RP-162: Formulation of solutions of a special standard cubic congruence of composite modulus modulo a special multiple of *square* of an odd prime

Prof. B M Roy

Head, Department of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon
Dist - Gondia M. S., India. PIN: 441801.

***Abstract*: In this paper, the author has formulated the solutions of a special standard cubic congruence of composite modulus modulo a special multiple of square of an odd prime. The effort for the formulation is presented here. This cubic congruence has exactly p incongruent solutions, where p is an odd prime present in the congruence. The formula is tested and verified true. Several numerical examples are solved here. The solutions are obtained using the established formula. No Need to use Chinese Remainder Theorem (CRT).Formulation is the merit of the paper.**

***Keywords*: Cubic congruence, cubic residues, Chinese Remainder Theorem (CRT), Odd primes, Formulation.**

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 standard cubic congruence of special composite modulus having p- incongruent solutions where p is an odd prime present in the congruence.

PROBLEM-STATEMENT

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

(1) $x^3 \equiv p^3\ (mod\ p^2)$; p odd prime,

(2) $x^3 \equiv p^3\ (mod\ p^2.q); p, q\ being\ different\ odd\ primes."$

(3) $x^3 \equiv p^3\ (mod\ p^2.3^n)$; p odd prime and n is any positive integer.

LITERATURE REVIEW

It is seen that cubic congruence are not studied in universities. Most of the Number Theory syllabus contains linear and quadratic congruence of prime modulus [1], [2], [3]. So no discussion is found in the literature of mathematics. But Zukerman [3], Koshy [2] had taken a bold attempt to define a congruence and cubic residues. But online searching provides many research formulations of the author only on cubic congruence of composite modulus [4], [5], [6], [7].

ANALYSIS & RESULTS

Case-I: Consider the congruence: $x^3 \equiv p^3\ (mod\ p^2)$, o being an odd prime.

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

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

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

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

$\equiv p^3\ (mod\ p^2)$

So, $x \equiv pk + p\ (mod\ p^2)$ satisfies the congruence and hence gives all the solutions for different k.

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

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

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

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

Also, for $k = p + 1$, similarly it is seen that the solution formula reduces to

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

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

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

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

Therefore, all the solutions are given by $x \equiv pk + p\ (mod\ p^2)k, k = 0, 1, 2, \dots \dots, (p - 1)$.

Case-II:

Consider the congruence: $x^3 \equiv p^3\ (mod\ p^2.q); p, q\ being\ different\ odd\ prime."$

For solutions, let $x \equiv pqk + p\ (mod\ p^2q)$.

Then, $x^3 \equiv (pqk + p)^3 \ (mod\ p^2q)$
$\equiv p^3q^3k^3 + 3.p^2q^2k^2.p + 3.pqk.p^2 + p^3 \ (mod\ p^2q)$
$\equiv p^3k(k^2 + 3k + 3) + p^3 \ (mod\ p^2q)$
$\equiv p^3 \ (mod\ p^2q)$
So, $x \equiv pqk + p \ (mod\ p^2q)$ satisfies the congruence and hence gives all the solutions for different k.
But for$k = pq$, the solutions formula reduces to $x \equiv p.p + p \ (mod\ p^2q)$
$\equiv p^2 + p \ (mod\ p^2q)$
$\equiv 0 + p \ (mod\ p^2q)$.
This is the same solution as for $k = 0$.
Also, for $k = pq + 1$, similarly it is seen that the solution formula reduces to
$x \equiv p.pq + pq + p \ (mod\ p^2q)$
$\equiv p^2q + pq + p \ (mod\ p^2q)$
$\equiv pq + p \ (mod\ p^2q)$.
This is the same solution as for $k = 1$.
Therefore, all the solutions are given by $x \equiv pqk + p \ (mod\ p^2q)k$,
$k = 0, 1, 2, \dots \dots, (p - 1)$.

Case-III:
Consider the congruence:
$x^3 \equiv p^3 \ (mod\ 3^n.p^2); p\ being\ odd\ odd\ prime, n\ any\ positive\ integer.$
For solutions, let $x \equiv 3^{n-1}.pk + p \ (mod\ 3^n.p^2)$.
Then, $it\ is\ also\ seen\ that$ the solutions formula: $x \equiv 3^{n-1}pk + p \ (mod\ 3^n.p^2)$ satisfies the congruence and hence gives all the solutions for different k.
But for $k = 3p$, the solutions formula reduces to $\equiv 0 + p \ (mod\ 3^n.p^2)$.
This is the same solution as for $k = 0$. Similarly, it is seen that the solution formula reduces to $x \equiv 3^{n-1}pk + p \ (mod\ 3^np^2)$ for $k = 3p + 1$.
This is the same solution as for $k = 1$.
Therefore, all the solutions are given by $x \equiv 3^{n-1}pk + p \ (mod\ 3^np^2)k$,
$k = 0, 1, 2, \dots \dots, (3p - 1)$.

ILLUSTRATIONS
Example-I: Consider the congruence $x^3 \equiv 125 \ (mod\ 25)$.
It can be written as $x^3 \equiv 5^3 \ (mod\ 5^2)$
It is of the type: $x^3 \equiv p^3 \ (mod\ p^2)$.
It has exactly p=5 solutions.
The solutions are given by
$x \equiv pk + p \ (mod\ p^2); k = 0, 1, 2, \dots \dots \dots, (p - 1)$.
$\equiv 5k + 5 \ (mod\ 5^2); k = 0, 1, 2, \dots \dots \dots, 5 - 1)$
$\equiv 5k + 5 \ (mod\ 25); k = 0, 1, 2, \dots \dots \dots, 4$.
$\equiv$ 5, 10, 15, 20, 25 (mod 25).
Example-2: Consider the congruence $x^3 \equiv 343 \ (mod\ 539)$.
It can be written as: $x^3 \equiv 7^3 \ (mod\ 7^2.11)\ with\ p = 7, q = 11,\ n = 2$.
It is of the type: $x^3 \equiv p^3 \ (mod\ p^2.q)$.
The solutions are given by
$x \equiv pqk + p \ (mod\ p^2q); k = 0, 1, 2, \dots \dots \dots, (p - 1)$.
$\equiv 7.11k + 7 \ (mod\ 7^2.11); k = 0, 1, 2, \dots \dots \dots, p - 1)$
$\equiv 7.11k + 7 \ (mod\ 7^2.11); k = 0, 1, 2, \dots \dots \dots \dots \dots, (7 - 1)$
$\equiv 77k + 7 \ (mod\ 539); k = 0, 1, 2, \dots \dots \dots .6$.
$\equiv$ 7, 84, 161, 238, 315, 392, 469 (mod 539).
These are the $p = 7$ solutions of the congruence.
Example-3: Consider the congruence $x^3 \equiv 125 \ (mod\ 325)$.
It can be written as: $x^3 \equiv 5^3 \ (mod\ 5^2.13)\ with\ p = 5, q = 13$.
It is of the type: $x^3 \equiv p^3 \ (mod\ p^2.q)$.
The solutions are given by
$x \equiv pqk + p \ (mod\ p^2q); k = 0, 1, 2, \dots \dots \dots, (p - 1)$.
$\equiv 5.13k + 5 \ (mod\ 5^2.13); k = 0, 1, 2, \dots \dots \dots, (5 - 1)$
$\equiv 65k + 5 \ (mod\ 325); k = 0, 1, 2, 3, 4$.
$\equiv$5, 70, 135, 200, 265 (mod 325).
These are the $p = 5$ solutions of the congruence.
Example-4: Consider the congruence $x^3 \equiv 1331 \ (mod\ 1573)$.
It can be written as: $x^3 \equiv 11^3 \ (mod\ 11^2.13)\ with\ p = 11, q = 13$.
It is of the type: $x^3 \equiv p^3 \ (mod\ p^2.q)$.
The solutions are given by

$x \equiv pqk + p\ (mod\ p^2q); k = 0, 1, 2, \dots\dots\dots., (p-1).$
$\equiv 11.13k + 11\ (mod\ 11^2.13); k = 0, 1, 2, \dots\dots\dots., (11-1)$
$\equiv 143k + 11\ (mod\ 1573); k = 0, 1, 2, 3, \dots\dots\dots\dots\dots\dots\dots\dots., 10.$
≡11, 154, 297, 440, 583, 726, 869, 1012, 1155, 1298, 1441 (mod 1573).
These are the $p = 11$ solutions of the congruence.
Example-5: Consider the congruence $x^3 \equiv 1331\ (mod\ 1089)$.
It can be written as: $x^3 \equiv 11^3\ (mod\ 3^2.11^2)\ with\ p = 11.$
It is of the type: $x^3 \equiv p^3\ (mod\ 3^n.p^2)$.
The solutions are given by
$x \equiv 3^{n-1}pk + p\ (mod\ 3^n.p^2); k = 0, 1, 2, \dots\dots\dots., (3p-1).$
$\equiv 3.11k + 11\ (mod\ 11^2.13); k = 0, 1, 2, \dots\dots\dots., (11-1)$
$\equiv 33k + 11\ (mod\ 1089); k = 0, 1, 2, 3, \dots\dots\dots\dots\dots\dots\dots\dots., 32.$
≡11, 154, 297, 440, 583, 726, 869, 1012, 1155, 1298, 1441 (mod 1089).
These are the $3p = 3.11 = 33$ solutions of the congruence.

CONCLUSION

Therefore, it is concluded that the standard cubic congruence: $x^3 \equiv p^3\ (mod\ p^2)$, p being different odd prime, has exactly p incongruent solutions given by
$x \equiv pk + p\ (mod\ p^2), k = 0, 1, 2, 3, \dots\dots\dots\dots., p-1.$
Also the congruence: $x^3 \equiv p^3\ (mod\ p^2.q)$, p, q being different odd primes, has exactly p incongruent solutions given by
$x \equiv pqk + p\ (mod\ p^2q), k = 0, 1, 2, 3, \dots\dots\dots\dots., p-1.$
Also the congruence: $x^3 \equiv p^3\ (mod\ 3^np^2)$, p being odd prime, has exactly $3p$ incongruent solutions given by
$x \equiv 3^{n-1}pk + p\ (mod\ 3^n.p^2), k = 0, 1, 2, 3, \dots\dots\dots\dots., 3p-1.$

MERIT OF THE PAPER

The established formula is tested and verified true solving some suitable numerical examples.
Oral calculation for solutions is also become possible. It made the study of the cubic congruence very simple and interesting. It is time saving. This is the merit of the paper.

REFERENCES

[1] Burton David M, 2012, *Elementary Number Theory*, McGraw Hill Education (India) Private Limited, Seventh edition, New Delhi, ISBN: 978-1-25-902576-1.
[2] Koshy Thomas, 2009, *Elementary Number Theory with Applications*, Academic Press (An Imprint of Elsevier), USA, Second edition, ISBN: 978-81-312-1859-4.
[3] Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.
[4] 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, Part-8, Page:699-703
[5] Roy B M, *Formulation of solutions of a special standard cubic congruence of prime-power modulus*, International journal for scientific Development and research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May-19. Page: 409-411.
[6] Roy B M, *A review and reformulation of a class of solvable standard cubic congruence of even composite modulus*, International Journal for research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-04, Issue-11, Nov-19. Page: 29-32.
[7] Roy B M, *Formulation of solutions of standard cubic congruence of special even composite modulus in special case*, International Journal of Engineering Technology Research and Management (IJETRM), ISSN: 2456-9348, Vol-04, Issue-09, Sep-20, Page: 50-53.