RP-93: Formulation of standard cubic congruence of composite modulus - A product of an odd prime, power of two & 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, Gogrgaon
Dist- Gondia, M. S., INDIA, Pin: 441801
(Affiliated to R T M Nagpur University, Nagpur).

***Abstract*: In this paper, a class of "standard cubic congruence of composite modulus- a product of an odd prime, power of two & power of three"- is considered for finding its solutions. The problem is discussed fully and studied the existed methods of finding solutions. The author established the formula for solutions and his efforts are presented here. The existed method is also discussed and illustrated with numerical examples. The methods of solutions and formulations of the congruence is the merit of this paper.**

***Keywords*: Chinese Remainder Theorem, Composite modulus, Cubic congruence.**

INTRODUCTION

In the current paper, the author wishes to consider a very special standard cubic congruence of composite modulus for study and discussion of findings the solutions.

The author already has written on the solutions of many standard cubic congruence of prime and composite modulus and all are published in different international journals.

A very little material is available in the literature of mathematics for study. Most of the books on Number Theory discusses only standard quadratic congruence of prime and composite modulus. The books of Zukerman and Koshy had slightly touched the topic but stopped

Abruptly without discussing the matter [1], [2]. Knowing these, only the author has tried to

Formulate the standard cubic congruence of prime and composite modulus of different kinds and papers have been published in different reputed International Journals [3], ….., [6].

PROBLEM-STATEMENT

The Problem for discussion is:

"To find the solutions of the standard cubic congruence of composite modulus-a product of odd prime, power of two and power of three: $x^3 \equiv a \pmod{p.2^m.3^n}$; p being an odd prime positive integer in four different cases:

Case-I: If $a \neq 3l$, an odd positive integer

Case-II: If $a \neq 3l$, an even positive integer

Case-III: If $a = 3l$, an odd positive integer

Case-IV: If $a = 3l$, an even positive integer.

EXISTED METHOD (CRT Method)

In this method, the said problem is solved by using Chinese Remainder Theorem (CRT).

At first, the congruence is split into individual congruence and their solutions are found separately. At last, the common solutions i. e. the required solutions are obtained using CRT.

Consider the congruence $x^3 \equiv a \pmod{p.2^m.3^n}$; it can be split into three congruence:

$x^3 \equiv a \pmod{2^m}$ ……. (I)

$x^3 \equiv a \pmod{p}$ ……. (II)

$x^3 \equiv a \pmod{3^n}$ ……. (III)

Consider the congruence (I). It is found after rigorous calculation that the congruence (I) has unique solution: $x \equiv a \pmod{m}$, only if a is an odd positive integer.

Consider the congruence (II). Such types of solvable cubic congruence has two types of solutions. If $p \equiv 2 \pmod{3}$, the congruence has unique solution: $x \equiv a^{\frac{2p-1}{3}} \pmod{p}$.

But, if $p \equiv 1 \pmod{3}$, the congruence has exactly three solutions but could not be formulated. It is solved by finding the cubic residues of p.

Now consider the congruence (III). It is already formulated by the author.

If the congruence can be written in the form $x^3 \equiv b^3 \pmod{3^n}$, then its solutions can be given by $x \equiv 3^{n-1}k + b \pmod{3^n}; k = 0, 1, 2$.

Then common solutions are obtained by CRT.

This method will take a long time.

ILLUSTRATIONS

Consider the congruence**:** $x^3 \equiv 27 \pmod{7.2^2.3^2}$.

It can be written as: $x^3 \equiv 3^3 \pmod{7.2^2.3^2}$.

It is of the type: $x^3 \equiv b^3 \pmod{p.2^m.3^n}$ with $b = 3, p = 7 \equiv 1 \pmod{3}$.

Therefore the congruence must have nine solutions.

These solutions can be obtained by using CRT method as it has no formulation.

The separate congruence with solutions are:

$x^3 \equiv 27 \pmod{4}$ i.e. $x^3 \equiv 3^3 \pmod{4}$ i.e. $x \equiv 3 \pmod{4}$.

$x^3 \equiv 27 \pmod{7}$ i.e. $x^3 \equiv 3^3 \pmod{7}$ i.e. $x \equiv 3, 5, 6 \pmod{7}$.

$x^3 \equiv 27 \pmod{3^2}$ i.e. $\equiv 3^3 \pmod{9}$ i.e. $x \equiv 3, 6, 9 \pmod{9}$.

Therefore, here, $\mathbf{a_1 = 3}$; $\mathbf{a_2 = 3, 5, 6}$; $\mathbf{a_3 = 3, 6, 9}$ & $m_1 = 4$; $m_2 = 7$; $m_3 = 9$.

$$M = [4, 7, 9] = 4.7.9 = 252.$$

So, $\mathbf{M_1 = \frac{M}{m_1} = 63}$; $\mathbf{M_2 = \frac{M}{m_2} = 36}$; $\mathbf{M_3 = \frac{M}{m_3} = 28}$.

Then, $M_1 x \equiv 1 \pmod{m_1}$ i.e. $63x \equiv 1 \pmod{4}$ i.e. $3x \equiv 1 \pmod{4}$ i.e. $\mathbf{x_1 = 3.}$

$M_2 x \equiv 1 \pmod{m_2}$ i.e. $36x \equiv 1 \pmod{7}$ i.e. $x \equiv 1 \pmod{7}$ i.e. $\mathbf{x_2 = 1.}$

$M_3 x \equiv 1 \pmod{m_3}$ i.e. $28x \equiv 1 \pmod{9}$ i.e. $x \equiv 1 \pmod{9}$ i.e. $\mathbf{x_3 = 1.}$

The common solutions are obtained by CRT as in tabular form:

$M_1a_1x_1$	$M_2a_2x_2$	$M_3a_3x_3$	$\sum(M_1a_1x_1)$	$x_0 \pmod M$
63.3.3.	36.3.1	28.3.1	567+108+84	3
63.3.3.	36.3.1	28.6.1	567+108+168	87
63.3.3.	36.3.1	28.9.1	567+108+252	171
63.3.3.	36.5.1	28.3.1	567+180+84	75
63.3.3.	36.5.1	28.6.1	567+180+168	159
63.3.3.	36.5.1	28.9.1	567+180+252	243
63.3.3.	36.6.1	28.3.1	567+216+84	111
63.3.3.	36.6.1	28.6.1	567+216+168	195
63.3.3.	36.6.1	28.9.1	567+216+252	27

Therefore, the required nine solutions are

$$x \equiv 3, 27, 75, 87, 111, 159, 171, 195, 243 \pmod{252}.$$

DEMERITS OF EXISTED METHOD

Thus it can be concluded that the existed method has many demerits. It is not simple. It is a long method. It is time-consuming. No formulation is available to find the solutions of the individual cubic congruence, except the author's formulation.

NEED OF RESEARCH

The need of this research is to remove all these demerits of the existed method. Also to provide the readers a time-saving method of solutions.

AUTHOR'S FORMULATION

Consider the congruence: $x^3 \equiv a \pmod{p.2^m.3^n}$; p an odd prime positive integer.

Let a be an odd positive integer. If so, it can be written as: $x^3 \equiv b^3 \pmod{p.2^m.3^n}$.

Also, let $p \equiv 2 \pmod 3$ and $a \neq 3l$ be an odd positive integer.

Let, $x \equiv p.2^m.3^{n-1}k + b \pmod{p.2^m.3^n}; n \geq 2$, with $k = 0, 1, 2, \ldots\ldots\ldots$

Therefore,

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

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

$$\equiv b^3 + p.2^m.3^n k\{b^2 + p.2^m.3^{n-2}k.b + (p.2^m.k)^2.3^{2n-3}\} \pmod{p.2^m.3^n}.$$

$$\equiv b^3 \pmod{p.2^m.3^n}.$$

Therefore, $x \equiv p.2^m.3^{n-1}k + b \pmod{p.2^m.3^n}$ is a solution of the congruence.

But for $k = 3$, it can be seen that $x \equiv p.2^m.3^{n-1}.3 + b \pmod{p.2^m.3^n}$

$$\equiv p.2^m.3^n + b \pmod{p.2^m.3^n}$$

$$\equiv b \pmod{p.2^m.3^n}$$

It is the same solution as can be obtained for $k = 0$.

For $k = 4, 5$ it can also be seen that the solutions are the same as for $k = 1, 2,$ respectively.

Therefore, the said congruence has exactly three incongruent solutions

$x \equiv p.2^m.3^{n-1}k + b \pmod{p.2^m.3^n}$ with $k = 0, 1, 2.$

But if $a \neq 3l$ is an even positive integer, then consider

$x \equiv p.2^{m-2}.3^{n-1}k + b \pmod{p.2^m.3^n}$ with $k = 0, 1, 2 \ldots \ldots \ldots$

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

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

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

$\equiv b^3 \pmod{p.2^m.3^n}$.

Therefore, $x \equiv p.2^{m-2}.3^{n-1}k + b \pmod{p.2^m.3^n}$ is a solution of the congruence.

But for $k = 12 = 4.3$, it can be seen that $x \equiv p.2^{m-2}.3^{n-1}.4.3 + b \pmod{p.2^m.3^n}$

$\equiv p.2^m.3^n + b \pmod{p.2^m.3^n}$

$\equiv b \pmod{p.2^m.3^n}$

It is the same solution as can be obtained for $k = 0$.

For $k = 13, 14, \ldots \ldots$ it can also be seen that the solutions are the same as for

$k = 1, 2, \ldots \ldots \ldots$ respectively.

Therefore, the said congruence has exactly twelve incongruent solutions

$x \equiv p.2^{m-2}.3^{n-1}k + b \pmod{p.2^m.3^n}$ with $k = 0, 1, 2 \ldots \ldots \ldots \ldots, 11$.

If $a = 3l$, an odd positive integer, and consider $x \equiv p.2^m.3^{n-2}k + 3l \pmod{p.2^m.3^n}$.

Then,

$x^3 \equiv (p.2^m.3^{n-2}k + 3l)^3 \pmod{p.2^m.3^n}$

$\equiv (p.2^m.3^{n-2}k)^3 + 3.(p.2^m.3^{n-2}k)^2.3l + 3.(p.2^m.3^{n-2}k.(3l)^2 + (3l)^3 \pmod{p.2^m.3^n}$.

$\equiv (p.2^m.3^{n-2}k)^3 + 3.(p.2^m.3^{n-2}k)^2.3l + 3.(p.2^m.3^{n-2}k).9l^2 + (3l)^3 \ (mod\ p.2^m.3^n)$.

$\equiv p.2^m.3^n k(p^2.2^{2m}.3^{2n-6}.k^2 + p.2^m.3^{n-2}.k.l + 3l^2 + (3l)^3 \ (mod\ p.2^m.3^n)$

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

But if $k = 9 = 3^2$, then the solution is $x \equiv p.2^m.3^{n-2}.3^2 + 3l \ (mod\ p.2^m.3^n)$

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

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

Therefore the congruence has exactly nine solutions:

$x \equiv p.2^m.3^{n-2}k + 3l \ (mod\ p.2^m.3^n); k = 0, 1, 2, \ldots \ldots \ldots \ldots, 8$.

If $a = 3l$, an even positive integer, and consider $x \equiv p.2^{m-2}.3^{n-2}k + 3l \ (mod\ p.2^m.3^n)$.

Then,

$x^3 \equiv (p.2^{m-2}.3^{n-2}k + 3l)^3 \ (modp.2^m.3^n)$

$\equiv (p2^{m-2}3^{n-2}k)^3 + 3(p2^{m-2}3^{n-2}k)^2 3l + 3(p2^{m-2}3^{n-2}k(3l)^2 + (3l)^3 (mod\ p.2^m.3^n)$.

$\equiv (p.2^{m-2}3^{n-2}k)^3 + 3(p2^{m-2}3^{n-2}k)^2 3l + 3(p2^{m-2}3^{n-2}k(3l)^2 + (3l)^3 \ (mod\ p.2^m.3^n)$.

$\equiv p.2^{m-2}.3^{n-2}k\{(p.2^{m-2}3^{n-2}k)^2 + 3.p.2^{m-2}.3^{m-2}k.3l + 3.p.2^{m-2}.3^{n-2}.9l^2\} + (3l)^3 \ (mod\ p.2^m.3^n)$.

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

But if $k = 36 = 2^2.3^2$, then the solution is $x \equiv p.2^{m-2}.3^{n-2}.2^2.3^2 + 3l \ (mod\ p.2^m.3^n)$

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

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

Therefore the congruence has exactly thirtysix solutions:

$x \equiv p.2^{m-2}.3^{n-2}k + 3l\ (mod\ p.2^m.3^n); k = 0, 1, 2, \ldots\ldots\ldots\ldots, 35.$

But for $p \equiv 1\ (mod\ 3)$, the congruence cannot be formulated though it has exactly nine incongruent solutions. Using the above formula, only three solutions can be obtained.

To find all the solutions, readers have to use CRT method.

ILLUSTRATIONS

Consider the congruence**:** $x^3 \equiv 125\ (mod\ 5.2^3.3^2)$.

It can be written as: $x^3 \equiv 5^3\ (mod\ 5.2^3.3^2)$.

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

Therefore the congruence must have three solutions given by

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

$\equiv 5.2^3.3^1k + 5\ (mod\ 5.2^3.3^2)$

$\equiv 120k + 5\ (mod\ 360); k = 0, 1, 2.$

$\equiv 5, 125, 245\ (mod\ 360).$

Consider the congruence**:** $x^3 \equiv 64\ (mod\ 5.2^3.3^2)$.

It can be written as: $x^3 \equiv 4^3\ (mod\ 5.2^3.3^2)$.

It is of the type: $x^3 \equiv b^3\ (mod\ p.2^m.3^n)\ with\ \ b = 4, p = 5 \equiv 2\ (mod\ 3).$

Therefore the congruence must have twelve solutions given by

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

$\equiv 5.2^1.3^1k + 4\ (mod\ 5.2^3.3^2$

$\equiv 30k + 4\ (mod\ 360); k = 0, 1, 2\ \ldots\ldots\ldots\ldots., 11.$

$\equiv 4{,}34, 64, 94, 124{,}154{,}184{,}214, 244, 274, 304{,}334\ \ (mod\ 360).$

Consider the congruence**:** $x^3 \equiv 216\ (mod\ 5.2^3.3^3)$.

It can be written as: $x^3 \equiv 6^3\ (mod\ 5.2^3.3^3)$.

It is of the type: $x^3 \equiv b^3\ (mod\ p.2^m.3^n)\ with\ \ b = 6, p = 5 \equiv 2\ (mod\ 3), n = 3.$

Therefore the congruence must have thirty six solutions given by

$x \equiv p.2^{m-2}.3^{n-2}k + b\ (mod\ p.2^m.3^n) with\ k = 0, 1, 2, \ldots\ldots\ldots.35.$

$\equiv 5.2^1.3^1k + 6\ (mod\ 5.2^3.3^3)$

$\equiv 30k + 6\ (mod\ 1080); k = 0, 1, 2\ \ldots\ldots\ldots\ldots., 35.$

$\equiv 6{,}36, 66, 96, 126{,}156{,}186{,}216, 246, 276, 306{,}336{,}366, 396, 426,$

$456, 486, 516, 546, 576, 606, 636, 666, 696, 726, 756, 786, 816,$

$846, 876, 906, 936, 966, 996, 1026, 1056\ \ (mod\ 1080).$

Consider the congruence: $x^3 \equiv 27\ (mod\ 5.2^3.3^3)$.

It can be written as: $x^3 \equiv 3^3\ (mod\ 5.2^3.3^3)$.

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

Therefore, the congruence must have nine solutions given by

$x \equiv p.2^m.3^{n-2}k + b\ (mod\ p.2^m.3^n) with\ k = 0, 1, 2 \dots \dots \dots, 8.$

$\equiv 5.2^3.3^1k + 3\ (mod\ 5.2^3.3^3)$

$\equiv 120k + 3\ (mod\ 1080); k = 0, 1, 2, \dots \dots, 8.$

$\equiv 3, 123, 243, 363, 483, 603, 723, 843, 963\ (mod\ 1080).$

Consider the congruence: $x^3 \equiv 729\ (mod\ 5.2^3.3^3)$.

It can be written as: $x^3 \equiv 9^3\ (mod\ 5.2^3.3^3)$.

It is of the type: $x^3 \equiv b^3\ (mod\ p.2^m.3^n)\ with\ \ b = 9, p = 5 \equiv 2\ (mod\ 3); n = 3$.

Therefore, the congruence must have nine solutions given by

$x \equiv p.2^m.3^{n-2}k + b\ (mod\ p.2^m.3^n) with\ \mathrm{k} = 0, 1, 2 \dots \dots \dots, 8.$

$\equiv 5.2^3.3^1k + 9\ (mod\ 5.2^3.3^3)$

$\equiv 120k + 9\ (mod\ 1080); k = 0, 1, 2, \dots \dots, 8.$

$\equiv 9, 129, 249, 369, 489, 609, 729, 849, 969\ (mod\ 1080).$

CONCLUSION

Thus it is concluded that the standard cubic congruence of composite modulus- a product of an odd prime, power of two & power of three:

$x^3 \equiv a\ (mod\ p.2^m.3^n);\ p\ an\ odd\ prime\ and\ a\ an\ odd\ positive\ integer$, and if

$p \equiv 2\ (mod\ 3), it$ has exactly three solutions, if $a \neq 3l$ is an odd positive integer and are given by: $x \equiv p.2^m.3^{n-1}k + b\ (mod\ p.2^m.3^n) with\ k = 0, 1, 2;$

If $a \neq 3l$ is an even positive integer, it has twelve incongruent solutions and are given by:

$x \equiv p.2^{m-2}.3^{n-1}k + b\ (mod\ p.2^m.3^n) with\ k = 0, 1, 2, \dots \dots \dots \dots \dots 11;$

If $a = 3l$ is an odd positive integer, it has nine incongruent solutions and are given by:

$\mathrm{x} \equiv \mathrm{p}.2^{\mathrm{m}}.3^{\mathrm{n}-2}\mathrm{k} + \mathrm{b}\ (\mathrm{mod}\ \mathrm{p}.2^{\mathrm{m}}.3^{\mathrm{n}})\mathrm{with}\ \mathrm{k} = 0, 1, 2, \dots \dots \dots \dots \dots 8;$

If $\mathrm{a} = 3\mathrm{l}$ is an even positive integer, it has thirty six incongruent solutions and are given by:

$\mathrm{x} \equiv \mathrm{p}.2^{\mathrm{m}-2}.3^{\mathrm{n}-2}\mathrm{k} + \mathrm{b}\ (\mathrm{mod}\ \mathrm{p}.2^{\mathrm{m}}.3^{\mathrm{n}})\mathrm{with}\ \mathrm{k} = 0, 1, 2, \dots \dots \dots \dots \dots 35.$

but if $\mathrm{p} \equiv 1\ (\mathrm{mod}\ 3)$, its solutions are obtained using CRT.

REFERENCES

[1] Zuckerman at el, 2008, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

[2] Thomas Koshy, 2009, "Elementary Number Theory with Applications", 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.

[3] Roy B M, 2019, Formulation of a class of solvable standard cubic congruence of even composite modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-01, Jan-19.

[5] **Roy B M, 2019**, Formulation of solutions of a class of standard cubic congruence modulo power of an integer multiple of power of three, International Journal of Recent Innovations in Academic Research (IJRIAR), ISSN: 2659-1561, Vol-03, Issue-01, Jan - 19.

[6] **Roy B M, 2019**, Formulation of solutions of a class of standard cubic congruence of even composite modulus- a power of an odd positive integer multiple of power of three, International Journal for Research, Trends and Innovations(IJRTI), ISSN:2456-3315,Vol-04, Issue-03, Mar-19.

[7] Roy B M., Formulation of two special types of standard cubic congruence of composite modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-05, Sep-19.