INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 1)
Available online at: www.ijariit.com

Formulation of a class of solvable standard cubic congruence of even composite modulus

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

ABSTRACT

In this paper, a class of solvable standard cubic congruence of composite modulus is formulated. A formula for solutions is established and found true by solving some examples. It is also found that the congruence has exactly three solutions. Establishment of the formula for the solutions is the merit of the paper. It is needless to use Chinese Remainder Theorem. The formulation is the alternative of CRT which gives solutions directly in a short time.

Keywords— *Standard cubic congruence, Chinese Remainder Theorem, Even composite modulus*

1. INTRODUCTION

A standard cubic congruence is a neglected part of Number Theory. No material is found in the literature of mathematics except the author's formulation of cubic congruence. Hence, the author wishes to rich the cubic congruence in its theory with formulation of the solutions. In this regard, here is another solvable standard cubic congruence of composite modulus, the author is going to formulate and takes the solvable standard cubic congruence under consideration as $x^3 \equiv a^3 \ (mod\ 2^m 3^n)$. Such types of congruence are always solvable.

2. EXISTED METHOD

Actually no method is found to solve the congruence. But Chinese Remainder Theorem can be used. In this case, the original congruence can be split into separate congruence as:

$$x^3 \equiv a^3 \ (mod\ 2^m) \quad (1)$$
$$x^3 \equiv a^3 \ (Mod\ 3^n) \quad (2)$$

Solving these congruence, solutions can be obtained. Then, using Chinese Remainder Theorem, common solutions $i.e.$ solutions of the original congruence can be obtained. It is a time-consuming method. It takes a long time for solutions.

The congruence (1) has unique solutions while the congruence (2) has exactly three solutions (by author's formulation). Therefore, the original congruence must have exactly three solutions. [3].

3. NEED OF RESEARCH

Students found no alternative of CRT for solutions of the said congruence. Such types of congruence create difficulties for students. An alternative formulation of CRT method is in an urgent need. This is the need of this research. The author tried his best to develop an alternative formulation of CRT and succeed.

4. PROBLEM-STATEMENT

The author wishes to formulate the solutions of the class of standard cubic congruence of composite modulus: $x^3 \equiv a^3 \ (mod\ 2^m.3^n);\ m,n \geq 1, are\ positive\ integer; a\ is\ positive\ integer.$

5. ANALYSIS AND RESULT (FORMULATION)

Consider the said congruence under consideration:

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

For the solutions, consider

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

Then,

$$\begin{aligned} x^3 &\equiv (3^{n-1}2^m k + a)^3 \\ &\equiv (3^{n-1}2^m k)^3 + 3.(3^{n-1}2^m k)^2.a + 3.(3^{n-1}2^m k).a^2 + a^3 \ (\text{mod } 2^m 3^n) \\ &\equiv a^3 (mod\ 2^m 3^n). \end{aligned}$$

Thus, $x \equiv 3^{n-1}2^m k + a\ (mod\ 2^m 3^n)$ satisfies the cubic congruence under consideration. Therefore, it must be a solution of it for some values of k, a positive integer with $k = 0, 1, 2$.

If $k = 3$, then, $x \equiv 3^{n-1}2^m.3 + a = 3^n 2^m + a \equiv a\ (mod\ 3^n 2^m)$. This is same as $k = o$. Similarly it can also be shown that for $k = 4, 5$, the solutions are the same as for $k = 1, 2$ respectively.Therefore, the congruence has only three solutions.

6. ILLUSTRATIONS

Consider the congruence $x^3 \equiv 3^3\ (mod\ 864)$.
Here, $864 = 32.27 = 2^5 3^3$.

So, the congruence under consideration becomes $x^3 \equiv 3^3\ (mod\ 2^5 3^3)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m 3^n)\ with\ a = 3, n = 3, m = 5$.

The solutions are given by:

$$\begin{aligned} x &\equiv 3^{n-1}2^m k + a\ (mod\ 3^n 2^m) for\ k = 0,1,2. \\ &\equiv 3^{3-1}2^5 k + 3\ (mod\ 2^5 3^3) \\ &\equiv 9.32.k + 3\ (mod\ 32.27) \\ &\equiv 288k + 3\ (mod\ 864) \\ &\equiv 3, 291, 579\ (mod\ 864)\ for\ k = 0, 1, 2. \end{aligned}$$

Consider the congruence $x^3 \equiv 2^3\ (mod\ 5184)$
Here, $5184 = 64.81 = 2^6 3^4$.

So, the congruence under consideration becomes $x^3 \equiv 2^3\ (mod\ 2^6 3^4)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m 3^n)\ with\ a = 2, n = 4, m = 6$.

The solutions are given by:

$$\begin{aligned} x &\equiv 3^{n-1}2^m k + a\ (mod\ 3^n 2^m) for\ k = 0,1,2. \\ &\equiv 3^{4-1}2^6 k + 2\ (mod\ 2^6 3^4) \\ &\equiv 17.64.k + 2\ (mod\ 64.81) \\ &\equiv 1728k + 2\ (mod\ 5184) \\ &\equiv 2, 1730, 3458\ (mod\ 5184)\ for\ k = 0, 1, 2. \end{aligned}$$

Consider the congruence $x^3 \equiv 343\ (mod\ 864)$.
Here, $864 = 32.27 = 2^5 3^3$; & $343 = 7^3$.

So, the congruence under consideration becomes $x^3 \equiv 7^3\ (mod\ 2^5 3^3)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m 3^n)\ with\ a = 7, n = 3, m = 5$.

The solutions are given by:

$$\begin{aligned} x &\equiv 3^{n-1}2^m k + a\ (mod\ 3^n 2^m) for\ k = 0,1,2. \\ &\equiv 3^{3-1}2^5 k + 7\ (mod\ 2^5 3^3) \\ &\equiv 9.32.k + 7\ (mod\ 32.27) \\ &\equiv 288k + 7\ (mod\ 864) \\ &\equiv 7, 295, 583\ (mod\ 864)\ for\ k = 0, 1, 2. \end{aligned}$$

7. CONCLUSION

Thus, it can be concluded that the solvable standard cubic congruence under consideration: $x^3 \equiv a^3\ (mod\ 2^m 3^n)$ is formulated by the establishment of the formula for solutions:

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

Therefore, the congruence has exactly three solutions.

8. MERIT OF THE PAPER

The cubic congruence under consideration is formulated. It makes finding the solutions easy. No need to use CRT. Formulation is the merit of the paper. A quick method is obtained to find the solutions.

9. REFERENCES

[1] Burton D M, "*Elementary Number Theory*", 2/e, 2003, Universal Book Stall.
[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] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to the Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.

