ISSN: 2455-2631 © December 2020 IJSDR | Volume 5 Issue 12

RP-152: A review and reformulation of solutions of standard cubic congruence of composite modulus modulo an odd prime power integer

Prof. B M Roy

Head, Department of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon
Dist-Gondia, M. S., India.

***Abstract*: In this paper, a very special standard cubic congruence of composite prime power modulus is studied and after a rigorous study, the author has formulated the solutions of the congruence successfully and the consequence is presented in this paper. It is found that this special cubic congruence has exactly p^2 incongruent solutions, where p is an odd prime positive integer. Due to this formulation of the solutions, it is now possible to find such a large numbers of solutions of a cubic congruence. So, it can be said that formulation is the merit of the paper.**

***Keywords*: Cubic Congruence, Composite Modulus, Cubic Residue, Formulation, Incongruent solutions.**

INTRODUCTION

If p is an odd positive prime integer, then the congruence $x^3 \equiv a(mod\ p)$ is called a standard cubic congruence of prime modulus. If m is a composite positive integer, then $x^3 \equiv a(mod\ m)$ is called a standard cubic congruence of composite modulus. Also, if a is **cubic residue** of the modulus, then the congruence is solvable. If the congruence is solvable. Then a can be written as $r^3 \equiv a\ (mod\ p), r\ being\ a\ residue\ of\ p.$

$In\ this\ case\ the\ solvable$ Congruence can be written as: $x^3 \equiv r^3\ (mod\ p)$.

In this paper the author considered the congruence: $x^3 \equiv p^3\ (mod\ p^n)$ for formulation of its solutions. It was already published in IJSDR-May-19.

PROBLEM-STATEMENT

Here the problem is-"To formulate the special standard cubic congruence of the type:

$$x^3 \equiv p^3 (mod\ p^n), p\ being\ an\ odd\ prime, n\ \ positive\ integer".$$

LITERATURE REVIEW

In the literature of mathematics, nothing is found about the solving standard cubic congruence of prime and composite modulus. Only a definition is seen in the book of Zuckerman, page-no. 136, problem no. 18 [1] and Thomas Koshy had defined only a cubic residue, page-548 [2]. David M Burton [3] in his book: "Elementary Number Theory", in the page no. 166, used the Theory of Indices to solve standard cubic congruence of prime modulus but established no formula for solutions. No pre-formulation is found for the congruence considered here. Only the author's formulations on standard cubic congruence of composite modulus are found in the literature of mathematics [4], [5], [6], [7]. Here is one more standard cubic congruence of composite modulus the author considered for formulation of its solutions.

ANALYSIS & RESULT

Consider the congruence under consideration: $x^3 \equiv p^3 (mod\ p^n), p\ being\ an\ odd\ prime.$

Let us consider that $1 \le n \le 2$.

Then for $n = 1$, the said congruence reduces to: $x^3 \equiv p^3\ (mod\ p)\ which\ is\ equivalent\ to$:

$x^3 \equiv 0\ (mod\ p)$. It is found that the congruence has a single solution $x \equiv p\ (mod\ p)$

$i.e.\ equivalently,\ x \equiv 0\ (mod\ p)$.

Then for $n = 2$, the said congruence reduces to: $x^3 \equiv p^3\ (mod\ p^2)\ which\ is\ equivalent\ to$:

$x^3 \equiv 0\ (mod\ p^2)$.

It is also found after a rigorous study that $x \equiv pk + p, k = 0, 1, 2, \ldots\ldots (p - 1)$, gives the p-solutions of the congruence. The truth of the formula is verified by illustrations.

Consider now that $n \ge 3$.

For solutions, consider $x \equiv p^{n-2}k + p\ (mod\ p^n)$.

Then, $x^3 \equiv (p^{n-2}k + p\ )^3\ (mod\ p^n)$

$$\equiv (\ p^{n-2}k\ )^3 + 3.(p^{n-2}k\ \ )^2.p + 3.p^{n-2}k.p^2 + p^3\ (mod\ p^n)$$
$$\equiv p^{3n-6}k^3 + 3p^{2n-3}k^2 + 3p^n k + p^3 (mod\ p^n)$$
$$\equiv p^n k(p^{2n-6}k^2 + 3p^{n-3}k + 3) + p^3 (mod\ p^n); n \ge 3.$$
$$\equiv p^3\ (mod\ p^n)$$

Thus it is seen that $x \equiv p^{n-2}k + p\ (mod\ p^n)$ satisfies the cubic congruence and hence must give all the solutions.

But it is seen that for $k = p^2$, the solution formula reduces to:

$$x \equiv p^{n-2}.\,p^2 + p \ (mod\ p^n)$$
$$\equiv p^n + p \ (mod\ p^n)$$
$$\equiv p \ (mod\ p^n)$$

This is the same solution as for $k = 0$.
Also if $k = p^2 + 1$, then the solution formula reduces to:

$$x \equiv p^{n-2}.\,(p^2 + 1) + p \ (mod\ p^n)$$
$$\equiv p^n + p^{n-2} + p \ (mod\ p^n)$$
$$\equiv p^{n-2} + p \ (mod\ p^n)$$

This is the same solution as for $k = 1$.
Therefore, all the solutions are given by:
$x \equiv p^{n-2}k + p \ (mod\ p^n); k = 0, 1, 2, \dots \dots, (p^2 - 1)$.
This gives p^2 $incongruent\ solutions\ of\ the\ congruence$.
Therefore, the result of this discussion is that the standard cubic congruence of composite modulus: $x^3 \equiv p^3\ (mod\ p^n)$ has p^2 incongruent solutions given by:
$x \equiv p^{n-2}k + p \ (mod\ p^n); k = 0, 1, 2, \dots \dots, (p^2 - 1)$.

ILLUSTRATIONS

Example-1: Consider the congruence $x^3 \equiv 0\ (mod\ 5)$.
It is of the type: $x^3 \equiv 0\ (mod\ p^n), with\ n = 1$.
It has a unique solution given by $x \equiv p\ (mod\ p^n)$
$\equiv 5\ (mod\ 5^1)$
$\equiv 5\ (mod\ 5)$.
Example-2: Consider the congruence $x^3 \equiv 0\ (mod\ 25)$.
It can be written as: $x^3 \equiv 0\ (mod\ 5^2)$.
It is of the type: $x^3 \equiv 0\ (mod\ p^n), n = 2$.
It has $p = 5$ incongruent solutions given by $x \equiv pk + p\ (mod\ p^n)$; k=0, 1, 2, 3, 4.
$\equiv 5k + 5\ (mod\ 5^2)$
$\equiv 5, 10, 15, 20, 25\ (mod\ 25)$.
These are the $p = 5$ solutions of the congruence.
Example-3: Consider the congruence $x^3 \equiv 0\ (mod\ 125)$.
It can be written as: $x^3 \equiv 0\ (mod\ 5^3)\ with\ n = 3$.
It is of the type: $x^3 \equiv 0\ (mod\ p^n), n = 3$.
It has $p^2 = 5^2 = 25$ solutions given by:
$x \equiv p^{n-2}k + p\ (mod\ p^n); k = 0, 1, 2, 3, \dots \dots \dots, (p^2 - 1)$.
$\equiv 5k + 5\ (mod\ 5^3); k =, 1, 2, 3, \dots \dots \dots, 24$.
$\equiv 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75, 80, 85, 90, 90,$
$100, 105, 110, 115, 120, 125\ (mod\ 125)$.
These are the 25 solutions of the congruence.
Example-4: Consider the Consider the congruence $x^3 \equiv 125\ (mod\ 625)$.
It can be written as: $x^3 \equiv 5^3\ (mod\ 5^4)\ withp = 5,\ n = 4$.
It is of the type: $x^3 \equiv p^3\ (mod\ p^n), p \geq 3$.
The solutions are given by
$x \equiv p^{n-2}k + p\ (mod\ p^n); k = 0, 1, 2, \dots \dots \dots, (p^2 - 1)$.
$\equiv 5^{4-2}k + 5\ (mod\ 5^4); k = 0, 1, 2, \dots \dots \dots, (5^2 - 1)$
$\equiv 5^2k + 5\ (mod\ 5^4); k = 0, 1, 2, \dots \dots \dots \dots \dots, (25 - 1)$
$\equiv 25k + 5\ (mod\ 625); k = 0, 1, 2, \dots \dots \dots, 24$.
$\equiv 5, 30, 55, 80, 105, 130, 155, 180, 205, 230, 255, 280, 305, 330, 355, 380,$
$405, 430, 455, 480, 505, 530, 555, 580, 605\ (mod\ 625)$.
These are the $p = 25$ solutions of the congruence.
Consider the Consider the congruence $x^3 \equiv 343\ (mod\ 2401)$.
It can be written as: $x^3 \equiv 7^3\ (mod\ 7^4)\ with\ p = 7,\ n = 4$.
It is of the type: $x^3 \equiv p^3\ (mod\ p^n), p \geq 3$.
The solutions are given by
$x \equiv p^{n-2}k + p\ (mod\ p^n); k = 0, 1, 2, \dots \dots \dots, (p^2 - 1)$.
$\equiv 7^{4-2}k + 7\ (mod\ 7^4); k = 0, 1, 2, \dots \dots \dots, (7^2 - 1)$
$\equiv 7^2k + 7\ (mod\ 7^4); k = 0, 1, 2, \dots \dots \dots \dots \dots, (49 - 1)$
$\equiv 49k + 7\ (mod\ 2401); k = 0, 1, 2, \dots \dots \dots, 48$.
≡7, 56, 105, 154, 203,252, ………………………, 2359 (mod 2401).
These are the $p = 49$ solutions of the congruence.

CONCLUSION

Therefore, it is concluded that the standard cubic congruence of composite modulus:
$x^3 \equiv p^3 \ (mod\ p^n), p \geq 3$, has exactly $p^2 -$ incongruent solutions, given by
$x \equiv p^{n-2}k + p \ (mod\ p^n); k = 0, 1, 2, \dots \dots \dots, (p^2 - 1), p$ being an odd prime positive integer.
But for $n = 1, the\ congruence\ has\ a\ unique$ solution $x \equiv p \ (mod\ p)$; also for n=2, the congruence has exactly p incongruent solutions $x \equiv pk + p; k = 0, 1, 2, \dots \dots, (p - 1)$.

MERIT OF THE PAPER

The author's formulation of solutions of the cubic congruence under consideration made the finding of solutions easy and time-saving. A large number of solutions can be obtained in a short time with an easy efforts. Thus formulation of solutions is the merit of the paper.

REFERENCES

[1]I. Niven, H. S. Zuckerman, 2008, An Introduction to the Theory of Numbers, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.

[2]Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press, Second Edition, Indian print, New Delhi, India, ISBN:978-81-312-1859-4.

[3]David M Burton, 2012, Elementary Number Theory, Mc Graw Hill education (Higher Education), Seventh Indian Edition, New Delhi, India, ISBN: 978-1-25-902576-1.

[4] Roy B M, Formulation of solutions of a special standard cubic congruence of prime-power modulus, International Journal of science and engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May-19.

[5]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-19.

[6]Roy B M, A Review and reformulation of the formulation of a standard cubic congruence of even composite modulus, International Journal of Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-04, Issue-11, Nov-19.

[7]Roy B M, Formulation of a class of standard cubic congruence of composite modulus-a product of power of three and power of an odd prime, International Journal of science and engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-02, Feb-20.