INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 3)
Available online at: www.ijariit.com

RP-69: Formulation of solutions of standard congruence of higher degree of composite modulus- A power of the degree

B. M. Roy
roybm62@gmail.com
Jagat Arts, Commerce and Indiraben Hariharbhai Patel Science College,
Goregaon, Maharashtra

ABSTRACT

In this paper, a special class of standard congruence of any higher degree is formulated. The formula established is tested and found true by solving different suitable examples and verifying the solutions obtained. Such a formulation is not found in the literature of mathematics. It makes the finding of solutions of the said congruence orally. Formulation of solutions is the merit of the paper. Formulation of solutions made the study of the congruence interesting.

Keywords— *Binomial Theorem, Bi-quadratic and Cubic congruence, Standard congruence of higher degree*

1. INTRODUCTION

Congruence of the type: $x^n \equiv b^n \ (mod\ m)$, m being a composite or prime positive integer is called a standard congruence of n^{th} higher degree with $n \geq 5$. The author already formulated some standard cubic $(n = 3)$ and standard bi-quadratic $(n = 4)$ Congruence of prime and composite modulus.

Also, some standard congruence of higher degree is formulated by the author. Even some remained to formulate. Here in this paper, a generalization of cubic and biquadratic congruence is considered for formulation. It is of the type:

$$x^n \equiv b^n \ (mod\ n^r)\ and\ \ x^n \equiv b^n \ (mod\ an^r)$$

2. LITERATURE REVIEW

In the books of Number Theory, it is found that only polynomial congruence of prime modulus of higher degree, are considered for discussion. Solutions were obtained by using Fermat's Little Theorem. In the method of solving of the congruence, the given congruence has to reduce to the equivalent congruence of lower degree and then solving the reduced congruence, solutions of the original congruence were obtained [6]. But, nowhere a method or formulation of the congruence under consideration is found in the literature of mathematics. Only some papers on cubic and bi-quadratic congruence of the author recently published are found. Thomas Koshy had made a very little discussion on standard cubic congruence but no method/formulation of the congruence is discussed [5]. Those papers are listed below:

$$x^3 \equiv a^3 \ \ (mod\ 3^n) \tag{1}$$

$$x^3 \equiv a^3 \ \ (mod\ 3^n.b) \tag{2}$$

$$x^4 \equiv a^4 \ \ (mod\ 4^n) \tag{3}$$

$$x^4 \equiv a^4 \ \ (mod\ 4^n.b) \tag{4}$$

Even some congruence are remained to formulate. Here in this paper, a generalization of cubic and bi-quadratic congruence is considered for formulation. It is of the type:

$$x^n \equiv b^n \ (mod\ n^r)\ and\ \ x^n \equiv b^n \ (mod\ an^r)$$

3. NEED OF RESEARCH

The existed method applies to the division process of polynomials. No formulation is found in the literature of mathematics for the congruence under consideration. The author wishes and tries his best to formulate the solutions of the said congruence and presents his sincere efforts in this paper. This is the need for the paper.

4. PROBLEM STATEMENT

The problem is "To establish suitable formulae for the solutions of the congruence

$$x^n \equiv b^n \ (mod\ n^r) \quad and \quad x^n \equiv b^n \ \ (mod\ an^r);$$

Where n is a positive integer and $1 \leq a \leq (n-1),\ 1 \leq b \leq (n-1)$.

5. ANALYSIS AND RESULT

For the solutions of the said congruence: $x^n \equiv b^n\ (mod\ n^r)\ with$ a positive integer n, r.
Let us consider that

$$x = n^{r-1}k + b\ for\ k = 0, 1, 2, \dots ....$$

Then, using Binomial Expansion theorem,

$$x^n = \ (n^{r-1}k + b)^n$$

$$= (n^{r-1}k)^n + n.(n^{r-1}k)^{n-1}.b + \cdots \dots \dots + n.(n^{r-1}k)^1 b^{n-1} + b^n$$

$$= b^n + n^r(\dots \dots.)$$

$$\equiv \ b^n\ (mod\ n^r)$$

Therefore, $x \equiv n^{r-1}k + b\ (mod\ n^r)$ is a solution of the congruence under consideration for

$$k = 0, 1, 2, 3, \dots \dots \dots, (n-1), n, n+1, \dots \dots$$

But it is seen that for $k = n$, one must get

$$x \equiv n.n^{r-1} + b = n^r + b \equiv b\ (mod\ n^r),$$

Which is the same as for k = 0.

It can also be seen that for $k = n + 1, the\ solution\ is\ the\ same\ for\ as\ k = 1.$ Thus, $k = 0, 1, 2, \dots \dots, (n-1)$ are the values of n. It can also be seen that $b = 1, 2, 3, \dots \dots n$ hold.

Thus, the said congruence has exactly n solutions and there must have n such congruence.

Now consider the congruence $x^n \equiv b^n\ (mod\ an^r) with\ 1 \leq a \leq n-1.$

For the solution, consider $x \equiv an^{r-1}k + b\ (mod\ an^r)$.
Then,

$$x^n = (an^{r-1}k + b)^n$$

$$= (an^{r-1}k)^n + n.(an^{r-1}k)^{n-1}.b + \cdots \dots \dots \dots. + n.(an^{r-1}k)^1.b^{n-1} + b^n$$

$$\equiv an^r.(\dots \dots..) + b^n$$

$$\equiv b^n\ (mod\ an^r)$$

Thus, $x \equiv an^{r-1}k + b\ (mod\ an^r)$ is a solution of the said congruence.

It is also seen that $for\ k = n, n+1$, ..., the said solutions repeat as for $k = 0, 1, 2,$ ....

Therefore, here, $k = 0, 1, 2, \dots., (n-1)\ and\ a = 1, 2, 3, \dots \dots., (n-1)$.

6. ILLUSTRATION

Consider the congruence $x^6 \equiv 28\ (mod\ 36)$.

It can be written as $x^6 \equiv 28 + 36 = 64 = 2^6\ (mod\ 6^2)$.

It is of the type

$$x^n \equiv b^n\ (mod\ n^r)\ with\ n = 6, \qquad b = 2, r = 2.$$

Thus it has exactly six solutions given by:

$$x \equiv n^{r-1}k + a\ (mod\ n^r)\ \ with\ k = 0, 1, 2, 3, 4, 5.$$

Therefore, the required solutions are:

$$x \equiv 6^{2-1}k + 2\ (mod\ 6^2); k = 0, 1, 2, 3, 4, 5.$$

$$\equiv 6k + 2\ (mod\ 6^2)\ ; k = 0, 1, 2, 3, 4, 5.$$

$$\equiv 0 + 2, 6 + 2, 12 + 2, 18 + 2, 24 + 2, 30 + 2\ (mod\ 36)$$

$$\equiv 2, 8, 14, 20, 26, 32\ (mod\ 36).$$

Consider the congruence $x^5 \equiv 243 \ (mod\ 625)$.

It can be written as $x^5 \equiv 243 = 3^5 \ (mod\ 5^4)$.

It is of the type

$$x^n \equiv b^n \ (mod\ n^r)\ with\ n = 5\ , \quad b = 3,\ \ r = 4.$$

Thus, the said congruence has exactly five solutions given by:

$$x \equiv n^{r-1}k + b \ (mod\ n^r) \ \ with\ k = 0, 1, 2, 3, 4.$$

Therefore, the required solutions are:

$$x \equiv 5^3k + 3 \ (mod\ 5^4); k = 0, 1, 2, 3, 4.$$

$$\equiv 125k + 3 \ (mod\ 5^4)$$

$$\equiv 0 + 3, 125 + 3, 250 + 3, 375 + 3, 500 + 3 \ (mod\ 625)$$

$$\equiv 3, 128, 253, 378, 503 \ \ (mod\ 625).$$

Also, consider the congruence $x^7 \equiv 27704 \ (mod\ 50421)$.

It can be written as:

$$x^7 \equiv 27704 + 50421 = 78125 = 5^7 \ (mod\ 3.7^5)$$

It is of the type

$$x^n \equiv b^n(mod\ an^r) \ \ with\ b = 5, a = 3\ , n = 7, \ \ r = 5.$$

The congruence has seven solutions and the corresponding solutions are given by

$$x \equiv an^{r-1}k + b \ (mod\ an^r)$$

$$\equiv 3.7^4.k + 5 \ (mod\ 3.7^3)$$

$$\equiv 7203k + 5 \ (mod\ 50421)\ with\ k = 0, 1, 2, 3, 4, 5, 6.$$

$\equiv$5, 7208, 14411, 21614, 28817, 36020, 43223 (mod 50421)

7. CONCLUSION

Thus, it is concluded that the congruence: $x^n \equiv b^n \ (mod\ n^r)$ and $x^n \equiv b^n \ (mod\ a.n^r)$, are formulated for any positive integer n. The formulae established as:

$$x \equiv n^{r-1}k + b \ (mod\ n^r) \ \ and \ \ x \equiv an^{r-1}k + b \ (mod\ an^r).$$

It is tested and found true by solving different examples.

8. MERIT OF THE PAPER

In this paper, the congruence under consideration is formulated. The sincere efforts of the author made it possible to find all the solutions easily and effectively in a short time. Formulation of the solutions of the said congruence is the merit of the paper.

9. REFERENCES

[1] Roy B M, “Discrete Mathematics and Number Theory”, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.
[2] Roy B M, Formulation of a class of standard cubic congruence of modulus nth power of three, International Journal of Research under literal access(IJRULA), Vol-1, Issue-3, Aug-18,
[3] Roy B M, 2019, Formulation of Two Special Classes of Standard Cubic Congruence of Composite Modulus—a power of three, (IJSRED), ISSN: Vol-02, Issue-03, and May-19.
[4] Roy B M, 2019, Formulation of solutions of some classes of standard bi-quadratic congruence of composite modulus, (IJETRM), ISSN: Vol-03, Issue-02, Feb-19.
[5] Thomas Koshy, “Elementary Number Theory with Applications”, 2/e (Indian print, 2009), Academic Press.
[6] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), “An Introduction to the Theory of Numbers”, 5/e, Wiley India (Pvt) Ltd.

