RESEARCH ARTICLE OPEN ACCESS

RP-115: Formulation of a Class of Standard Cubic Congruence of Even Composite Modulus- an Even-Multiple of a Power of an Odd Prime

Prof B M Roy
Head, Department of Mathematics
Hon. Ph. D., Hon. D. Sc.
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 study, the solutions of a class of standard cubic congruence of even composite modulus- an even multiple of power of prime- isconsidered for study and is formulated. The problem is studied in three different cases. A different formula is developed for each case. The established formulae are tested and found true by citing some examples.No need to use Chinese Remainder Theorem. Here lies the merit of the paper.

KEY-WORDS: Cubic Congruence, Composite modulus, Chinese Remainder Theorem, Formulation.

INTRODUCTION

A congruence of the type: $x^3 \equiv a\ (mod\ m), m\ being$ a composite positive integer, is a standard cubic congruence of composite modulus. If a is a cubic residue of m, then the congruence is solvable [2]. If r is a residue of m, then r^3 is a cubic residue of m [1].

Author already has formulated some standard cubic congruence of composite modulus. Here isone more cubic congruence considered for its formulationentitled "Formulation of solutions of a class of standard cubic congruence of even composite modulus-a power of an even multiple of power of an odd prime.

PROBLEM-STATEMENT

Here, the problem is

"To establish a formulation for the solutions of the standard cubic congruence of the type:

$x^3 \equiv a^3 (mod 2^m . p^n)$;p being an odd positive prime; $m, narepositiveintegers$ in three cases:

Case-I: when a is any even positive integer;

Case-II: when a is an odd positive integer such that $a = p$.

Case-III: when a is any other odd positive integer.

LITERATURE REVIEW

The standard cubic congruence has not been considered and discussed systematically in the literature of mathematics. Much had been written on standard quadratic congruence and a detailed study is found in the literature. Not more literature on cubic congruence is found but only a definition of it [2].

The author's previous formulations of standard cubic congruence of the type are [3], [4], [5], [6], [7].

Here the congruence under consideration is one more cubic congruence of even composite modulus.

ANALYSIS & RESULT

CASE-I: Let a be an even positive integer and the congruence: $x^3 \equiv a^3 (mod\ 2^m p^n)$.

For its solutions, let $x = 2^{m-2}.p^n k + a;\ \ k = 0, 1, 2, 3, 4, 5 \dots \dots \dots$

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

$$= (2^{m-2}.p^n k)^3 + 3.(2^{m-2}.p^n.k)^2.a + 3.2^{m-2}.p^n k.a^2 + a^3$$

$$= a^3 + 2^{m-2}.p^n(\ 2^{2m-4}.p^{2n}k^3 + 2^{m-2}.p^n k^2.3a + 3ka^2)$$

$$\equiv a^3 (mod 2^m.p^n); if\ a\ is\ \ an\ even\ positive\ integer.$$

Thus, it is a solution of the said congruence.

But for $k = 4$, it can be seen easily that $x \equiv a\ (mod 2^m.p^n)$ which gives the same result as for

$k = 0$; similar results are for other higher values of k.

Therefore, it is concluded that the said congruence has only four solutions for $k = 0, 1, 2, 3$.

These solutions are:

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

CASE-II: Let a be an odd positive integer and $a = p\ and$ the congruence: $x^3 \equiv a^3 (mod\ 2^m p^n)$.

For its solutions, let $x = 2^m.p^{n-2}.k + a;\ \ k = 0, 1, 2, 3, 4, 5 \dots \dots \dots$

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

$$= (2^m.p^{n-2}.k)^3 + 3.(2^m.p^{n-2}.k)^2.a + 3.2^m.p^{n-2}k.a^2 + a^3$$

$$= a^3 + 2^m.p^{n-2}.(\ 2^{2m}.p^{2n-4}k^3 + 2^m.p^{n-2}k^2.3a + 3ka^2)$$

$$= a^3 + 2^m.p^n.(t); if\ a = p.$$

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

Thus, it is a solution of the said congruence.

But for k = p^2 the solutions are

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

 ©IJSRED: All Rights are Reserved

$\equiv 2^m.p^n + a \equiv a\ (mod\ 2^m.p^n)$which is the same result as for k = 0.

Similarly for other values of k = p^2+1, p^2 +2, ……., the same result is obtained as for k = 1, 2, ……

These are the p^2- solutions of the congruence $k = 0, 1, 2, \dots\dots\dots, p^2 - 1$.

Case-III: Let a be any other odd positive integer.

Then it is found that the cubic congruence $x^3 \equiv a^3(mod 2^m.p^n)$ has only one solution

$x \equiv a\ (mod 2^m.p^n)$; it has no other solution.

ILLUSTRATION

Consider the congruence: $x^3 \equiv 8\ (mod\ 96)$

It can be written as $x^3 \equiv 8\ (mod\ 32.3) i.e.\ x^3 \equiv 2^3(mod 2^5.3)$.

It is of the type: $x^3 \equiv a^3(mod 2^m.p^n) with a = 2, n = 1, m = 5$.

Such congruence has four solutions.

The solutions are given by $x \equiv 2^{m-2}.p^n k + a\ (mod 2^m.p^n)$

$$\equiv 2^{5-2}.3k + 2\ (mod 2^5.3^1)$$

$$\equiv 24k + 2\ (mod\ 96) with k = 0, 1, 2, 3.$$

$$\equiv 0 + 2, 24 + 2, 48 + 2, 72 + 2\ (mod\ 96)$$

$$\equiv 2, 26, 50, 74\ (mod\ 96).$$

Consider the congruence: $x^3 \equiv 216\ (mod\ 576)$.

It can also be written as:$x^3 \equiv 6^3\ (mod 2^6.3^2)$

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

Such congruence always has four solutions.

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

$$\equiv 2^{6-2}.3^2 k + 6\ \ (mod 2^6.3^2)$$

$$\equiv 144k + 6\ (mod 64.9) with k = 0, 1, 2,3.$$

$$\equiv 0 + 6, 144 + 6; 288 + 6; 432 + 6\ (mod\ 64.9)$$

≡6, 150, 294, 438 (mod 576).

Consider the congruence $x^3 \equiv 343\ (mod\ 38416)$.

It can be written as $x^3 \equiv 343\ = 7^3\ (mod 2^4.7^4)$

 ©IJSRED: All Rights are Reserved

It is of the type $x^3 \equiv a^3 (mod 2^m.p^n) with a = 7, m = 4, n = 4.$

It has p=$7^2 = 49$ solutions given by

$$x \equiv 2^m.p^{n-2}.k + a(mod 2^m.p^n), \qquad k = 0, 1, 2 \dots \dots .., 48.$$

$$\equiv 2^4.7^2.k + 7\ (mod\ 2^4.7^4)$$

$$\equiv 784k + 7\ (mod\ 38416)$$

$$\equiv 7, 791, 1575, 2359, \qquad 3143, \dots \dots \dots \dots 37639\ \ (mod\ 38416).$$

Consider the congruence $x^3 \equiv 125\ (mod\ 576)$.

It can be written as $x^3 \equiv 5^3\ (mod 2^6.3^2)$

It is of the type $x^3 \equiv a^3 (mod 2^m.p^n) with a = 5, m = 6, n = 2.$

It has single solution given by $x \equiv a(mod 2^m.p^n)$.

$$\equiv 5\ (mod\ 576).$$

CONCLUSION

Therefore, it can be concluded that the standard cubic congruence of the type:

$x^3 \equiv a^3 (mod 2^m.p^n); p$any odd prime integer, has exactly four solutions given by

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

But if a is an odd positive integer and a=p, then the p^2-solutions are given by

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

Then it has exactly p^2-solutions.

If a is any other odd positive integer, then the congruence has unique solution $x \equiv a\ (mod\ 2^m p^n)$.

MERIT OF THE PAPER

In this paper, a class of standard cubic congruence of the said type is considered for study and aformulation is established to find all the solutions. The problem is discussed in different cases.It is the merit of the paper.

REFERENCE

1. Thomas Koshy, 2009, "*Elementary Number Theory with Applications*", 2/e (Indian print), Academic Press, Page No. 548, supplementary Exercises No.4,ISBN: 978-81-312-1859-4.

 ©IJSRED: All Rights are Reserved

2. Zuckerman H. S., Niven I., Montgomery H. L. 1960(Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, Page No. 136-136, Exercise-18,ISBN: 978-81-265-1811-1.
3. Roy, B. M., Formulation of solutions of a class of standard cubic congruence of even composite modulus, Research Journal of Mathematical and Statistical Sciences,(RJMSS-ISCA), Vol-7 (2), ISSN: 2320-6047, page:30-32, May-19.
4. Roy, B. M.(2018), *Formulation of solutions of a class of standard cubic congruence modulo nth power of three, International Journal for Research Under Literal Access(IJRULA),* Vol. 01, Issue-08, Page No. 254-257, www.ijrula.com
5. Roy, B. M. (2018)*Formulation of solutions of a class of standard cubic congruence modulo an integer multiple of nth power of three, International Journal for Research Under Literal Access* (IJRULA), Vol.01, Issue-09, Page No. 297-300, www.ijrula.com
6. Roy, B. M.(2019), *Formulation of solutions of a class of standard cubic congruence modulo rth power of an integer multiple of nth power of three, International Journal of Recent Innovations In Academic research (*IJRIAR), Vol. 03, Issiue-1,https://www.ijriar.com/docs , ISSN(online): 2635-3040, ISSN(print): 2659-1561.
7. Roy, B M, *Formulation of solutions of a class of standard cubic congruence of even composite modulus*, Research Journal of Mathematical and Statistical Sciences,(RJMSS-ISCA), Vol-7 (2), ISSN: 2320-6047, page:30-32, May-19.

……………………………………………………………………xxx……………………………………………………………………