International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 6 June 2021, pp: 466-469 www.ijaem.net ISSN: 2395-5252

RP-168: Formulation of Solutions of aClass of Standard Bi-quadratic CongruenceModulo nth Power of an Odd Prime Multiplied by Four

Prof B M Roy
Head, Department of Mathematics Jagat Arts, Commerce & I H P Science College, Goregaon Dist-Gondia, M.S., India, Pin: 441801

Submitted: 25-05-2021 Revised: 01-06-2021 Accepted: 05-06-2021

ABSTRACT: In this paper, a standard bi-quadratic congruence of a special even composite modulus modulo nth power of an odd prime multiplied by four is formulated for the solutions in different cases. A new formula is established in every case.The established formulae are tested,verified and found true. Solved examples are illustrated using established formulae. The formulae workedwell. Time of calculation for readers is lessened. Formulation is the merit of the paper.

KEY-WORDS: Bi-quadratic congruence, Binomial expansion formula, Chinese Remainder Theorem.

I. INTRODUCTION

A congruence of the type: $x^4 \equiv b \pmod m$; m a composite positive integer,is called a standard bi-quadratic congruence of composite modulus.

The congruence is said to be solvable if b is a bi-quadratic residue of m [1], [2]. If b is so, then there must exist a positive integer a such thatb $\equiv a^4 \pmod m$. Then the congruence reduces to the form: $x^4 \equiv a^4 \pmod m$.

The author already has formulated some classes of standard bi-quadratic congruence of composite modulus.

II. PROBLEM-STATEMENT

The problem of study is-

"To establish formulae for the solutions of the standard bi-quadratic congruence:

$$(1) x^4 \equiv a^4 \pmod{4.p^n}; a \neq p, n \geq 2.$$

$$(2) x^4 \equiv p^4 \pmod{4.p^n}; n = 2, n = 3, \&n \geq 4,$$

p being a positive prime integer; n any positive integer.

III. LITERATURE REVIEW

The author referred many books on Number theory and found a very little discussion on the said congruence; but no formulation is found. The readers may use the famous Chinese Remainder Theorem. But it has its own demerits. The original congruence is to reduce to the individual congruence and they have to solve. Some individual congruence could not be solved easily. No formulation or any suitable method is mentioned in the literature.

The author already has formulated many standard bi-quadratic congruence of composite modulus [4], [5], [6], [7].

NEED OF RESEARCH

The literature of mathematics says approximately nothing about the said standard bi-quadratic congruence. Some discussion on general bi-quadratic congruence is found. The bi-quadratic congruence under consideration can be solved by a time-consuming and complicated method, known as Chinese Remainder Theorem (CRT) [3]. Readers do not want to use the CRT for solutions. The author tried his best with sincere effort to formulate some more congruence and presented the result in this paper. This is the need of the research.

IV. ANALYSIS & RESULTS

Case-I: When $a \neq p, n \geq 2$.

Consider the congruence: $x^4 \equiv a^4 \pmod{4p^n}$; p being a positive prime integer.

If $x = 2p^n k \pm a$, then by binomial expansion formula

$$x^4 = (2p^n k \pm a)^4$$

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

$$= 4p^n(\dots\dots) + a^4$$

$$\equiv a^4 \pmod{4p^n}.$$

Therefore, $x = 2p^n k \pm a$ satisfies the congruence $x^4 \equiv a^4 (\mathrm{mod}\ 4p^n)$ and hence it is a solution of the said congruence.

But for $k = 2, x = 2p^n.2 \pm a = 4p^n \pm a \equiv 0 \pm a\ (\mathrm{mod}\ 4p^n)$.

This is the same solutions as for $k = 0$.

Also, for $k = 3 = 2 + 1$, it is easily seen that the solutions are the same as for k=1.

Hence it can be concluded that the congruence has exactly four incongruent solutions

$$x \equiv 2p^n k \pm a\ (\mathrm{mod}\ 4p^n) \text{with } k = 0, 1.$$

Sometimes the congruence are given in the form: $x^4 \equiv b\ (\mathrm{mod}\ 4p^n)$

In such cases, it can be written as: $x^4 \equiv b + k.4p^n = a^4 (\mathrm{mod}\ 4p^n)$.

Case-II: When $a = p, n = 2$.

Then the congruence reduces to: $x^4 \equiv p^4 (\mathrm{mod}\ 4p^2)$;

p being a positive prime integer.

If $x = 2pk + p$, then by binomial expansion formula

$$x^4 = (2pk + p)^4$$
$$= (2pk)^4 + 4.(2pk)^3.p + \frac{4.3}{1.2}(2pk)^2.p^2 + \frac{4.3.2}{1.2.3}(2pk)^1.p^3 + p^4$$
$$= 4p^4(\dots\dots) + p^4$$
$$\equiv p^4\ (\mathrm{mod}\ 4p^2).$$

Therefore, $x = 2pk + p$ satisfies the congruence $x^4 \equiv p^4 (mod\ 4p^2)$ and hence it is a solution of the said congruence.

But for $k = 2p, x = 2p.2p + p = 4p^2 + p \equiv 0 + p\ (mod\ 4p^2)$.

This is the same solutions as for $k = 0$.

Also, for $k = 2p + 1$, it is easily seen that the solutions are the same as for k=1.

Hence it can be concluded that the congruence has exactly $2p$ incongruent solutions

$$x \equiv 2pk \pm p\ (mod\ 4p^2) with\ k = 0, 1, 2, \dots\dots\dots, (2p - 1).$$

Sometimes the congruence are given in the form: $x^4 \equiv b\ (mod\ 4p^2)$

In such cases, it can be written as: $x^4 \equiv b + k.4p^2 = a^4 (mod\ 4p^2)$.

Case-III: When $\boldsymbol{a = p, n = 3}$.

Then the congruence reduces to: $x^4 \equiv p^4 (mod\ 4p^3)$;

$p\ being\ a\ positive\ prime\ integer.$

If $x = 2p^2 k + p$, then by binomial expansion formula

$$x^4 = (2p^2 k + p)^4$$
$$= (2p^2 k)^4 + 4.(2p^2 k)^3.p + \frac{4.3}{1.2}(2p^2 k)^2.p^2 + \frac{4.3.2}{1.2.3}(2p^2 k)^1.p^3 + p^4$$
$$= 4p^n(\dots\dots) + p^4$$
$$\equiv p^4\ (mod\ 4p^3).$$

Therefore, $x = 2p^2 k + p$ satisfies the congruence $x^4 \equiv p^4 (mod\ 4p^3)$ and hence it is a solution of the said congruence.

But for $k = 2p^2, x = 2p^2.2p^2 + p = 4p^4 + p \equiv 0 + p\ (mod\ 4p^3)$.

This is the same solutions as for $k = 0$.

Also, for $k = 2p^2 + 1$, it is easily seen that the solutions are the same as for k=1.

Hence it can be concluded that the congruence has exactly $2p^2$ incongruent solutions

$$x \equiv 2p^2 k \pm p\ (mod\ 4p^3) with\ k = 0, 1, 2, \dots\dots\dots, (2p^2 - 1).$$

Sometimes the congruence are given in the form: $x^4 \equiv b\ (mod\ 4p^3)$

In such cases, it can be written as: $x^4 \equiv b + k.4p^3 = a^4 (mod\ 4p^3)$.

Case-IV: When $\boldsymbol{a = p, n} \geq \mathbf{4}$.

Consider the congruence: $x^4 \equiv a^4 (mod\ 4p^n); p\ being\ a\ positive\ prime\ integer.$

If $x = 2p^{n-3}k + p$, then by binomial expansion formula

$$x^4 = (2p^{n-3}k + p)^4$$
$$= (2p^{n-3}k)^4 + 4.(2p^{n-3}k)^3.p + \frac{4.3}{1.2}(2p^{n-3}k)^2.p^2 + \frac{4.3.2}{1.2.3}(2p^{n-3}k)^1.p^3 + p^4$$
$$= 4p^n(\dots\dots) + p^4$$
$$\equiv p^4\ (mod\ 4p^n).$$

Therefore, $x = 2p^{n-3}k + p$ satisfies the congruence $x^4 \equiv p^4 (mod\ 4p^n)$ and hence it is a solution of the said congruence.

But for $k = 2p^3, x = 2p^{n-3}.2p^3 + p = 4p^n + p \equiv 0 + p\ (mod\ 4p^n)$.

This is the same solutions as for $k = 0$.

Also, for $k = 2p^3 + 1$, it is easily seen that the solutions are the same as for k=1.

Hence it can be concluded that the congruence has exactly $2p^2$ incongruent solutions

$$x \equiv 2p^{n-3}k \pm p\ (mod\ 4p^n) with\ k = 0, 1, 2, \dots\dots\dots, (2p^3 - 1).$$

Sometimes the congruence are given in the form: $x^4 \equiv b\ (mod\ 4p^n)$

In such cases, it can be written as: $x^4 \equiv b + k.4p^n = a^4 (mod\ 4p^n)$.

V. ILLUSTRATIONS

Example-1: Consider the congruence $x^4 \equiv 81(mod\ 196)$.

It can be written as $x^4 \equiv 3^4 (mod\ 4.49)$ $i.e.$ $x^4 \equiv 3^4\ (mod\ 4.7^2)$

It is of the type $x^4 \equiv a^4 (mod\ 4.p^n)$ with $a = 3$, $p = 7$, $n = 2$, $a \neq p$.
It has exactly four incongruent solutions given by

$$x \equiv 2p^n k \pm a\ (mod\ 4.p^n)\ with\ k = 0, 1.$$
$$\equiv 2.7^2 k \pm 3\ (mod\ 4.7^2)$$
$$\equiv 98k \pm 3\ (mod\ 4.7^2)$$
$$\equiv 0 \pm 3;\ 98 \pm 3\ (mod\ 196)$$
$$\equiv 3, 193, 95, 101\ (mod\ 196)$$
$$\equiv 3, 95, 101, 193, (mod\ 196).$$

These are the required four solutions.

Example-2: Consider the congruence $x^4 \equiv 16 (mod\ 196)$.
It can be written as $x^4 \equiv 2^4 (mod\ 4.49)$ i.e. $x^4 \equiv 2^4\ (mod\ 4.7^2)$
It is of the type $x^4 \equiv a^4 (mod\ 4.p^n)$ with $a = 2$, $p = 7$, $n = 2$, $a \neq p$.
It has exactly four incongruent solutions given by

$$x \equiv 2p^n k \pm a\ (mod\ 4.p^n)\ with\ k = 0, 1.$$
$$\equiv 2.7^2 k \pm 2\ (mod\ 4.7^2)$$
$$\equiv 98k \pm 2\ (mod\ 4.7^2)$$
$$\equiv 0 \pm 2;\ 98 \pm 2\ (mod\ 196)$$
$$\equiv 2, 194, 96, 100\ (mod\ 196)$$
$$\equiv 2, 96, 100, 194, (mod\ 196).$$

These are the required four solutions.

Example-3: Consider the congruence $x^4 \equiv 25\ (mod\ 100)$
It can be written as $x^4 \equiv 25 + 6.100 = 625 = 5^4\ (mod\ 4.5^2)$
It is of the type $x^4 \equiv a^4 (mod\ 4.p^2)$ with $a = 5$, $p = 5, n = 2, a = p$.
It has exactly $2p$ incongruent solutions given by

$$x \equiv 2p^{n-1} k + p\ (mod\ 4.p^n); k = 0, 1 \ldots\ldots\ldots, (2p - 1)$$
$$\equiv 2.5k + 5\ (mod\ 4); k = 0, 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.5 - 1)$$
$$\equiv 10k + 5\ (mod\ 100); k = 0, 1, 2, 3, 4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, 9.$$
$$\equiv 0 + 5; 10 + 5; 20 + 5; 30 + 5; 40 + 5; 50 + 5; \ldots\ldots\ldots\ldots\ldots\ldots, 90 + 5\ (mod\ 100)$$
$$\equiv 5, 15, 25, 35, 45; \ldots\ldots\ldots\ldots\ldots\ldots\ldots, 95\ (mod\ 100).$$

These are the ten incongruent solutions of the congruence.

Example-3: Consider the congruence $x^4 \equiv 125\ (mod\ 500)$
It can be written as $x^4 \equiv 125 + 500 = 625 = 5^4\ (mod\ 4.5^3)$
It is of the type $x^4 \equiv a^4 (mod\ 4.p^n)$ with $a = 5$, $p = 5, n = 3, a = p$.
It has exactly $2p^2$ incongruent solutions given by

$$x \equiv 2pk + p\ (mod\ 4.p^n); k = 0, 1 \ldots\ldots\ldots, (2p^2 - 1)$$
$$\equiv 2.5k + 5\ (mod\ 4); k = 0, 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.5^2 - 1)$$
$$\equiv 10k + 5\ (mod\ 500); k = 0, 1, 2, 3, 4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, 49.$$
$$\equiv 0 + 5; 10 + 5; 20 + 5; 30 + 5; 40 + 5; 50 + 5; \ldots\ldots\ldots\ldots\ldots\ldots.490 + 5\ (mod\ 500)$$
$$\equiv 5, 15, 25, 35, 45; \ldots\ldots\ldots\ldots\ldots\ldots\ldots, 495\ (mod\ 500).$$

These are the fiftysolutions of the congruence.

Example-4: Consider the congruence $x^4 \equiv 625\ (mod\ 2500)$
It can be written as $x^4 \equiv 625 = 5^4\ (mod\ 4.5^4)$
It is of the type $x^4 \equiv p^4 (mod\ 4.p^n)$ with $a = 5$, $p = 5, n = 4, a = p$.
It has exactly $2p^3$ incongruent solutions given by

$$x \equiv 2p^{n-3} k + p\ (mod\ 4.p^n); k = 0, 1 \ldots\ldots\ldots, (2p^3 - 1)$$
$$\equiv 2.5k + 5\ (mod\ 4); k = 0, 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.5^3 - 1)$$
$$\equiv 10k + 5\ (mod\ 2500); k = 0, 1, 2, 3, 4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, 249.$$
$$\equiv 0 + 5; 10 + 5; 20 + 5; 30 + 5; 40 + 5; 50 + 5; \ldots\ldots\ldots\ldots\ldots\ldots.2490 + 5\ (mod\ 2500)$$
$$\equiv 5, 15, 25, 35, 45; \ldots\ldots\ldots\ldots\ldots\ldots\ldots, 2495\ (mod\ 500).$$

These are the two hundred and fifty solutions of the congruence.

Example-5: Consider the congruence $x^4 \equiv 81\ (mod\ 2916)$
It can be written as $x^4 \equiv 3^4\ (mod\ 4.3^6)$
It is of the type $x^4 \equiv p^4 (mod\ 4.p^n)$ with $a = p = 5, n = 6, a = p$.
It has exactly $2p^3$ incongruent solutions given by

$$x \equiv 2p^{n-3} k + p\ (mod\ 4.p^n); k = 0, 1 \ldots\ldots\ldots, (2p^3 - 1)$$
$$\equiv 2.3^{6-3} k + 3\ (mod\ 4.3^6$$
$$\equiv 2.27k + 3\ (mod\ 4.729); k = 0, 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (2.3^3 - 1)$$
$$\equiv 54k + 3\ (mod\ 2916); k = 0, 1, 2, 3, 4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, 53.$$
$$\equiv 0 + 3; 54 + 3; 108 + 3; 162 + 3; 216 + 3, \ldots\ldots\ldots\ldots\ldots\ldots, 2862 + 3\ (mod\ 2916)$$
$$\equiv 5, 15, 25, 35, 45; \ldots\ldots\ldots\ldots\ldots\ldots\ldots, 2865\ (mod\ 2916).$$

These are the fifty – four incongruent solutions of the congruence.

VI. CONCLUSION

Thus, it is concluded that the standard bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ 4.p^n)$
has exactly four incongruent solutions: $x \equiv 2p^n k \pm a\ (mod\ 4.p^n)$ with $k = 0, 1$
and p an odd prime, when $a \neq p$.
But the congruence $x^4 \equiv p^4\ (mod\ 4.p^2)$ has $2p$ incongruent solutions:

$x \equiv 2pk + p \pmod{4p^2}; k = 0, 1 \ldots \ldots \ldots, (2p - 1)$, when $n = 2$.
And the congruence $x^4 \equiv p^4 \pmod{4p^3}$ has $2p^2$ incongruent solutions:
$x \equiv 2pk + p \pmod{4.p^3}; k = 0, 1 \ldots \ldots \ldots, (2p^2 - 1)$, when $n = 3$.
And the congruence $x^4 \equiv p^4 \pmod{4.p^n}$ has $2p^3$ incongruent solutions:
$x \equiv 2p^{n-3}k + p \pmod{4.p^n}; k = 0, 1 \ldots \ldots \ldots, (2p^3 - 1)$, when $n \geq 4$.

MERIT OF THE PAPER

The standard bi-quadratic congruence is not found formulated in the literature of mathematics. The author established direct formulae for the solutions of the said congruence. Formulation makes the problems simple and time-saving. This is the merit of the paper.

REFERENCE

[1]. Zuckerman et al, 2008, An Introduction to The Theory of Numbers, Willey India (Pvt) Ltd, Fifth edition(Indian Print), ISBN: 978-81-265-1811-1.
[2]. Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press, second edition, ISBN: 978-81-312-1859-4.
[3]. David M Burton, 2012, Elementary Number Theory, McGraw Hill education, Seventh edition, ISBN: 978-1-25-902576-1.
[4]. Roy B M, Formulation of solutions of some classes of standard bi-quadratic congruence of composite modulus, (IJETRM), ISSN: 2456-9348, Vol-03, Issue-02, Feb-19.
[5]. Roy B M, Formulation of a Class of Standard Solvable Bi-quadratic Congruence of Even Composite Modulus- a Power of Prime-integer, (IJSDR), ISSN: 2455-2631, Vol-04, Issue-02, Feb-19.
[6]. Roy B M,Formulation of a Special Class of Solvable Standard Bi-quadratic Congruence of Composite Modulus- an Integer Multiple of Power of Prime, (IJSDR), ISSN: 2455-2631, Vol-04, Issue-03, Mar-19.
[7]. Roy B M,An Algorithmic Method of Finding Solutions of Standard Bi-quadratic Congruence of Prime Modulus,(IJSDR), ISSN: 2455-2631, Vol-04, Issue-04, April-19.