RP-126: Formulation of a Special Class of Standard Cubic Congruence of Even Composite Modulus

Prof. B M Roy

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 special class of standard cubic congruence of even composite modulus is formulated. A formula for solutions is established and found true by solving some examples and verifying the results. It is also found that some congruence have exactly three solutions and some others have exactly twelve solutions. No method or formulation is found for the solutions of the congruence under consideration. Only Chinese Remainder Theorem can be used. It is a very long and time-consuming. Establishment of the formula for the solutions is the merit of the paper. Now, it is needless to use Chinese Remainder Theorem.

KEY-WORDS: Chinese Remainder Theorem, Even composite modulus, Standard cubic congruence.

INTRODUCTION

A standard cubic congruence of composite modulus is a congruence: \( x^3 \equiv a \pmod{m} \); m being a composite positive integer. If \( a \) is a cubic residue of \( m \), i.e. if \( a \equiv b^3 \pmod{m} \), then the congruence reduces to \( x^3 \equiv b^3 \pmod{m} \) and the congruence is said to be solvable [1].

The values of \( x \) that satisfy the congruence are called its solutions.

No material is found in the literature of mathematics except a definition of cubic residue of a prime \( p \) [1]& [2] and the author’s formulation of some cubic congruence [3], …., [7].

Hence, the author wishes to enrich the theory of cubic congruence with formulation of the solutions.

In this regard, here is another solvable standard cubic congruence of composite modulus, the author is going to formulate. The author considers the standard cubic congruence: \( x^3 \equiv a^3 \pmod{2^m \cdot 3^n \cdot b} \).
Such types of congruence are always solvable.

**PROBLEM-STATEMENT**

The author wishes to formulate the solutions of the special class of standard cubic congruence of composite modulus:

\[ x^3 \equiv a^3 \mod (2^m \cdot 3^n \cdot b); a, m, n \geq 1, \text{are positive integers} \]

In two cases:

Case-I: if \( a \) is an even positive integer;

Case-II: if \( a \) is an odd positive integer.

**EXISTED METHOD**

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

\[ x^3 \equiv a^3 \mod (2^m) \]
\[ x^3 \equiv a^3 \mod (3^n) \]
\[ x^3 \equiv a^3 \mod (b) \]

Solving these congruence separately, solutions can be obtained. Then, using Chinese Remainder Theorem, the common solutions i.e. solutions of the original congruence can be obtained [1]& [2].

**DEMERITS OF EXISTED METHOD**

Chinese Remainder Theorem (CRT) is a time-consuming method.

It takes a long time for solutions.

Sometimes it become very difficult to find the solutions of the individual congruence.

No literature is found suitable for solutions.

**NEED OF RESEARCH**

To come over the demerits of CRT and to find an alternative of CRT, a formulation of the solutions of the congruence is in an urgent need. The author tried his best to develop a formulation and succeed. It is presented in this paper. This is the need of this research.

**ANALYSIS & RESULT (Formulation)**

**Case-I: When \( a \) is even positive integer.**
Consider the congruence under consideration: $x^3 \equiv a^3 (mod 2^m 3^n \cdot b)$.

For the solutions, consider $x \equiv 3^{n-1} 2^{m-2} \cdot b \cdot k + a (mod 2^m 3^n \cdot b)$

Then,

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

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

$$\equiv a^3 + 3 \cdot 3^{n-1} 2^{m-2} \cdot b \cdot ((3^{n-1} 2^{m-2} k)^2 + 3(3^{n-1} 2^{m-2} 5)^1 \cdot a + 3a^2)$$

$$\equiv a^3 + 3^{n-1} 2^{m-2} \cdot b \cdot (4.3t), if a is even positive integer$$

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

Thus, $x \equiv 3^{n-1} 2^{m-2} \cdot b \cdot k + a (mod 2^m 3^n \cdot b)$ satisfies the cubic congruence under consideration.

Therefore, it must be a solution of it for some values of $k$, a positive integer with $k = 0, 1, 2, \ldots, 11$.

If $k = 12 = 3.4$, then, $x \equiv 3^{n-1} 2^{m-2} \cdot b \cdot (3.4) + a = 3^n 2^m b + a \equiv a (mod 3^n 2^m b)$.

This is same as $k = 0$.

Similarly it can also be shown that for $k = 13, 14, \ldots$ the solutions are the same as for $k = 1, 2, \ldots$, respectively. Therefore, the congruence has exactly twelve solutions.

**Case-II: When $a$ is odd positive integer.**

Consider the congruence under consideration: $x^3 \equiv a^3 (mod 2^m 3^n \cdot b)$.

For the solutions, consider $x \equiv 3^{n-1} 2^m \cdot b \cdot k + a (mod 2^m 3^n \cdot b)$

Then,

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

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

$$\equiv a^3 + 3^n 2^m \cdot b \cdot ((3^{n-1} 2^m k)^2 + 3(3^{n-1} 2^m 5)^1 \cdot a + 3a^2)$$

$$\equiv a^3 + 3^n 2^m \cdot b \cdot t, if a is odd positive integer.$$

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

Thus, $x \equiv 3^{n-1} 2^m \cdot b \cdot k + a (mod 2^m 3^n \cdot b)$ satisfies the cubic congruence under consideration.

Therefore, it must be a solution of it for some values of $k$, a positive integer with $k = 0, 1, 2, \ldots,$.
If \( k = 3 \), then, \( x \equiv 3^{n-1}2^m \cdot b \cdot (3) + a = 3^n2^m \cdot b + a \equiv a \pmod{3^n2^m \cdot b} \). This is same as \( k = 0 \).

Similarly it can also be shown that for \( k = 4, 5, \ldots \) the solutions are the same as for \( k = 1, 2 \) Respectively. Therefore, the congruence has exactly three solutions for \( k = 0, 1, 2 \).

**ILLUSTRATIONS**

Consider the congruence \( x^3 \equiv 27 \pmod{720} \).

Here, \( 720 = 16 \cdot 9 \cdot 5 = 2^4 \cdot 3^2 \cdot 5 \).

So, the congruence under consideration becomes \( x^3 \equiv 3^3 \pmod{2^4 \cdot 3^2 \cdot 5} \).

It is of the type \( x^3 \equiv a^3 \pmod{2^m3^n \cdot b} \) with \( a = 3, n = 2, m = 4, b = 5 \).

It has three solutions.

These solutions are given by \( x \equiv 3^{n-1}2^m \cdot b \cdot k + a \pmod{3^n2^m \cdot b} \) for \( k = 0, 1, 2 \).

\[
\equiv 3^2 - 1^2 \cdot 4 \cdot 5 \cdot k + 3 \pmod{3^2 \cdot 2^4 \cdot 3^2 \cdot 5} \\
\equiv 3.16.5k + 3 \pmod{32.9.5} \\
\equiv 240k + 3 \pmod{720} \\
\equiv 3, 243, 483 \pmod{720} \]

Consider the congruence \( x^3 \equiv 8 \pmod{2016} \).

Here, \( 2016 = 32 \cdot 9 \cdot 7 = 2^5 \cdot 3^2 \cdot 7 \).

So, the congruence under consideration becomes \( x^3 \equiv 2^3 \pmod{2^5 \cdot 3^2 \cdot 7} \).

It is of the type \( x^3 \equiv a^3 \pmod{2^m3^n \cdot b} \) with \( a = 2, n = 2, m = 5, b = 7 \).

As \( a \) is even positive integer, the congruence must have twelve solutions.

These twelve solutions are given by

\[
x \equiv 3^{n-1}2^m \cdot b \cdot k + a \pmod{3^n2^m \cdot b} \text{ for } k = 0, 1, 2 \ldots \ldots 11.
\]

\[
\equiv 3^2 - 1^2 \cdot 5 \cdot 2^5 \cdot 7 \cdot k + 2 \pmod{3^2 \cdot 2^5 \cdot 3^2 \cdot 7} \\
\equiv 3.8.7k + 2 \pmod{32.9.7} \\
\equiv 168k + 2 \pmod{2016} \\
\equiv 2, 170, 338, 506, 674, 842, 1010, 1178, 1346, 1514, 1682, 1850 \pmod{2016} \text{ for } k = 0, 1, 2 \ldots \ldots 11.
\]
Consider the congruence \( x^3 \equiv 343 \pmod{4320} \).

Here, \( 4320 = 32 \cdot 27 \cdot 5 = 2^5 \cdot 3^3 \cdot 5 \); \( 343 = 7^3 \).

So, the congruence under consideration becomes \( x^3 \equiv 7^3 \pmod{2^5 \cdot 3^3 \cdot 5} \)

It is of the type \( x^3 \equiv a^3 \pmod{2^m \cdot 3^n \cdot 5} \) with \( a = 7, n = 3, m = 5, b = 5 \).

Here \( a \) is odd positive integer. It has only three solutions.

These solutions are given by \( x \equiv 3^{n-1} \cdot 2^m \cdot 5 \cdot k + a \pmod{2^m \cdot 3^n \cdot 5} \) for \( k = 0, 1, 2 \).

\[
\equiv 3^{n-1} \cdot 2^5 \cdot 5 \cdot k + 7 \pmod{2^5 \cdot 3^3 \cdot 5} \\
\equiv 9 \cdot 32 \cdot 5 \cdot k + 7 \pmod{32 \cdot 27 \cdot 5} \\
\equiv 1440 \cdot k + 7 \pmod{4320} \\
\equiv 7, 1447, 2887 \pmod{4320} \text{ for } k = 0, 1, 2.
\]

Thus the congruence has exactly three solutions.

**CONCLUSION**

Thus, it is concluded that the standard cubic congruence under consideration:

\( x^3 \equiv a^3 \pmod{2^m \cdot 3^n \cdot b} \) is formulated. The established formula for solutions is given by:

\( x \equiv 3^{n-1} \cdot 2^m \cdot 2^n \cdot k + a \pmod{2^m \cdot 3^n \cdot b} \) with \( k = 0, 1, 2, 3, 4, 5 \ldots, 10, 11 \) when \( a \) is an even positive integer. Therefore, the congruence has exactly twelve solutions, if \( a \) is even positive integer.

But, if \( a \) is an odd positive integer, the congruence under consideration has only three solutions given by

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

These solutions are tested and verified true.

**MERIT OF THE PAPER**

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

**REFERENCE**


