RP-173: Solving four standard cubic congruence modulo an even 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 the current paper, the author considered four standard cubic congruence of even composite modulus modulo an even multiple of square of an odd prime for his study.**
After a rigorous study, the author has established formulations for the solutions of the congruence under his consideration. It is seen that the four congruence have two different formulation of solutions. These formulations are examined solving numerical examples and tested & verified true. No suitable literature of the solutions of the congruence considered is found in the literature of mathematics. The author first time formulated the solutions which are very simple and easy to remember.

***Keywords*: Cubic congruence, Cubic residues, Chinese Remainder Theorem (C R T).**

INTRODUCTION

Standard cubic congruence of prime and composite modulus are not found studied in the schools and in the universities. Earlier mathematicians showed no interest in it. Studies had been done on quadratic congruence of prime modulus but not on of composite modulus. No
Complete study is found in the literature. The author has tried his best to study the standard cubic congruence of prime and composite modulus and formulated its solutions. Here is also the solutions of some standard cubic congruence of composite modulus are formulated.

PROBLEM-STATEMENT

The problem is
"To formulate the solutions of the standard cubic congruence of the type:
(1) $x^3 \equiv p^2 \pmod{2p^2}$
(2) $x^3 \equiv p^2 \pmod{4p^2}$
(3) $x^3 \equiv p^2 \pmod{6p^2}$
(4) $x^3 \equiv p^2 \pmod{8p^2}$; p an odd positive integer".

LITERATURE REVIEW

The standard cubic congruence considered here for study are of very special types.
Similar special types of cubic congruence are already published by the author [1], [2], [3]. Here some other special types are considered for formulation of solutions. The literature of mathematics say nothing about these cubic congruence [4], [5]. But the readers can use Chinese remainder theorem [6].

ANALYSIS & RESULTS

Case-I: Consider the congruence $x^3 \equiv p^2 \pmod{2p^2}$
Consider $x \equiv 2pk + p \ (mod\ 2p^2)$
$\equiv (2k+1)p\ (mod\ 2p^2)$
Then, $x^3 - p^2 \equiv [(2k+1)p]^3 - p^2 = (2k+1)^3p^3 - p^2 = p^2[\text{odd integer} - 1]$
$\equiv p^2.(even\ integer)$
$\equiv p^2.2t$
$\equiv 0 \pmod{2p^2}$
So, $x^3 \equiv p^2\ (mod\ 2p^2)$
Thus, $x \equiv 2pk + p \ (mod\ 2p^2)$ may be considered as solutions of the congruence.
But for $k = p$, the solutions formula reduces to $x \equiv 2p.p + p \ (mod\ 2p^2)$
$\equiv 2p^2 + p\ (mod\ 2p^2)$
$\equiv 0 + p\ (mod\ 2p^2)$
This is the same solution as for $k = o$.
Also, for $k = p + 1$, the solutions formula reduces to $x \equiv 2p.(p+1) + p \ (mod\ 2p^2)$
$\equiv 2p^2 + 2p + p\ (mod\ 2p^2)$
$\equiv 0 + 2p + p (mod\ 2p^2)$
$\equiv 2p + p\ (mod\ 2p^2)$
This is the same solution as for $k = 1$.

Therefore, all the solutions are given by
$x \equiv 2pk + p \ \ (mod\ 2p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$

Case-II: Let $p \equiv 1\ (mod\ 4)$. Then, $p - 1 = 4t$.
Consider the cubic congruence $x^3 \equiv p^2\ (mod\ 4p^2)$.
Consider $x \equiv 4pk + p \ \ (mod\ 4p^2)$
$\equiv (4k + 1)p\ (mod\ 4p^2)$
Then, $x^3 - p^2 \equiv [(4k + 1)p]^3 - p^2 = (4k + 1)^3 p^3 - p^2 = p^2[\text{odd integer} - 1]$
$\equiv p^2.(even\ integer)$
$\equiv p^2.4t$
$\equiv 0(\text{mod } 4p^2)$
So, $x^3 \equiv p^2\ (mod\ 4p^2)$
Thus, $x \equiv 4pk + p \ \ (mod\ 4p^2)$ may be considered as solutions of the congruence.
But for $k = p$, the solutions formula reduces to $x \equiv 4p.p + p \ \ (mod\ 4p^2)$
$\equiv 4p^2 + p\ (mod\ 4p^2)$
$\equiv 0 + p\ (mod\ 4p^2)$
This is the same solution as for $k = o$.
Also, for $k = p + 1$, the solutions formula reduces to $x \equiv 4p.(p + 1) + p \ \ (mod\ 4p^2)$
$\equiv 4p^2 + 4p + p\ (mod\ 4p^2)$
$\equiv 0 + 4p + p(mod\ 4p^2)$
$\equiv 4p + p\ (mod\ 4p^2)$
This is the same solution as for $k = 1$.
Therefore, all the solutions are given by
$x \equiv 4pk + p \ \ (mod\ 4p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$

Case-III: Consider the cubic congruence $x^3 \equiv p^2\ (mod\ 6p^2)$.
Consider $x \equiv 6pk + p \ \ (mod\ 6p^2)$
$\equiv (6k + 1)p\ (mod\ 6p^2)$
Then, $x^3 - p^2 \equiv [(6k + 1)p]^3 - p^2 = (6k + 1)^3 p^3 - p^2 = p^2[\text{odd integer} - 1]$
$\equiv p^2.(even\ integer)$
$\equiv p^2.6t$
$\equiv 0(\text{mod } 6p^2)$
So, $x^3 \equiv p^2\ (mod\ 6p^2)$
Thus, $x \equiv 6pk + p \ \ (mod\ 6p^2)$ may be considered as solutions of the congruence.
But for $k = p$, the solutions formula reduces to $x \equiv 6p.p + p \ \ (mod\ 6p^2)$
$\equiv 6p^2 + p\ (mod\ 6p^2)$
$\equiv 0 + p\ (mod\ 6p^2)$
This is the same solution as for $k = o$.
Also, for $k = p + 1$, the solutions formula reduces to $x \equiv 6p.(p + 1) + p \ \ (mod\ 6p^2)$
$\equiv 6p^2 + 6p + p\ (mod\ 6p^2)$
$\equiv 0 + 6p + p\ (mod\ 6p^2)$
$\equiv 6p + p\ (mod\ 6p^2)$
This is the same solution as for $k = 1$.
Therefore, all the solutions are given by
$x \equiv 6pk + p \ \ (mod\ 6p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$

Case-IV: Consider the cubic congruence $x^3 \equiv p^2\ (mod\ 8p^2)$.
Consider $x \equiv 4pk + p \ \ (mod\ 8p^2)$
$\equiv (4k + 1)p\ (mod\ 8p^2)$
Then, $x^3 - p^2 \equiv [(4k + 1)p]^3 - p^2 = (4k + 1)^3 p^3 - p^2 = p^2[\text{odd integer} - 1]$
$\equiv p^2.(even\ integer)$
$\equiv p^2.8t$
$\equiv 0(\text{mod } 8p^2)$
So, $x^3 \equiv p^2\ (mod\ 8p^2)$
Thus, $x \equiv 4pk + p \ \ (mod\ 8p^2)$ may be considered as solutions of the congruence.
But for $k = 2p$, the solutions formula reduces to $x \equiv 4p.2p + p \ \ (mod\ 8p^2)$
$\equiv 8p^2 + p\ (mod\ 8p^2)$
$\equiv 0 + p\ (mod\ 8p^2)$
This is the same solution as for $k = o$.
Also, for $k = 2p + 1$, the solutions formula reduces to $x \equiv 4p.(2p + 1) + p \ \ (mod\ 8p^2)$
$\equiv 8p^2 + 4p + p\ (mod\ 8p^2)$
$\equiv 0 + 4p + p\ (mod\ 8p^2)$

$$\equiv 4p + p \ (mod\ 8p^2)$$

This is the same solution as for $k = 1$.
Therefore, all the solutions are given by
$x \equiv 4pk + p \ \ (mod\ 8p^2); k = 0, 1, 2, 3, \dots \dots, (2p - 1).$

ILLUSTRATIONS

Ex-1: consider $x^3 \equiv 25\ (mod\ 50)$
$x \equiv 2pk + p \ \ (mod\ 2p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$
$\equiv 2.5k + 5\ (mod\ 2.25)$
$\equiv 10k + 5\ (mod\ 50); k = 0, 1, 2, 3, 4$
$\equiv 5, 15, 25, 35, 45\ (mod\ 50)$

Ex-2: consider $x^3 \equiv 25\ (mod\ 100)$
$x \equiv 4pk + p \ \ (mod\ 4p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$
$\equiv 4.5k + 5\ (mod\ 4.25)$
$\equiv 20k + 5\ (mod\ 100); k = 0, 1, 2, 3, 4.$
$\equiv 5, 25, 45, 65, 85\ (mod\ 100)$

Ex-3: consider $x^3 \equiv 49\ (mod\ 98)$
It can be written as $x^2 \equiv 7^2 (mod\ 2.7^2)$
It is of the type $x^2 \equiv p^2 (mod\ 2.p^2)$
Therefore, it has exactly $p = 7$ incongruent solutions given by
$x \equiv 2pk + p \ \ (mod\ 2p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$
$\equiv 2.7k + 7\ (mod\ 2.7^2)$
$\equiv 14k + 7\ (mod\ 98); k = 0, 1, 2, 3, 4, 5, 6.$
$\equiv 7, 21, 35, 49, 63, 77, 91\ (mod\ 98)$

Ex-4: consider $x^3 \equiv 49\ (mod\ 196)$
It can be written as $x^2 \equiv 7^2 (mod\ 4.7^2)$
It is of the type $x^2 \equiv p^2 (mod\ 4.p^2)$
Therefore, it has exactly $p = 7$ incongruent solutions given by
$x \equiv 2pk + p \ \ (mod\ 4p^2); k = 0, 1, 2, 3, \dots \dots, (2p - 1).$
$\equiv 2.7k + 7\ (mod\ 4.7^2)$
$\equiv 14k + 7\ (mod\ 196); k = 0, 1, 2, 3, 4, \dots \dots \dots, (2.7 - 1).$
$\equiv 7, 21, 35, 49, 63, 77, 91, 105, 119, 133, 147, 161, 175, 189\ (mod\ 196)$

Ex-5: consider $x^3 \equiv 49\ (mod\ 294)$
It can be written as $x^2 \equiv 7^2 (mod\ 6.7^2)$
It is of the type $x^2 \equiv p^2 (mod\ 6.p^2)$
Therefore, it has exactly p incongruent solutions given by
$x \equiv 6pk + p \ \ (mod\ 6p^2); k = 0, 1, 2, 3, \dots \dots, (p - 1).$
$\equiv 6.7k + 7\ (mod\ 6.7^2)$
$\equiv 42k + 7\ (mod\ 294); k = 0, 1, 2, 3, 4, 5, 6.$
$\equiv 7, 49, 91, 133, 175, 217, 259\ \ (mod\ 294)$

Ex-6: consider $x^3 \equiv 25\ (mod\ 200)$
It can be written as $x^2 \equiv 5^2 (mod\ 8.5^2)$
It is of the type $x^2 \equiv p^2 (mod\ 8.p^2)$
Therefore, it has exactly 2p incongruent solutions given by
$x \equiv 4pk + p \ \ (mod\ 8p^2); k = 0, 1, 2, 3, \dots \dots, (2p - 1).$
$\equiv 4.5k + 5\ (mod\ 8.5^2)$
$\equiv 20k + 5\ (mod\ 200); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$
$\equiv 5, 25, 45, 65,\ 85, 105, 125, 145, 165, 185\ \ (mod\ 200)$

CONCLUSION

Therefore, it is concluded that the standard cubic congruence: $x^3 \equiv p^2\ (mod\ 2p^2)$ has exactly p incongruent solutions $x \equiv 2pk + p\ (mod\ 2p^2), p\ an\ odd\ prime; k = 0, 1, 2, \dots., (p - 1).$
Similarly, the standard cubic congruence: $x^3 \equiv p^2\ (mod\ 6p^2)$ has exactly p incongruent solutions $x \equiv 6pk + p\ (mod\ 6p^2), p\ an\ odd\ prime; k = 0, 1, 2, \dots \dots., (p - 1).$
Also, the standard cubic congruence: $x^3 \equiv p^2\ (mod\ 4p^2)$ has exactly $2p$ incongruent solutions $x \equiv 2pk + p\ (mod\ 4p^2), p\ an\ odd\ prime; k = 0, 1, 2, 3, \dots \dots, (2p - 1).$

Also, the standard cubic congruence: $x^3 \equiv p^2 \ (mod\ 8p^2)$ has exactly p incongruent solutions $x \equiv 4pk + p\ (mod\ 8p^2), p\ an\ odd\ prime; k = 0, 1, 2, 3, \ldots \ldots .., (2p - 1)$.

REFERENCES

[1] Roy B M, *Formulation of solutions of three very special standard cubic congruence of composite modulus*, International Journal for research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-05, Issue-02, Feb-20.
[2] Roy B M, *A review and reformulation of solutions of standard cubic congruence of Composite modulus modulo an odd prime power integer*, International journal for scientific Development and research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-12, Dec-20.
[3] Roy B M, *Solving some special standard cubic congruence modulo an odd prime multiplied by eight*, International Journal of Scientific Research and Engineering Development International Journal for research Trends and Innovations (IJSRED), ISSN: 2581-7175, Vol-04, Issue-01, Jan-21.
[4] Zukerman[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.
[5] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.
[6] David M Burton, 2012, *Elementary Number Theory*, Mc Graw Hill education (Higher Education), Seventh Indian Edition, New Dehli, India, ISBN: 978-1-25-902576-1.