RP-85: Formulation of a Class of Standard Solvable Bi-quadratic Congruence of Even Composite Modulus- a Power of Prime-integer

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 class of standard solvable bi-quadratic congruence of even composite modulus is formulated. Now, it becomes possible to find all the solutions directly and very easily. No need to use Chinese Remainder Theorem. It is a time-consuming and complicated method. A formulation is established first time for the solutions of the congruence under consideration. This is the merit of the paper.**

***Keywords*: Bi-quadratic congruence, Binomial expansion, Chinese Remainder Theorem.**

INTRODUCTION

Quadratic congruence is an important topic in Number Theory and much had been discussed and studied earlier. Euler, Gauss and Fermat had given much attention to the topic. Even the author found a vast gap in the literature for research and has done well. Then the author turned to the standard cubic congruence and also found more place to do some research. At last the author himself takes the responsibility to do some more research in standard solvable bi-quadratic congruence of composite modulus.

LITERATURE-REVIEW

A standard bi-quadratic congruence is seldom studied and is an unseen topic of Mathematics (Number Theory). Nothing is seen in the literature of mathematics. Only a definition of bi-quadratic residue is mentioned. Also the solvability condition is not found. It is said that if $x^4 \equiv a\ (mod\ p)$ is solvable, then a is called the bi-quadratic residue of p [3]. Earlier mathematicians approached less to the topic. The author first time tried his best to formulate some standard bi-quadratic congruence successfully such as:

$x^4 \equiv a^4\ (mod\ 4.p^n)$ & $x^4 \equiv a^4\ (mod\ 8.p^n)$; p being a positive prime integer; n any positive integer. **[2]**

In continuation of the above last research, the author considered the next research paper:

$x^4 \equiv a^4\ (mod\ 2^m.p^n); m \geq 4.$

NEED OF RESEARCH

As no formulation of the said congruence under consideration was found in the literature of mathematics, it was difficult to find all the solutions using the existed method of solutions.

There is no other method except the use of Chinese Remainder Theorem. It is a long and time-consuming method. To get rid of such difficulty, the author tried his best to formulate the congruence and presented his sincere efforts in this paper. To have a formula for solutions is the need of the research.

PROBLEM-STATEMENT

Here the problem is:

"To formulate a class of standard solvable bi-quadratic congruence of even

Composite modulus - a power of a prime-integer of the type:

$$x^4 \equiv a^4\ (mod\ 2^m.p^n); m \geq 4;$$

and to elaborate the formulation for the reliability with suitable examples.

ANALYSIS & RESULT

Consider the said congruence

$$x^4 \equiv a^4 \ (mod\ 2^m.p^n); m \geq 4.$$

It can be separated in two congruence: (1) $x^4 \equiv a^4(mod\ 2^m); m \geq 4;$

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

Congruence (1) has exactly four solutions while the congruence (2) has exactly two solutions as p is an odd prime. Thus the congruence under consideration has exactly eight solutions [4].

For solutions, let $x = 2^m p^n \pm a.$

Then $x^4 = (2^m.p^n \pm a)^4$

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

$$= 2^m p^n(\dots \dots .) + a^4$$

$$\equiv a^4 \ (mod\ 2^m p^n).$$

Similarly it can also be proved that $x = 2^{m-1}p^n \pm a\ \ also\ satisfies: x^4 \equiv a^4(mod\ 2^m p^n).$

Thus, $x \equiv 2^m p^n \pm a;\ \ 2^{m-1}p^n \pm a \ (mod\ 2^m p^n)$ are the four obvious solutions of the said congruence.

Let $x = \pm(2^{m-2}p^n \pm a).$

Then $x^4 = (2^{m-2}p^n \pm a)^4$

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

$$= a^4 + 2^{m-1}p^n(\dots \dots \dots \dots .)$$

$$= a^4 + 2^{m-1}p^n(2t)$$

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

Therefore, $x = \pm(2^{m-2}p^n \pm a)$ are the four other solutions of the congruence.

It is also found that there is no other solution.

Hence the sad congruence has exactly eight solutions given by

$x \equiv 2^m p^n \pm a;\ \ 2^{m-1}p^n \pm a;\ \pm(2^{m-2}p^n \pm a)\ (mod\ 2^m p^n).$

Sometimes, the bi-quadratic congruence can be given as $x^4 \equiv b\ (mod\ 2^m p^n).$

If $b = a^4$, then nothing remains to prove. But if $b \neq a^4$, then the congruence is solved as under: $x^4 \equiv b + k.2^m p^n = a^4\ (mod\ 2^m p^n)$ for a suitable k, a positive integer. Then, the congruence can be solved as above [1].

ILLUSTRATIONS

Consider the congruence $x^4 \equiv 81\ (mod\ 144).$

It can be written as $x^4 \equiv 3^4\ (mod\ 2^4.3^2).$

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

The solutions are given by $x \equiv 2^m p^n \pm a;\ \ 2^{m-1}p^n \pm a;\ \pm(2^{m-2}p^n \pm a)\ (mod\ 2^m p^n).$

$$\equiv 2^4 3^2 \pm 3;\ 2^{4-1}3^2 \pm 3;\ \pm(2^{4-2}3^2 \pm 3)\ (mod\ 2^4 3^2)$$

$$\equiv 144 \pm 3; 72 \pm 3;\ \pm(36 \pm 3)\ \ (mod\ 144)$$

$$\equiv 3, 141; 69, 75;\ \pm 33;\ \pm 39\ (mod\ 144)$$

$$\equiv 3, 141; 69, 75; 33,111; 39,105 \ (mod\ 144).$$

Consider the congruence $x^4 \equiv 736 \ (mod\ 4000)$.

It can be written as $x^4 \equiv 736 + 5.4000 = 20736 = 12^4 \ (mod\ 2^5 5^3)$.

It is of the type $x^4 \equiv a^4 \ (mod\ 2^m p^n) \quad with\ a = 12, m = 5, n = 3, p = 5$.

Hence all the eight solutions are given by

$$x \equiv 2^m p^n \pm a;\ \ 2^{m-1} p^n \pm a;\ \pm(2^{m-2} p^n \pm a)\ (mod\ 2^m p^n).$$

$$\equiv 2^5 5^3 \pm 12;\ 2^4 5^3 \pm 12;\ \pm(2^3 5^3 \pm 12)(mod\ 2^5 5^3).$$

$$\equiv 4000 \pm 12;\ \ 2000 \pm 12;\ \pm(1000 \pm 12)\ (mod\ 4000)$$

$$\equiv 4000 \pm 12; 2000 \pm 12;\ \pm 988;\ \pm 1012\ (mod\ 4000)$$

$$\equiv 12, 3988; 1988, 2012; 988, 3012; 1012, 2988\ (mod\ 4000).$$

CONCLUSION

Therefore, as per the discussion made above, it can be concluded that the standard bi-quadratic solvable congruence under consideration $x^4 \equiv a^4 (mod\ 2^m p^n)$ has exactly eight incongruent solutions which are given by

$$x \equiv 2^m p^n \pm a;\ \ 2^{m-1} p^n \pm a;\ \pm(2^{m-2} p^n \pm a)\ (mod\ 2^m p^n).$$

MERIT OF PAPER

Sometimes, it takes long time to find solutions by existed method.

In this paper the standard solvable bi-quadratic congruence is formulated. It now becomes easy to find all the solutions directly with an ease. Thus, formulation of the solutions of the congruence is the merit of the paper.

REFERENCE

[1] Roy B M, "*Discrete Mathematics & Number Theory*", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.

[2] Roy, B. M., *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.

[3] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.

[4] Zuckerman H. S., Niven I., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.