International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 2, Mar-Apr 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-119: Formulation of Solutions of a Standard Cubic Congruence of Composite Modulus- Twice a Prime Multiple of Power Of Three

Prof B M Roy

M. Sc. (Maths); Ph. D. (Hon); D. Sc. (Hon).

Head, Department of Mathematics

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

Dist. Gondia, M. S., (INDIA). PIN: 441801

(Affiliated to R T M Nagpur University, Nagpur)

ABSTRACT

In this paper, a standard cubic congruence of even composite modulus-an even- prime multiple of power of three- is considered for discussion and also to find a formulation of the solutions of the said congruence. It is found that some of the standard cubic congruence under consideration have exactly three solutions and some others have exactly nine solutions, if it is solvable. In one case, author's formulation is used and in other case, Chinese Remainder Theorem is used.

KEY-WORDS: Composite modulus, Chinese remainder theorem, Standard cubic Congruence.

.....

INTRODUCTION

The values of x in the congruence $x^3 \equiv a\ (mod\ m)$, that satisfy the cubic congruence is called its solutions. Not all cubic congruence are solvable. If a is a cubic residue of m, then it is solvable. Here our aim is to investigate a formulation of solutions of a special type of cubic congruence of composite modulus of the type:$x^3 \equiv a\ (mod\ 2p.3^n), p$ an odd prime.

LITERATURE REVIEW

A very little material is found in the literature of mathematics about the solutions of the cubic congruence of prime and composite modulus.

A cubic congruence of prime modulus is found in the literature.

It is seen that for $p \equiv 2\ (mod\ 3)$, the cubic congruence have unique solutions; but for

$p \equiv 1\ (mod\ 3)$, the cubic congruence has exactly three solutions [1].

If $p \equiv 2\ (mod\ 3)$, then there are $(p-1)$residues and hence $(p-1)$ $solvable\ cubic\ congruence$, and every congruence has a unique solution

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

But no formulation is found for the cubic congruence of composite modulus.

NEED OF MY RESEARCH

Such types of standard cubic congruence of composite modulus is not studied earlier. No formulation is present in the literature of mathematics. For solutions of the said congruence, formulation is needed. Thus for formulation, this study and discussion is carried out. This is the need of the research.

PROBLEM STATEMENT

Here, the problem is to find a formulation of the solutions of the standard cubic congruence of even composite modulus-twice a prime multiple of power of three of the type:

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

ANALYSIS & RESULT (Existed Method)

These cubic congruence can be solved using Chinese Remainder Theorem (CRT).

In this method, the congruence under consideration can be split into individual congruence:

$$x^3 \equiv a \ (mod\ 2) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (I)$$

$$x^3 \equiv a \ (mod\ p) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (II)$$

$$x^3 \equiv a \ (mod\ 3^n) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (III).$$

Each of the above congruence are solved and the common solutions can be obtained by

Chinese Remainder Theorem.

Congruence (I) can be solved easily and it has a single solution and congruence (III) can be solved by author's formulation [4], [5]. Congruence (II) has unique solution if $p \equiv 2\ (mod\ 3)$

$$buhas\ exactly\ three\ solutions\ if\ p \equiv 1\ (mod\ 3).$$

In the case $p \equiv 2\ (mod\ 3)$, the original congruence has exactly three solutions and the solutions can be formulated. But in case $p \equiv 1\ (mod\ 3)$, the original congruence has exactly nine solutions and can be obtained by Chinese Remainder Theorem; it cannot be formulated.

ANALYSIS & RESULT (Author's Formulation)

Consider the cubic congruence $x^3 \equiv a\ + k.2p.3^n \equiv b^3 (mod\ 2p.3^n)$; p being a positive odd prime integer [2].

If $p \equiv 2\ (mod\ 3)$, then this congruence has exactly three solutions.

For the solutions, let us consider $x \equiv 2p.3^{n-1}k + b\ (mod\ 2p.3^n); k = 0, 1, 2 \ldots\ldots\ldots$

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

$$\equiv (2p.3^{n-1}k)^3 + 3.(2p.3^{n-1}k)^2.b + 3.2p3^{n-1}k.b^2 + b^3\ (mod\ 2p.3^n)$$

$$\equiv 2p.3^n k\{b^2 + 2p3^{n-1}kb + 2^2.p^2.3^{2n-3}k\} + b^3\ (mod\ 2p.3^n)$$

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

Thus, $x \equiv 2p.3^{n-1}k + b \ (mod\ 2p.3^n)$ satisfies the said congruence and it is a solution.

But for$k = 3, the\ solution\ becomes\ x \equiv 2p.3^{n-1}.3 + b \ (mod\ 2p.3^n)$

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

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

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

For $k = 4, 5,$ the solutions are also the same as for $k = 1, 2$.

Thus, the congruence has exactly three incongruent solutions

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

But if $p \equiv 1 \ (mod\ 3)$, then the congruence must have nine solutions and cannot be formulated. This congruence can be solved using Chinese Remainder Theorem.

ILLUSTRATION BY EXISTED METHOD

Consider the congruence $x^3 \equiv 64 \ (mod\ 2.7.3^3)\ i.e.\ x^3 \equiv 64 \ (mod\ 378)$

Here, $p = 7 \equiv 1 \ (mod\ 3)$.

Therefore, this congruence can only be solved by CRT method as under:

It can be split into three congruence with solutions

$$x^3 \equiv 64 \ (mod\ 2)\ i.e. x^3 \equiv 0 \ (mod\ 2)\ i.e. \quad \boldsymbol{x \equiv 2\ (mod\ 2)}.$$

$$x^3 \equiv 64 \ (mod\ 7)\ i.e.\ x^3 \equiv 1 \ (mod\ 7)\ i.e. \quad \boldsymbol{x \equiv 1, 2, 4\ (mod\ 7)}.$$

$$x^3 \equiv 64 \ (mod\ 3^3)\ i.e.\ x^3 \equiv 4^3 (mod\ 27)\ i.e.\ \boldsymbol{x \equiv 4, 13, 22\ (mod\ 27)}.$$

Now Chinese Remainder Theorem can be used to find all the nine solutions.

Here, $a_1 = 2;$

$$a_2 = 1, 2, 3;$$

$$a_3 = 4, 13, 22.$$

Also, $M = [2, 7, 27] = 2.7.27 = 378.$

Therefore, $M_1 = 7.27 = 189; \quad M_2 = 2.27 = 54; \quad M_3 = 2.7 = 14.$

Now $M_1 x \equiv 1 \ (mod\ m_1)\ i.e. 189x \equiv 1 \ (mod\ 2)\ i.e.\ x_1 = 1.$

$$M_2 x \equiv 1 \ (mod\ m_2)\ i.e. 54x \equiv 1 \ (mod\ 7)\ i.e.\ x_2 = 3.$$

$$M_3 x \equiv 1 \ (mod\ m_3)\ i.e. 14x \equiv 1 \ (mod\ 27)\ i.e.\ x_2 = 2.$$

Then, the common solutions are given by

$$\boldsymbol{x_0 \equiv M_1 a_1 x_1 + M_2 a_2 x_2 + M_3 a_3 x_3\ (mod\ M)}$$

It can be written in tabular form as under:

1	2	3	1+2+3	
$M_1a_1x_1$	$M_2a_2x_2$	$M_3a_3x_3$		$x_0\ (mod\ M)$
189.2.1 = 378	54.1.3 = 162	14.4.2 = 112	652≡ 274	274
189.2.1 = 378	54.1.3 = 324	14.13.2 = 112	814≡ 58	148
189.2.1 = 378	54.1.3 = 486	14.22.2 = 112	976≡ 220	22
189.2.1 = 378	54.2.3 = 162	14.4.2 = 364	904≡ 148	58
189.2.1 = 378	54.2.3 = 324	14.13.2 = 364	1156≡ 22	310
189.2.1 = 378	54.2.3 = 486	14.22.2 = 364	1156≡ 22	184
189.2.1 = 378	54.4.3 = 162	14.4.2 = 616	1156≡ 22	4
189.2.1 = 378	54.4.3 = 324	14.13.2 = 616	1156≡ 22	256
189.2.1 = 378	54.4.3 = 486	14.22.2 = 616	1480≡ 346	130

Therefore, the said congruence has exactly nine incongruent solutions

$$x \equiv 4, 22, 58, 130, 148, 184, 310, 256, 274\ (mod\ 378).$$

.ILLUSTRATION (by Proposed Method)

Consider the congruence: $x^3 \equiv 35\ (mod\ 2.5.3^2)$.

Here $p = 5 \equiv 2(mod\ 3)$.

It can be written as $x^3 \equiv 35 + 90 = 125 = 5^3(mod\ 2.5.3^2)\ with\ b = 5, p = 5$.

It is always solvable.

Such congruence has exactly three solutions which are giving by

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

$$\equiv 2.5.3^1k + 5\ (mod\ 2.5.3^2); k = 0, 1, 2.$$

$$\equiv 30k + 5\ (mod\ 90)$$

$$\equiv 5, 35, 65\ (mod\ 90).$$

CONCLUSION

Thus, it can be concluded that the said congruence: $x^3 \equiv a^3\ (mod\ 2p.3^n)$

has exactly three incongruent solutions

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

If $p \equiv 1\ (mod\ 3)$, then the congruence have nine solutions which can be obtained using CRT method.

MERIT OF THE PAPER

In this paper, the standard cubic congruence of even composite modulus is studied for its solutions and is formulated. This lessens the labour of the readers to find the solutions. This is the merit of the paper.

REFERENCE

1. Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.
2. Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.
3. Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.
4. 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.
5. Roy B M,*Solving some cubic congruence of prime modulus*, International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-03, Issue-04, Jun-19.

