RP-125: A Review & Re- formulation of Solutions of Standard Biquadratic Congruence of Even Composite Modulus

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 study, a review and reformulation of a standard bi-quadratic congruence of even composite modulus is considered. It is reviewed and reformulated. A simple formula is established. Using the formula developed, solutions of the standard bi-quadratic congruence can also be obtained orally. First formulation was not discussed fully. Later it is found that the solutions depends on odd and even positive integer. Thus, in the Re-formulation, the formula is developed considering different cases. A new formulation is the merit of the paper.**

Keywords**: Bi-quadratic congruence, Binomial expansion, Even Composite Modulus, Re-formulation.**

INTRODUCTION

A congruence of the form: $x^4 \equiv a\ (mod\ m)$; m being a composite positive integer, is a standard bi-quadratic congruence of composite modulus. If one can have $a \equiv b^4\ (mod\ m)$, then the congruence reduces to the form: $x^4 \equiv b^4\ (mod\ m)$ and the congruence is said to be solvable.

The values of x are called the solutions of the congruence. Here, in this paper, these solutions are to calculate by formulation of the congruence. In the literature of mathematics, no discussion of the congruence is found. Only quadratic congruence is considered as a prominent topic and much had been discussed and studied earlier. The author found a vast gap in the literature. After Euler, Fermat and Gauss, nothing was done on congruence. The author takes the opportunity to study and have some research for the standard bi-quadratic congruence of composite modulus.

In the literature, only a definition of bi-quadratic residue is mentioned. It is said that if

$x^4 \equiv a\ (mod\ m)$ is solvable, then a is called the bi-quadratic residue of m **[7].** The author first time tried to formulate the standard bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ m\ )$ for different values of m. For $m = p,\ 4p^n, 8p^n, 2^m.p^n, 4^n.b, etc.$, the author already has some formulation **[1], [2], [3], [4], [5], [6].**

. Now, in continuation of the above research, the author considered the next research paper for $m = 2^m$.

Then the congruence of study for formulation is:

$x^4 \equiv a^4\ (mod\ 2^m), m \geq 4.$

NEED OF REVIEW & REFORMULATION

The above problem is already formulated and published in IJETRM, Vol-03, Issue-02,Feb-19.

But unfortunately it was not considered for different cases for a. After reviewing the paper, it is found that there needs a reformulation of the paper considering different cases of a. It is considered in this paper. Thus, a reformulation is in need.

PROBLEM-STATEMENT

Here the problem is:

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

Composite modulus of the type: $x^4 \equiv a^4\ (mod\ 2^m); m \geq 4;$

in two different cases:

Case-I: If $a \neq 1$ is an odd positive integer;

Case-II: If a is an even positive integer.

ANALYSIS & RESULT

Case-I: Let $a \neq 1$ be an odd positive integer.

Consider the said congruence: $x^4 \equiv a^4 \ (mod\ 2^m); m \geq 4$.

Let us consider that $x = (2^{m-2}.k \pm a); k = 0, 1, 2, \ldots\ldots\ldots\ldots$

Then,

$x^4 = (2^{m-2}.k \pm a)^4$

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

$= a^4 + 2^m.k(t); t\ a\ positive\ integer.$

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

Therefore, $x \equiv (2^{m-2}.k \pm a)$ (mod 2^m) are the solutions of the said congruence.

For $k = 4,\ the\ solution - formla\ becomes: x \equiv (2^{m-2}.4 \pm a)\ (mod\ 2^m)$

$\equiv (2^m \pm a)\ (mod\ 2^m)$

$\equiv \pm a\ (mod\ 2^m)$, which is the same solution as for $k = 0$.

For $k = 5 = 4 + 1 = 2^2 + 1$, then the solution formula becomes

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

$\equiv \{2^{m-2}.2^2 + 2^{m-2}.1\} \pm a \quad (mod\ 2^m)$

$\equiv \{2^m + 2^{m-2}\} \pm a)\ (\ mod\ 2^m)$

$\equiv (2^{m-2} \pm a)\ (\ mod\ 2^m)$

Which is the same solution as for k=1.

Similarly for $k =$ 6,7, the solutions are the same as for $k =$ 2, 3,

Thus, all the solutions are given by $x \equiv (2^{m-2}.k \pm a)\ (mod\ 2^m); k = 0, 1, 2, 3.$

Therefore, the congruence has exactly eight solutions.

Case-II: Let a be an even positive integer.

Consider the said congruence: $x^4 \equiv a^4 \ (mod\ 2^m); m \geq 4$.

Let us consider that $x = (2^{m-3}.k \pm a); k = 0, 1, 2, \ldots\ldots\ldots\ldots$

Then,

$x^4 = (2^{m-3}.k \pm a)^4$

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

$= a^4 + 2^m.k(t); t\ a\ positive\ integer.$

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

Therefore, $x \equiv (2^{m-3}.k \pm a)$ (mod 2^m) are the solutions of the said congruence.

For $k = 8,\ the\ solution - formla\ becomes: x \equiv (2^{m-3}.8 \pm a)\ (mod\ 2^m)$

$\equiv (2^m \pm a)\ (mod\ 2^m)$

$\equiv \pm a\ (mod\ 2^m)$, which is the same solution as for $k = 0$.

For $k = 9 = 8 + 1 = 2^3 + 1$, then the solution formula becomes

$x \equiv 2^{m-3}.(2^3 + 1) \pm a\ (\ mod\ 2^m)$

$\equiv \{2^{m-3}.2^3 + 2^{m-3}.1\} \pm a \quad (mod\ 2^m)$

$\equiv \{2^m + 2^{m-3}\} \pm a)\ (mod\ 2^m)$

$\equiv (2^{m-3} \pm a)\ (mod\ 2^m)$

Which is the same solution as for k=1.

Similarly for $k = 10, 11$, the solutions are the same as for $k = 2, 3, \ldots \ldots$

Thus, all the solutions are given by $x \equiv (2^{m-3}.k \pm a)\ (mod\ 2^m); k = 0, 1, 2, 3 \ldots \ldots .7.$

Therefore, the congruence has exactly sixteen solutions.

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

If $c \equiv a^4\ (mod\ 2^m)$, then nothing remains to prove. But if not, then the congruence is solved as under: $x^4 \equiv c + l.2^m = a^4\ (mod\ 2^m)$ for a suitable l, a positive integer. Then, the congruence can be solved as above.

ILLUSTRATIONS

Consider the congruence $x^4 \equiv 1\ (mod\ 16)$.

It can be written as $x^4 \equiv 1^4\ (mod\ 2^4)$.

It is of the type $x^4 \equiv a^4 (mod\ 2^m)\ \ with\ a = 1,\ m = 4.$

The solutions are given by

$x \equiv (2^{m-2}.k \pm a)\ (mod\ 2^m).$

$\equiv (2^{4-2}.k \pm 1)\ (mod\ 2^4)$

$\equiv (4.k \pm 1)\ (mod\ 2^4); k = 0, 1, 2, 3.$

$\equiv \pm 1; 4 \pm 1, ; 8 \pm 1;\ 12 \pm 1\ (mod\ 16)$

$\equiv 1, 15; 5, 7; 11, 13; 17, 19; 23, 25; 29, 31;\ 35, 37; 41, 43\ (mod\ 48).$

These are the sixteen solutions of the congruence. They are tested and verified true.

Consider the congruence $x^4 \equiv 17\ (mod\ 64)$.

It can be written as $x^4 \equiv 17 + 64 = 81 = 3^4\ (mod\ 2^6)$.

It is of the type $x^4 \equiv a^4\ (mod\ 2^m)\ \ \ with\ a = 7, m = 6.$

As a is an odd positive integer, the congruence must have eight incongruent solutions.

All these solutions are given by

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

$\equiv (2^4.k \pm 3)(mod\ 2^6)$

$\equiv (16k \pm 3)\ (mod\ 64)$

$\equiv 0 \pm 3;\ 16 \pm 3; 32 \pm 3;\ 48 \pm 3\ \ (mod\ 64)$

$\equiv 3, 61; 13, 19; 29, 35; 45, 51\ (mod\ 64).$

Let us consider one more example: $x^4 \equiv 256 (mod\ 512)$.

It can be written as: $x^4 \equiv 4^4 (mod\ 2^9.)$.

Here, $a = 4, m = 9.$

As a is an even positive integer, the congruence must have sixteen incongruent solutions.

All these solutions are given by

$x \equiv (2^{m-3}.k \pm a)\ (mod\ 2^m); k = 0, 1, 2, 3, 4, 5, 6, 7.$

$\equiv (2^{9-3}.k \pm 4)\ (mod\ 2^9).$

$\equiv (2^6.k \pm 4)\ (mod\ 2^9).$

$\equiv (64.k \pm 4)\ (mod\ 512)$.

$\equiv 0 \pm 4; 64 \pm 4; 128 \pm 4; 192 \pm 4; 256 \pm 4; 320 \pm 4; 384 \pm 4; 448 \pm 4\ (mod\ 512)$.

$\equiv 4, 508; 60, 68; 124, 132; 188, 196; 252, 260; 316, 324;\ 380, 388; 444, 452\ (mod\ 1536)$.

These are the required sixteen incongruent solutions of the congruence.

CONCLUSION

Therefore, it can be concluded that the standard bi-quadratic congruence under consideration

$x^4 \equiv a^4 (mod\ 2^m); m \geq 4$ has exactly eight incongruent solutions which are

given by: $x \equiv (2^{m-2}.k \pm a)\ (mod\ 2^m); k = 0, 1, 2, 3.$

$if\ a\ is\ an\ odd\ positive\ integer.$

It is also concluded that the standard solvable bi-quadratic congruence under consideration

$x^4 \equiv a^4 (mod\ 2^m); m \geq 4$ has exactly sixteen incongruent solutions which are

given by: $x \equiv (2^{m-3}.k \pm a)\ (mod\ 2^m); k = 0, 1, 2, 3, 4, 5, 6, 7,$

$if\ a\ is\ an\ even\ positive\ integer.$

MERIT OF PAPER

In this paper, the standard solvable bi-quadratic congruence is studied, reviewed and re-formulated. It now becomes easy to find all the solutions directly. Thus, formulation of the solutions of the congruence is the merit of the paper.

REFERENCES

[1] 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, Vol-02; Issue-01, Feb-19.
[2] Roy B. M., *Formulation of Special Class of Standard Bi-quadratic Congruence of Composite Modulus*, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN-2581-7175, Vol-04; Issue-09, Sep-19.
[3] 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), ISSN: 2455-2631, Vol-04, Issue 02, Feb-19.
[4] Roy B. M., An Algorithmic Method of Finding Solutions of Standard Bi-quadratic Congruence of Prime Modulus, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-04, Issue 02;April-19.
[5] Roy B. M., *Formulation of solutions of some classes of standard bi-quadratic congruence of composite modulus*, International Journal of Engineering Technology Research & Management (IJETRM), ISSN: 2456-9348, Vol-03, Issue-02, Feb-19.
[6] Roy B M, *Formulation of solutions of some of standard bi-quadratic congruence of even composite modulus-a multiple of an odd Integer*, International Journal of Engineering Technology Research & Management (IJETRM), ISSN: 2456-9348, Vol-03, Issue-12, Dec-19.
[7] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.