International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 4 | May-Jun 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

Rp-91: Solving Some Standard Cubic Congruence of Prime Modulus

Prof B M Roy

Head, Departmant of Mathematics,
Jagat Arts, Commerce & I H P Science College, Goregaon, Maharashtra , India

How to cite this paper: Prof B M Roy "Rp-91: Solving Some Standard Cubic Congruence of Prime Modulus" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-4, June 2019, pp.1485-1488, URL: https://www.ijtsrd.com/papers/ijtsrd25117.pdf

IJTSRD25117

ABSTRACT
In this paper, finding solutions of some classes of standard cubic congruence of prime modulus are considered for study and then formulated. Formulation of the solutions is proved time-saving, simple and quick. It made the finding solutions of cubic congruence of prime modulus easy. Formulation is the merit of the paper. . Here, solvability condition is obtained. This saves time in calculation. This is the merit of the paper.

Keywords: *Cubic Congruence. Fermat's Little Theorem, Prime modulus, Solvability condition*

I. INTRODUCTION

The congruence $x^3 \equiv a \ (mod\ p)$ is called a standard cubic congruence of prime modulus as p is an odd prime positive integer. The author had discussed many standard cubic congruence of composite modulus, successfully [1] [2], [3], [4] .

Here, the author considered the congruence for study is $x^3 \equiv a \ (mod\ p)$, p being a positive odd prime integer.

In books on Number Theory, no discussion is found for the said congruence. Only the standard quadratic congruence are discussed. No formulation/ discussion for standard cubic congruence prime modulus is found except for a short discussion, found in the book of Thomas Koshy [5].

Also, Zuckerman at el, in his book in an exercise, mentioned that if (a, p) = 1, p prime and $p \equiv 2 \ (mod\ 3)$, then the congruence under consideration has a unique solution given by

$x \equiv a^{\frac{2p-1}{3}} \ (mod\ p)$[6].

But nothing is said about the cubic congruence, if $p \equiv 1 \ (mod\ 3)$. Also, in another problem in the same exercise, told the reader to construct an algorithm for computing the solutions of the said congruence [6].

The congruence $x^3 \equiv a \ (mod\ p) with\ p \equiv 1 \ (mod\ 3)$ has exactly three solutions as this p has one-third of its reduced residues as cubic residues. Thus, it can be said that not all congruence of the said type are solvable.

PROBLEM STATEMENT

The problem for discussion is "To find Solvability condition and solutions of some classes of standard cubic congruence of prime modulus of the type:

1. $\boldsymbol{x^3 \equiv a \ (mod\ p) \ with\ p \equiv 1 \ (mod\ 3)}$.
2. $ax^3 \equiv b \ (mod\ p)$, a, b being positive integers, $p\ being\ an\ odd\ prime.$

ANALYSIS & RESULT

Consider the congruence $\boldsymbol{x^3 \equiv a \ (mod\ p) \ with\ p \equiv 1 \ (mod\ 3)}$.

At first solvability condition is to investigate.
Let u be a solution of the congruence $x^3 \equiv a \ (mod\ p)$.

Then, $u^3 \equiv a \ (mod\ p)$ and $k = \frac{p-1}{3}, an\ integer\ as\ p = 3k + 1.$

Therefore, $(u^3)^{\frac{p-1}{3}} \equiv a^{\frac{p-1}{3}} \ (mod\ p) \quad i.e.\ u^{p-1} \equiv a^{\frac{p-1}{3}} \ (mod\ p)$.

By Fermat's Theorem, $\mathbf{1 \equiv a^{\frac{p-1}{3}} \ (mod\ p)}$.

Thus, this can be considered as the condition of solvability for the said congruence.

As $p = 1\ (mod\ 3)$, *the congruence under consideration has exactly three solutions.*

These solutions are the members of the residues of p satisfying the congruence.

As $p = 3k + 1$, one-third of the members in the residue system modulo p are cubic residues.

Thus, the cubic congruence of the type $ax^3 \equiv b\ (mod\ p),\ p \equiv 1\ (mod\ 3)$, must have exactly three solutions.

We have $p - 1 = 3k\ \ i.e.\ \frac{p-1}{3} = k,\ for\ an\ integer\ k$.

If $\boldsymbol{x \equiv u\ (mod\ p)}$ ***be a solution of the congruence:*** $\boldsymbol{ax^3 \equiv b\ (mod\ p)}$, then

$(u, p) = 1\ and\ the\ congruence$ can be written as: $(au^3)^{\frac{p-1}{3}} \equiv b^{\frac{p-1}{3}} \ (mod\ p)$.

Simplifying, one gets: $a^{\frac{p-1}{3}}.u^{p-1} \equiv b^{\frac{p-1}{3}} \ (mod\ p)$.

But using Fermat's Little Theorem, one must get: $\boldsymbol{a^{\frac{p-1}{3}} \equiv b^{\frac{p-1}{3}} \ (mod\ p)}$.

Also then, $\boldsymbol{a^{\frac{p-1}{3}}.b^{\frac{2p-2}{3}} \equiv b^{\frac{p-1}{3}}.b^{\frac{2p-2}{3}} \ (mod\ p)\ \ i.e.\ a^{\frac{p-1}{3}}.b^{\frac{2p-2}{3}} \equiv 1\ (mod\ p)}$.

It is the condition of solvability of the said congruence.

Now consider the congruence $\boldsymbol{ax^3 \equiv b\ (mod\ p)}$ ***with the condition*** $\boldsymbol{p \equiv 2\ (mod\ 3)}$.

As p is of the form $p \equiv 2\ (mod\ 3),\ p = 3k + 2$, then every members in the reduced residue system modulo p are cubic residues. Thus, the cubic congruence of the type $ax^3 \equiv b\ (mod\ p),\ p \equiv 2\ (mod\ 3)$, must have a unique solution.

We have $p - 2 = 3k\ \ i.e.\ \frac{p-2}{3} = k,\ for\ odd\ integer\ k$.

Hence, $ax^3 \equiv b\ (mod\ p)$ can be written as: $(ax^3)^{\frac{p-2}{3}} \equiv b^{\frac{p-2}{3}} \ (mod\ p)$.

Simplifying, one gets: $a^{\frac{p-2}{3}}.x^{p-2} \equiv b^{\frac{p-2}{3}} \ (mod\ p)\ i.e.\ a^{\frac{p-2}{3}}.x^{p-1} \equiv b^{\frac{p-2}{3}} x\ (mod\ p)$.

But using Fermat's Little Theorem, one must get: $\boldsymbol{x \equiv a^{\frac{p-2}{3}}.b^{\frac{2p-1}{3}} (mod\ p)}$.

This is the unique solution of the said congruence and the congruence is solvable.

ILLUSTRATIONS

Consider the congruence $x^3 \equiv 12\ (mod\ 13); 13$ being an odd prime integer.

Here $a = 12,\ p = 13 \equiv 1\ (mod\ 3)$. Then $a^{\frac{p-1}{3}} = 12^4 = (-1)^4 = 1$.

Therefore the congruence is solvable and the congruence has exactly three solutions.

These solutions are the members of the residues of 13 which are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

It can be seen that $4^3 \equiv 10^3 \equiv 12^3 \equiv 12\ (mod\ 13)$.

Thus the required solutions are $x \equiv 4, 10, 12\ (mod\ 13)$.

Consider the congruence: $x^3 \equiv 3\ (mod\ 19)$.

Here, $a = 3,\ p = 19 \equiv 1\ (mod\ 3)$.

Therefore, it is of the type $x^3 \equiv a\ (mod\ p)\ \ with\ p \equiv 1\ (mod\ 3)$.

So, we test for solvability first $i.e.\ \ a^{\frac{p-1}{3}} = 3^{\frac{19-1}{3}} = 3^6 = 7 \neq 1\ (mod\ 19)$.

Therefore, the congruence is not solvable.

Consider the congruence: $5x^3 \equiv 1\ (mod\ 13)$.

Here, $a = 5, p = 13 \equiv 1\ (mod\ 3) and\ so$

$5^{\frac{13-1}{3}} = 5^4 = 25.25 \equiv (-1).(-1) = 1\ (mod\ 13)$.

Therefore the congruence is solvable.
As $5.8 = 40 \equiv 1\ (mod\ 13), hence\ a = 8$.

The reduced congruence is, then, $x^3 \equiv \bar{a}\ \equiv 8 (mod\ 13)$.

Now non-zero residues of 13 are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.

It can be seen that $2^3 \equiv 8,\ \ 5^3 \equiv 8,\ \ 6^3 \equiv 8\ \ (mod\ 13)\ \&\ no$ other possibility found.

Therefore the required solutions are: $x = 2, 5, 6\ (mod\ 13)$.

Let us now consider the congruence $3x^3 \equiv 5\ (mod\ 19)$.

Here, $a = 3, p = 19 \equiv 1\ (mod\ 3)\ \ , a = 3, b = 5$.

Such congruence, if it is solvable, then has exactly three solutions.
The condition of solvability is: $a^{\frac{p-1}{3}}.b^{\frac{2p-1}{3}} \equiv 1\ (mod\ p)$

$i.e.\ \ 3^6.5^{12} \equiv 3^6.5^6.5^6 \equiv 15^6.5^6 \equiv (-4)^6.5^6 \equiv (20)^6 \equiv 1^6 \equiv 1\ (mod\ 19)$.

Thus, it is solvable.
For the congruence $2x^3 \equiv 3\ (mod\ 41)$, $a = 2, b = 3,\ p = 41 \equiv 2\ (mod\ 3)$.

It is solvable and has unique solution given by
$x \equiv a^{\frac{p-2}{3}}.b^{\frac{2p-1}{3}}\ (mod\ p)$
$i.e.\ \ x \equiv 2^{13}.3^{27} \equiv 2^3 2^{10}.(\ 3^4)^6.3^3 \equiv 8.1024.27 \equiv 8.40.27 \equiv 30\ (mod\ 41)$.

Therefore, $x \equiv 30\ (mod\ 41)$ is the required solution.

CONCLUSION

In the conclusion, it can be said that the standard cubic congruence of prime modulus of the type $x^3 \equiv a\ (mod\ p)$, has the **solvability condition:** $\boldsymbol{a^{\frac{p-1}{3}} \equiv 1\ (mod\ p)}$; p being a prime positive integer.

The congruence has exactly three solutions which are members of cubic residues of p.

But if p is very large, then it is difficult to solve.
If $p \equiv 2\ (mod\ 3)$, then the congruence: $ax^3 \equiv b\ (mod\ p)$, has the unique solution given by
$x \equiv \boldsymbol{a^{\frac{p-2}{3}}.b^{\frac{2p-1}{3}} (mod\ p)}$.

But if $\boldsymbol{p \equiv 1\ (mod\ 3), then\ the\ solvavility\ condition\ of}$ **the congruence**
$ax^3 \equiv b\ (mod\ p)$ is given by $\boldsymbol{a^{\frac{p-1}{3}}.b^{\frac{2p-2}{3}} \equiv 1\ (mod\ p)}$.

MERIT OF THE PAPER

It is seen that some cubic congruence have solutions and some have no solutions. So, one should know the condition of solvability. In this paper, the condition is established. Derivation of solvability condition is the merit of the paper. It lessens the labour of the reader. This derivation of the solvability condition makes to find the solutions of the said cubic congruence easy.

REFERENCE

[1] Roy B M, 2019, *Formulation of a class of standard cubic congruence of even composite modulus-a power of an odd positive integer multiple of a power of three*, International Journal of Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-04, issue-03, March-2019.

[2] Roy B M, 2019, *Formulation of a class of solvable standard cubic congruence of even composite modulus*, International Journal of Advanced Research, Ideas & Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-01, Jan-Feb 2019.

[3] Roy B M,2019, *Formulation of Solutions of a Special Standard Cubic Congruence of Composite Modulus--an Integer Multiple of Power of Prime*, International Journal of Advanced Research, Ideas & Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-03, May-Jun-19.

[4] Roy B M, 2019, *Formulation of Solutions of a Special Standard Cubic Congruence of Prime-power Modulus,* International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May-19.

[5] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.

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