RP-140: Formulation of standard cubic congruence of composite modulus modulo a powered even prime multiplied by a powered three in two special case

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)

***Abstract*: In this paper, the author has considered a standard cubic congruence of even composite modulus in two different cases for formulation. A formula of each case is established and tested true by solving some numerical examples. It is found that the congruence has exactly twelve / thirty-six solutions as the case. 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.**

***Keywords*: Standard Cubic Congruence, Chinese Remainder Theorem (CRT), Composite Modulus.**

1. INTRODUCTION

A standard cubic congruence of the type: $x^3 \equiv a \pmod m$ is seldom studied in mathematics. A very little study material is found in the literature of mathematics. The author studied the congruence and started the formulation of solutions of such congruence. In this regard, here is a solvable standard cubic congruence of composite modulus, the author is going to formulate.

So the author considers the standard cubic congruence of the type:

$x^3 \equiv a^3 \ (mod\ 2^m 3^n)\ for\ formulation$. Such types of congruence are always solvable.

2. LITERATURE-REVIEW

No detailed study is found in the literature for the solutions of the congruence under consideration. Only readers use CRT method [1] for solutions. 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. Some are listed here as [4], [5], [6], [7].

3. PROBLEM-STATEMENT

Here, the problem is

"To formulate the solutions of the standard cubic congruence of composite modulus of the type: $x^3 \equiv a^3 \ (mod\ 2^m.3^n);\ m, n \geq 1\ \&\ a\ are\ positive\ integers,$ in two different cases as:

Case-I: $If\ a \neq 6l\ is\ even\ positive\ integer;$

Case-II: $If\ a = 6l,\ \ is\ even\ positive\ integer.$

4. ANALYSIS & RESULT (Formulation)

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

Case-I: Let $a \neq 6l$ be an even positive integer, $l$being any positive integer.

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

Then,

$$x^3 \equiv (3^{n-1}2^{m-2}k + a)^3 \ (mod\ 2^m 3^n)$$
$$\equiv (3^{n-1}2^{m-2}k)^3 + 3.(3^{n-1}2^{m-2}k)^2.a + 3.(3^{n-1}2^{m-2}k).a^2 + a^3 \ (mod\ 2^m 3^n)$$
$$\equiv a^3 + 3^{n-1}2^{m-2}\{(3^{n-1}2^{m-2}k)^2 + 3(3^{n-1}2^{m-2}5)^1.a + 3a^2\} \ (mod\ 2^m 3^n)$$
$$\equiv a^3 + 3^{n-1}2^{m-2}\{(4.3)t\} \ (mod\ 2^m 3^n), if\ a\ is\ even\ positive\ integer$$
$$\equiv a^3 (mod\ 2^m 3^n).$$

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

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

If $k = 12 = 3.4$, then, $x \equiv 3^{n-1}2^{m-2}.(3.4) + a = 3^n 2^m + a \equiv a\ (mod\ 3^n 2^m)$. This is same solution as for $k = o$.

Similarly it can also be shown that for $k = 13, 14, \dots$. the solutions are the same as for

$k = 1, 2, \dots$, Respectively. Therefore, the congruence has exactly twelve solutions.

Case-II: Let $a = 6l$ be an even positive integer, l being odd positive integer.

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

Then,

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

$\equiv a^3 + 3^{n-1}2^{m-2}k\{(3^{2n-3}2^{m-2}k)^2 + (3^{n-1}2^{m-2}5)^1.a + a^2\}\ (mod\ 2^m3^n)$
$\equiv a^3 + 3^{n-1}2^{m-1}\{(4.9)t\}\ (mod\ 2^m3^n), if\ a = 6l\ is\ even\ positive\ integer$
$\equiv a^3 (mod\ 2^m3^n).$

Thus, $x \equiv 3^{n-2}2^{m-2}k + a\ (mod\ 2^m3^n)$ satisfies the cubic congruence under consideration.
Therefore, it must be a solution of it for some values of k.
If $k = 36 = 4.9$, then, $x \equiv 3^{n-2}2^{m-2}.(9.4) + a = 3^n2^m + a \equiv a\ (mod\ 3^n2^m)$. This is same as $k = o$.
Similarly it can also be shown that for $k = 36, 37, \ldots ..$ the solutions are the same as for
$k = 1, 2, \ldots .,$ Respectively. Therefore, the congruence has exactly thirty-six solutions.

5. ILLUSTRATIONS

Example-2: Consider the congruence $x^3 \equiv 10^3\ (mod\ 5184)$
Here, $5184 = 64.81 = 2^63^4$ & 1000=10^3.
So, the congruence under consideration becomes $x^3 \equiv 10^3\ (mod\ 2^63^4)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)\ with\ a = 10, n = 4, m = 6$.
Here a is an even positive integer.
The twelve solutions are given by

$x \equiv 3^{n-1}2^{m-2}k + a\ (mod\ 3^n2^m) for\ k = 0, 1, 2 \ldots \ldots 11.$
$\equiv 3^{4-1}2^{6-2}k + 10\ (mod\ 2^63^4)$
$\equiv 27.16.k + 10\ (mod\ 64.81)$
$\equiv 432k + 10\ (mod\ 5184)$
$\equiv 2, 442, 874, 1306, 17308, 2170, 2602,$ 3034, 3466, 3898, 4330, 4762 $(mod\ 5184).$

Example-3: Consider the congruence $x^3 \equiv 2^3\ (mod\ 5184)$
Here, $5184 = 64.81 = 2^63^4$.
So, the congruence under consideration becomes $x^3 \equiv 2^3\ (mod\ 2^63^4)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)\ with\ a = 2, n = 4, m = 6$.
Here a is an even positive integer.
The twelve solutions are given by

$x \equiv 3^{n-1}2^{m-2}k + a\ (mod\ 3^n2^m) for\ k = 0, 1, 2 \ldots \ldots 11.$
$\equiv 3^{4-1}2^{6-2}k + 2\ (mod\ 2^63^4)$
$\equiv 27.16.k + 2\ (mod\ 64.81)$
$\equiv 432k + 2\ (mod\ 5184)$
$\equiv 2, 434, 866, 1298, 1730, 2162, 2594,$ 3026, 3458, 3890, 4322, 4754 $(mod\ 5184).$ **Example-5: Consider the congruence $x^3 \equiv 216\ (mod\ 1296)$.**
Here, $1296 = 16.81 = 2^43^4$ & $216 = 6^3$.
So, the congruence under consideration becomes $x^3 \equiv 6^3\ (mod\ 2^43^4)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)\ with\ a = 6 = 3.2, n = 4, m = 4$.
Here, $a = 3l$. So, the congruence has exactly Thirty-six solutions.
The nine solutions are given by

$x \equiv 3^{n-2}2^{m-2}k + a\ (mod\ 3^n2^m) for\ k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots .. 35.$
$\equiv 3^{4-2}2^{4-2}k + 6\ (mod\ 2^43^4)$
$\equiv 9.4.k + 6\ (mod\ 16.81)$
$\equiv 36k + 6\ (mod\ 1296)$
$\equiv 6, 42, 78, 114, 150, 186, 222, 258, 294, 330, 366, 402, 438, 474, 510, 546, \ldots \ldots \ldots .. 1230, 1266\ (mod\ 1296).$

Example-7: Consider the congruence $x^3 \equiv 1728\ (mod\ 2592)$.
Here, 2592= $32.81 = 2^53^4$ & $1728 = 12^3$.
So, the congruence under consideration becomes $x^3 \equiv 12^3\ (mod\ 2^53^4)$.
It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)\ with\ a = 12 = 3.4, n = 4, m = 5$.
Here, $a = 3l, an\ even\ multiple\ of\ three.$
So, the congruence has exactly thirty-six solutions given by

$x \equiv 3^{n-2}2^{m-1}k + a\ (mod\ 3^n2^m) for\ k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots .. 34, 35..$
$\equiv 3^{4-2}2^{5-2}k + 12\ (mod\ 2^53^4)$
$\equiv 9.8.k + 12\ (mod\ 32.81)$
$\equiv 72k + 12\ (mod\ 2592)$
$\equiv 12, 84, 156, 228, 300, \ldots \ldots \ldots \ldots, 2460, 2532\ (mod\ 2592).$

6. CONCLUSION

Thus, it can be concluded that the solvable standard cubic congruence under consideration: $x^3 \equiv a^3\ (mod\ 2^m3^n)$ has exactly three solutions given by
If $a \neq 6l$ is an even positive integer, then the congruence has exactly twelve solutions given by $x \equiv 3^{n-1}2^{m-2}k + a\ (mod\ 2^m3^n)\ with\ k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11.$

If $a = 6l$ is an even positive integer, then the congruence has exactly thirty- six solutions given by $x \equiv 3^{n-2}2^{m-2}k + a \; (mod\; 2^m 3^n) \; with \; k = 0, 1, 2, \dots \dots \dots \dots .. 34, 35$.

REFERENCES

[1] Roy B M, "*Discrete Mathematics & Number Theory*", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.

[2] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.

[3] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to the Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd

[4] Roy B M, *Formulation of two special classes of standard cubic congruence of composite modulus-a power of three*, (IJSRED), ISSN: 2581-7175, Vol-02, Issue-03, May-19.

[5] Roy B M, *Formulation of solutions of a special standard cubic congruence of prime-power modulus*, (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May-19.

[6] Roy B M, *Formulation of solutions of a special standard cubic congruence of composite modulus*, (IJRTI), ISSN: 2456-3315, Vol-04, Issue-06, Jun-19.

[7] Roy B M, *Formulation of a class of standard cubic congruence of composite modulus- a product of power of three &a power of an odd prime*, (IJSDR), ISSN: 2455-2631, Vol-05, Issue-02, Feb-20.