RP-184: Formulation of solutions of standard bi-quadratic congruence modulo double of a prime integer raised to the power n

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

This paper presents the results of the author's study on formulation of solutions of the standard bi-quadratic congruence of composite modulus modulo double of an odd prime integer raised to the power n. It is found that the congruence under consideration has exactly two incongruent solutions in first case while it has exactly p^3 incongruent solutions in the second case. A large number of solutions are formulated here in the second case. This makes the study and finding of the solutions very interesting and easy way for the said congruence. Such type of congruence is never formulated earlier; first time the author has formulated the congruence.

KEY-WORDS

Bi-quadratic congruence, Bi-quadratic residue, Binomial expansion.

INTRODUCTION

The congruence of the type: $x^4 \equiv b\ (mod\ m)$ is called a standard *bi-quadratic congruence*. It is said to be solvable if b is *bi-quadratic residue* of m and so it can be written as:

$b \equiv a^4\ (mod\ m)$. Then the congruence becomes: $x^4 \equiv a^4 (mod\ m)$. It is always solvable.

In this paper, the author considered $m = 2p^n, p\ being\ an\ odd\ prime\ positive\ integer$.

PROBLEM-STATEMENT

Here the author's problem of study for the current paper is-

"To formulate the solutions of the standard bi-quadratic congruence:

$x^4 \equiv a^4 (mod\ 2p^n); p\ odd\ prime\ in\ two\ different\ cases$".

LITERATURE REVIEW

The author referred many books of Number Theory [1], [2], [3]; but found no discussion on standard bi-quadratic congruence of prime and composite modulus. Only a definition of standard bi-quadratic congruence in [1] and a definition of bi-quadratic residue in [2]. The author first time started formulating the standard bi-quadratic congruence of composite modulus and his research-results are presented in different international journals [4], [5], [6], [7].

At last it is found that the current problem of study was remained unformulated by the author; hence, the same congruence is considered here for study and formulation.

ANALYSIS & RESULTS

Case-I: Let a be any positive integer, odd or even but a$\neq p$.

Now, consider the congruence: $x^4 \equiv a^4(mod\ 2p^n); p\ an\ odd\ prime.$

Then, $x^4 - a^4 \equiv 0\ (mod\ 2p^n)$

It can be factored as: $(x-a)(x+a)(x^2+a^2) \equiv 0\ (mod\ 2p^n)$

So, $x \equiv a, -a\ (mod\ 2p^n)$

$\equiv \pm a\ (mod\ 2p^n).$

These are the two solutions as the congruence $x^2 \equiv a\ (mod\ p) and\ hence$

$x^2 \equiv a\ (mod\ p^n)$ always has two solutions [1], [2], [3].

Case-II: Let $a = p$, p an odd prime.

Consider the congruence: $x^4 \equiv p^4(mod\ 2p^n); p\ odd\ prime.$

For the solutions, consider $x \equiv 2p^{n-3}k + p\ (mod\ 2p^n)$

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

Expanding by using Binomial Expansion Formula, one must have

$$x^4 \equiv (2p^{n-3}k\ )^4 + 4(\ 2p^{n-3}k)^3.p + \frac{4.3}{2.1}(\ 2p^{n-3}k)^2.p^2 + \frac{4.3.2}{3.2.1}2p^{n-3}k.p^3 + p^4\ (mod\ 2p^n)$$

$$\equiv 2p^nk\{8p^{3n-12}k^3 + 16k^2p^{2n-8} + 12kp^{n-4} + 4\} + p^4\ (mod\ 2p^n)$$

$$\equiv 0 + p^4\ (mod\ 2p^n)$$

$$\equiv p^4(mod\ 2p^n)$$

So, $x \equiv 2p^{n-3}k + p\ (mod\ 2p^n)$ can be considered as solutions formula of the said congruence.

But for $k = p^3, the\ solutions\ formula\ reduces\ to$

$x \equiv 2p^{n-3}.p^3 + p\ (mod\ 2p^n)$

$\equiv 2p^n + p\ (mod\ 2p^n)$

$\equiv 0 + p\ (mod\ 2p^n).$

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

Also, for $k = p^3 + 1,, the\ solutions\ formula\ reduces\ to$

$x \equiv 2p^{n-3}.(p^3+1) + p\ (mod\ 2p^n)$

$\equiv 2p^n + 2p^{n-3} + p\ (mod\ 2p^n)$

$\equiv 0 + 2p^{n-3} + p\ (mod\ 2p^n).$

$\equiv 2p^{n-3} + p\ (mod\ 2p^n)$

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

Therefore, all the solutions of the said congruence are given by

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

ILLUSTRATIONS

Example-1: Consider the congruence: $x^4 \equiv 16\ (mod\ 54)$

It can be written as: $x^4 \equiv 2^4\ (mod\ 2.3^3)$.

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

It has exactly two incongruent solutions given by

$x \equiv \pm a\ (mod\ 2p^n)$

$\equiv \pm 2\ (mod\ 2.3^3)$

$\equiv 2, 54 - 2\ (mod\ 54)$

$\equiv 2, 52\ (mod\ 54).$

Example-2: Consider the congruence: $x^4 \equiv 81\ (mod\ 250)$

It can be written as: $x^4 \equiv 3^4\ (mod\ 2.5^3)$.

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

It has exactly two incongruent solutions given by

$x \equiv \pm a\ (mod\ 2p^n)$

$\equiv \pm 3\ (mod\ 2.3^3)$

$\equiv 3, 250 - 3\ (mod\ 250)$

$\equiv 2, 247\ (mod\ 250).$

Example-3: Consider the congruence: $x^4 \equiv 625\ (mod\ 1250)$

It can be written as: $x^4 \equiv 5^4\ (mod\ 2.5^4)$.

It is of the type: $x^4 \equiv p^4\ (mod\ 2p^n) with\ p = 5, n = 4, a = 5, a = p.$

It has $p^3 = 125$ incongruent solutions given by

$x \equiv 2p^{n-3}k + p\ (mod\ 2p^n)$

$\equiv 2.5^{4-3}k + 5\ (mod\ 2.5^4); k = 0, 1, 2, \ldots\ldots, p^3 - 1.$

$\equiv 2.5^1k + 5\ (mod\ 1250); k = 0, 1, 2, 3, 4, \ldots\ldots\ldots\ldots\ldots 125 - 1.$

$\equiv 10k + 5\ (mod\ 1250); k = 0, 1, 2, \ldots\ldots\ldots\ldots, 124.$

$\equiv 0 + 5; 10 + 5; 20 + 5; 30 + 5; 40 + 5; \ldots\ldots\ldots; 1240 + 5\ (mod\ 1250)$

≡5, 15, 25, 35, 45, ……, 1245 (mod 1250).

CONCLUSION

Therefore it can be concluded that the bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ 2p^n)$,

$p\ an\ odd\ prime$, has exactly two incongruent solutions given by

$x \equiv \pm a\ (mod\ 2p^n)$ for odd as wel as even positive integer a.

But, if $a = p$, then the congruence: $x^4 \equiv p^4\ (mod\ 2p^n)$ has exactly p^3 incongruent solutions given by $x \equiv 2p^{n-3}k + p\ (mod\ 2p^n); k = 0, 1.2, 3, 4, \ldots\ldots\ldots (p^3 - 1).$

REFERENCES

[1] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.

[2] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley India (P) Ltd, 2008, ISBN: 978-81-265-1811-1.

[3] Burton David M., *Elementary Number Theory*, seventh edition, Mc Graw Hill education (India), 2017. ISBN: 978-1-25-902576-1.

[4] 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.

[5] Roy B M, *Formulation of solutions of standard biquadratic congruence of even composite modulus*, International Journal of Engineering Technology Research & Management (IJETRM), ISSN: 2456-9348, Vol-03, Issue-11, Nov-19.

[6] Roy B M, *Formulation Solutions of a special standard bi-quadratic congruence- modulo a powered odd prime*, (IJETRM), ISSN: 2456-9348, Vol-05, Issue-04, April-21.

[7] 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.