RP-114: A Review and Reformulation of the Formulation of a Class of Solvable 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 review study, the author's previously published paper, "Formulation of a class of solvable standard cubic congruence of even composite modulus" is again considered for formulation. The formula for solutions already obtained by the author is found true as was formulated. It was also found that the congruence had exactly three solutions. But on rigorous review of the paper, the formula for the solutions is modified in terms of odd-even integers. The new formulation 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*: cubic congruence, Chinese Remainder Theorem, Even composite modulus, Review & Reformulation.**

INTRODUCTION

The standard cubic congruence is a part of Number Theory, not much studied. A very little material is found in the literature except the author's formulation of cubic congruence [1] to [9]. Hence, the author wants to study the cubic congruence for the formulation of the solutions. Here is another solvable standard cubic congruence of even composite modulus, the author considered for formulation: $x^3 \equiv a^3 \ (mod\ 2^m 3^n)$.

EXISTED METHOD

The literature of Mathematics says that the said congruence can be easily solved by using CRT (Chinese Remainder Theorem) [10]. In this method, the original congruence can be split into two separate standard cubic congruence as under:

$x^3 \equiv a^3 \ (mod\ 2^m) \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots (1)$

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

Solving these congruence, separate solutions can be obtained (**how?**).

(These congruence can be solved easily by author's published methods).Then, using CRT, the common solutions $i.e.$ solutions of the original congruence can be obtained. It is a time-consuming method.

NEED OF RESEARCH

It is found that the already published paper needs a review and a review is made for the urgent publication through a thorough review study. This is the need of this paper.

There is no alternative of the use of CRT for solutions of the said congruence. An alternative formulation of CRT method is in an urgent need. Also, the previous formulation needs a modification. The author tried his best to develop a modified formulation of this problem as an alternative of CRT and succeed. This is the need of this research paper.

PROBLEM-STATEMENT

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

$in\ two\ cases$:

Case-I: When a is an even positive integer;

Case-II: When a is an odd positive integer.

ANALYSIS & RESULT

The congruence under consideration is: $x^3 \equiv a^3 \ (mod\ 2^m 3^n)$.

Case-I: Let a be an even positive integer.

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

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

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

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

$\equiv a^3 + 3^{n-1}2^{m-2}\{(4.3)t\}, \boldsymbol{if\ a\ is\ even\ positive\ integer}\ \&\ \boldsymbol{m \geq 4},$

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

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 $k = 0, 1, 2, \ldots\ldots, 11, 12, \ldots\ldots$

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 as $k = o$.

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

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

Case-II: Let a be an odd positive integer.

So, as seen in case-I, it cannot be applied for odd positive integer. So, some other formulation is needed. For that, consider

$x \equiv 2^m.3^{n-1}k + a\ (mod\ 2^m.3^n); k = 0, 1, 2,$ which is the same as the previous formulation.These gives only **three** solutions for $k = 0, 1, 2.$

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 $x^3 \equiv a^3\ (mod\ 2^m 3^n)\ with\ a = 3, an\ odd\ positive\ integer;\ n = 3, m = 5.$

Therefore, the congruence has exactly three solutions.

The three solutions are given by $x \equiv 3^{n-1}2^m k + a\ (mod\ 3^n 2^m) for\ k = 0,1,2.$

$\equiv 3^{3-1}2^5 k + 3\ (mod\ 2^5 3^3)$

$\equiv 9.32.k + 3\ (mod\ 32.27)$

$\equiv 288k + 3\ (mod\ 864)$

$\equiv 3, 291, 579\ (mod\ 864)\ for\ k = 0, 1, 2.$

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

$with\ a = 2, an\ even\ positive\ integer;\ n = 4, m = 6.$

It has twelve solutions.

The twelve solutions are given by $x \equiv 3^{n-1}2^{m-2}k + a\ (mod\ 3^n2^m) for\ k = 0,1,2 \ldots \ldots 11.$

$$\equiv 3^{4-1}2^{6-2}k + 2\ (mod\ 2^63^4)$$

$$\equiv 27.16.k + 2\ (mod\ 64.81)$$

$$\equiv 432k + 2\ (mod\ 5184)$$

$$\equiv 2, 434, 866, 1298, 1730,\ 2162, 2594, 3026,$$

$$3458, 3890, 4322, 4754\ (mod\ 5184)$$

$for\ k = 0, 1, 2 \ldots \ldots 11.$

Consider the congruence $x^3 \equiv 343\ (mod\ 864)$.

Here, $864 = 32.27 = 2^53^3$; & $343 = 7^3$.

So, the congruence under consideration becomes $x^3 \equiv 7^3\ (mod\ 2^53^3)$.

It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)\ with\ a = 7, an\ odd\ positive\ integer;\ n = 3, m = 5.$

It has exactly three solutions.

The three solutions are given by $x \equiv 3^{n-1}2^mk + a\ (mod\ 3^n2^m) for\ k = 0,1,2.$

$$\equiv 3^{3-1}2^5k + 7\ (mod\ 2^53^3)$$

$$\equiv 9.32.k + 7\ (mod\ 32.27)$$

$$\equiv 288k + 7\ (mod\ 864)$$

$$\equiv 7, 295, 583\ (mod\ 864)\ for\ k = 0, 1, 2.$$

Consider the congruence $x^3 \equiv 4^3\ (mod\ 2592)$

Here, $2592 = 32.81 = 2^53^4$.

So, the congruence under consideration becomes $x^3 \equiv 4^3\ (mod\ 2^53^4)$.

It is of the type $x^3 \equiv a^3\ (mod\ 2^m3^n)$

$with\ a = 4, an\ even\ positive\ integer;\ n = 4, m = 5.$

It has twelve solutions.

The twelve solutions are given by $x \equiv 3^{n-1}2^{m-2}k + a\ (mod\ 3^n2^m) for\ k = 0,1,2 \ldots \ldots 11.$

$$\equiv 3^{4-1}2^{5-2}k + 2\ (mod\ 2^53^4)$$

$$\equiv 27.8k + 2\ (mod\ 32.81)$$

$$\equiv 216k + 4\ (mod\ 2592)$$

$$\equiv 4, 220, 436, 652, 868, 1084, 1300,1516, 1732,$$

$$1948, 2164, 2380\ (mod\ 2592)$$

$for\ k = 0, 1, 2 \ldots \ldots 11.$

CONCLUSION

Thus, it can be concluded that the standard cubic congruence under consideration is reviewed and formulated by the establishment of the new formula for solutions:

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

Therefore, the congruence has exactly three solutions.

But if a is an even positive integer, the congruence has exactly twelve solutions given by

$$x \equiv 3^{n-1}2^{m-2}k + a \ (mod\ 2^{m}3^{n})\ with\ k = 0, 1, 2, \ldots\ldots, 11, if\ a\ is\ an\ even\ positive.$$

MERIT OF THE PAPER

The standard cubic congruence under consideration is re-formulated without using CRT. Formulation is the merit of the paper. It is a time-saving and simple method.

REFERENCES

[1] Roy B M, Formulation of a class of solvable standard cubic congruence of even composite modulus, International Journal of Advance Research, Ideas and Innovations in Technology(ijariit), issn: 2454-132X ,Vol-05; Issue-01,Jan-Feb-19.

[2] Roy B M, Formulation of a class of standard cubic congruence modulo a positive prime integer multiple of nine, (IJRIAR), ISSN: 2635-3040, Vol-02, Issue-05, Sep-18.

[3] Roy B M, Formulation of solutions of a class of standard cubic congruence modulo r^{th} power of an integer multiple of n^{th} power of even composite modulus, (IJRIAR), ISSN: 2635-3040, Vol-02, Issue-01, Jan-19.

[4] Roy B M, Formulation of solutions of a class of standard cubic congruence of even composite modulus- an r^{th} power of an odd positive integer multiple of n^{th} power of three, (IJRTI), ISSN: 2456-3315, Vol-04, Issue-03, March-19.

[5] Roy B M, Formulation of Two Special Classes of Standard Cubic Congruence of Composite Modulus—a power of three, (IJSRED), ISSN: 2581-2631, Vol-04, Issue-05, May-19.

[6] 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.

[7] Roy B M, Formulation of Solutions of a Special Standard Cubic Congruence of Composite Modulus--an Integer Multiple of Power of Prime, (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-03, May-June-19.

[8] Roy B M, Formulation of standard cubic congruence of even composite modulus, (IJRAR), ISSN:2348-1269, vol-06, Issue-02, Sep-19

[9] Roy B M, Formulation of Standard Cubic Congruence of Composite Modulus- a Multiple of the Power of the Modulus, (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-01, Nov-19.

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