iJETRM
International Journal of Engineering Technology Research & Management

RP-172: SOLVING STANDARD BI-QUADRATIC CONGRUENCE MODULO A PRODUCT OF POWERED ODD PRIME & POWERED 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
(Affiliated to R T M Nagpur University)

ABSTRACT
In the present paper, the author has considered a standard bi-quadratic congruence for his study andformulated the solutions of the congruence under consideration. The formulation of the congruence is studied in twodifferent cases establishing four different formulae.Formulation proved a time-saving method of solving such congruence.In the literature referred for the solutions, the author found no formulation of solutions of the said congruence. The author has tried his best to formulate the solutions and his efforts are presented here.

Keywords
Bi-quadratic congruence, Binomial Expansion Formula, Incongruent Solutions, Formulation.

INTRODUCTION

A congruence of the type:$x^4 \equiv a^4 (mod\ k), k\ being\ a\ positive\ integer,$ is a standard bi-quadratic congruence. If k is a prime, it is called a congruence of prime modulus; otherwise, it is called a congruence of composite modulus. Finding no method or formulation for solutions of the congruence in the literature of mathematics [1], [2], [3], the author has attempted a formulation for solutions of the said congruence. Formulating and publishing many standard bi-quadratic congruence of various composite modulus in different international journals [4], [5], [6], [7], [8], the author considered the said congruence for its formulation.

PROBLEM-STATEMENT

Here the problem of the study is-"To formulate the solutions of the congruence:

$$x^4 \equiv a^4 (mod\ p^m . 4^n), p\ being\ an\ odd\ prime; a, m, n\ positive\ integers$$
$$in\ four\ different\ cases:$$

$case - I$: When a is an odd positive integer
$case - II$:When a is an odd positive integer

iJETRM
International Journal of Engineering Technology Research & Management

ANALYSIS & RESULTS

Consider the congruence: $x^4 \equiv a^4 (mod\ p^m.4^n); p\ an\ odd\ prime.$

Case-I: Let a be an odd positive integer.

For the solutions, consider $x \equiv p^m.4^{n-1}k \pm a\ (mod\ p^m.4^n)$

Then, $x^4 \equiv (p^m.4^{n-1}k \pm a)^4\ (mod\ p^m.4^n)$

$$\equiv (p^m.4^{n-1}k)^4 \pm 4.(p^m.4^{n-1}k)^3.a + \frac{4.3}{2.1}(p^m.4^{n-1}k)^2.a^2 \pm \frac{4.3.2}{1.2.3}p^m.4^{n-1}k.a^3 + a^4\ (mod\ p^m.4^n)$$

$$\equiv p^m.4^n k\{p^{3m}.4^{3n-4}.k^3 \pm p^{2m}.4^{2n-3}k^2.a + 2p^m.4^{n-2}k.a^2 \pm a^3\} + a^4\ (mod\ p^m 4^n)$$

$$\equiv 0 + a^4\ (mod\ p^m.4^n)$$

$$\equiv a^4 (mod\ p^m 4^n).$$

Therefore, $x \equiv p^m.4^{n-1}k \pm a\ (mod\ p^m.4^n)$ satisfies the congruence and hence is considered as the solutions formula. But if $k = 4$, the solutions formula reduces to

$$x \equiv p^m.4^{n-1}.4 \pm a\ (mod\ p^m.4^n)$$

$$\equiv p^m.4^n \pm a\ (mod\ p^m.4^n)$$

$$\equiv 0 \pm a\ (mod\ p^m.4^n).$$

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

Also for$k = 5 = 4 + 1$, the formula reduces to

$$x \equiv p^m.4^{n-1}(4+1) \pm a\ (mod\ p^m.4^n)$$

$$\equiv p^m.4^n + p^m.4^{n-1} \pm a\ (mod\ p^m.4^n)$$

$\equiv p^m.4^{n-1} \pm a(\ mod\ p^m.4^n).$

This is the same solutions as for $k = 1$.

Therefore, all the solutions are given by

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

Hence, the congruence has exactly eight solutions.

Case-II: Let a be even positive integer but $a \not\equiv 0\ (mod\ 4)$.

For the solutions, consider $x \equiv p^m.4^{n-3}k \pm a\ (mod\ p^m.4^n)$

Then, $x^4 \equiv (p^m.4^{n-3}k \pm a)^4\ (mod\ p^m.4^n)$

$$\equiv (p^m.4^{n-3}k)^4 \pm 4.(p^m.4^{n-3}k)^3.a + \frac{4.3}{2.1}(p^m.4^{n-3}k)^2.a^2 \pm \frac{4.3.2}{1.2.3}p^m.4^{n-3}k.a^3 + a^4\ (mod\ p^m.4^n)$$

$$\equiv p^m.4^{n-2}k\{p^{3m}.4^{3n-11}.k^3 \pm p^{2m}.4^{3n-8}k^2.a + 3p^m.4^{n-4}k.a^2 \pm a^3\} + a^4\ (mod\ p^m 4^n)$$

$$\equiv p^m.4^{n-2}k\{8t\} \pm a^4 (mod\ p^m.4^n), if\ a\ is\ even\,.$$

$$\equiv 0 + a^4\ (mod\ p^m.4^n)$$

$$\equiv a^4 (mod\ p^m 4^n).$$

Therefore, $x \equiv p^m.4^{n-3}k \pm a\ (mod\ p^m.4^n)$ satisfies the congruence and hence is considered as the solutions formula. But if $k = 64 = 4^3$, the solutions formula reduces to

$$x \equiv p^m.4^{n-3}.4^3 \pm a\ (mod\ p^m.4^n)$$

iJETRM
International Journal of Engineering Technology Research & Management

$$\equiv p^m.4^n \pm a\ (mod\ p^m.4^n)$$
$$\equiv 0 \pm a\ (mod\ p^m.4^n).$$

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

Also for$k = 65 = 4^3 + 1$, the formula reduces to

$$x \equiv p^m.4^{n-3}(4^3 + 1) \pm a\ (mod\ p^m.4^n)$$
$$\equiv p^m.4^n + p^m.4^{n-3} \pm a\ (mod\ p^m.4^n)$$

$\equiv p^m.4^{n-3} \pm a(\ mod\ p^m.4^n)$.

This is the same solutions as for $k = 1$.

Therefore, all the solutions are given by

$$x \equiv p^m.4^{n-3}.4 \pm a\ (mod\ p^m.4^n); k = 0, 1, 2, 3, \ldots\ldots\ldots (4^3 - 1).$$

Hence, the congruence has exactly one hundred and twenty-eight incongruent solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^4 \equiv 81\ (mod\ 6400)$.

It can be written as $x^4 \equiv\ 3^4(mod\ 5^2.4^4)$.

It is of the type $x^4 \equiv\ a^4(mod\ p^m.4^n)\ with\ p = 5,\ m = 2, n = 4,$
$a = 3, an\ odd\ positive\ integer.$

It has exactly eight solutions given by

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

$\equiv 5^2.4^3k \pm 3(mod 5^2.4^4)$

$$\equiv 25.64k \pm 3\ (mod\ 6400)$$
$$\equiv 1600k \pm 3\ (mod\ 6400)$$
$$\equiv 0 \pm 3; 1600 \pm 3; 3200 \pm 3; 4800 \pm 3\ (mod\ 6400)$$

$\equiv 3, 6397; 1597, 1603; 3197, 3203; 4897, 4803\ (mod\ 6400)$.

Example-2: Consider the congruence $x^4 \equiv 256\ (mod\ 6400)$.

It can be written as $x^4 \equiv\ 4^4(mod\ 5^2.4^4)$.

It is of the type $x^4 \equiv\ a^4(mod\ p^m.4^n)\ with\ p = 5, m = 2, n = 4,\ a = 4,$
$an\ even\ positive\ integer.$

It has exactly $4^3 = 64$ incongruent solutions given by

$x \equiv p^m.4^{n-3}k \pm 4\ (mod\ p^m.4^n)\ with\ k = 0, 1, 2, 3, \ldots\ldots.63.$

$\equiv 5^2.4^1k \pm 4(mod 5^2.4^4)$

$$\equiv 25.4k \pm 4\ (mod\ 6400)$$
$$\equiv 100k \pm 4\ (mod\ 6400)$$
$$\equiv 0 \pm 4; 100 \pm 4; 200 \pm 4; 300 \pm 4; \ldots\ldots\ldots; 6300 \pm 4\ (mod\ 6400)$$

$\equiv 4, 6396; 96, 104; 196, 204; 296, 304; \ldots\ldots\ldots\ldots\ldots\ldots; 6296, 6304\ (mod\ 6400)$.

Example-3: Consider the congruence $x^4 \equiv 1296\ (mod\ 32000)$.

It can be written as $x^4 \equiv 1296 =\ 6^4(mod\ 5^3.4^4)$.

It is of the type $x^4 \equiv\ a^4(mod\ p^m.4^n)\ with\ p = 5,\ a = 6, an\ even\ positive\ integer.$

It has exactly $4^3 = 64$ incongruent solutions given by

$x \equiv p^m.4^{n-3}k \pm 6\ (mod\ p^m.4^n)\ with\ k = 0, 1, 2, 3, \ldots\ldots (64 - 1).$

$\equiv 5^3.4k \pm 6(mod 5^3.4^4)$

iJETRM
International Journal of Engineering Technology Research & Management

$$\equiv 125.4k \pm 6\ (mod\ 32000)$$
$$\equiv 500k \pm 6\ (mod\ 32000)$$
$$\equiv 0 \pm 6; 500 \pm 6; 1000 \pm 6; 1500 \pm 6; \dots\dots\dots; 1260 \pm 6\ (mod\ 32000)$$
$$\equiv 6, 1274; 14, 26; 34, 46; 54, 66; \dots\dots\dots\dots\dots\dots; 1254, 1266\ (mod\ 32000).$$

CONCLUSION

Therefore, it can be the conclusion that the standard bi-quadratic congruence:
$x^4 \equiv a^4 (mod\ p^m.4^n)$, p an odd prime has exactly eight incongruent solutions:
$x \equiv p.4^{n-1}k \pm a\ (mod\ p^m.4^n)\ with\ k = 0,1,2,3$, if a is an odd positive integer
but the congruence has exactly one-hundred and twenty-eight incongruent solutions:
$x \equiv p.4^{n-3}k \pm a\ (mod\ p^m.4^n)\ with\ k = 0,1,2,3,\dots\dots..(64-1), if\ a$ is an even positive integer but $a \not\equiv 0\ (mod\ 4)$.

REFERENCE

[1] Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.
[2] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.
[3] David M Burton,2012,*Elementary Number Theory*, McGraw Hill education (Higher Education), Seventh Indian Edition, New Dehli, India, 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.
[8] Roy B M, Formulation of solutions of a class of standard bi-quadratic congruence modulo nth power of an odd prime multiplied by four, International Journal of Advances in Engineering and Management (IJAEM), ISSN: 2395-5252, Vol-03, Issue-06, Jun-21.