RP-86 Formulation of a Special Class of Solvable Standard Bi-quadratic Congruence of Composite Modulus-an Integer Multiple of Power of Prime

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, a special class of standard bi-quadratic congruence of composite modulus-an integer multiple of power of prime, is formulated. The established-formula is tested true. First time, a formula is developed for the solutions of the bi-quadratic congruence of the said type. Without formulation, it was very difficult to find the solutions of such congruence. Formulation makes it possible to do so. Here lies the merit of the paper.**

***Keywords*: Bi-quadratic congruence, Composite Number, Chinese Remainder Theorem.**

INTRODUCTION

A congruence of the type: $x^4 \equiv a \ (mod\ m)$; m being any positive integer, is called a standard bi-quadratic congruence. If m is an odd prime positive integer, then it is called a bi-quadratic congruence of prime modulus. If m is a composite positive integer, it is called a standard congruence of composite modulus. It is found that some bi-quadratic congruence has exactly one solution; some other has exactly four solutions and some has no solutions.

e.g. The congruence:

$x^4 \equiv 1 \ (mod\ 7)$ has exactly two solutions x$\equiv 1, 6 \ (mod\ 7)$;

$x^4 \equiv 1$ (mod 5)has exactly four solutions $x \equiv 1, 2, 3, 4$ (mod 5);

$x^4 \equiv 3$ (mod 7) has no solution.

Here the author wishes to formulate the standard bi-quadratic congruence of composite modulus. It is said that the standard bi-quadratic congruence: $x^4 \equiv a \ (mod\ p)$ is solvable if a is bi-quadratic residue of p [1].

LITERATURE REVIEW

The standard bi-quadratic congruence has not been considered and discussed systematically in the literature of mathematics. More literature on bi-quadratic congruence is not found but only a definition of it [2].

The author already formulated some classes of standard bi-quadratic congruence of the type:

$x^4 \equiv a^4 \ (mod\ 4p^n)$ & $x^4 \equiv a^4 \ (mod\ 8\ p^n)$ [3]

Also, $x^4 \equiv a^4 \ (mod\ 2^m\ p^n)$ [4]

NEED OF RESEARCH

Even some standard congruence of composite modulus of the type: $x^4 \equiv a^4 \ (mod\ b.p^n)$;

$b \neq p; b \neq 4k$, is remained to formulate. The author wishes to formulate such type of congruence.

The congruence under consideration can be solved by using Chinese Remainder Theorem.

But it is a lengthy producer and complicated. It takes a long time to get all the solutions.

Readers are always in search of an alternative.

Finding the standard bi-quadratic congruence a neglected chapter in Number Theory, the author willingly has gone through the chapter and found much material for the research work. He (the author) tried his best to formulate the bi-quadratic congruence, not previously formulated and wish to present his effort in this paper. This is the need of this study.

PROBLEM-STATEMENT

Here, the problem is

"To establish a formulation for the solutions of a class of standard bi-quadratic congruence

$x^4 \equiv a^4\ (mod\ b.p^n.)$; b≠ $4k, b \neq p,\ p\ prime\ \&\ b,\ n\ any\ positive\ integers.$

ANALYSIS & RESULT

Consider the congruence under consideration: $x^4 \equiv a^4(mod\ b.p^n\ ); b \neq 4k; b \neq p.$

For its solutions, let $x = b.p^{n-1}k + a;\ \ k = 0, 1, 2, 3, 4, 5 \dots \dots \dots$

Then, $x^4 = (b.p^{n-1}k + a)^4$

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

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

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

Thus, it is a solution of the said congruence.

If $k = p, p + 1, \dots \dots .., the\ solutions\ repeats\ as\ for\ k = 0,1, \dots .. (p - 1).$

Therefore, it is concluded that the said congruence has only p- solutions.

These are: $x \equiv b.p^{n-1}k + a\ \ (mod\ b.p^n)\ with\ k = 0, 1, 2,3 \dots \dots ., (p - 1); b \neq p, b \neq 4k.$

Sometimes said congruence can be written as: $x^4 \equiv c\ (mod\ b.p^n).$

In this case, it can be written as $x^4 \equiv c + k.b.p^n\ (mod\ b\ .p^n)$ [5]

$$\equiv a^4\ (mod\ b.p^n),\ if\ \ c + k.b.p^n = a^4.$$

The solutions are given by as before.

ILLUSTRATION

Consider the congruence: $x^4 \equiv 16\ (mod\ 2835)$

It can be written as $x^4 \equiv 16\ (mod\ 35.81).$

$$i.e.\ x^4 \equiv 2^4\ (mod\ 35.3^4).$$

It is of the type: $x^4 \equiv a^4\ (mod\ b.p^n)\ \ with\ a = 2, n = 4, b = 35.$

Such congruence always has p- solutions for k=0, 1 , 2, 3, ……., (p-1).

These solutions are given by $x \equiv b.p^{n-1}k + a\ (mod\ b.p^n)$

$$\equiv 35.3^3k + 2\ (mod\ 35.3^4)$$

$$\equiv 945k + 2\ (mod\ 2835)\ with\ k = 0, 1, 2.$$

$$\equiv 0 + 2, 945 + 2, 1890 + 2\ (mod\ 2835)$$

$$\equiv 2, 947, 1892\ (mod\ 2835).$$

Consider the congruence: $x^4 \equiv 81\ (mod\ 11250).$

$$i.e.\ x^4 \equiv 3^4\ (mod\ 18.625)$$

It can also be written as: $x^4 \equiv 3^4\ (mod\ 18.5^4)$.

It is of the type: $x^4 \equiv a^4\ (mod\ b.p^n)\ \ with\ a = 3, n = 4, b = 18,\ p = 5$.

Such congruence always has five solutions.

These solutions are given by $x \equiv b.p^{n-1}k + a\ (mod\ b.p^n)$; k = 0, 1, 2, …..,(p-1).

$$\equiv 18.5^3k + 3\ \ (mod\ 18.5^4)$$

$$\equiv 2250k + 3\ (mod\ 18.625)\ with\ k = 0, 1, 2, 3, 4.$$

$$\equiv 0 + 3, 2250 + 3, 4500 + 3, 6750 + 3, 9000 + 3\ (mod\ 11250)$$

$$\equiv 3, 2253, 4503, 6753, 9003\ (mod\ 11250).$$

Consider the congruence $x^4 \equiv 387\ (mod\ 3087)$.

It can be written as $x^4 \equiv 387 + 2.3087 = 6561\ = 9^4\ (mod\ 9.7^3)$

It is of the type $x^4 \equiv a^4\ (mod\ b.p^n)\ \ with\ a = 9, n = 3, b = 9,\ p = 7$.

It has four solutions given by $x \equiv b.p^{n-1}k + a\ \ (mod\ b.p^n),\ k = 0, 1, 2, 3, 4, 5, 6.$

$$\equiv 9.7^2\ k + 9\ (mod 2.35.4^3)$$

$$\equiv 441k + 9\ (mod\ 3087),\ k = 0, 1, 2, 3, 4, 5, 6.$$

$$\equiv 0 + 9,\ 441 + 9, 882 + 9, 1323 + 9, 1764 + 9, 2205 + 9, 2646 + 9\ (mod\ 3087).$$

≡9, 450, 891, 1332, 1773, 2214, 2655 (mod 3087)

CONCLUSION

Therefore, it is concluded that the standard bi-quadratic congruence of the type $x^4 \equiv a^4\ (mod\ b.p^n); b$ any integer with the conditions stated, has exactly p- solutions given by

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

MERIT OF THE PAPER

First time, a bi-quadratic congruence of the said type is considered for study and a formula is established to find all the solutions. Such type of standard bi-quadratic congruence is not yet formulated. Formulation is the merit of the paper.

REFERENCES

[1] Thomas Koshy, "*Elementary Number Theory with Applications*", 2/e (Indian print, 2009), Academic Press.
[2] Zuckerman H. S., Niven I., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.
[3] Roy B. M., Formulation of some classes of Solvable Standard Bi-quadratic Congruence of Prime-power Modulus, International Journal of Scientific Research & Engineering Development (IJSRED), Vol. 02; Issue-01; Feb. 2019, ISSN: Pages: 243-247.
[4] Roy B. M., 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), Vol.04; Issue-02; Feb. 2019.ISSN:2455-2631, Pages: 363-365.
[5] Roy B M, "*Discrete Mathematics & Number Theory*", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.