International Journal of Scientific Research and Engineering Development-– Volume 2 Issue 5, Sep – Oct 2019

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-97: Formulation of Special Class of Standard Bi-Quadratic Congruence 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 considereda special type of standard bi-quadratic congruence of composite modulus for formulation of its solutions. The author's efforts has provided a formulation of solutions of the said congruence. The discovered formula is tested true by solving different examples and by its verifications. Such formulation was not considered by earlier mathematicians and no effective method is found to find its solutions. Formulation is the merit of the paper. It is proved time-saving, easy and simple. Sometimes the solutions can be obtained orally. This is one more merit of the paper.This made the study of bi-quadratic congruence more interesting.

Keywords— Binomial expansion, Bi-quadratic Congruence, Composite Modulus, Formulation.

----------**********----------

INTRODUCTION

A congruence of the type $x^4 \equiv a\ (mod m)$ is called a bi-quadratic congruence. If m is a composite integer, then it is called a bi-quadratic congruence of composite modulus. If m is a prime, then it is called a bi-quadratic congruence of prime modulus. The value of x that satisfies the congruence is called its solution. If a is bi-quadratic residue of m, then the congruence:$x^4 \equiv a\ (mod m)$ is called solvable. If b is a residue of m &$b^4 \equiv a\ (mod m)$,

then,a is called bi-quadratic residue of m [1]**.**

The author already formulated some classes of standard biquadratic congruence of Prime and composite modulus and the papers are published in different international journals. Those papers are liked by the readers and the author got an up-thrust from it and planned to write one more paper on the formulation of a special standard bi-quadratic congruence of composite modulus.

A solvable standard Bi-quadratic congruence of composite modulus is a congruence of the type:

$x^4 \equiv a^4 (mod\ m); m$ being a composite positive integer. Its solutions are the values of x that satisfies the congruence. Some standard Bi-quadratic congruence has unique solutions; some has three solutions; some has four solutions and some has $p\ or\ p^2$or other solutions; p being a positive prime integer.

LITERATURE-REVIEW

Referring many books of Number Theory and surfing on Internet, no formulation is found in the literature. Only a definition and two problems of finding solutions of bi-quadratic residues are seen **[1]**.Thus, a very little literature about bi-quadratic congruence is present. There is no formulation and no suitable method found in the literature except the Chinese Remainder Theorem in which one has to solve the separated congruence and using the said theorem, complete solutions are obtained which has its own demerits. Readers found it very difficult to find solutions of the bi-quadratic congruence. In the book of Zuckerman et al, only a bi-quadratic congruence in the exercise is mentioned which is not solvable **[2].** The standard bi-quadratic congruence is neglected by the earlier mathematicians and do no research on it. It is a very important topic in Number Theory. No one showed interest to do some research on the topic. The author tried his best to formulate some standard bi-quadratic congruence of prime and composite modulus [4], [5], [6], [7].

NEED OF RESEARCH

To have an easy method of finding solutions, the author tried his best to formulate the congruence and presented his efforts in this paper, because the author knows the only way out is the formulation. It is a time-saving attempt of the author.

This is the need of the research.

PROBLEM-STATEMENT

The problem is "To formulate some classes of standard solvable bi-quadratic congruence of composite modulus of the type:

$$(1)\ x^4 \equiv a^4 (mod a^n); n > 4.$$

$(2) x^4 \equiv a^4\ (mod a^n . b)$; b $\neq al.$

ANALYSIS & RESULT

Consider the said congruence: $x^4 \equiv a^4 (mod a^n)$.

Then, for $x = a^{n-3}k \pm a,\ k = 0, 1, 2, 3, 4, \ldots\ldots$

$$x^4 = (a^{n-3}k \pm a)^4$$

Expanding using binomial theorem, one get

$$x^4 = (a^{n-3}k)^4 \pm 4.(a^{n-3}k)^3.a + \frac{4.3}{1.2}(a^{n-3}k)^2a^2 \pm \frac{4.3.2}{1.2.3}(a^{n-3})^1a^3 + a^4$$

$$= a^4 + a^n(\ldots\ldots)$$

$$\equiv a^4\ (mod a^n)$$

Thus, $x = a^{n-3}k \pm a$ satisfies the congruence and hence is a solution of it.

For $k = a^3,\ x = a^{n-3}.a^3 \pm a = a^n \pm a \equiv \pm a\ (mod a^n)$ which is same as $k = 0$.

Similarly, for next higher values of k,it can be seen that the solutions are the same as for

$$k = 1, 2, 3, etc.$$

Therefore, all the solutions are obtained for $k = 0, 1, 2, 3, \ldots\ldots\ldots a^3 - 1$.

Hence, the congruence has exactly $2a^3$ solutions.

Consider the congruence: $x^4 \equiv a^4 (mod b.a^n); b \neq al; lbeingapositiveinteger.$

Then, for $x = b.a^{n-3}k \pm a,\ k = 0, 1, 2, 3, 4, \ldots\ldots$

$$x^4 = (b.a^{n-3}k \pm a)^4$$

Expanding using binomial theorem, one get

$$x^4 = (b.a^{n-3}k)^4 \pm 4.(b.a^{n-3}k)^3.a + \frac{4.3}{1.2}(b.a^{n-3}k)^2a^2 \pm \frac{4.3.2}{1.2.3}(b.a^{n-3})^1a^3 + a^4$$

$$= a^4 + b.a^n(\ldots\ldots)$$

$$\equiv a^4\ (mod b.a^n)$$

Thus, $x = b.a^{n-3}k \pm a$ satisfies the congruence and hence is a solution of it.

For $k = a^3,\ x = b.a^{n-3}.a^3 \pm a = b.a^n \pm a \equiv \pm a\ (mod b.a^n)$ which is same as $k = 0$.

Similarly,for next higher values of k, it can be seen that the solutions are the same as for

$$k = 1, 2, 3 \ldots\ldots a^3 - 1.$$

Therefore, all the solutions are obtained for $k = 0, 1, 2, 3 \ldots\ldots\ldots a^3 - 1$.

Hence, the congruence has exactly $2a^3$ solutions.

Sometimes the congruence is of the type:$x^4 \equiv b\ (mod\ a^n)\ with\ b \neq a^4$.

If the congruence is solvable, them it can be written as:

$$x^4 \equiv b + k.a^n\ (mod\ a^n)$$

$\equiv a^4 (mod\ a^n),\ if\ b + k.a^n = a^4$ for some k **[3].**

Then the solutions are given as the formula established.

ILLUSTRATIONS

Consider the congruence: $x^4 \equiv 16$ (mod 32).

It can be written as:$x^4 \equiv 2^4 (mod 2^5)$**.**

It is of the type $x^4 \equiv a^4 (mod a^n) with a = 2, n = 5$. It has $2.2^3 = 16$ solutions.

Its solutions are given by $x \equiv a^{n-3}k \pm a (mod a^n)$.

$$\equiv 2^2k \pm 2\ (mod 2^5)$$

$\equiv 4k \pm 2\ (mod\ 32); k = 0, 1, 2, \ldots\ldots, (2^3 - 1)$

$$i.e.\ k = 0,1,2, \ldots\ldots, 7.$$

$$\equiv \pm 2, 4 \pm 2, \quad 8 \pm 2, 12 \pm 2, 16 \pm 2, 20 \pm 2, 24 \pm 2, 28 \pm 2 \ (mod\ 32).$$

$\equiv 2,30; 2, 6; 6, 10; 10, 14; 14, 18; 18, 22; 22, 26; 26, 30(mod\ 32).$

$\equiv 2, 6, 10, 14, 18, 22, 26, 30\ (mod\ 32)$. Some solutions repeats.

Consider the congruence $x^4 \equiv 81\ (mod\ 243)$.Here, $243 = 3^5$.

Then the congruence becomes $x^4 \equiv 3^4(mod 3^5)$.

It is of the type: $x^4 \equiv a^4(mod a^n) with a = 3,\ n = 5$.It has $2a^3 = 2(3^3 - 1) = 2(27) = 54\ solutions$.

The solutions are given by $x \equiv a^{n-3}k \pm a(mod a^n) for k = 0, 1, 2, \ldots \ldots 3^3 - 1$.

$$\equiv 3^2k \pm 3\ (mod 3^5)$$

$$\equiv 9k \pm 3\ (mod\ 243); k = 0, 1, 2, 3, \ldots \ldots \ldots, 26.$$

$$\equiv 0 \pm 3; 9 \pm 3; 18 \pm 3; 27 \pm 3; \ldots \ldots \ldots, 234 \pm 3\ (mod\ 243).$$

$$\equiv 3, \quad 240; 6, 12; 15, 21; 24, 30; \ldots \ldots .231, 237\ (mod\ 243).$$

$$\equiv 3, 6, 12, 15, 21, 24, 30, \ldots \ldots \ldots, 231, 237, 240\ (mod\ 243).$$

These are the 54 such solutions.

Consider the congruence $x^4 \equiv 256\ (mod\ 4096)$.Here,$4096 = 4^6$.

The congruence can be written as $x^4 \equiv 4^4(mod 4^6)$.

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

Then the solutions are given by

$$x \equiv a^{n-3}k \pm a(mod a^n) for k = 0, 1, 2, 3 \ldots \ldots a^3 - 1.$$

$$\equiv 4^3.k \pm 4\ (mod 4^6); k = 0, 1, 2, 3, \ldots \ldots \ldots .63.$$

$$\equiv 64k \pm 4\ (mod\ 4096)$$

$$\equiv 0 \pm 4; 64 \pm 4; 128 \pm 4; \ldots \ldots \ldots, 4032 \pm 4\ (mod\ 4096).$$

$$\equiv 4, 4092; 60, 68; 124, 132; \ldots \ldots \ldots .4028, 4036\ (mod\ 4096).$$

Consider one more example as $x^4 \equiv 3^4\ (mod\ 7.3^5$.

It is of the type: $x^4 \equiv a^4(mod b.a^n) with a = 3,\ n = 5, b = 7$.

Then the solutions are given by $x \equiv b.a^{n-3}k \pm a(mod\ b.a^n) for k = 0, 1, 2, 3 \ldots \ldots a^3 - 1$.

$$\equiv 7.3^2.k \pm 3\ (mod\ 7.3^5); k = 0, 1, 2, 3, \ldots \ldots \ldots .26.$$

$$\equiv 63k \pm 3\ (mod\ 1701)$$

$$\equiv 0 \pm 3; 63 \pm 3; 126 \pm 3; \ldots \ldots \ldots, 1638 \pm 3\ (mod\ 1701).$$

$$\equiv 3, 1698; 60, 66; 123, 129; \dots\dots\dots.1635,1641\ (mod\ 1701).$$

These are 54 incongruent solutions.

CONCLUSION

It can be concluded that the congruence under consideration$i.e.$

$$(1)x^4 \equiv a^4\ (moda^n)$$

$(2)x^4 \equiv a^4(modb.a^n); b \neq al.$

Each has exactly $2a^3$ incongruent solutions,as k has two solutions for every value of k, given by

(1) $x \equiv a^{n-3}.k \pm a(moda^n); k = 0, 1, 2, 3 \dots\dots\dots\dots a^3 - 1.$

$$(2)x \equiv b.a^{n-3}k \pm a(modb.a^n); k = 0, 1, 2, 3 \dots\dots\dots\dots a^3 - 1.$$

MERIT OF THE PAPER

First time, special class of standard solvable bi-quadratic congruence of composite modulus is formulated. Formulation is the merit of the paper. It is proved time-saving, easy and simple. Sometimes the solutions can be obtained orally. This is one more merit of the paper. This made the study of bi-quadratic congruence more interested

REFERENCE

[1]Thomas Koshy, 2009, *"Elementary Number Theory with Applications",* 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.

[2]Zuckerman H S at el, 2008, *An Introduction to The Theory of Numbers,* fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

[3] Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016,page No- 88, Das Ganu Prakashan, Nagpur.

[4]Roy B M, 2019,*Formulation of Some Classes of Solvable Standard Bi-quadratic Congruence of Prime-power Modulus,* International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-01,Jan-Feb- 19.

[5] Roy B M, 2019,*Formulation of a Special Class of Solvable Standard Bi-quadratic Congruence of Composite Modulus- an Integer Multiple of Power of Prime*, International Journal of science & Engineering Development (IJSDR), ISSN: 2456-3315, Vol-04, issue-03, March-2019.

[6]Roy B M, 2019,*An Algorithmic Method of Finding Solutions of Standard Bi-quadratic Congruence of Prime Modulus;* International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-04, APR-19.

[7] Roy B M, 2019,*Formulation of a Class of Standard Solvable Bi-quadratic Congruence of Even Composite Modulus- a Power of Prime-integer*,International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue-002, Feb-19.

……

