International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 3, April 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

# RP-64: A Review of Finding Solutions of Standard Cubic Congruence of Prime Modulus

**Prof B M Roy**

Head, Department of Mathematics, Jagat Arts,
Commerce & I H P Science College, Goregaon, Gondia, Maharashtra, India
(Affiliated to R T M Nagpur University, Nagpur)

**ABSTRACT**

In this paper, the solutions of a standard cubic congruence of prime modulus is discussed. Also, the condition of solvability is established. The literature of mathematics is silent for finding the solutions of such congruence. Even no method to solve such types of congruence is discussed. Here, solvability condition is obtained. The solvability condition makes it easy to find the solutions. It saves the time in calculation. This is the merit of the paper.

***KEYWORDS:*** *Fermat's Little Theorem, Standard Cubic Congruence, Modular Inverse, Solvability condition*

***How to cite this paper:*** Prof B M Roy "RP-64: A Review of Finding Solutions of Standard Cubic Congruence of Prime Modulus" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-3, April 2020, pp.388-390, URL: www.ijtsrd.com/papers/ijtsrd30421.pdf

**IJTSRD30421**



## INTRODUCTION

The congruence $x^3 \equiv a\ (mod\ p)$ is called a **standard cubic congruence** of prime modulus. The values of x that satisfy the congruence are called its solutions. The author already formulated some standard cubic congruence of composite modulus and got published in different international journals [1], [2], ……..[6].

Now the author takes a special type of cubic congruence under consideration for formulation: $x^3 \equiv a\ (mod\ p)$.

## LITERATURE REWIEW

The author has referred many books of Number Theory in which Linear & quadratic congruence are discussed. In this paper, the author wishes to discuss the standard cubic congruence of prime modulus, which is not found in the literature. Thomas Koshy has only defined a standard cubic congruence in a supplementary exercise.

Also, in Zuckerman's book it is found that (in an exercise) if (a, p) = 1, p prime and

$p \equiv 2\ (mod\ 3)$, then the congruence $x^3 \equiv a\ (modp)$ has unique solution:

$x \equiv a^{\frac{2p-1}{3}}\ (mod\ p)\ [page - 115]$. But nothing is said about the cubic congruence,

if $p \equiv 1\ (mod\ 3)$ [8]. The author wishes to find the **condition of solvability** of the said congruence and also wish to formulate a cubic congruence of special type: $x^3 \equiv a\ (modp)$ under the cases: $p \equiv 1\ (mod\ 3)$.

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[9]. Thus, it can be said that not all congruence of the said type are solvable.

## NEED OF RESEARCH

Nothing is said for the solutions of the above said cubic congruence and hence there is the possibility of research for the solutions. Here is the need of the research. Finding no satisfactory discussion on standard cubic congruence, the author tried his best to find solutions of the said congruence when $p \equiv 1\ (mod\ 3)$ and presented his efforts in this paper.

## PROBLEM STATEMENT

The problem for discussion is "To find Solvability condition and solutions of a class of standard cubic congruence of prime modulus of the type: $x^3 \equiv a\ (mod\ p), p\ being\ an\ odd\ prime$, in two cases:
Case-I: $p \equiv 2\ (mod\ 3)$;
Case-II: $p \equiv 1\ (mod\ 3)$.

**ANALYSIS & RESULT**

**Case-I:** Let us consider the congruence: $x^3 \equiv a\ (mod\ p)$ with the condition:
$p \equiv 2\ (mod\ 3)$. As per Zukerman, such types of cubic congruence is always solvable and it has a unique solution given by $x \equiv a^{\frac{2p-1}{3}}\ (mod\ p)$.

Even some difficulties arises in finding the solutions. The difficulties must be removed. It can be done in three subcases:
Subcase-I: when $a = r^3$. Then the congruence can be written as: $x^3 \equiv r^3\ (mod\ p)$. As it has a unique solution, it must be $x \equiv r\ (mod\ p)$.

Subcase-II: when $a \neq r^3$ but can be easily obtained as: $a + k.p = r^3$ for some fixed small value of k [7], then the solution is also $x \equiv r\ (mod\ p)$.

Subcase-III: When subcases I & II fails, then one has to use the formula for solution:
$x \equiv a^{\frac{2p-1}{3}}\ (mod\ p)$.

**Case-II**: Let us consider the case: $p \equiv 1\ (mod\ 3)$.
Let us first find the solvability condition of the congruence.

**SOLVABILITY CONDITION**

As p is of the form $p \equiv 1\ (mod\ 3)$, it is of the type $3k + 1\ i.e. p = 3k + 1$, then the only one-third of the members in the reduced residue system modulo p are cubic residues [4]. Thus, the every such cubic congruence of the type $x^3 \equiv a\ (mod\ p), p \equiv 1\ (mod\ 3)$, must have exactly three solutions.

From above, we have $p - 1 = 3k\ i.e. \frac{p-1}{3} = k, for\ even\ integer\ k.$

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

Hence, $r^3 \equiv a\ (mod\ p)$
*It* can be written as: $(r^3)^{\frac{p-1}{3}} \equiv a^{\frac{p-1}{3}}\ (mod\ p)$.

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

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

**It is the condition of solvability of the said congruence.**

**SOLUTIONS OF THE CONGRUENCE**

Consider the said congruence $x^3 \equiv a\ (mod\ p)$ with the condition $p \equiv 1\ (mod\ 3)$.

If $a^{\frac{p-1}{3}} \equiv 1\ (mod\ p)$, then it is solvable as seen above and always has three solutions.

The congruence can also be written as: $x^3 \equiv a\ (mod\ p)$.
To solve the said congruence, one has to write the non-zero residues of p such as:
1, 2, 3, ....., p-2, p-1. Then obtain their cubic residues and select the three which are congruent to $a$ modulo p.

Now consider the congruence $ax^3 \equiv 1\ (mod\ p)$ with the condition $p \equiv 2\ (mod\ 3)$.

As p is of the form $p \equiv 2\ (mod\ 3)$, it is of the type $3k + 2\ i.e. p = 3k + 2$, then every members in the reduced residue system modulo p is cubic residue [1]. Thus, the cubic congruence of the type $ax^3 \equiv 1\ (mod\ p), p \equiv 2\ (mod\ 3)$, must have a unique solution.

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

If $x \equiv u\ (mod\ p)$ is a solution, then one have $au^3 \equiv 1\ (mod\ p)$ And $(au^3)^{\frac{p-2}{3}} \equiv 1\ (mod\ p)$.

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

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

**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 $a^{\frac{p-1}{3}} = 12^4 \equiv (-1)^4 (mod\ p) \equiv 1 (mod\ p)$.

Therefore the congruence is solvable. It has three incongruent solutions.

The reduced residue system of 13 $= \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

It is also seen that $4^3 \equiv 12\ (mod\ 13); 10^3 \equiv 12\ (mod\ 13);\ 12^3 \equiv 12\ (mod\ 13)$.

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

Consider the standard cubic congruence $x^3 \equiv 5\ (mod\ 7)$.

Here, $a = 5, p = 7 \equiv 1\ (mod\ 3)\ and\ so\ 5^{\frac{7-1}{3}} = 5^2 = 25 \equiv 4\ (mod\ 7)$.

Therefore, the congruence is not solvable.
Let us consider the congruence as per requirement: $x^3 \equiv 6\ (mod\ 13)$.

Here, $a = 6, p = 13 \equiv 1\ (mod\ 3) and\ so$
$6^{\frac{13-1}{3}} = 6^4 = 36.36 \equiv (10).(10) = 100 \equiv 9\ (mod\ 13)$.

Therefore the congruence is not solvable.

Let us consider the congruence: $5x^3 \equiv 1\ (mod\ 13)$.
Here, $a = 5, p = 13 \equiv 1\ (mod\ 3) and\ so$
$5^{\frac{13-1}{3}} = 5^4 = 25.25 \equiv (-1).(-1) \equiv 1\ (mod\ 13)$. Hence it is solvable and has exactly three incongruent solutions.
As $5.8 = 40 \equiv 1\ (mod\ 13), hence\ \bar{a} = 8$.

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: $x \equiv 2, 5, 6\ (mod\ 13)$.

Let us now consider the congruence $3x^3 \equiv 1\ (mod\ 17)$.

Here, $a = 3, p = 17 \equiv 2\ (mod\ 3)$.

Such congruence is solvable and always has unique solution.

The solution is given by $x \equiv a^{\frac{p-2}{3}} \equiv 3^5 \equiv 5\ (mod\ 17)$.

For the congruence $2x^3 \equiv 1\ (mod\ 41)$.

Here, $a = 2, p = 41 \equiv 2\ (mod\ 3)$.

It is solvable and has unique solution given by
$x \equiv a^{\frac{p-2}{3}} \equiv 2^{13} \equiv 2^3 2^{10} \equiv 8.1024 \equiv 8.40 \equiv 33\ (mod\ 41)$.

Therefore, $x \equiv 33\ (mod\ 41)$ is the required solution.

**CONCLUSION**

Therefore, it is concluded that the congruence $x^3 \equiv a\ (mod\ p)$ has three solutions with the solvability condition: $a^{\frac{p-1}{3}} \equiv 1\ (mod\ p)$ when $p \equiv 1\ (mod\ 3)$.

Also, it is concluded that the congruence $ax^3 \equiv 1\ (mod\ p)$ has three solutions with the solvability condition: $a^{\frac{p-1}{3}} \equiv 1\ (mod\ p)$ when $p \equiv 1\ (mod\ 3)$.

It is also found that the congruence $ax^3 \equiv 1\ (mod\ p)$ has a unique solution given by
$x \equiv a^{\frac{p-2}{3}}\ (mod\ p)$*and all such congruence are solvable* if $p \equiv 2\ (mod\ 3)$.

**MERIT OF THE PAPER**

A special type of cubic congruence is formulated. A very simple method is discussed for finding solutions of the said congruence. Formulation is the merit of the paper.

**REFERENCE**


[1] Roy, B M, *Formulation of Two Special Classes of Standard Cubic Congruence of Composite Modulus- a Power of Three*, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-03, May-June 2019, Page-288-291.

[2] Roy, B M, *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, *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.

[4] Roy, B M, *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-2019.

[5] Roy, B M, *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-2019 .

[6] Roy, B M, *Formulation of Solutions of a Special Standard Cubic Congruence of Composite Modulus,* International Journal of Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-04, Issue-06, Jun-2019.

[7] Roy B M, "*Discrete Mathematics & Number Theory*", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.

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

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