RP-156: Formulation of solutions of standard cubic congruence modulo an odd prime multiple of nth power of another odd prime

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon
Dist-Gondia M. S., India.

Abstract: In this paper, the author has formulated the solutions of a class of standard cubic congruence of composite modulus modulo an odd prime multiple of nth power of another odd prime. The effort for the formulation is presented here. This cubic congruence has exactly p^2 incongruent solutions, where p is an odd prime. The formula is tested and verified true. Several numerical examples are presented here. The solutions are obtained using the established formula. Formulation is the merit of the paper.

Keywords: ***Cubic Congruence, Composite Modulus, Cubic Residue, Formulation, Incongruent solutions.***

INTRODUCTION

If m is an odd prime integer, then the congruence $x^3 \equiv a\ (mod\ m)$ is called a standard cubic congruence of prime modulus. If m is a composite positive integer, then the congruence is termed as a standard cubic congruence of composite modulus. Also, if a is cubic residue of the modulus, then the congruence is solvable. If the congruence is solvable. Then a can be written as $r^3 \equiv a\ (mod\ m), r\ being\ a\ residue\ of\ m.$

$In\ this\ case\ the\ solvable$ Congruence can be written as: $x^3 \equiv r^3\ (mod\ m)$.

In this paper the author considered the congruence: $x^3 \equiv p^3\ (mod\ p^n q)$ for formulation of its solutions, with $n \geq 2$.

PROBLEM-STATEMENT

Here the problem is-"To formulate the solutions of the standard cubic congruence of the type:

$x^3 \equiv p^3\ (mod\ p^n q), p\ \&\ q\ being\ odd\ primes$

in two cases:

Case-I: $n \geq 3$;

Case-II: $n = 2$.

LITERATURE REVIEW

In the literature of mathematics, no literature is found about the solving of standard cubic congruence of prime and composite modulus. Only a definition is seen in the book of Zuckerman [1]. Thomas Koshy had defined only a cubic residue, page-548 [2]. David M Burton [3] in his book: "Elementary Number Theory", in the page no. 166, used the Theory of Indices to solve standard cubic congruence of prime modulus but established no formula for solutions. No pre-formulation is found for the congruence considered here. Only the author's formulations on standard cubic congruence of composite modulus are found in the literature of mathematics [4], [5], [6], [7]. Here is one more standard cubic congruence of composite modulus is considered for formulation of solutions.

ANALYSIS & RESULT

Case-I: $n \geq 3$.

Consider the congruence under consideration:

$x^3 \equiv p^3 (mod\ p^n q); n \geq 3;\ p\ \&\ q\ being\ an\ odd\ primes.$

For solutions, consider $x \equiv p^{n-2} qk + p\ (mod\ p^n q)$.

Then, $x^3 \equiv (p^{n-2} qk + p\ )^3\ (mod\ p^n q)$

$\equiv (\ p^{n-2} qk\ )^3 + 3.(p^{n-2} qk\ )^2 . p + 3. p^{n-2} qk . p^2 + p^3\ (mod\ p^n q)$

$$\equiv p^{3n-6}q^3k^3 + 3p^{2n-3}q^2k^2 + 3p^nqk + p^3 (mod\ p^nq)$$

$$\equiv p^nqk(p^{2n-6}q^2k^2 + 3p^{n-3}qk + 3) + p^3 (mod\ p^nq)$$

$$\equiv p^3\ (mod\ p^nq)$$

Thus it is seen that $x \equiv p^{n-2}qk + p\ (mod\ p^nq)$ satisfies the cubic congruence and hence must give all the solutions.

But it is seen that for $k = p^2$, the solution formula reduces to:

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

$$\equiv p^nq + p\ (mod\ p^nq)$$

$$\equiv p\ (mod\ p^nq)$$

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

Also if $k = p^2 + 1$, then the solution formula reduces to:

$$x \equiv p^{n-2}.q.(p^2 + 1) + p\ (mod\ p^nq)$$

$$\equiv p^nq + p^{n-2}q + p\ (mod\ p^nq)$$

$$\equiv p^{n-2}q + p\ (mod\ p^nq)$$

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

Therefore, all the solutions are given by:

$x \equiv p^{n-2}qk + p\ (mod\ p^nq); k = 0, 1, 2, \dots\dots, (p^2 - 1)$.

This gives $p^2\ incongruent\ solutions\ of\ the\ congruence$.

Therefore, the result of this discussion is that the standard cubic congruence of composite modulus: $x^3 \equiv p^3\ (mod\ p^nq)$ has p^2 solutions given by:

$x \equiv p^{n-2}qk + p\ (mod\ p^nq); k = 0, 1, 2, \dots\dots, (p^2 - 1)$.

Case-II: $n = 2$.

Then the said congruence reduces to:

$x^3 \equiv p^3\ (mod\ p^2q)$.

It is found that for the solutions, $x \equiv pqk + p\ (mod\ p^2q)$ is considered and found that it gives all the solutions of the congruence.

But for $k = p$, the formula reduces to $x \equiv pqp + p\ (mod\ p^2q)$

$$\equiv p^2q + p\ (mod\ p^2q)$$

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

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

Also, $for = p + 1$, the solution is the same as for $k = 1$.

Therefore, it is concluded that all the solutions are given by

$x \equiv pqk + p\ (mod\ p^2q); k = 0, 1, 2, 3, \dots\dots\dots\dots, (p - 1)$.

This gives only p incongruent solutions of the congruence.

ILLUSTRATIONS

Example-1: Consider the congruence $x^3 \equiv 343\ (mod\ 1715)$.

It can be written as: $x^3 \equiv 7^3\ (mod\ 7^3.5)\ with\ p = 7, q = 5$.

It is of the type: $x^3 \equiv p^3\ (mod\ p^3.q); n = 3$.

The solutions are given by

$x \equiv p^{n-2}qk + p \ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots, (p^2 - 1).$

$\equiv 7^{3-2}.5k + 7 \ (mod\ 7^3.5); k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p^2 - 1)$

$\equiv 7.5k + 7 \ (mod\ 7^2.5); k = 0, 1, 2, \ldots\ldots\ldots\ldots\ldots\ldots, (7^2 - 1)$

$\equiv 35k + 7 \ (mod\ 1715); k = 0, 1, 2, \ldots\ldots\ldots\ldots 48.$

≡7, 42, 77, 112, 147, ……,1687 (mod 1715).

These are the $p^2 = 49$ solutions of the congruence.

Example-2: Consider the congruence $x^3 \equiv 343 \ (mod\ 7203)$.

It can be written as: $x^3 \equiv 7^3 \ (mod\ 7^4.3)\ with\ p = 7, q = 3,\ n = 4.$

It is of the type: $x^3 \equiv p^3 \ (mod\ p^n.q); n = 4.$

The solutions are given by

$x \equiv p^{n-2}qk + p \ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots, (p^2 - 1).$

$\equiv 7^{4-2}.3k + 7 \ (mod\ 7^4.3); k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p^2 - 1)$

$\equiv 7^2.3k + 7 \ (mod\ 7^4.3); k = 0, 1, 2, \ldots\ldots\ldots\ldots\ldots\ldots, (p^2 - 1)$

$\equiv 147k + 7 \ (mod\ 7203); k = 0, 1, 2, \ldots\ldots\ldots 48.$

≡7, 154, 301, 448,595, ……,7063 (mod 7203).

These are the $p^2 = 49$ solutions of the congruence.

Example-3: Consider the congruence $x^3 \equiv 343 \ (mod\ 245)$.

It can be written as: $x^3 \equiv 7^3 \ (mod\ 7^2.5)\ with\ p = 7, q = 5,\ n = 2.$

It is of the type: $x^3 \equiv p^3 \ (mod\ p^2.q).$

The solutions are given by

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

$\equiv 7.5k + 7 \ (mod\ 7^2.5); k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p - 1)$

$\equiv 35k + 7 \ (mod\ 245); k = 0, 1, 2, \ldots\ldots\ldots, 6.$

≡7, 42, 77, 112, 147,182, 217 (mod 245).

These are the $p = 7$ solutions of the congruence.

CONCLUSION

Therefore, it is concluded that the standard cubic congruence of composite modulus:

$x^3 \equiv p^3 \ (mod\ p^n q), n \geq 3$ has exactly $p^2 -$ incongruent solutions, given by

$x \equiv p^{n-2}qk + p \ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots, (p^2 - 1), p$ being an odd prime.

But for $n = 2$, the solutions are given by $x \equiv pqk + p \ (mod\ p^2 q); k = 0, 1, 2, \ldots\ldots, (p - 1).$

These are p - solutions.

MERIT OF THE PAPER

Here the author has formulated a very nice standard cubic congruence. Using the formula, all the solutions are obtained very easily. It is time saving. This is the merit of the paper.

REFERENCES

[1] Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.

[2]Thomas Koshy, 2009, *Elementary Number Theory and Applications*, Academic Press, An Imprint of Elsevier, New Delhi, Second edition (Indian Print), ISBN: 978-81-312-1859-4.

[3]David M. Burton, *Elementary Number Theory*, McGraw Hill Education (India) private limited, New Delhi, Seventh Indian edition, ISBN: 978-1-25-902576-1.

[4] B M Roy, *Formulation of two special classes of standard cubic congruence of composite modulus-a power of three*, (IJSRED), ISSN: 2581-7175, Vol-02, Issue-03, May-19.

[5] B M Roy, *Formulation of solutions of special standard cubic congruence of prime-power modulus*, (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May-19.

[6] B M Roy, *Formulation of solutions of standard cubic congruence of even composite modulus-an eighth multiple of nth power of three*, International Journal of (IJSRED), ISSN: 2581-7175, Vol-03, Issue-04, Jul-20.

[7] B M Roy**,** *Formulation of standard cubic congruence of composite modulus modulo a product of odd prime and nth power of three*, International Journal of (IJETRM), ISSN: 2456-9348, Vol-04, Issue-10, Oct-20.