Formulation of a class of congruence of higher degree of composite modulus

Prof. B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist-Gondia, M. S., INDIA, Pin: 441801
(Affiliated to R T M Nagpur University, Nagpur)

***Abstract*: In this paper, the author formulated a class of standard congruence of higher degree of composite modulus. The formula is tested and found true by solving suitable examples. No such formulation is found in the literature of mathematics. Even no method is found how to solve such congruence except Chinese Remainder Theorem- a time consuming method. Now it is needless to use CRT for solutions. Formulation is the merit of the paper.**

***Keywords*: Binomial Theorem, Composite Modulus, Chinese Remainder Theorem.**

INTRODUCTION

A congruence of the type $x^n \equiv a\ (mod\ m)$ is called a congruence of higher degree. If m is a composite integer, then it is called a congruence of higher degree of composite modulus. The author formulated the solutions of quadratic, cubic congruence of prime and composite modulus. He also formulated congruence of higher degree of prime and composite modulus. Even some congruence is remained to formulate. Here is a class of congruence of higher degree of the type: $x^n \equiv a^n\ (mod\ b.n^r)$ considered for formulation. Such types of congruence are not formulated earlier. In the literature of mathematics, no formulation of such congruence is found. First time the author tried his best to formulate the congruence under consideration.

EXISTED METHOD

No method is yet found how to solve such types of congruence. But one can use Chinese Remainder Theorem. It can create a serious difficulty for solutions that how to solve the separate congruence: $x^n \equiv a^n\ (mod\ b)$ & $x^n \equiv a^n\ (mod\ n^r)$ and to find the common solutions of the separate congruence. This method is time-consuming. It may take hours/ days. Finding the solutions of the said congruence is seemed to be impossible. Now it becomes possible to find the solutions in very short time. The problem of finding the solutions made the problem more interesting.

PROBLEM-STATEMENT

Here, the problem is" To formulate a class of congruence of higher degree of composite modulus of the type: $x^n \equiv a^n\ (mod\ bn^r); n, a, b, r\ are\ positive\ integers.$

ANALYSIS & RESULT

Consider the congruence $x^n \equiv a^n\ (mod\ b.n^r); a, b, n, r\ are\ poditive\ integers.$

To find its solutions, consider $x \equiv bn^{r-1}k + a\ (mod\ b.n^r).\ with\ k = 0, 1, 2, \ldots\ldots\ldots\ldots$ and $b \neq n$.

Then, $x^n \equiv (bn^{r-1}k + a\ )^n\ (mod\ bn^{r-1})$

$$\equiv (bn^{r-1}k)^n + n.(bn^{r-1}k)^{n-1}.a + \cdots \ldots + n.(bn^{r-1}k).a^{n-1} + a^n\ \ (mod\ bn^r)$$

$$\equiv a^n + nbn^{r-1}k(\ldots\ldots\ldots)(mod\ bn^r)$$

$$\equiv a^n\ (mod\ bn^r).$$

Thus, $x \equiv bn^{r-1}k + a\ (mod\ bn^r)$ satisfies the congruence $x^n \equiv a^n\ (mod\ bn^r)$.

Hence it can be considered as a solution of the said congruence.

If $k = 0, 1, 2, 3, \ldots\ldots\ldots, (n-1, n, \ldots\ldots$, for $for\ k = n$, it is seen that $x \equiv a^n\ (mod\ bn^r)$

Which is same as for $k = 0$.

Similarly, for $k = n+1, n+2, \ldots\ldots$, it can be seen that the values of x are the same as for $k = 1, 2, 3, \ldots\ldots, (n-1)$. Therefore, it can be concluded that

$$x \equiv bn^{r-1}k + a \ (mod\ bn^r)\ for\ k = 0, 1, 2, \ldots\ldots, (n-1).$$

Also for a fixed k, if $b = n$, then also one get the same result as for k=n.

Thus such congruence has exactly n solutions.

Sometimes it is given of the type: $x^n \equiv c \ (mod\ b.n^r)$.

It can be written as $x^n \equiv c + m.n^r = a^n \ (mod\ bn^r)$ [2].

For $b = 1$, the above congruence reduces to: $x^n \equiv a^n (mod\ n^r)$ having the solutions

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

ILLUSTRATION

Consider the congruence $x^{10} \equiv 1024 \ (mod\ 3000)$.

It can be written as $x^{10} \equiv 2^{10} \ (mod\ 3.10^3)$.

It is of the type $x^n \equiv a^n (mod\ b.n^r)\ \ with\ \ a = 2, b = 3, r = 3, n = 10$.

The corresponding solutions are $x \equiv bn^{r-1}k + a \ (mod\ bn^r); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$.

Putting the values, $x \equiv 3.10^{3-1}k + 2 \ (mod\ 3.10^3)$

$$\equiv 3.10^2k + 2 \ (mod\ 3000)$$

$$\equiv 300k + 2 \ (mod\ 3000)$$

$$\equiv 2, 302, 602, 902, 1202, 1502, 1802, 2102, 2402, 2702 \ (mod\ 3000)$$

$$for\ k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

Consider the congruence $x^5 \equiv 243 \ (mod\ 500)$.

It can be written as $x^5 \equiv 3^5 \ (mod\ 4.5^3)$.

It is of the type $x^n \equiv a^n (mod\ b.n^r)\ \ with\ \ a = 3, b = 4, r = 3, n = 5$.

The corresponding solutions are $x \equiv bn^{r-1}k + a \ (mod\ bn^r); k = 0, 1, 2, 3, 4$.

Putting the values, $x \equiv 4.5^{3-1}k + 3 \ (mod\ 4.5^3)$

$$\equiv 4.25k + 3 \ (mod\ 500)$$

$$\equiv 100k + 3 \ (mod\ 500)$$

$$\equiv 3, 103, 203, 303, 403 \ (mod\ 500)\ \ for\ k = 0, 1, 2, 3, 4.$$

Consider $x^6 \equiv 640 \ (mod\ 864)$

It can be written as $x^6 \equiv 640 + 4.864 \ (mod\ 864)$.

$$\equiv 4096 \ (864)$$

$$\equiv 4^6 \ (mod\ 4.6^3).$$

It is of the type $x^n \equiv a^n (mod\ b.n^r)\ \ with\ \ a = 4, b = 4, r = 3, n = 6$.

The corresponding solutions are $x \equiv bn^{r-1}k + a \ (mod\ bn^r); k = 0, 1, 2, 3, 4, 5$.

Putting the values, $x \equiv 4.6^{3-1}k + 4 \ (mod\ 4.6^3)$

$$\equiv 4.6^2k + 4\ (mod\ 864)$$

$$\equiv 144k + 4(mod\ 864)$$

$$\equiv 4, 148, 292, 436, 580, 724\ (mod\ 864)\ \ for\ k = 0, 1, 2, 3, 4, 5.$$

Lastly consider the congruence $x^8 \equiv 256\ (mod\ 3072)$.

It can be written as $x^8 \equiv 2^8\ (mod\ 8^4)$ with $a = 2, n = 8, b = 1, r = 4$.

It is of the type $x^n \equiv a^n\ (mod\ n^r)$.

Therefore the solutions are given by $x \equiv n^{r-1}k + a\ (mod\ n^r)$

$$\equiv 8^{4-1}k + 2\ (mod\ 8^4)$$

$$\equiv 8^3k + 2\ (mod\ 8^4)$$

$$\equiv 384k + 2\ (mod\ 3072);\ \ k = 0, 1, 2, 3, 4, 5, 6.$$

$$\equiv 2, 386, 770, 1154, 1538, 1922, 2306\ (mod\ 3072).$$

CONCLUSION

Therefore, it is concluded that the congruence

$x^n \equiv a^n\ (mod\ b.n^r);\ k = 0, 1, 2, \ldots\ldots, (n-1)$ has been formulated and the solutions are given by the formula $x \equiv bn^{r-1}k + a\ (mod\ b.n^r); b = 1, 2, 3, \ldots\ldots, (n-1)$.

MERIT OF THE PAPER

Formulation of the solutions of the said congruence is the merit of the paper. No such formulation is found in the literature of mathematics. Now it is needless to use CRT.

REFERENCE

[1] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to the Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd
[2] Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur
[3] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.