RP-124: Formulation of Solutions of a Special Class of Standard Cubic Congruence of Composite Modulus-an Integer- Multiple of Power of an Odd Prime

Prof. B M Roy

M. Sc. (Maths), Hon. Ph. D., Hon. D. Sc.
Head, Dept. of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon,
GONDIA (M.S), India. Pin-441801
(Affiliated to RTM Nagpur University, Nagpur)

***Abstract*: In this paper, solutions of a special class of standard cubic congruence of composite modulus-an integer multiple of power of an odd prime- is formulated. The formula established is tested and verified true one by one. The merit of the paper is the formulation of the solutions. Readers need not use the preferred Chinese Remainder Theorem (CRT) - a time-consuming method. Formulation of the solutions is the merit of the paper.**

***Keywords*: Cubic congruence, Composite modulus, Chinese Remainder Theorem, Prime-power integer, Formulation.**

1. INTRODUCTION

The congruence of the type: $x^3 \equiv a \pmod{m}$ is called a standard cubic congruence of prime or composite modulus, if m is prime or composite integer.

The author has formulated many standard cubic congruence of prime and composite modulus [1] to [8]. Here is a very special type of standard cubic congruence of composite modulus of the type: $x^3 \equiv p^3 \pmod{b.p^n}$, $n \geq 3$, and b an integer, is considered for the formulation of the solutions.

2. REVIEW OF LITERATURE

It is found that no attempt had been made for formulation of the above congruence by earlier mathematicians. No special literature is found. Readers preferred to use Chinese Remainder Theorem to solve the congruence, which takes a long time. Thomas Koshy had mentioned the definition of standard cubic congruence but no method of solutions is discussed nor mention any formulation of the congruence [9].

3. NEED OF THIS RESEARCH

The author found no direct formulation in the literature of mathematics, but only a definition of cubic congruence [9]. Readers must need a time-saving method or formulation. This is the need of the research. For the time saving purpose, the author has tried his best to formulate the congruence and his efforts are presented in this paper. This is the need of the paper.

4. PROBLEM STATEMENT

"To formulate the congruence:

$$x^3 \equiv p^3 \pmod{b.p^n},\ n \geq 3,\ \text{and b an integer, p an odd prime".}$$

ANALYSIS & RESULT

The congruence under consideration is:

$$x^3 \equiv p^3 \pmod{b.p^n},\ m \geq 3.$$

For the solutions, consider, $x = b.p^{n-2}k + p; k = 0, 1, 2, 3, \ldots\ldots\ldots$

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

$$= b^3.p^{3n-6}.k^3 + 3.b^2.p^{2n-4}.k^2.p + 3\,b\,p^{n-2}k.p^2 + p^3$$

$$= p^3 + b.p^n(\ldots\ldots)$$

$\equiv p^3 \pmod{b.p^n}$

Thus, $x \equiv b.p^{n-2}k + p \pmod{b.p^n}$ are the solutions for $k = 0, 1, 2, 3, \ldots \ldots$

But if $k = p^2$, then $x \equiv b.p^{n-2}.p^2 + p \pmod{b.p^n}$

$\equiv b.p^n + p \pmod{b.p^n}$

$\equiv o + p \pmod{b.p^n}$, which is the same solution as for $k = o$.

For $k = p^2 + 1$, it can be easily seen that the solution is the same as for $k = 1$.

Thus, all the solutions can be given by

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

Therefore, the above congruence has p^2 solutions and the solutions are

$x \equiv (b.p^{n-2}kp) \pmod{b.p^n}; k = 0, 1, 2, \ldots \ldots . (p^2 - 1)$.

If one take $b = 1$, the congruence under consideration reduces to

$x^3 \equiv p^3 \pmod{p^n}$. In this case, we definitely have $n \geq 4$.

And the solutions are given by

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

These are p^2 solutions of the congruence.

ILLUSTRATIONS

Consider the congruence $x^3 \equiv 27 \pmod{189}$

Here, $189 = 7.27 = 7.3^3$ with $n = 3, b = 7,$ and $p = 3$.

The congruence can also be written as $x^3 \equiv 3^3 \pmod{7.3^3}$ with $p = 3$.

Thus the congruence has $p^2 = 9$ solutions, given by

$x \equiv (bp^{n-2}k + p) \pmod{b.p^n}, k = 0, 1, 2, \ldots \ldots \ldots (p^2 - 1)$.

$\equiv 7.3^{3-2}k + 3 \pmod{7.3^3}; k = 0, 1, 2, \ldots \ldots . (9 - 1) = 8$.

$\equiv 7.3^1k + 3 \pmod{7.27}$

$\equiv 21k + 3 \pmod{189}; k = 0, 1, 2, \ldots \ldots, 8$.

$\equiv 0 + 3; 21 + 3; 42 + 3; 63 + 3; 84 + 3; 105 + 3; 126 + 3;$

$147 + 3; 168 + 3 \pmod{189}$

$\equiv 3, 24, 45\ 66, 87, 108, 129, 150, 171 \pmod{189}$.

Let us consider another example. $x^3 \equiv 125 \pmod{500}$

The congruence can also be written as $x^3 \equiv 5^3 \pmod{4.5^3}$.

Here, $500 = 4.125 = 4.5^3$ with $p = 5, b = 4, n = 3$.

Thus, the congruence has $p^2 = 25$ solutions given by

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

$\equiv 4.5^{3-2}k + 5 \pmod{4.5^3}; k = 0, 1, 2, \ldots \ldots \ldots, (25 - 1)$.

$\equiv 20k + 5 \pmod{500}; k = 0, 1, 2, \ldots \ldots \ldots, 24$.

$\equiv 0 + 5; 20 + 5; 40 + 5, 60 + 5; \ldots \ldots \ldots \ldots \ldots \ldots, 480 + 5 \pmod{500}$.

≡5, 25, 45, 65, ……., 485 (mod 500).

These are twenty five solutions.

Consider one more example: $x^3 \equiv 343 \pmod{2401}$

It can be written as $x^3 \equiv 7^3 \pmod{7^4}$ **with** $p = 7, n = 4$.

It has $p^2 = 49$ **incongruent solutions.**

These are given by

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

$\equiv 7^{4-2}k.+7 \pmod{7^4}; k = 0, 1, 2, \ldots\ldots\ldots, (49 - 1).$

$\equiv 49k + 7 \pmod{2401}; k = 0, 1, 2, \ldots\ldots\ldots, 48.$

$\equiv 0 + 7; 49 + 7; 98 + 7; \ldots\ldots\ldots\ldots\ldots\ldots, 2352 + 7 \pmod{2401}.$

≡7, 56, 105 , ……., 2359 (mod 2401).

These are the 49 incongruent solutions of the said congruence.

CONCLUSION

Thus, it can be concluded that the solutions of the standard bi-quadratic congruence of composite modulus of the type: $x^3 \equiv p^3 \pmod{b.p^n}$**, with p an odd prime integer, is formulated. The solutions are given by**

$x \equiv (bp^{n-2}k + p) \pmod{b.p^n}, k = 0, 1, 2, \ldots\ldots\ldots (p^2 - 1),$ **which are** p^2 **in number.**

The established formula is tested and verified true by solving some examples. It is a very quick method to find all the solutions.

MERIT OF THE PAPER

A very simple formulation is made. The solutions can be calculated orally.

No need to use Chinese Remainder Theorem. This is the merit of the congruence under consideration.

REFERENCE

[1] 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.

[2] Roy B. M., Formulation of Solutions of a Special Standard Cubic Congruence of Prime-power Modulus, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-05, May -19.

[3] Roy B. M., Formulation of Solutions of a Special Standard Cubic Congruence of Composite Modulus--an Integer Multiple of Power of Prime, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132x, Vol-05, Issue-03, May-Jun-19.

[4] Roy B. M., Formulation of a Special Type of Standard Cubic Congruence of Composite Modulus- an Odd Multiple of Power of Two, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-04, Issue-06, June-19.

[5] Roy B. M., Formulation of a special class of bi-quadratic congruence of composite modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132x, Vol-05, Issue-04, Jul-Aug-19.

[6] Roy B. M., Formulation Two Special Types of standard cubic congruence of composite modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132x, Vol-05, Issue-05, Sep-Oct-19.

[7] Roy B. M., Formulation of standard cubic congruence of even composite modulus, International Journal of Research and Analytical Reviews (IJRAR), ISSN: 2348-1269, Vol-06, Issue-02, Sep-19.

[8] Roy B. M., Formulation of Solutions of a Standard Cubic Congruence of Composite Modulus- an Odd Multiple of an even Integer, International Journal of Trend in Scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-01, Nov-19.

[9] Koshy Thomas; Elementary Number Theory with Applications; 2/e; 2009, Academic press.