RP-111: Formulation of a class of standard cubic congruence of composite modulus-a product of Power of Three & a power of odd prime

Prof B M Roy

Hon. Ph. D., Hon. D. Sc.
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, the solutions of a class of standard cubic congruence of composite modulus – a product of power of three and a of power of an odd prime- is discussed for formulation. It is found that the author's formulations made the study of standard cubic congruence of composite modulus interesting and simple. No such formulation is found in the literature of mathematics. In this study, the said standard cubic congruence is discussed in various cases for solutions. The discovered formulae are simple and very easy to calculate the solutions. Formulation is the merit of the paper.**

***Keywords*: Cubic congruence, Composite modulus, Formulation, Prime-power.**

INTRODUCTION

The congruence of the type: $x^3 + ax^2 + bx + c \equiv 0\ (mod\ p); p\ being$ a prime positive integer, is called a general cubic congruence of prime modulus. If p is replaced by a composite positive integer, then the congruence is called a general cubic congruence of composite modulus. But the congruence $x^3 \equiv a\ (mod\ m)$, m being a composite positive integer, is a standard cubic congruence of composite modulus. Here in this study, the author discusses the solutions of a new standard cubic congruence of a very special type of composite modulus.

PROBLEM-STATEMENT

The problem is "To formulate the solutions of the standard cubic congruence of composite modulus of the type: $x^3 \equiv 3\ (mod\ 3^m p^n)$ in three different cases:

Case-I: when a is an odd integer and a = p;

Case-II: when a is a multiple of three;

Case-III: when a is any other integer (odd or even).

LITERATURE REVIEW

Referring different books of Number Theory, it is found that only linear and quadratic congruence are discussed prominently. Cubic congruence is not considered for formulation.

Only it is mentioned in [1] that the congruence: $x^3 \equiv a\ (mod\ p)\ , p\ an\ odd\ prime$, is solvable if a is a cubic residue of p and a problem of finding cubic residue of an integer [page-548, supplementary exercises] .

In [2], only a definition of cubic residue of prime p is mentioned for $x^3 \equiv a\ (mod\ p)$,

$p\ an\ odd\ prime\ [page - 136, Problem - 18]$.

The author studied the standard cubic congruence of prime and composite modulus and formulated many such congruence [3], [4], [5], [6], [7], [8], [9], [10].

EXISTED METHOD

Searching for a methods of finding solutions of the said congruence, no formulation or method is found in the literature of mathematics**.** It is also found that Chinese Remainder Theorem can be used to find the required solutions. But it has some demerits.

To use CRT method, one has to solve the individual cubic congruence:

$x^3 \equiv 3\ (mod\ 3^m)$; $x^3 \equiv 3\ (mod\ p^n)$. But again the same difficulties arise here: how to solve these two cubic congruence. No method is found. Only author's formulations are found.

ANALYSIS & RESULT

Case-I: Let us consider $a = p$.

Consider $x = 3^{m-1}p^{n-2}k + a$.

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

$= 3^{3m-3}.p^{3n-6}.k^3 + 3.3^{2m-2}.p^{2n-4}.k^2.a + 3.3^{m-1}.p^{n-2}.k.a^2 + a^3$

$= 3^m p^{n-2}(ka^2 + k^2a.p^{n-2}3^{m-2} + k^3 3^{2m-3}p^{2n-4}) + a^3$

$= 3^m p^{n-2}(kp^2 + k^2p^n 3^{m-2} + k^3 3^{2m-3}p^{2n-2}) + a^3$

$= 3^m p^n(k + k^2p^{n-2}3^{m-2} + k^3 3^{2m-3}p^{2n-4}) + a^3$, if $a = p$.

$\equiv a^3\ (mod\ 3^m p^n)$

Thus, it is seen that $x \equiv 3^{m-1}p^{n-2}k + a\ (mod\ 3^m p^n)$ satisfies the congruence and hence it can be considered a solution of it. But for $k = 3p^2$, the solutions reduces to

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

$\equiv 3^m p^n + a\ (mod\ 3^m p^n)$

$\equiv a\ (mod\ 3^m p^n)$, which is the same solution as for $k = 0$.

For other higher values of k. the solutions repeats as for $k = 1, 2, \ldots \ldots$

Therefore, it can be concluded that the congruence has exactly $3p^2$- solutions for

$k = 0, 1, 2, \ldots \ldots, 3p^2 - 1$.

Case-II: Let a be a multiple of three.

Consider $x = 3^{m-2}p^n k + a$.

Therefore, $x^3 = (3^{m-2}p^n k + a)^3$

$= (3^{m-2}p^n k)^3 + 3.(3^{m-2}p^n k)^2.a + 3.3^{m-2}p^n k.a^2 + a^3$

$= 3^{m-1}p^n k(3^{2m-3}p^{2n}k^2 + 3^{m-2}p^n k.a + a^2) + a^3$

$= 3^{m-1}p^n k(3t) + a^3$, *if a is a multiple of* 3.

$= 3^m p^n kt + a^3$

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

Thus, $x \equiv 3^{m-2}p^n k + a\ (mod\ 3^m p^n)$ is a solution of the said congruence.

But for $k = 9$, the solution becomes $x \equiv 3^{m-2}p^n.9 + a\ (mod\ 3^m p^n)$

$\equiv 3^m p^n + a\ (mod\ 3^m p^n)$

$\equiv a\ (mod\ 3^m p^n)$

Which is the same solution as for $k = 0$.

Also, for other higher values of k, the solutions repeats as for $k = 1, 2, \ldots \ldots$

Therefore, it is concluded that the congruence has nine solutions when a is a multiple of three.

Case-III: Let a be any other positive integer (even or odd).

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

Then, for $x = 3^{m-1}p^n k + a$, $k = 0, 1, 2, 3, 4, \ldots \ldots$

$x^3 = (3^{m-1}p^n k + a)^3$

Expanding using binomial theorem, one get

$x^3 = (3^{m-1}p^n k)^3 + 3.(3^{m-1}p^n k)^2.a + 3(3^{m-1}p^n k)\ \ a^2 + a^3$

$= a^3 + 3^m p^n(\ldots\ldots)$

$\equiv a^3\ (mod\ 3^m p^n)$

Thus, $x = 3^{m-1}p^n k \pm a$ satisfies the congruence and hence is a solution of it.

For $k = 3,\ x = 3^{m-1}p^n.3 + a = 3^m p^n + a \equiv a\ (mod\ 3^m p^n)$ which is same as $k = 0$.

Similarly, for $k = 4, 5$ .... it can be seen that the solutions are the same as for $k = 1, 2$.

Therefore, all the solutions are obtained for $k = 0, 1, 2$.

Hence, the congruence has exactly three solutions.

ILLUSTRATIONS

Consider the congruence $x^3 \equiv 125\ (mod\ 10125)$.

Here, $10125 = 81.125 = 3^4.5^3$

Then the congruence becomes $x^3 \equiv 5^3\ (mod\ 3^4.5^3)$.

It is of the type: $x^3 \equiv a^3\ (mod\ 3^m p^n)\ \ with\ a = 5, m = 4,\ n = 3, p = 5\ with\ \ a = p.$

The p-solutions are given by

$x \equiv 3^{m-1}p^{n-2}k + a\ (mod\ 3^m.5^n) for\ k = 0, 1, 2, 3\ \ldots\ldots\ldots, 3p^2 - 1.$

$\equiv 3^3 5^1 k + 5\ (mod\ 3^4 5^3)$

$\equiv 135k + 5\ (mod\ 10125); k = 0, 1, 2, 3, 4, 5, \ldots\ldots\ldots\ldots, 75 - 1.$

$\equiv\ 0 + 5, 135 + 5, 270 + 5, 405 + 5, 540 + 5, 675 + 5, \ldots\ldots$

$\ldots\ldots\ldots\ldots 9990{+}5\ \ (mod\ 10125).$

$\equiv\ 5, 140, 275, 410, 545, 680, \ldots\ldots\ldots\ldots\ldots\ldots, 9995\ (mod\ 10125).$

Thus the congruence has exactly $3p^2 = 3.25 = 75$ solutions.

Consider the congruence $x^3 \equiv 216\ (mod\ 1323)$.

Here, $1323 = 27.49 = 3^3.7^2$ and $216 = 6^3$.

Then the congruence becomes $x^3 \equiv 6^3\ (mod\ 3^3.7^2)$.

It is of the type: $x^3 \equiv a^3\ (mod\ 3^m p^n)\ \ with\ a = 6, m = 3,\ \ n = 2, p = 7.$

The the solutions are given by

$x \equiv 3^{m-2}p^n k + a\ (mod\ 3^m.7^2) for\ k = 0, 1, 2, \ldots\ldots 8.$

$\equiv 3^1 7^2 k + 6\ (mod\ 3^3 7^2)$

$\equiv 147k + 6\ (mod\ 1323)$

$\equiv\ 0 + 6, 147 + 6, 294 + 6, 441 + 6, 588 + 6, 735 + 6, 882 + 6\ ,$

$1029 + 6, 1176 + 6\ (mod\ 1323).$

$\equiv\ 6, 153, 300, 447, 594, 741, 888, 1035, 1182, (mod 1323\ ).$

Thus the congruence has exactly nine solutions.

Consider the congruence $x^3 \equiv 64\ (mod\ 3375)$.

It can be written as $x^3 \equiv 4^3\ (mod\ 27.125)\ i.e\ x^3 \equiv 4^3\ (mod\ 3^3.5^3)$

It is of the type $x^3 \equiv a^3\ (mod\ 3^m.p^n)$ with $a = 4, m = 3, n = 3, p = 5.$

It has exactly three solutions given by $x \equiv 3^{m-1}p^n k + a \ ; k = 0, 1, 2.$

$$\equiv 3^2 5^3 k + 4 \ (mod\ 3^3.5^3)$$

$$\equiv 1125k + 4 \ (mod\ 27.125)$$

$$\equiv 1125k + 4 \ (mod\ 3375); k = 0, 1, 2.$$

$$\equiv 0 + 4, 1125 + 4, 2250 + 4 \ (mod\ 3375)$$

$$\equiv 4, 1129, 2254 \ (mod\ 3375).$$

These are the required three solutions of the congruence.

Consider the congruence $x^3 \equiv 27 \ (mod\ 1323)$.

It can be written as $x^3 \equiv 3^3 \ (mod\ 3^3 7^2)$.

It is of the type $x^3 \equiv a^3 \ (mod\ 3^m p^n)$.

It has exactly three solutions given by $x \equiv 3^{m-1}p^n k + a \ (mod\ 3^m p^n) \ ; k = 0, 1, 2.$

$$\equiv 3^2 7^2 k + 3 \ (mod\ 3^3 7^2)$$

$$\equiv 9.49k + 3 \ (mod\ 27.49)$$

$$\equiv 441k + 3 \ (mod\ 1323); k = 0, 1, 2.$$

$$\equiv 0 + 3, 441 + 3, 882 + 3 \ (mod\ 1323)$$

$$\equiv 3, 444, 885 \ (mod\ 1323).$$

These are the three solutions.

CONCLUSION

It can be concluded that the congruence under consideration: $x^3 \equiv a^3 \ (mod\ \ 3^m p^n)$

has exactly $3p^2$-solutions given by

$x \equiv 3^{m-1}p^{n-2}k + a \ (mod\ 3^m.5^n) for\ k = 0, 1, 2, 3 \ldots\ldots\ldots, 3p^2 - 1, if\ a = p.$

But if, a is a multiple of three, then it has exactly nine incongruent solutions given by

$x \equiv 3^{n-2}p^n k + a \ (mod\ 3^m p^n); k = 0, 1, 2, \ldots\ldots\ldots, 8$.

The congruence has exactly three incongruent solutions given by

$x \equiv 3^{m-1}.p^n k \pm a \ (mod\ 3^m p^n), k = 0, 1, 2$, if a is any positive integer.

MERIT OF THE PAPER

A new class of standard cubic congruence is formulated. Formulation made the finding of solutions easy. No need to use CRT. Formulation is the merit of the paper. It saves the time of calculations.

REFERENCES

[1] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), page no.548, Academic Press.

[2] Zuckerman H. S., Niven I., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, page no. 147, Wiley India (Pvt) Ltd.

[3] Roy B M, *Formulation of two special classes of standard cubic congruence of composite modulus- a power of three*, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-03, May-19.

[4] Roy B M, *Formulation of solutions of a special standard Cubic congruence of prime-power modulus*, International Journal of Science and Engineering Development Research (IJSDR),ISSN: 2455-2631, Vol-04, Issue-05, May-19.

[5] Roy B M, *Formulation of solutions of a special standard Cubic congruence of composite modulus-an integer multiple of power of prime*, International Journal of Advanced Research, Ideas, and Innovations in Technology (IJARIIT), ISSN: 2454-132, Vol-05, Issue-03, May-Jun-19.

[6] Roy B M, *Formulation of special type of standard Cubic congruence of composite modulus-an odd multiple of power of two*, International Journal for Research Trends and Innovation (IJRTI), ISSN: 2456-3315, Vol-4, Issue-05, May-19.

[7] Roy B M, *Formulation of two special types of standard cubic congruence of composite modulus*, International Journal of Advanced Research, Ideas, and Innovations in Technology (IJARIIT), ISSN: 2454-132, Vol-05, Issue-05, Sep-Oct-19.

[8] Roy B M, *Formulation of standard cubic congruence of even composite modulus*, International Journal of Research and Analytical Reviews (IJRAR), ISSN: 2348-1269, Vol-06, aiassue-02, June-19.

[9] Roy B M, *Formulation of standard cubic congruence of composite modulus-a multiple of the power of the modulus*, International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-01, Oct-19.

[10] Roy B M, *Formulation of Solutions of a standard cubic congruence of composite modulus-an odd multiple of an even integer*, International Journal for Research Trends and Innovation IJRTI), ISSN: 2456-3315, Vol-4, Issue-10, Oct-19.