INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

**ISSN: 2454-132X**
**Impact factor: 4.295**
***(Volume 5, Issue 5)***
Available online at: www.ijariit.com

# Formulation of two special types of standard cubic congruence of composite modulus

*B. M. Roy*
roybm62@gmail.com
*Jagat Arts Commerce Indraben Hariharbhai Patel Science College,*
*Goregaon, Maharashtra*

## ABSTRACT

***In this paper, two special types of standard cubic congruence of composite modulus are formulated successfully. The first congruence has exactly four incongruent solutions while the second one has twelve incongruent solutions. The formulation is tested and verified true by solving different suitable examples. A simple and easy formula is established. Formulation is the merit of the paper.***

***Keywords***— *Cubic congruence, Composite modulus, Formulation, Incongruent solutions*

## 1. INTRODUCTION

In this paper, the author considered two special type of standard cubic congruence of composite modulus. These were not considered for formulation earlier. The author's main intention is to develop a simple and easy formulation of the solutions of the congruence under consideration. The author already formulated many standard cubic congruence of prime and composite modulus and the papers have been published in different International Journals.

## 2. LITERATURE REVIEW

The author tried his best to find some formulations or methods to find the solutions of the cubic congruence in the literature of mathematics. But the author is so unfortunate that he failed to find any. Only his own formulations for some other standard cubic congruence of composite modulus are found [1], [2], [3], [4].

## 3. PROBLEM-STATEMENT

The problem is "To formulate the solutions of the standard cubic congruence of composite modulus such as:

(1) $x^3 \equiv a^3 \ (mod\ 2^m); m \geq 4;$

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

## 4. ANALYSIS AND RESULTS

Consider the congruence: $x^3 \equiv a^3 \ (mod\ 2^m); m \geq 4,$

If $x \equiv 2^{m-2}k + a \ (mod\ 2^m)$, then

$$\begin{aligned} x^3 &\equiv (2^{m-2}k + a)^3 \\ &\equiv (2^{m-2}k)^3 + 3(2^{m-2}k)^2.a + 3(2^{m-2}k).a^2 + a^3 \\ &\equiv a^3 + \ 2^{m-2}k\{3a^2 + 3a.2^{m-2}k + (2^{m-2}k)^2\} \\ &\equiv a^3 + 2^{m-2}k\{4}, \qquad if\ a\ is\ an\ even\ integer. \\ &\equiv a^3 + 2^{m-2}k.2^2 \\ &\equiv a^3 + 2^m k \\ &\equiv a^3 \ (mod\ 2^m) \end{aligned}$$

Thus, it is seen that the cubic congruence under consideration has solutions given by

$$x \equiv 2^{m-2}k + a \ (mod\ 2^m); m \geq 4; k = 0, 1, 2, 3, 4, \dots \dots \dots \dots$$

But if $k = 4$, then the solution is $x \equiv 2^{m-2}.4 + a = 2^m + a \equiv a \ (mod\ 2^m)$. It is the same solution as can be obtained for $k = o$. Similarly, for $k = 5, 6, 7, 8, \dots \dots..$, the solutions are the same as for $k$ =1, 2, 3,0.

Thus it can be concluded that the solutions are $x \equiv 2^{m-2}k + a \ (mod\ 2^m); k = 0, 1, 2, 3.$

 

Therefore, the congruence always has four incongruent solutions.

But if $a$ is an odd positive integer, then form above discussion, it can be seen that $x \equiv a \ (mod\ 2^m)$ has the only solution for the congruence $x^3 \equiv a^3 \ (mod\ 2^m)$

Which is trivially true.

Consider the congruence $x^3 \equiv a^3 \ (mod\ 2^m.3^n)$
If $x \equiv 2^{m-2}.3^{n-1}k + a \ (mod\ 2^m.3^n)$, then

$$\begin{aligned} x^3 &\equiv (2^{m-2}.3^{n-1}k + a)^3 \\ &\equiv (2^{m-2}.3^{n-1}k)^3 + 3(2^{m-2}.3^{n-1}k)^2.a + 3(2^{m-2}.3^{n-1}k).a^2 + a^3 \\ &\equiv a^3 + 2^{m-2}.3^{n-1}k\{3a^2 + 3a.2^{m-2}.3^{n-1}k + (2^{m-2}.3^{n-1}k)^2\} \\ &\equiv a^3 + 2^{m-2}3^{n-1}3k\{4t\}, \quad if\ a\ is\ an\ even\ integer. \\ &\equiv a^3 + 2^{m-2}3^n.3.k.2^2.t \\ &\equiv a^3 + 2^m3^nkt \\ &\equiv a^3 \ (mod\ 2^m.3^n) \end{aligned}$$

Thus, it is seen that the cubic congruence under consideration has solutions given by

$$x \equiv 2^{m-2}.3^{n-1}k + a \ (mod\ 2^m.3^n); m \geq 4; k = 0, 1, 2, 3, 4, \ldots\ldots\ldots\ldots$$

But if $k = 4.3 = 12$, then the solution is

$$x \equiv 2^{m-2}.3^{n-1}.4.3 + a = 2^m.3^n + a \equiv a \ (mod\ 2^m.3^n).$$

It is the same solution as can be obtained for $k = o$.
Similarly, for $k = 13, 14, 15\ \ldots\ldots$., the solutions are the same as for $k$ =1, 2, 3….
as $k = 13 = 12 + 1$, then

$$x \equiv 2^{m-2}.3^{n-1}(12 + 1) + a \ (mod\ 2^m.3^n)$$

$\equiv 2^{m-2}.3^{n-1}(12 + 1) + a \ (mod\ 2^m.3^n)$
$\equiv 2^m.3^n + 2^{m-2}.3^{n-1} + a \ (mod\ 2^m.3^n)$
$\equiv 2^{m-2}.3^{n-1} + a \ (mod\ 2^m.3^n)$ which is same as for k=1.

Thus it can be concluded that the solutions are $x \equiv 2^{m-2}.3^{n-1}k + a \ (mod\ 2^m.3^n); k = 0, 1, 2, 3, \ldots\ldots\ldots, 10, 11.$

Therefore, the congruence always has twelve incongruent solutions.

But if $a$ is an odd positive integer, then form above discussion, it can be seen that the solutions of the congruence $x^3 \equiv a^3 \ (mod\ 2^m.3^n)$ are given by

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

These are the three solutions of the congruence.
Which is trivially true.

## 5. ILLUSTRATIONS

Consider the congruence $x^3 \equiv 2^3 \ (mod\ 2^4)$.

It is of the type $x^3 \equiv a^3 \ (mod\ 2^m)\ with\ a = 2, m = 4.$
Then the solutions are given by

$$\begin{aligned} x &\equiv 2^{m-2}.k + a \ (mod\ 2^m.); k = 0, 1, 2, 3. \\ &\equiv 2^{4-2}.k + 2 \ (mod\ 2^4) \\ &\equiv 2^2.k + 2 \ (mod\ 2^4) \\ &\equiv 4k + 2 \ (mod\ 16) \\ &\equiv 2, 6, 10, 14 \ (\text{mod } 16). \end{aligned}$$

These are the required four solutions of the congruence under consideration.

One more congruence is $x^3 \equiv 4^3 \ (mod\ 2^9)$.
It is of the type $x^3 \equiv a^3 \ (mod\ 2^m)\ with\ a = 4, m = 9.$
Then the solutions are given by

$$\begin{aligned} x &\equiv 2^{m-2}.k + a \ (mod\ 2^m); k = 0, 1, 2, 3. \\ &\equiv 2^{9-2}k + 4 \ (mod\ 2^9) \\ &\equiv 2^7k + 4 \ (mod\ 2^9) \\ &\equiv 128k + 4 \ (mod\ 512) \\ &\equiv 4, 132, 260, 388 \ (mod\ 512). \end{aligned}$$

These are the required four solutions of the congruence under consideration.

Consider the congruence $x^3 \equiv 11 = 11 + 16 = 27 = 3^3 \ (mod\ 2^4)$ [5].
It is of the type $x^3 \equiv a^3 \ (mod\ 2^m)\ with\ a = 3, an\ odd\ positive\ integer.$

 

Thus, the congruence has a unique solution given by $x \equiv a \ (mod\ 2^m)$.

$$\equiv 3 \ (mod\ 2^4).$$

Consider the congruence $x^3 \equiv 2^3 \ (mod\ 2^4.3^2)$.
It is of the type $x^3 \equiv a^3 \ (mod\ 2^m.3^n)\ with\ a = 2, m = 4, n = 2$.
Then the solutions are given by,

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

$\equiv 2^{4-2}.3k + 2 \ (mod\ 2^4.3^2)$
$\equiv 2^2.3k + 2 \ (mod\ 2^4.3^2)$
$\equiv 12k + 2 \ (mod\ 144)$
$\equiv 2, 14, 26, 38, 50, 62, 74$, 86, 98,110, 122, 134 (mod 144).
These are the required four solutions of the congruence under consideration.

One more congruence is $x^3 \equiv 4^3 \ (mod\ 2^9.3^3)$.
It is of the type $x^3 \equiv a^3 \ (mod\ 2^m.3^n)\ with\ a = 4, m = 9, n = 3$.
Then the solutions are given by,

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

$\equiv 2^{9-2}.3^2k + 4 \ (mod\ 2^9.3^3)$
$\equiv 2^7.3^2k + 4 \ (mod\ 2^9.3^3)$
$\equiv 1152k + 4 \ (mod\ 13824)$
$\equiv 4, 1156, 2308, 3460, 4612, 5764, 6916, 8068, 9220, 10372, 11524, 12676 \ (mod\ 13824)$.
These are the required twelve solutions of the congruence under consideration.

Consider the congruence $x^3 \equiv 55 = 55 + 2.144 = 343 = 7^3 \ (mod\ 2^4.3^2)$ [5].
It is of the type $x^3 \equiv a^3 \ (mod\ 2^m.3^n)\ with\ a = 37, an\ odd\ positive\ integer$.
Thus, the congruence has three solutions given by,

$$x \equiv 2^m 3^{n-1}k + a \ (mod\ 2^m.3^n).$$
$$\equiv 2^4 3^{2-1}k + 7 \ (mod\ 2^4.3^2).$$
$$\equiv 2^4.3k + 7 \ (mod\ 144).$$
$$\equiv 48k + 7 \ (mod\ 144)$$
$$\equiv 7, 55, 103 \ (mod\ 144).$$

## 6. CONCLUSION

From the above discussion, it can be concluded that

(a) The standard cubic congruence $x^3 \equiv a^3 \ (mod\ 2^m)$ has exactly four incongruent solutions given by $\equiv 2^{m-2}.k + a \ (mod\ 2^m); k = 0, 1, 2, 3, if\ a$ is an even positive integer.

But if $a$ is an odd positive integer, then the congruence has only one solution given by

$$x \equiv a \ (mod\ 2^m).$$

(b) The standard cubic congruence $x^3 \equiv a^3 \ (mod\ 2^m.3^n)$ also has exactly twelve incongruent solutions given by

$$x \equiv 2^{m-2}.3^{n-1}k + a \ (mod\ 2^m.3^n); k = 0, 1, 2, 3, \ldots, 10, 11.$$

But if $a$ is an odd positive integer, then the congruence has only three solution given by

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

These formulations are verified and found true by solving suitable examples.

## 7. MERIT OF THE PAPER

In this paper, two special type of standard cubic congruence of composite modulus are formulated and formulation is found true. It is simple and easy. Solutions can be obtained orally using these formulations. This is the merit of the paper.

## 8. REFERENCES

[1] Roy B M, 2019, 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, Issu-03, May-Jun-19.
[2] Roy B M, 2018, Formulation of a class of standard cubic congruence modulo a positive prime integer multiple of nine, International Journal of (IJRIAR), ISSN: 2635-3040, Vol-2, Issue-5, Sept-18,
[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.
[4] Roy B M, 2019, Formulation of a Special Type of Standard Cubic Congruence of Composite Modulus-an Odd Multiple of Power of Two, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2453-3315, Vol-4, Issue-5, May-19.
[5] Roy B M, 2016, “Discrete Mathematics & Number Theory”, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur, ISBN: 978-93-84336-12-7

 