Vol.9.Issue.3.2021 (July-Sept)
©KY PUBLICATIONS

http://www.bomsr.com
Email:editorbomsr@gmail.com

RESEARCH ARTICLE

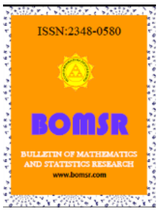
BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH

A Peer Reviewed International Research Journal

ISSN INTERNATIONAL STANDARD SERIAL NUMBER 2348-0580

SOLVING A SPECIAL STANDARD CUBIC CONGRUENCE OF COMPOSITE MODULUS MODULO A SPECIAL COMPOSITE INTEGER

B M ROY[1], A A QURESHI[2]
[1]Department of Mathematics, Jagat Arts, Commerce & I H P ScienceCollege, Dist-Gondia
[2]Department of Mathematics DRB Sindhu Mahavidyalaya, Nagpur
Corresponding author: A.A. Qureshi, aaq_maths@yahoo.com; mathspdft@gmail.com
DOI:10.33329/bomsr.9.3.24


ISSN:2348-0580
BOMSR
BULLETIN OF MATHEMATICS AND STATISTICS RESEARCH
www.bomsr.com

ABSTRACT

Here, the authors have studied and formulated the solutions of a special standard cubic congruence of composite modulus modulo a special composite integer in different cases. It is found that the said congruence has three types of solutions as per the case. It has exactly $3p^2$ incongruent solutions in the first case, only 3 incongruent solutions in the second case and has exactly $3p$ incongruent solutionsin the third case, p being an odd prime integer. Formulation of solutions has provided a simple procedure of finding the required solutions easily. This is the merit of the paper.

Keywords: Cubic Congruence, Composite Modulus, Chinese Remainder Theorem.

INTRODUCTION

The congruence is part of Number Theory which is a branch of pure mathematics. The general and the standard quadratic congruence of prime modulus were studied in the college syllabus in mathematics. The standard cubic and standard bi-quadratic congruence suffer a negligence; nowhere is found any discussion of it.

Here in this paper, the authors considered a standard cubic congruence of composite modulus of very special type. It is of the type:

$x^3 \equiv a \ (mod\ p^m.3^n)$, p being an odd prime.

PROBLEM-STATEMENT

"To formulate the solutions of $x^3 \equiv p^3 (mod\, p^m.3^n) in\ three\ cases$

$$as\ for\ \ m \geq 3; m = 1, m = 2".$$

LITERATURE REVIEW

The authors have gone through many Books of Number Theory [1], [2], [3] and found nothing about the said cubic congruence. Only a definition of standard cubic congruence in [1]; also a definition of cubic residues in [2]. But it is the author's opinion that the readers can use Chinese Remainder Theorem to find all the solutions of the said congruence by splitting the original congruence into individual congruence and solving separately.

But the procedure has its own demerits. Due to the demerits of CRT, the readers feel a need of formulation of solutions. Therefore, the author wants formulating the solutions of the said congruence. The first author already has formulated some standard cubic congruence of composite and prime modulus [4], [5], [6], [7], [8], [9].

ANALYSIS & RESULTS

Consider the congruence under consideration: $x^3 \equiv p^3 (mod\, p^m.3^n)$.

Case-I: Let $m \geq 3$.

Then the congruence reduces to the form: $x^3 \equiv p^3 (mod\, p^m.3^n)$.

For the solutions, let $x \equiv p^{m-2}.3^{n-1}k + p\ (mod\, p^m.3^n)$.

Then, $x^3 \equiv (p^{m-2}.3^{n-1}k + p\,)^3\ (mod\, p^m.3^n)$

$$\equiv (p^{m-2}.3^{n-1}k)^3 + 3.(p^{m-2}.3^{n-1}k)^2.p + 3.p^{m-2}.3^{n-1}k.p^2 + \ p^3\ (mod\, p^m.3^n)$$

$$\equiv p^m.3^n k\{3^{2n-6}k^2 + p^{m-4}3^{n-1}k + 1\} + p^3\ (mod\, p^m.3^n)$$

$\equiv p^3 (mod\, p^m.3^n)$.

So, $x \equiv p^{m-2}.3^{n-1}k + p\ (mod\, p^m.3^n)$ satisfies the congruence and hence is a solution. But for $k = 3p^2$, one has

$$x \equiv p^{m-2}.3^{n-1}.3p^2 + p\ (mod\, p^m.3^n).$$

$$\equiv p^m.3^n + p\ (mod\, p^m.3^n)$$

$\equiv 0 + p\ (mod\, p^m.3^n)$. This is the same solution as for $k = 0$.

Also, for $k = 3p^2 + 1$, it is seen that

$$x \equiv p^m.3^n + p^{m-2}.3^{n-1} + p\ (mod\, p^m.3^n).$$

$\equiv p^{m-2}.3^{n-1} + p\ (mod\, p^m.3^n)$. This is the same solution as for $k = 1$.

Therefore, it is seen that the solution- formula gives exactly $3p$ incongruent solutions of the congruence. So, all the solutions are given by

$$x \equiv p^{m-2}.3^{n-1}k + p\ (mod\, p^m.3^n); k = 0, 1, 2, \dots\dots\dots\dots\dots, (3p^2 - 1).$$

Case-II: Let $m = 1$.

Then the congruence reduces to the form: $x^3 \equiv p^3 (mod\, p.3^n)$.

For the solutions, let us consider that $x \equiv p.3^{n-1}k + p\ (mod\ p.3^n)$.

Then, $x^3 \equiv (p.3^{n-1}k + p\ )^3\ (mod\ p.3^n)$

$$\equiv (\ p.3^{n-1}k)^3 + 3.(\ p.3^{n-1}k)^2.p + 3.p.3^{n-1}k.p^2 + p^3\ (mod\ p.3^n)$$

$$\equiv p^3.3^n k\{3^{2n-3}k^2 + 3^{n-1}k + 1\} + p^3\ (mod\ p.3^n)$$

$\equiv p^3 (mod\ p.3^n)$.

So, $x \equiv p.3^{n-1}k + p\ (mod\ p.3^n)$ satisfies the congruence and hence is a solution. But for $k = 3$, the solutions formula reduces to:

$$x \equiv p.3^{n-1}.3 + p\ (mod\ p.3^n).$$

$$\equiv p.3^n + p\ (mod\ p.3^n)$$

$\equiv 0 + p\ (mod\ p.3^n)$. This is the same solution as for $k = 0$.

Also, for $k = 4 = 3 + 1$, it is seen that

$$x \equiv p.3^n + p.3^{n-1} + p\ (mod\ p.3^n).$$

$\equiv p.3^{n-1} + p\ (mod\ p.3^n)$. This is the same solution as for $k = 1$.

Therefore, it is seen that the solution- formula gives exactly three incongruent solutions of the congruence. So, all the solutions are given by

$$x \equiv p.3^{n-1}k + p\ (mod\ p.3^n); k = 0, 1, 2.$$

Case-II: Let $m = 2$.

Then the congruence reduces to the form: $x^3 \equiv p^3 (mod\ p^2.3^n)$.

For the solutions, let $x \equiv p^{2-1}.3^{n-1}k + p\ (mod\ p^2.3^n)$

$\equiv p.3^{n-1}k + p\ (mod\ p^2.3^n)$.

Then, $x^3 \equiv (p.3^{n-1}k + p\ )^3\ (mod\ p^2.3^n)$

$$\equiv (\ p.3^{n-1}k)^3 + 3.(\ p.3^{n-1}k)^2.p + 3.p.3^{n-1}k.p^2 + p^3\ (mod\ p^2.3^n)$$

$$\equiv p^3.3^n k\{3^{2n-3}k^2 + 3^{n-1}k + 1\} + p^3\ (mod\ p^2.3^n)$$

$\equiv p^3\ (mod\ p^2.3^n)$.

So, $x \equiv p.3^{n-1}k + p\ (mod\ p^2.3^n)$ satisfies the congruence and hence is a solution. But for $k = 3p$, the solutions formula reduces to:

$$x \equiv p.3^{n-1}.3p + p\ (mod\ p^2.3^n).$$

$$\equiv p^2.3^n + p\ (mod\ p^2.3^n)$$

$\equiv 0 + p\ (mod\ p^2.3^n)$. This is the same solution as for $k = 0$.

Also, for $k = 3p + 1$, it is seen that

$$x \equiv p^2.3^n + p.3^{n-1} + p\ (mod\ p^2.3^n).$$

$\equiv p.3^{n-1} + p\ (mod\ p^2.3^n)$. This is the same solution as for $k = 1$.

Therefore, it is seen that the solution- formula gives exactly $3p$ incongruent solutions of the congruence. So, all the solutions are given by

$$x \equiv p.3^{n-1}k + p\ (mod\ p^2.3^n); k = 0, 1, 2, \dots \dots \dots \dots \dots, (3p - 1).$$

ILLUSTRATIONS

Example-1: Consider the congruence: $x^3 \equiv 125\ (mod\ 405)$.

It can be written as: $x^3 \equiv 5^3 (mod\ 3^4.5)$.

It is of the type: $x^3 \equiv p^3 (mod\ 3^n.p)$ with $p = 5, n = 4, m = 1$.

It has exactly 3 incongruent solutions given by

$$x \equiv 3^{n-1}.p\ k + p\ (mod\ 3^n.p); k = 0, 1, 2.$$

$$\equiv 3^3.5k + 5\ (mod\ 3^2.5^2); k = 0, 1, 2.$$

$$\equiv 135k + 5\ (mod\ 405)$$

$$\equiv 5, 140, 275\ (mod\ 405).$$

Example-2: Consider the congruence: $x^3 \equiv 125\ (mod\ 225)$.

It can be written as: $x^3 \equiv 5^3 (mod\ 3^2.5^2)$.

It is of the type: $x^3 \equiv p^3 (mod\ 3^n.p^m)$ with $p = 5, n = 2, m = 2$.

It has $3p$ incongruent solutions given by

$$x \equiv 3^{n-1}.p^{m-1}k + p\ (mod\ 3^n.p^m); k = 0, 1, 2, \dots \dots \dots ., (3p - 1).$$

$$\equiv 3.5k + 5\ (mod\ 3^2.5^2); k = 0, 1, 2, \dots \dots \dots .14.$$

$$\equiv 15k + 5\ (mod\ 225)$$

$$\equiv 5, 20, 35, 50, 65, 80, 95, 110, 125, 140, 155,170, 185, 200, 215\ (mod\ 225).$$

Example-3: Consider the congruence: $x^3 \equiv 125\ (mod\ 1125)$.

It can be written as: $x^3 \equiv 5^3 (mod\ 3^2.5^3)$.

It is of the type: $x^3 \equiv p^3 (mod\ 3^n.p^m)$ with $p = 5, n = 2, m = 3$.

It has $3p^2$ incongruent solutions given by

$$x \equiv 3^{2-1}.5^{m-2}k + p\ (mod\ 3^n.p^m); k = 0, 1, 2, \dots \dots \dots ., (3p^2 - 1).$$

$$\equiv 3.5k + 5\ (mod\ 3^2.5^3); k = 0, 1, 2, 3,4,5,6, \dots \dots \dots .74.$$

$$\equiv 15k + 5\ (mod\ 1125)$$

$$\equiv 5, 20, 35, 50, 65, 80, 95, \dots \dots \dots \dots \dots \dots .., 1115\ (mod\ 1125).$$

Example-4: Consider the congruence: $x^3 \equiv 125\ (mod\ 16875)$.

It can be written as: $x^3 \equiv 5^3 (mod\ 3^3.5^4)$.

It is of the type: $x^3 \equiv p^3 (mod\ 3^n.p^m)$ with $p = 5, n = 3, m = 4$.

It has $3p^2 = 3.25 = 75$ incongruent solutions given by

$$x \equiv 3^{n-1}.p^{m-2}k + p\ (mod\ 3^n.p^m); k = 0, 1, 2, \dots \dots \dots ., (3p^2 - 1).$$

$$\equiv 3^2.5^2k + 5\ (mod\ 3^3.5^4); k = 0, 1, 2, \dots \dots \dots .74.$$

$$\equiv 225k + 5\ (mod\ 16875)$$

$$\equiv 5, 230, 455, \dots\dots\dots\dots\dots\dots., 16655 \ (mod\ 16875).$$

CONCLUSIONS

Therefore it is concluded that the standard cubic congruence: $x^3 \equiv p^3 (mod\ p^m. 3^n)$, $m \geq 3$, p an odd prime has exactly $3p^2 -$ incongruent solutions given by

$$x \equiv 3^{n-1}. p^{m-2}k + p\ (mod\ p^2. 3^n); k = 0, 1, 2, 3, \dots\dots\dots, (3p^2 - 1).$$

Also, the standard cubic congruence: $x^3 \equiv p^3 (mod\ p. 3^n), m = 1$, p an odd prime has exactly $3 -$ incongruent solutions given by

$$x \equiv 3^{n-1}. pk + p\ (mod\ p. 3^n); k = 0, 1, 2.$$

Also, the standard cubic congruence:$x^3 \equiv p^3 (mod\ p^m. 3^n), m = 2,$ p an odd prime has exactly $3p -$ incongruent solutions given by

$$x \equiv 3^{n-1}. p^{m-1}k + p\ (mod\ p^2. 3^n); k = 0, 1, 2, 3, \dots\dots\dots, (3p - 1).$$

REFERENCES

[1]. Zuckerman H. S., Niven I., 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 Dehli, India, ISBN: 978-81-312-1859-4.

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

[4]. Roy, B. M., “Formulation of solutions of standard cubic congruence of a special even composite modulus in a special case,” *International Journal of Engineering Technology Research and Management* (IJETRM), ISSN: 2456-9348, Vol-04, Issue-09, Sep-20.

[5]. Roy, B. M., “Formulation of standard cubic congruence of composite modulus modulo a powered even prime multiplied by a powered three in two special case”,*International Journal for Research Trends and Innovations (IJRTI),* ISSN: 2456-3315, Vol-05, Issue-09, Sep-20.

[6]. Roy, B. M., “A review and reformulation of solutions of standard cubic congruence of composite modulus modulo an odd prime power integer”, *International Journal for scientific development and Research* (IJSDR), ISSN: 2455-2631, Vol-05, Issue-12, Dec-20.

[7]. Roy, B. M., “Solving some special standard cubic congruence modulo an odd prime multiplied by eight”, *International Journal of scientific Research and Engineering Development* (IJSRED), ISSN: 2581-7175, Vol-04, Issue-01, Jan-21.

[8]. Roy, B. M., “Solving some special standard cubic congruence of composite modulus modulo a multiple of an odd prime”, *International Journal of Trend in scientific Research and Development* (IJTSRD), ISSN: 2456-6470, Vol-05, Issue-04, May-21.

[9]. Roy B. M*., “*Solving four standard cubic congruence modulo an even multiple of square of an odd prime”, *International Journal for scientific development and Research* (IJSDR), ISSN: 2455-2631, Vol-06, Issue-06, Jun-21