solutions of

$$x^2 \equiv a^4 \ (mod\ p).$$

Such congruence have exactly two solutions [2]. Testing these solutions for (C), the required solutions can be obtained.

ILLUSTRATION

Consider the congruence $x^6 \equiv 3 \ (mod\ 11)$. It can be written as: $x^{\frac{11+1}{2}} \equiv 3 \ (mod\ 11)$.

Here, $p = 11 \ and\ 6 = \frac{11+1}{2}$.

Therefore, the congruence is of the type:

$$x^{\frac{p+1}{2}} \equiv a \ (mod\ p).$$

It can be reduced to its equivalent quadratic congruence:

$$x^2 = a^2 \ (mod\ 11)$$

$$having\ two\ solutions$$

$$x \equiv \pm a = a, p-a \ (mod\ p).$$

Therefore,

$x^6 \equiv 3 \ (mod\ 11) \ reduces\ to\ x^2 \equiv 3^2 \ (mod\ 11)$

with solutions

$x \equiv 3, 11-3 = 3, 8 \ (mod\ 11).$

It is tested that both the solutions are the solutions of the congruence: $x^6 \equiv 3 \ (mod\ 11)$.

Thus, required solutions are $x \equiv 3, 8 \ (mod\ 11)$.

Consider the congruence $x^8 \equiv 4 \ (mod\ 23)$.

Here, $8 = \frac{23+1}{3}$ and the congruence is of the type: $x^{\frac{23+1}{3}} \equiv 4 \ (mod\ 23)$.

It is of the type $x^{\frac{p+1}{3}} \equiv a \ (mod\ p)$.

Its equivalent quadratic congruence is:

$x^2 \equiv a^3 \ (mod\ p) \ i.e. \ x^2 \equiv 4^3 \equiv 8^2 \ (mod\ 23).$

Its two solutions are

$x \equiv \pm 8 \ (mod\ 23) \ i.e. \ x \equiv 8, 15 \ (mod\ 23).$

It is tested that $x \equiv 8, 15 \ (mod\ 23)$ are the solutions of the congruence.

Now consider the congruence $x^6 \equiv 4 \ (mod\ 23)$.

It can be written as: $x^{\frac{23+1}{4}} \equiv 4 \ (mod\ 23)$.

It is of the type: $x^{\frac{p+1}{4}} \equiv a \ (mod\ p)$.

It equivalent quadratic congruence is:

$x^2 \equiv a^4 \equiv 4^4 \equiv 256 \equiv 16^2 \ (mod\ 23).$

Therefore, the solutions are:

$x \equiv \pm 16 = 16, 23-16 = 16, 7 \ (mod\ 23).$

It is seen that $x \equiv 7 \ (mod\ 23)$ is the only solution of the original congruence.

Consider the congruence

$$x^5 \equiv 2 \ (mod\ 19). \text{ Here, } \frac{19+1}{4} = 5.$$

Then, $x^5 \equiv 2 \ (mod\ 19)$ is of the type $x^{\frac{p+1}{4}} \equiv a \ (mod\ p)$, and hence can be reduced to the quadratic congruence: $x^2 \equiv 2^4 \equiv 16 \equiv 4^2 \ (mod\ 19)$. It has exactly two solutions. Those are

$x \equiv \pm 4 \equiv 4, 19-4 \equiv 4, 15 \pmod{19}$.

But $x \equiv 15 \pmod{19}$ satisfies the congruence $x^5 = 2 \pmod{19}$. Thus, $x \equiv 15 \pmod{19}$ is the only solution of the said congruence of higher degree.

CONCLUSION

The congruence: $x^{\frac{p+1}{2}} \equiv a \pmod p$ can be reduced to the *equivalent quadratic congruence of the type*: $x^2 \equiv a^2 \pmod p$.

The required solutions are also the solutions of it.

The congruence: $x^{\frac{p+1}{3}} \equiv a \pmod p$

can be reduced to the equivalent quadratic congruence of the type:

$$x^2 \equiv a^3 \pmod p.$$

The required solutions are also the solutions of it.

The congruence: $x^{\frac{p-1}{4}} \equiv a \pmod p$ can be reduced to the equivalent quadratic congruence of prime modulus of the type: $x^2 \equiv a^4 \pmod p$ which is always solvable.

Therefore, it can be concluded that all the three said congruence under consideration can be reduced to standard quadratic congruence of prime modulus and can be solved easily.

MERIT OF THE PAPER

The congruence under consideration are formulated successfully and tested true by solving some suitable examples. It makes the finding of solutions simple and easy. 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 Two special classes of standard congruence of prime modulus of higher degree, International Journal of Trend in Scientific Research and development(IJTSRD), Issn:2456-6470, vol-3, Issue-3.

[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-1, Issue-4, 2018, Papes :105-107.