International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 2, Mar- Apr 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-154: Formulation of Solutions of a Special Standard Cubic Congruence Modulo nth Power of an Odd Prime Multiplied by mth Power of Three

Prof B M Roy

Head, Department of Mathematics

Jagat Arts, Commerce & I H P Science College, Goregaon

Dist- Gondia, M. S., INDIA. Pin: 441801

ABSTRACT

In the present paper, the author considered the standard cubic congruence of composite modulus for finding its solutions.It is found that the congruence has exactly $3p^2$ solutions incongruent to each other. But no formulation for solutions of the congruence is found in the literature of Mathematics. Only Chinese Remainder Theorem (CRT) can be applied. It is time consuming method. Sometimes the individual congruence create difficulty for finding solutions. No separate formulation is found. Hence, the author established a formulation to find all the solutions at a time and presented here. The author's formulation is very simple and time-saving.

KEY-WORDS

Cubic Residues, Chinese Remainder Theorem (CRT), Cubic Congruence, Formulation.

INTRODUCTION

The congruence$x^3 \equiv a\ (mod\ m)$ is a standard **cubic congruence** of composite modulus. It is called solvable if a is **cubic residue** of m. Here the author considered a standard cubic congruence modulo nth power ofan odd prime multiplied by $mth\ power$ of three,

$i.e.\ x^3 \equiv p^3 (mod\ 3^m p^n)$.It is found that Thomas Koshy [1] has discussed these types of congruence but used **Chinese Remainder theorem(CRT)** [2] for solutions. Such congruence have exactly $3p^2$ incongruent solutions, where p is an odd prime present in the corresponding congruence [3].

PROBLEM STATEMENT

Here the problem is-"To formulate the solutions of the congruence

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

LITERATURE REVIEW

No Formulation of solutions is found in the literature of mathematics. Readers are compelled to use CRT only as the existed method. It is very long procedure and sometimes becomes more difficult to use.The existed method is discussed here.

EXISTED METHOD

The Chinese Remainder Theorem can be used to find the solutions of the congruence.

In this method, the congruence in the problem is split into two separate congruence as:

$x^3 \equiv p^3 (mod\ 3^m)$..... (1)

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

Both are solved separately.

Here lies another difficulty. No method or formulation of solutions is found in the literature. Only trial &error method can be used. It is time consuming. But the author has already formulated these congruence and hence the individual congruence can be solved easily. By the author's formulation, the congruence (1) has exactly three solutions [4]; the congruence (2) has p^2solutions [5]and then using CRT method, the common solutions $i.e. 3p^2$

$solutions$[3] are obtained!!This can be elaborated by an example:

Consider an example: $x^3 \equiv 125\ (mod\ 3375)$.

It can be written as: $x^3 \equiv 125\ (mod\ 27.125)$.

It can be solved using CRT method.

The original congruence can be split into two congruence:

$x^3 \equiv 125\ (mod\ 27) i.e.\ x^3 \equiv 17\ (mod\ 27)$ ..... (3)

$x^3 \equiv 125\ (mod\ 125) i.e.\ : x^3 \equiv 0\ (mod\ 125)$..... (4)

These congruence (3) and (4) are solved by trial & error method, because no other method is available except the author's formulations. The trial & error method would take a long time.It can also be solved using the author's formulation as under:

Congruence (3) can be written as: $x^3 \equiv 5^3 (mod\ 3^3) with\ m = 3.$

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

The solutions, by author's formulation, are given by

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

$$\equiv 3^2k + 5\ (mod\ 3^3)$$

$$\equiv 9k + 5\ (mod\ 27)$$

$$\equiv 5, 14, 23\ (mod\ 27).$$

These are the three solutions.

Also the congruence (4) can be written as:

$x^3 \equiv 125\ (mod\ 125) i.e.\ x^3 \equiv 5^3 (mod\ 5^3) with\ p = 5, n = 3.$

It is of the type: $x^3 \equiv p^3 (mod\ p^n)$

It has p^2solutions given by:$x \equiv p^{n-2}k + p\ (mod\ p^n); k = 0, 1, 2, \dots\dots, (p^2 - 1).$

$$\equiv 5^1k + 5\ (mod\ 5^3)$$

$$\equiv 5k + 5\ (mod\ 125); k = 0, 1, 2, 3, \dots\dots..24.$$

$$\equiv 5, 10, 15, 20, 25, 30, \dots\dots\dots\dots, 125\ (mod\ 125).$$

These are the twenty –five solutions.

Then using CRT, all solutions are obtained. The original congruence has exactly $(3.25 = 75)$ solutions. By CRT, it is a big solution table and hence time consuming.

NEED OF THE RESEARCH

The need of the research can be understood from the example cited above. A direct formulation is in an urgent need.Therefore, the author formulated the congruence and presented here.

ANALYSIS & RESULT (AUTHOR'S FORMULATION)

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

For solutions of it, consider $x \equiv 3^{m-1}p^{n-2}k + p\ (mod\ 3^m p^n)$

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

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

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

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

So, $x \equiv 3^{m-1}p^{n-2}k + p\ (mod\ 3^m p^n)$ satisfies the cubic congruence and must be a solution. But $for\ k = 3p^2$, it is seen that

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

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

$\equiv 0 + p\ (mod\ 3^m p^n)$.

This is the same solution as for $k = 0$.

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

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

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

It is the same solution as for $k = 1$.

Therefore it is concluded that

$x \equiv 3^{m-1}p^{n-2}k + p\ (mod\ 3^m p^n); n \geq 3,\ k = 0, 1, 2, \ldots\ldots (3p^2 - 1)$gives all the solutions of the said congruence

ILLUSTRATIONS

Example-1: 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 $x^3 \equiv p^3 (mod\ 3^m p^n)\ with\ \ p = 5, , n = 3, m = 2$.

It has exactly $3p^2 = 3.5^2 = 75$ incongruent solutions.

These solutions are given by

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

$$\equiv 3^1.5^1 k + 5\ (mod\ 3^2.5^3)$$

$$\equiv 15k + 5\ (mod\ 1125); k = 0, 1, 2, 3, \ldots\ldots\ldots, 74.$$

$$\equiv 5, 20, 35, 50, 65, 80, 95, 110, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, 1115\ (mod\ 1125)$$

These are all the seventy five solutions of the congruence.

Example-2: Consider the congruence $x^2 \equiv 343\ \ (mod\ 9261))$.

It can be written as $x^3 \equiv 7^3 (mod\ 3^3.7^3)$.

It is of the type $x^3 \equiv p^3 (mod\ 3^m p^n)\ with\ \ p = 7, n = 3, m = 3$.

It has exactly $3p^2 = 3.7^2 = 147$ incongruent solutions.

These solutions are given by

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

$$\equiv 3^2.7^1 k + 7\ (mod\ 3^3.7^3)$$

$$\equiv 63k + 7\ (mod\ 9261); k = 0, 1, 2, 3, \dots\dots\dots, 146.$$

$$\equiv 7, 70, 133, 196, 259, 322, 385, \dots\dots\dots\dots\dots\dots\dots\dots\dots, 9205\ (mod\ 9261)$$

These are all the one hundred & forty-seven solutions of the congruence.

Example-3: Consider the congruence $x^3 \equiv 1331\ \ (mod\ 35937)$.

It can be written as $x^3 \equiv 11^3 (mod\ 3^3.11^3)$.

It is of the type $x^3 \equiv a^3 (mod\ 3^m.p^n)\ with\ \ p = 11, m = 3, n = 3$.

It has exactly three hundred &sixty-three incongruent solutions.

These solutions are given by

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

$$\equiv 3^2.11^1k + 11\ (mod\ 3^3.11^3)$$

$$\equiv 99k + 11\ (mod\ 35); k = 0, 1, 2, 3, \dots\dots\dots, 363.$$

$$\equiv 11, 110, 209, 308, 407, 506, 605, \dots\dots\dots\dots\dots\dots\dots\dots\dots, 35849\ (mod\ 35937)$$

These are all the three hundred & sixty-three solutions of the congruence.

CONCLUSION

Therefore, it can be concluded that the congruence under consideration has exactly $3p^2$ incongruent solutions, p being an odd prime in the corresponding congruence. The solutions aregiven by $x \equiv 3^{m-1}p^{n-2}k + p\ (mod\ 3^m p^n); k = 0, 1, 2, \dots\dots.. (3p^2 - 1)$.

Also, we found two more formulation of two more congruence as under.

The congruence $x^3 \equiv a^3\ (mod\ 3^m)\ has\ exactly\ three\ solutions\ given\ by$

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

The cubic congruence $x^3 \equiv p^3\ (mod\ p^n)$ has exactly p^2 solutions, given by

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

MERIT OF THE PAPER

The author's formulation has provided a suitable time-saving formulation for the solutions of the congruence under consideration. Thus, it can be said that the formulation is the merit of the paper.

REFERENCE

[1] Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press, Second Edition, New Delhi, ISBN: 978-81-312-1859-4, page-535.

[2]David M Burton, 2012, *Elementary Number Theory*, McGraw Hill Education (INDIA) Private Limited, New Delhi,Seventh Edition, ISBN: 978-1-902576-1,Pages: 372.

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

[4] B M Roy,*Formulation of Two special classes of standard cubic congruence of composite modulus-a power of three*, International Journal of Scientific Research and Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-03, May-19.

[5]B M Roy, International Journal for scientific Development and Research(IJSDR), ISSN: 2455-2631, vol-05, Issue-12, Dec-20.

[6] B M Roy, *Formulation of standard cubic congruence of composite modulus modulo a product of odd primes and nth power of three*, International Journal of Engineering Technology Research and Management (IJETRM), ISSN: 2456-9348, Vol-04, Issue-10, Oct-20.

……xxx……

