FORMULATION OF SOLUTIONS OF STANDARD CUBIC CONGRUENCE OF A SPECIAL EVEN COMPOSITE MODULUS IN A SPECIAL CASE.

Prof B M Roy
Head, Department of Mathematics,
Jagat Arts, Commerce & I H P Science College, Goregaon
(Affiliated to R T M Nagpur University)

ABSTRACT
In this current paper, the author has given a formulation of standard cubic congruence of a special even composite modulus in two different cases. A formula for solutions of each case is established and found true by solving some numerical examples. It is found that the congruence has exactly three / nine solutions as the case. Now it is needless to use Chinese Remainder Theorem for finding solutions. The formulation is the alternative of CRT which gives solutions directly in a short time. Establishment of the formulae for the solutions is the merit of the paper.

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

INTRODUCTION
A standard cubic congruence is a congruence of the type: \( x^3 \equiv a \pmod{m} \). A very little material is found in the literature of mathematics. The author wishes to study the cubic congruence for 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 \( x^3 \equiv a^3 \pmod{2^m 3^n} \). Such types of congruence are always solvable.

EXISTED METHOD
Actually no method is found to solve the said congruence. But Chinese Remainder Theorem [1] can be used. In this case, the original congruence can be split into separate congruence as

\[
x^3 \equiv a^3 \pmod{2^m} \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (1)
\]

\[
&x^3 \equiv a^3 \pmod{3^n} \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad (2).
\]

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.

LITERATURE-REVIEW
It is found that no method or formulation is available in the literature of mathematics. Thomas Koshy has mentioned the definition of a standard cubic congruence of prime modulus in his book in a supplementary exercises [2]. Zuckerman has defined a cubic residue in his book [3]. The author already has formulated many standard cubic congruence of composite modulus [4], [5], [6], [7].

**PROBLEM-STATEMENT**

Here, the problem is “To formulate the solutions of the standard cubic congruence of composite modulus of the type:

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

in two different cases as:

**Case-I:** If \( a \) is odd & \( a \neq 3l, l \) being odd positive integer;

**Case-II:** If \( a \) is odd & \( a = 3l, l \) being odd positive integer.

**ANALYSIS & RESULT (Formulation)**

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

**Case-I:** Let \( a \neq 3l \) be an odd positive integer, \( l \) being an odd integer.

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

Then,

\[
\begin{align*}
x^3 & \equiv (3^{n-1} 2^m k + a)^3 (mod 2^m 3^n) \\
& \equiv (3^{n-1} 2^m k)^3 + 3. (3^{n-1} 2^m k)^2. a + 3. (3^{n-1} 2^m k). a^2 + a^3 (mod 2^m 3^n) \\
& \equiv a^3 + 3^n 2^m \{ (3^{n-2} 2^m k)^2 + (3^{n-1} 2^m 5)^1. a + a^2 \} (mod 2^m 3^n) \\
& \equiv a^3 + 3^n 2^m \{ t (mod 2^m 3^n) \}, \text{if } a \neq 3l, \text{is odd positive integer} \\
& \equiv a^3 (mod 2^m 3^n).
\end{align*}
\]

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 \( k \).

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 solution as for \( k = 0 \).

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

**Case-II:** Let \( a = 3l \) be an odd positive integer, \( l \) being odd.

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

\[ x^3 \equiv (3^{n-2}2^m k + a)^3 \]
\[ \equiv (3^{n-2}2^m k)^3 + 3 \cdot (3^{n-2}2^m k)^2 \cdot a + 3 \cdot (3^{n-2}2^m k) \cdot a^2 + a^3 \pmod{2^m 3^n} \]
\[ \equiv a^3 + 3^{n-2}2^m \{(3^{n-2}2^m k)^2 + 3(3^{n-2}2^m 5^1) \cdot a + 3a^2\} \pmod{2^m 3^n} \]
\[ \equiv a^3 + 3^{n-2}2^m \{9t\} \pmod{2^m 3^n} \] if \( a = 3l, is\ odd\ positive\ integer. \]
\[ \equiv a^3 \pmod{2^m 3^n}. \]

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

Therefore, it must be a solution of it for some values of \( k \).

If \( k = 9 \), then, \( x \equiv 3^{n-2}2^m \cdot (9) + a = 3^n 2^m + a \equiv a \pmod{2^m 3^n} \). This is same solution as for \( k = 0 \).

Similarly it can also be shown that for \( k = 9, 10, \ldots \) the solutions are the same as for \( k = 1, 2, \ldots \), Respectively. Therefore, the congruence has **exactly nine** solutions.

**ILLUSTRATIONS**

**Example-1:** Consider the congruence \( x^3 \equiv 343 \pmod{864} \).

Here, \( 864 = 32.27 = 2^5 3^3; \) & \( 343 = 7^3 \).

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

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

Here, \( a \neq 3l \) is an odd positive integer.

Hence, the three solutions are given by \( x \equiv 3^{n-12}2^m k + a \pmod{3^n 2^m} \) \( for k = 0, 1, 2. \)

\[ \equiv 3^{3-12^5}k + 7 \pmod{2^5 3^3} \]
\[ \equiv 9.32. k + 7 \pmod{32.27} \]
\[ \equiv 288k + 7 \pmod{864} \]
\[ \equiv 7, 295, 583 \pmod{864} \] \( for k = 0, 1, 2. \)

**Example-4:** Consider the congruence \( x^3 \equiv 3^3 \pmod{864} \).

Here, \( 864 = 32.27 = 2^5 3^3 \)

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

It is of the type \( x^3 \equiv a^3 \pmod{2^m 3^n} \) \( witha = 3, n = 3, m = 5 \).
Here, \( a = 3l \). So, the congruence has exactly nine solutions.

The nine solutions are given by

\[
x \equiv 3^{n-2}2^m k + a (\mod 3^n 2^m) f o r k = 0, 1, 2 \ldots \ldots 8.
\]

\[
\equiv 3^{3-2} 2^5 k + 3 (\mod 2^5 3^3)
\]

\[
\equiv 3.32k + 3 (\mod 32.27)
\]

\[
\equiv 96k + 3 (\mod 864)
\]

\[
\equiv 3, 99, 201, 291, 387, 483, 579, 675, 721, (\mod 864).
\]

Example-6: Consider the congruence \( x^3 \equiv 729 (\mod 1296) \).

Here, \( 1296 = 2^4 3^4 \) & \( 729 = 9^3 \).

So, the congruence under consideration becomes \( x^3 \equiv 9^3 (\mod 2^4 3^4) \).

It is of the type \( x^3 \equiv a^3 (\mod 2^m 3^n) \) with \( n = 3, m = 4 \).

Here, \( a = 3l \), an odd multiple of three.

So, the congruence has exactly nine solutions given by

\[
x \equiv 3^{n-2}2^m k + a (\mod 3^n 2^m) f o r k = 0, 1, 2, 3, \ldots \ldots \ldots 8.
\]

\[
\equiv 3^{4-2} 2^4 k + 9 (\mod 2^4 3^4)
\]

\[
\equiv 9.144k + 9 (\mod 16.81)
\]

\[
\equiv 144k + 9 (\mod 1296)
\]

\[
\equiv 9, 153, 297, 441, 513, 729, 873, 1017, 1161, (\mod 1296).
\]

CONCLUSION

Thus, it can be concluded that the solvable standard cubic congruence under consideration:

\( x^3 \equiv a^3 (\mod 2^m 3^n) \) has exactly three solutions given by

\[
x \equiv 3^{n-1}2^m k + a (\mod 2^m 3^n) \) with \( k = 0, 1, 2 \) if \( a \neq 3l \), is an odd positive integer.
\]

But if \( a = 3l \), then it has exactly nine solutions given by

\[
x \equiv 3^{n-1}2^m k + a (\mod 2^m 3^n) \) with \( k = 0, 1, 2, 3, 4, 5, 6, 7, 8.
\]

REFERENCE