International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 3, May –June 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-92: Solutions of three Special Classes of Congruence of Prime Modulus of Higher Degree

Prof. B. M. Roy
Head, Dept. of Mathematics
Jagat Arts,Commerce & I. H. P. Science College, Goregaon(Gondia),
M. S., India Pin: 441801
(Affiliated to RTM Nagpur University)

Abstract:

In this paper, three formulae are established for solutions of three special classes of congruence of prime modulus ofhigher degree.The formulae are tested true by citing example. The said congruence are possible to solve very easily in the least time. Formulation is the merit of the paper.

No discussion on such standard congruence of higher degree are found in the literature of mathematics. Formulation made the congruence easily solvable.

Key words & phrases: Congruence of higher degree,Fermat's theorem, Inverse-modulo a prime, Prime-modulus.

……

INTRODUCTION

Many more congruence is solved by a number of mathematicians establishing formulae or algorithmic methods. Even then many more congruence is yet remains to formulate. The author has successfully formulated many such congruence. Here, three congruence are considered for formulation. No method or formula is found in the literature of mathematics. Without using any formula, such congruence becomes more complicated to find solutions. In [1], Problem-7, page-115, a problem is found: If $(a,p)=1$, and p is prime such that $p \equiv 2\ (mod\ 3)$, then the congruence $x^3 \equiv a\ (mod\ p)$, has the unique solution $x \equiv a^{\frac{2p-1}{3}}(mod\ p)$. Abruptly, an idea of the three congruence of consideration comes in the author's mind.

Such type of congruence are:

$x^7 \equiv 3(mod\ 11)$; $x^{11} \equiv 11\ (mod\ 17)$; $x^{15} \equiv 7\ (mod\ 23)$; $x^{19} \equiv 2\ (mod\ 29)$;

And $4x^3 \equiv 3\ (mod\ 5), etc.$

These are of the type $x^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$; $ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$ and $x^{p-5} \equiv a\ (mod\ p)$

The author has tried his best to find the formulation of these congruence and his efforts are presented in this paper.

PROBLEM-STATEMENT

CASE-I:

To formulate the congruence: $x^{p-5} \equiv a\ (mod\ p)$, ……(A)

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

CASE-II:

To formulate the congruence: $x^{\frac{2p-1}{3}} \equiv b(modp) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (B)$

$$poddprime.$$

CASE-III:

To formulate the congruence:

$$ax^{\frac{2p-1}{3}} \equiv b(modp) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (C)$$

$$poddprime.$$

ANALYSIS & RESULT:

CASE-I: Consider the congruence $x^{p-5} \equiv a\ (mod\ p)$.

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

Then, $r^{p-5} \equiv a\ (mod\ p)\ \ with\ (r,p) = 1\ \&(r^4,p) = 1.$

Multiplying above equation by r^4:

$$r^4.r^{p-5} \equiv r^4.a\ (mod\ p)\ \ i.e.\ r^{p-1} \equiv a\, r^4 (mod\ p)$$

$$i.e.\ \ 1 \equiv ar^4 (mod\ p)\ , by\ Fermat's\ theorem.$$

$$i.e\ \ r^4 \equiv \bar{a} (mod\ p).$$

Thus r satisfies the bi-quadratic congruence $x^4 \equiv \bar{a} (mod\ p)$.

It is a bi-quadratic congruence of prime modulus. Thus, the congruence under consideration is reduced to a bi-quadratic congruence of prime modulus. It can be easily solved by author's method furnished in a paper [6].

CASE-II:

If $x \equiv r\ (mod\ p)$ is a solution of the congruence (B), then

$$r^{(2p-1)/3} \equiv a(modp) giving r^{2p-1} \equiv a^3 (modp).$$

It can also be written as $r^{p-1}.r^{p-1}.r \equiv a^3 (modp)$ which gives $r \equiv a^3 (modp)$ *by Fermat's Theorem.*

Thus, the congruence has unique solution $x \equiv a^3\ (modp)$.

CASE-III:

Consider the third congruence$ax^{\frac{2p-1}{3}} \equiv b(modp)$.

If $x \equiv r\ (mod\ p)$ is a solution of the congruence (C), then

$$ar^{(2p-1)/3} \equiv b(modp) giving\ a\bar{a}r^{\frac{2p-1}{3}} \equiv \bar{a}b(modp)\ i.e. r^{2p-1} \equiv (\bar{a}b)^3$$

Where $\bar{a}$ is the *inverse modulo prime pi.e.* $\bar{a}a \equiv 1\ (mod\ p)$[2].

It can also be written as $r^{p-1}.r^{p-1}.r \equiv \bar{a}^3 b^3 (modp)$ which gives $r \equiv \bar{a}^3 b^3 (modp)$.

by Fermat's Theorem.

Thus, the congruence has unique solution $x \equiv \bar{a}^3 b^3 \equiv (\bar{a}b)^3 \ (mod p)$.

ILLUSTRATIONS BY EXAMPLES:

Consider the congruence $x^{14} \equiv 9 \ (mod\ 19)$.

Here, $14 = 19 - 5; \ \ a = 9$

It is of the type: $x^{p-5} \equiv a \ (mod\ p)$.

Thus the congruence under consideration can be reduced to a bi-quadratic congruence:

$x^4 \equiv \bar{a} \equiv 17 \ (mod\ p)as\bar{a} = \ a^{19-2} = a^{17} = 9^{17} \equiv 17 \ (mod\ 19)$.

Hence the reduced bi-quadratic congruence is $x^4 \equiv 17 \ (mod\ 19)$.

It is seen that $\left(\frac{17}{19}\right) = 1$ & hence 17 is a quadratic residue of 19.

So, the congruence is solvable and has only two solutions as $19 \equiv 3 \ (mod\ 4)$.

It can be solved by author's method [6].

It can be written as $x^4 \equiv 17 \ (mod\ 19)$

$$\equiv 17 + 19 = 36 = 6^2 (mod\ 19).$$

Then the bi-quadratic congruence is separated quadratic congruence are:

$$x^2 \equiv 6 \ (mod\ 19) \& x^2 \equiv -6 \ (mod\ 19).$$

The congruence $x^2 \equiv 6 \ (mod\ 19) \ \ can\ be\ written\ as\ x^2 \equiv 6 + 19 = 25 = 5^2 (mod\ 19)$

Its two solutions are $x \equiv \pm 5 \ (mod\ 19) \ \ i.e. \ x \equiv 5, 14 \ (mod\ 19)$.

Here the congruence$x^2 \equiv -6 \ (mod\ 19)$ is not solvable.

Thus the required solutions are $x \equiv 5, 14 \ (mod\ 19)$.

Here the congruence$x^2 \equiv -6 \ (mod\ 19)$ is not solvable.

Thus, the required solutions of $x^{14} \equiv 9 \ (mod\ 19)$ are $x \equiv 5, 14 \ (mod\ 19)$.

Verification:

For$x \equiv 5 \ (Mod\ 19)$, it is seen that:$5^{14} = (5^2)^7 = 6^7 = 6.(6^2)^3 = 6.(-2)^3 = 6.(-8) = -48 = -48 + 57 = 9 \ (mod\ 19)$.

Thus $x \equiv 5 \ (mod\ 19)$ satisfies the congruence and hence it is a solutions verified.

Similarly, $x \equiv 14 \ (mod\ 19)$ can be verified as a solutions of the congruence.

Consider $x^7 \equiv 3 \ (mod\ 11) with b = 3, p = 11 \ giving \ 7 = \frac{2.11-1}{3}$.

Therefore, given congruence is of the type $x^{(2p-1)/3} \equiv b (mod p)$.

Its solution is given by $x \equiv b^3 (mod p)$.

Hence the solution of given congruence is $x \equiv 3^3 = 27 \equiv 5\ (mod\ 11)$.

Verification:

Substituting $x \equiv 5$ (mod 11) in the given congruence, we get

$$5^7 = 5^3.5^3.5 = 125.125.5 \equiv 4.4.5 = 80 \equiv 3\ (mod\ 11).$$

Thus $x \equiv 5\ (mod\ 11)$ satisfies the given congruence and so it is the unique solution of the congruence.

Consider the congruence $4x^3 \equiv 3\ (mod\ 5)\ with\ p = 5, b = 3, a = 4$ giving $3 = \frac{2.5-1}{3}$.

So, the congruence is of the type $ax^{\frac{2p-1}{3}} \equiv b(modp)$.

Then its solution is given by $x \equiv \bar{a}^3 b^3 (mod\ p\ )$.

Therefore, for this congruence the solution is $x \equiv \bar{4}^3 3^3 (mod\ p\ )$.

As we know that $4.4 \equiv 1\ (mod\ 5)$, hence$\bar{a} = 4$,

and solution is $x \equiv 4^3 3^3 \equiv 12^3 \equiv 3\ (mod\ 5)$.

Verification:

Substituting $x \equiv 3$ (mod 5) in the above congruence, we get

$$4.3^3 = 4.3.3.3 = 108 \equiv 3\ (mod\ 11).$$

Thus $x \equiv 3\ (mod\ 5)$ satisfies the given congruence and so it is the unique solution of the congruence which is proved as before. Hence the solution is verified true.

CONCLUSION

In this paper, three special types of congruence are formulated and the formulae are tested true by solving suitable examples.

It is found that the congruence $x^{p-5} \equiv a\ (mod\ p)$ can be transformed into a bi-quadratic congruence of prime modulus and can be solved easily by authors proposed method.

It is also found that the congruence $x^{\frac{2p-1}{3}} \equiv b(modp), poddprime,$ has exactly one solution. It is given by$x \equiv b^3(modp)$.

Also, the congruence $ax^{\frac{2p-1}{3}} \equiv b(modp), poddprime,$ has exactly one solution.

It is given by $x \equiv \bar{a}^3 b^3 (modp)$.

MERIT OF THE PAPER

Formulationmakes finding the solutions of a congruence very simple and quick. It gives solutions in less time and sometimes the solutions can be obtained orally. This is the merit of the paper.

REFERENCE

[1] Burton David M, *Elementary Number Theory*, Seventh Indian edition, McGraw Hill(Pvt) Ltd.

[2] Koshy Thomas, *Elementary Number Theory with Applications*, second edition, Indian Print, 2009.

[3] Roy B M , *Discrete Mathematics & Number Theory,* First edition, Das GanuPrakashan, Nagpur (INDIA)

[4] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, 2008.

