RP-110: Formulation of Solutions of a Standard Cubic Congruence of Composite Modulus- an Odd Multiple of an even Integer

Prof. B M Roy

M. Sc. (Maths), Hon. Ph. D., Hon. D. Sc.
Head, Department of mathematics
Jagat Arts, commerce & I H P Science College, Gogrgaon
Dist- Gondia, M. S., INDIA, Pin: 441801
(Affiliated to R T M Nagpur University, Nagpur).

***Abstract*: Here, a standard cubic congruence of composite modulus- an odd multiple of an even integer, is considered for study. Knowing that it was not formulated earlier, the author established a formulation for the solutions of the congruence under consideration. A formula is discovered. It is also found that the congruence has exactly four solutions. Formulation is the merit of the paper.**

***Keywords*: Binomial expansion, Cubic congruence, Composite modulus, Formulation.**

INTRODUCTION

A congruence of the type: $x^3 \equiv a \ (mod\ m), m$ being a positive composite integer, is called a standard cubic congruence of composite modulus. Much had not been found about the cubic congruence in the literature of mathematics. A standard cubic congruence of composite modulus is an interesting congruence of study, failed to attract the mathematicians for its discussion. This attracted the author's attention to study the congruence. The author started his study on standard cubic congruence of composite modulus and written many papers on it [3], [4], [5].

Here, the congruence under consideration is of the type: $x^3 \equiv a^3 \ (mod\ 2^m.b^n); b\ an\ odd\ positive\ integer$ with one more speciality that $a\ is\ an\ even\ positive\ integer$.

LITERATURE REVIEW

It is found that a standard cubic congruence of composite modulus is seldom discussed in the literature of mathematics. A very brief discussion is found in the book of Thomas Koshy [1]. Also, Zuckerman had defined a cubic congruence and a cubic residue [2]. But no detailed discussion is found. Recently, the author has written some papers on formulations of such cubic congruence and has been published in different international journals such as:

1) $\boldsymbol{x^3 \equiv a^3 \ (mod\ 2^m 3^n)}$ [3],

2) $\boldsymbol{x^3 \equiv a^3 \ (mod\ 3^n.b^r)}$ [4],

3) $\boldsymbol{x^3 \equiv a^3 \ (mod\ 2^m.3^n.b^r)}$ [5].

Even the author found a special type of standard cubic congruence of composite modulus yet not formulated. The author wished to formulate the said congruence and his efforts are presented in this paper.

PROBLEM-STATEMENT

Here the problem is-

To discover a suitable formula for the solutions of the cubic congruence of composite modulus- an odd multiple of an even integer:

$x^3 \equiv a^3 \ (mod\ 2^m.b^n), b\ being\ an\ odd\ positive\ integer.$

ANALYSIS & RESULT

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

$b\ being\ an\ odd\ positive\ integer.$

If $x \equiv 2^{m-2}.b^n k + a \ (mod\ 2^m.b^n), m \geq 3$; k=0, 1, 2, 3…………, then

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

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

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

$\equiv 2^{m-2}.b^n k(4t) + a^3 \pmod{2^m.b^n}$, if a is an even integer but b an odd positive integer.

$\equiv a^3 \pmod{2^m.b^n}$.

Therefore, it is seen that the said congruence has solutions given by

$x \equiv 2^{m-2}.b^n k + a \pmod{2^m.b^n}; k = 0, 1, 2, 3, 4, 5, 6, \dots \dots \dots.$

But for $k = 4, 5, \dots \dots$

$x \equiv 2^{m-2}.b^n.4 + a \equiv 2^m.b^n + a \equiv a \pmod{2^m.b^n}$,

which is same as for k=0,1, ……..

Therefore, it can be said that the said congruence has exactly four solutions for $k = 0, 1, 2, 3$.

Sometimes the cubic congruence may be of the type: $x^3 \equiv d \pmod{2^m.b^n}$.

It can be written as:

$x^3 \equiv d + k.2^m.b^n = a^3 \pmod{2^m.b^n}$ $for\ a\ fixed\ k, a\ positive\ integer$ [3].

It is also seen in the above analysis that a is always be even positive integer; it cannot be an odd positive integer.

ILLUSTRATION

Consider the congruence $x^3 \equiv 216 \pmod{10976}$.

It can be written as $x^3 \equiv 6^3 \pmod{2^5.343}$ $i.e.$ $x^3 \equiv 6^3 \pmod{2^5.7^3}$

It is of the type $x^3 \equiv a^3 \pmod{2^m.b^n}$

With $m = 5, b = 7, an\ odd\ integer;\ a = 6, an\ even\ positive\ integer.$

By author's formulation, it has exactly four solutions given by

$x \equiv 2^{m-2}.b^n k + a \pmod{2^m.b^n}$

$\equiv 2^{5-2}.343k + 6 \pmod{2^5.343}$

$\equiv 2^3.343k + 6 \pmod{32.343}$

$\equiv 8.343k + 6 \pmod{10976}$

$\equiv 2744k + 6 \pmod{10976}; k = 0, 1, 2, 3.$

$\equiv 6, 2750, 5494, 8238 \pmod{10976}$.

These are the required solutions.

Consider one more example $x^3 \equiv 64 \pmod{5000}$.

It can be written as $x^3 \equiv 4^3 \pmod{2^3.625}$ $i.e.$ $x^3 \equiv 4^3 \pmod{2^3.5^4}$

It is of the type $x^3 \equiv a^3 \pmod{2^m.5^4}$

with $m = 3, b = 5, an\ odd\ integer; a = 4, an\ even\ positive\ integer.$

By author's formulation, it has exactly four solutions given by

$x \equiv 2^{m-2}.b^n k + a \pmod{2^m.b^n}$

$\equiv 2^{3-2}.625k + 4 \ (mod\ 2^3.625\ )$

$\equiv 2^1.625k + 4 \ (mod\ 8.625)$

$\equiv 1250k + 4 \ (mod\ 5000)$

$\equiv 1250k + 4 \ (mod\ 5000); k = 0, 1, 2, 3.$

$\equiv 4, 1254, 2504,\ 3754 \ (mod\ 5000).$

These are the required solutions.

Also consider the congruence $x^3 \equiv 103 \ (mod\ 240)$.

It can be written as $x^3 \equiv 103 + 240 = 343 = 7^3 \ (mod\ 240)$.

It can also be written as $x^3 \equiv 7^3 \ (mod\ 2^4.15)$.

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

$b = 15, m = 4, n = 1.$

So, as per above analysis, we can say that this congruence has no solution.

CONCLUSION

Thus, in the conclusion it can be said that the standard cubic congruence of the type $x^3 \equiv a^3 \ (mod\ 2^m.b^n), b\ odd\ positive\ integer, and\ a\ even\ positive\ integer,$ has exactly four solutions given by

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

MERIT OF THE PAPER

A standard cubic congruence of the type:

$x^3 \equiv a^3 \ (mod\ 2^m.b^n); b\ odd\ positive\ integer, a\ even\ positive\ integer,$ is formulated. A formula for all the solutions is established. The solutions can also be obtained orally using this formulation. This is the merit of the paper.

REFERENCE

[1] Thomas Koshy, 2009, "Elementary Number Theory with Applications", 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.

[2] H S Zuckerman at el, 2008, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

[3] Roy B M, 2016, Discrete Mathematics & Number Theory, First edition, Das Ganu Prakashan, Nagpur (INDIA),ISBN: 978-93-84336-12-7.

[4] **Roy B M, 2019**, Formulation of a class of solvable standard cubic congruence of even composite modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-05, Issue-01, Jan-19.

[5] **Roy B M, 2019**, Formulation of solutions of a class of standard cubic congruence modulo power of an integer multiple of power of three, International Journal of Recent Innovations in Academic Research (IJRIAR), ISSN: 2659-1561, Vol-03, Issue-01, Jan-19.

[6] **Roy B M, 2019**, Formulation of solutions of a class of standard cubic congruence of even composite modulus- a power of an odd positive integer multiple of power of three, International Journal for Research, Trends and Innovations(IJRTI), ISSN:2456-3315,Vol-04, Issue-03, Mar-19.