iJETRM
International Journal of Engineering Technology Research & Management

RP-161: FORMULATION OF SOLUTIONS OF STANDARD CUBIC CONGRUENCE MODULO SQUARE OF ODD PRIME MULTIPLIED BY POWERED EVEN PRIME

Prof B M Roy
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist-Gondia, M. S., India. Pin: 441801

ABSTRACT

Here in this paper, the author considered a special type of standard cubic congruence for study. After a rigorous study, the author has formulated the solutions of the standard cubic congruence modulo a powered odd prime multiplied by a powered even prime.

It is found that the said congruence has exactly $p^2 -$ incongruent solutions, p being an odd prime present in the congruence. A formula is established for the solutions. This is the first time a formula is provided for solutions of such congruence.

KEY-WORDS

Cubic congruence, Chinese Remainder Theorem, Composite modulus.

INTRODUCTION

A standard cubic congruence of the type:$x^3 \equiv b\ (mod\ m)$, has different number of solutions depending upon the modulus m. If $b \equiv a^3\ (mod\ m)$, then b is called cubic residue of m; a being the residue of m and the congruence reduces to $x^3 \equiv a^3\ (mod\ m)$ and is always solvable [1].

Here the author considered a special type of cubic congruence having p^2 incongruent solutions where p is an odd prime present in the cubic congruence.

PROBLEM-STATEMENT

Here the problem is "To study the solutions of the standard cubic congruence of composite modulus of the type:

$$x^3 \equiv p^3(mod\ 2^m.p^2), p\ an\ odd\ prime, m\ a\ positive\ integer."$$

LITERATURE REVIEW

The author already has formulated the standard cubic congruence: $x^3 \equiv p^3(mod\ p^2)$, $p\ an\ odd\ prime$. It has exactly p- incongruent solutions given by $x \equiv pk + p\ (mod\ p^2)$ [2] . The author also formulated the congruence $x^3 \equiv p^3\ (mod\ 2^m.3^n)$in different cases [3]. The author already has formulated some related standard cubic congruence of composite modulus [4], [5].

Now the author insisted to formulate the congruence$x^3 \equiv p^3(mod\ 2^m p^2)$.

iJETRM
International Journal of Engineering Technology Research & Management

EXISTED METHOD

It is found that there is no proper and suitable method to find the solutions of a standard cubic congruence of composite modulus. But David M Burton used the theory of indices to find the solutions of cubic congruence [6**]**.No Formulationis found for the solutions. Hence the author aimed to formulate the solutions of the congruence.

ANALYSIS & RESULT

Consider the congruence $x^3 \equiv p^3 (mod\ 2^m.p^2), p\ an\ odd\ prime, m\ a\ positive\ integer.$

For solutions, consider $x \equiv 2^m pk + p\ (mod\ 2^m.p^2)$.

Then $x^3 \equiv (2^m pk + p)^3 (mod\ 2^m.p^2)$.

$$\equiv (2^m pk)^3 + 3.(2^m pk)^2.p + 3.2^m pk.p^2 + p^3\ (mod\ 2^m.p^2)$$
$$\equiv 2^{3m} p^3 k^3 + 3.2^{2m}.p^2 k^2.p + 3.2^m pk.p^2 + p^3\ (mod\ 2^m p^2)$$
$$\equiv 2^m p^3 k(2^{2m} k^2 + 3.2^m k + 3\ ) + p^3\ (mod\ 2^m.p^2)$$
$$\equiv 0 + p^3\ (mod\ 2^m p^2)$$
$$\equiv p^3 (mod\ 2^m p^2).$$

Therefore, $x \equiv 2^m pk + p\ (mod\ 2^m.p^2)$ satisfies the cubic congruence and hence it gives the solutions of the congruence.

But if $k = p$, then the solutions formula reduces to

$$x \equiv 2^m p^2 + p\ (mod\ 2^m.p^2)$$

$\equiv 0 + p(mod\ 2^m p^2)$.

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

Also, for $k = p + 1$, then the solutions formula reduces to

$$x \equiv 2^m p.(p + 1) + p\ (mod\ 2^m.p^2)$$
$$\equiv 2^m p^2 + 2^m p + p\ (mod\ 2^m p^2)$$

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

This is the same solution as for $k = 1$.

Therefore, all the solutions are given by

$x \equiv 2^m pk + p\ (mod\ 2^m.p^2); k =, 1, 2, 3, \ldots\ldots, (p - 1)$.

ILLUSTRATIONS

Example-1: Consider the congruence: $x^3 \equiv 125\ (mod\ 400)$.

It can be written as $x^3 \equiv 5^3 (mod\ 2^4.5^2)$.

It is of the type $x^3 \equiv p^3 (mod\ 2^m.p^2)\ with\ p = 5, m = 4$.

It has exactly $p = 5$ incongruent solutions given by

$$x \equiv 2^m pk + p\ (mod\ 2^m p^2); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, (p - 1).$$
$$\equiv 2^4.5k + 5\ (mod\ 2^4.5^2); k = 0, 1, 2, 3,4.$$
$$\equiv 80k + 5\ (mod\ 400); k = 0, 1, 2, 3,4.$$
$$\equiv 5, 85, 165, 245, 325, (mod\ 400).$$

Example-2: Consider the congruence: $x^3 \equiv 343\ (mod\ 1568)$.

It can be written as $x^3 \equiv 7^3 (mod\ 2^5.7^2)$.

iJETRM
International Journal of Engineering Technology Research & Management

It is of the type $x^3 \equiv p^3 (mod\ 2^m . p^2)\ with\ p = 7, n = 5.$
It has exactly $p = 7$ incongruent solutions given by

$$x \equiv 2^m pk + p\ (mod\ 2^m p^2); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, (p-1).$$
$$\equiv 2^5 . 7k + 7\ (mod\ 2^5 . 7^2); k =, 1, 2, 3, \ldots\ldots\ldots .6.$$
$$\equiv 224k + 7\ (mod\ 1568); k = 0, 1, 2, 3, \ldots\ldots, 6.$$
$$\equiv 7, 231, 455, 679, 903, \quad 1127, 1351\ (mod\ 1568).$$

CONCLUSION

Therefore it is concluded that the cubic congruence:
$x^3 \equiv p^3 (mod\ 2^m p^2), p\ an\ odd\ prime$has exactlyp - incongruent solutions given by

$$x \equiv 2^m pk + p\ (mod\ 2^m p^2); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, (p-1).$$

MERIT OF THE PAPER

A formulation is provided to the readers and finding of solutions of the cubic congruence become interesting. This is the merit of the paper.

REFERENCE

[1] Thomas Koshy,2009,*Elementary Number Theory with Applications*, Academic Press (An Imprint of Elsevier), Second Indian edition, ISBN: 978-81-312-1859-4.
[2]Roy B M,*Formulation of standard cubic congruence of composite modulus modulo a powered even prime multiplied by a powered three in two special case***,**International Journal for Research Technology and Innovations (IJRTI),ISSN: 2456-3315, Vol-05, Issue-09, Sep-20.
[3] Roy B M, *Formulation of standard cubic congruence of composite modulus modulo a product of odd primes and nth power of three*, International Journal of Engineering Technology Research and Management (IJETRM), ISSN:2456-9348, Vol-04, Issue-10, Oct-20.
[3]Roy B M, *A review and reformulation of solutions of standard cubic congruence of composite modulus modulo an odd prime power integer*, (IJSDR), ISSN:2455-2631,Vol-05, Issue-12, Dec-20.
[4] Roy B M,*Solving some special standard cubic congruence modulo an odd prime multiplied by eight*, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-04, Issue-01, Jan-21.
[5] Roy B M,*Formulation of solutions of standard cubic congruence modulo an odd prime multiple of nth power ofanother odd prime***,** International Journal for Research Technology and Innovations (IJRTI),ISSN: 2456-3315, Vol-06, Issue-02, Feb-21.
[6] David M Burton, 2012, *Elementary Number Theory*, Seventh Indian edition, McGraw Hill Education (India) Private limited, New Delhi, ISBN: 978-1-25-902576-1.