RP-175: Solving Special Standard Biquadratic Congruence of composite modulus - A Review and Reformulation

Prof. B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce, & I H P Science College, Goregaon
Dist- Gondia, M. S., India. Pin: 441801

***Abstract*: In this paper, two special standard biquadratic congruence of composite modulus modulo a powered four and a positive integer multiple of powered four are reviewed and reformulated for its solutions in new cases. The truth of the formulae established is tested and verified by solving some suitable examples. Earlier mathematicians had shown no interest in studying and formulating such congruence. First time the author has taken the attempt to formulate the congruence for its solutions.**

***Keywords*: Biquadratic congruence, Biquadratic Residues, Binomial Theorem, Incongruent solutions.**

INTRODUCTION

A congruence of the type $x^4 \equiv a \ (mod\ m)$ is called a standard bi-quadratic congruence modulo m. If m is a composite integer, then it is called a bi-quadratic congruence of composite modulus. If m is a prime, then it is called a bi-quadratic congruence of prime modulus. The values of x that satisfy the congruence are called its solutions. If a is bi-quadratic residue of m, the congruence: $x^4 \equiv a \ (mod\ m)$ is called solvable.
If b is a residue of m, and $b^4 \equiv a \ (mod\ m)$, then a is called bi-quadratic residue of m .
The author already formulated some classes of standard cubic congruence of composite modulus and the papers are published in different international journals. Those papers are liked by the readers and the author got an up-thrust from it and planned to write papers on the formulation of standard bi-quadratic congruence of composite modulus.

LITERATURE-REVIEW

Referring many books of Number Theory and surfing on Internet, no formulation is found in the literature. Only a definition and two problems of finding bi-quadratic residues are seen **[1]**.Thus, a very little literature about bi-quadratic congruence is present. There is no formulation and no suitable method found in the literature except the Chinese Remainder Theorem in which one has to solve the separated congruence and using the said theorem, complete solutions are obtained **[2],** which has its own demerits. Readers found it very difficult to find solutions of the bi-quadratic congruence. In the book of Zuckerman et al, only a bi-quadratic congruence in the exercise is mentioned which is not solvable **[3].** The condition of solvability is also not stated or discussed.

NEED OF REVIEW & REFORMULATION

Previously the author had published a paper on formulation of solutions of the congruence: $x^4 \equiv a^4 \ (mod\ 4^n)\ \ and\ \ x^4 \equiv a^4 \ (mod\ b.4^n); b \neq 4l,$ [5]. There the problem was solved siting only eight solutions. But at present some new cases are considered and discussed and formulated
Hence a fresh review is made and a reformulation is done.

PROBLEM-STATEMENT

The problem is "To formulate two classes of standard solvable bi-quadratic congruence of composite modulus of the type:

(1) $x^4 \equiv a^4 \ (mod\ 4^n)$
(2) $x^4 \equiv a^4 \ (mod\ 4^n.b)$; b $\neq 4l\ i.e.\ b \not\equiv 0 \ (mod\ 4)$.

ANALUSIS & RESULTS

Consider the first congruence: $x^4 \equiv a^4 \ (mod\ \ 4^n)$.
Case-I: Let $a\ be\ an\ odd\ positive\ integer$.
Then, for the solutions, consider

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

So, $x^4 \equiv (4^{n-1}k \pm a)^4 \ (mod\ 4^n)$

Expanding using binomial theorem, one get

$$x^4 \equiv (4^{n-1}k)^4 \pm 4.(4^{n-1}k)^3.a + \frac{4.3}{1.2}(4^{n-1}k)^2a^2 \pm \frac{4.3.2}{1.2.3}(4^{n-1}k)^1a^3 + a^4$$
$$\equiv 4^nk\left(4^{3n-4}k^3 \pm 4^{2n-2}k^2a + \frac{3}{2}4^{n-1}ka^2 \pm\ a^3\right) + a^4 \ (mod\ 4^n)$$
$$\equiv 0 + a^4 \ (mod\ 4^n), if\ a\ is\ an\ odd\ positive\ integer.$$

$\equiv a^4 \ (mod\ 4^n)$

Thus, $x = 4^{n-1}k \pm a$ satisfies the congruence and hence is a solution of it for odd a.
For $k = 4$, $x = 4^{n-1}.4 \pm a = 4^n \pm a \equiv 0 \pm a \ (mod\ 4^n)$ which is same as $k = 0$.
Similarly, for $k = 5, 6, 7,$ it can be seen that the solutions are the same as for $k = 1, 2, 3$ $respectively$. Therefore, all the solutions are obtained for $k = 0, 1, 2, 3$.
Hence, the congruence has exactly eight solutions, if a is an odd positive integer.

Case-II: Let a be an even positive integer.
Then, for the solutions, consider

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

Expanding using binomial theorem, one get

$$x^4 \equiv (4^{n-2}k)^4 \pm 4.(4^{n-2}k)^3.a + \frac{4.3}{1.2}(4^{n-2}k)^2a^2 \pm \frac{4.3.2}{1.2.3}(4^{n-2}k)^1a^3 + a^4$$
$$\equiv 4^{n-1}k(4^{3n-7}k^3 \pm 4^{2n-2}k^2a + 4^{n-2}ka^2 \pm a^3) + a^4 \ (mod\ 4^n)$$
$$\equiv 4^{n-1}k(4t) + a^4 \ (mod\ 4^n)$$
$$\equiv 0 + a^4 \ (mod\ 4^n), if\ a\ is\ an\ even\ positive\ integer.$$
$$\equiv a^4 \ (mod\ 4^n)$$

Thus, $x \equiv 4^{n-2}k \pm a \ (mod\ 4^n)$ satisfies the congruence and hence is a solution of it for even a.
For $k = 16 = 4^2$, $x = 4^{n-2}.4^2 \pm a = 4^n \pm a \equiv 0 \pm a \ (mod\ 4^n)$ which is same as $k = 0$.
Similarly, for $k = 17,$ it can be seen that the solutions are the same as for $k = 1$.
Therefore, all the solutions are obtained for $k = 0, 1, 2, 3, \dots\dots\dots, 15$.
Hence, the congruence has exactly $2.4^2 = 32$ Solutions, if a is an even positive integer.

Case-III: Let $a = 4$.
Then, for the solutions, consider

$$x \equiv 4^{n-3}k \pm 4 \ (mod\ 4^n), k = 0, 1, 2, 3, 4, \dots\dots$$
$$\equiv (4^{n-3}k \pm 4)^4 \ (mod\ 4^n)$$

Expanding using binomial theorem, one get

$$x^4 \equiv (4^{n-3}k)^4 \pm 4.(4^{n-3}k)^3.4 + \frac{4.3}{1.2}(4^{n-3}k)^2 4^2 \pm \frac{4.3.2}{1.2.3}(4^{n-3}k)^1 4^3 + 4^4$$
$$\equiv 4^{n-2}k\left(4^{3n-10}k^3 \pm 4^{2n-6}k^2.4 + \frac{3}{2}4^{n-3}k4^2 \pm 4^3\right) + 4^4 \ (mod\ 4^n)$$
$$\equiv 4^{n-2}k(4^2t) + 4^4 \ (mod\ 4^n)$$
$$\equiv 0 + 4^4 \ (mod\ 4^n).$$
$$\equiv 4^4 \ (mod\ 4^n)$$

Thus, $x \equiv 4^{n-3}k \pm 4 \ (mod\ 4^n)$ satisfies the congruence and hence is a solution.
For $k = 64 = 4^3$, $x = 4^{n-3}.4^3 \pm 4 = 4^n \pm 4 \equiv 0 \pm 4 \ (mod\ 4^n)$ which is same as $k = 0$.
Similarly, for $k = 65 = 64 + 1 = 4^3 + 1,$ it can be seen that the solutions are the same as for $k = 1$.
Therefore, all the solutions are obtained for $k = 0, 1, 2, 3, \dots\dots\dots, 63$.
Hence, the congruence has exactly $2.4^3 = 2.64 = 128$ Solutions.

Now, consider the second congruence: $x^4 \equiv a^4 \ (mod\ b.4^n); b \not\equiv 0 \ (mod\ 4); a\ oddinteger$.
Then, for $x = b.4^{n-1}k \pm a,\ k = 0, 1, 2, 3, 4, \dots\dots$

$$x^4 = (b.4^{n-1}k \pm a)^4$$

Expanding using binomial theorem, one get

$$x^4 = (b.4^{n-1}k)^4 \pm 4.(b.4^{n-1}k)^3.a + \frac{4.3}{1.2}(b.4^{n-1}k)^2a^2 \pm \frac{4.3.2}{1.2.3}(b.4^{n-1})^1a^3 + a^4$$
$$= a^4 + b.4^n(\dots\dots), if\ a\ is\ odd\ positive\ integer;$$
$$\equiv a^4 \ (mod\ b.4^n)$$

Thus, $x = b.4^{n-1}k \pm a$ satisfies the congruence and hence is a solution of it.
For $k = 4$, $x = b.4^{n-1}.4 \pm a = b.4^n \pm a \equiv \pm a \ (mod\ b.4^n)$ which is same as $k = 0$.
Similarly, for $k = 5, 6, 7,$ it can be seen that the solutions are the same as for $k = 1, 2, 3$.
Therefore, all the solutions are obtained for $k = 0, 1, 2, 3$.
Hence, the congruence has exactly eight solutions.
As in the above, the congruence: $x^4 \equiv a^4 \ (mod\ b.4^n); b \not\equiv 0 \ (mod\ 4)$, a is even positive integer, it can be seen that the congruence has exactly $2.4^2 = 32$ Incongruent solutions given by $x \equiv b.4^{n-2}k \pm a \ (mod\ b.4^n) for\ k = 0, 1, 2, \dots\dots, 15$.
Also it can be seen that if $a = 4$, the solutions are given by
$x \equiv b.4^{n-3}k \pm 4 \ (mod\ b.4^n) for\ k = 0, 1, 2, \dots\dots, 63$.
This gives one hundred and twenty- eight solutions.

ILLUSTRATIONS
Example-1: Consider the congruence: $x^4 \equiv 113$ (mod 256).
It can be written as: $x^4 \equiv 113 + 2.256 = 625 = 5^4 (mod\ 4^4)$.

It is of the type $x^4 \equiv a^4 \ (mod\ 4^n)\ \ with\ a = 5, n = 4.$
Its solutions are given by $x \equiv 4^{n-1}k \pm a\ (mod\ 4^n).$
$\equiv 4^3k \pm 5\ (mod\ 4^4)$
$\equiv 64k \pm 5\ (mod\ 256)$
$\equiv \pm 5{,}59,\ 69, 123, 133, 187, 197\ (mod\ 256).$
$\equiv 5, 251;\ 59, 69;\ 123{,}133;\ 187, 197\ (mod\ 256)$
$\equiv 5, 59, 69, 123, 133, 187, 197, 251\ (mod\ 256)$

Example-2: Consider the congruence $x^4 \equiv 16\ (mod\ 384).$
Here $256 = 4^4.$
The congruence can be written as $x^4 \equiv 2^4\ (mod\ 4^4).$
It is of the type: $x^4 \equiv a^4 (mod\ 4^n)\ \ with\ a = 2,\ \ n = 4.$
Then the solutions are given by
$x \equiv 4^{n-2}k \pm a\ (mod\ 4^n) for\ k = 0, 1, 2, \ldots\ldots, 15.$
$\equiv 4^2.k \pm 2\ (mod\ 4^4)$
$\equiv 16k \pm 2\ (mod\ 256)$
$\equiv 0 \pm 2; 16 \pm 2; 32 \pm 2; 48 \pm 2; 64 \pm 2; 80 \pm 2; 96 \pm 2; 112 \pm 2; 128 \pm 2;$
$144 \pm 2; 160 \pm 2; 176 \pm 2; 192 \pm 2; 208 \pm 2; 224 \pm 2; 240 \pm 2\ (mod\ 256).$
$\equiv 2, 254; 14, 18; 30{,}34; 46, 50; 62, 66; 78, 82; 94, 98; 110, 114; 126, 130;$
$142, 146; 158, 162; 174, 178; 190, 194; 206, 210; 222, 226; 238, 242\ (mod\ 256).$

Example-3: Consider $x^4 \equiv 256 (mod\ 1024)$
It can be written as $x^4 \equiv 4^4 (mod\ 4^5)$
It is of the type: $x^4 \equiv 4^4 (mod\ 4^n)$
Its solutions are $x \equiv 4^{n-3}k \pm 4\ (mod\ 4^n)$
$\equiv 4^2k \pm 4\ (mod\ 4^5)$
$\equiv 16k \pm 4\ (mod\ 1024); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots, 63.$
$\equiv 0 \pm 4; 16 \pm 4; 32 \pm 4; 48 \pm 4; \ldots\ldots\ldots\ldots; 1008 \pm 4\ (mod\ 1024).$
$\equiv 4{,}1020; 12, 20; 28, 36; 44{,}52; \ldots\ldots\ldots; 1004, 1012\ (mod\ 1024).$
These are the required one hundred and twenty-eight solutions of the congruence.

Example-4: Consider $x^4 \equiv 16 (mod\ 128)$
It can be written as $x^4 \equiv 2^4 (mod\ 2.4^3)$
It is of the type: $x^4 \equiv a^4 (mod\ 2.4^n)$
Its solutions are $x \equiv 2.4^{n-2}k \pm 2\ (mod\ 2.4^n)$
$\equiv 2.4^1k \pm 2\ (mod\ 2.4^3)$
$\equiv 8k \pm 2\ (mod\ 128); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, (4^2 - 1).$
$\equiv 0 \pm 2; 8 \pm 2; 16 \pm 2; 24 \pm 2; 32 \pm 2; 40 \pm 2; 48 \pm 2; 56 \pm 2; 64 \pm 2; 72 \pm 2; 80 \pm 2; 88 \pm 2; 96 \pm 2; 104 \pm 2; 112 \pm 2; 120 \pm 2\ (Mod\ 128).$
$\equiv 2, 126; 6, 10; 14, 18; 22, 26; 30, 34; 38, 42; 46, 50; 54, 58; 62, 66;$
$70, 74; 78, 82; 86, 90; 94, 98; 102, 106; 110, 114; 118, 122\ (mod\ 128).$
These are the required thirty two solutions of the congruence.

Example-5: Consider $x^4 \equiv 81\ (mod\ 320).$
It can be written as $x^4 \equiv 3^4\ (mod\ 5.4^3)$
It is of the type $x^4 \equiv a^4\ (mod\ b.4^n)\ with\ b = 5.$
It has exactly eight solutions.
The solutions are given by $x \equiv b.4^{n-1}k \pm a\ (mod\ b.4^n)\ with\ n = 3, b = 5.$
$\equiv 5.4^2k \pm 3\ (mod\ 5.4^3)$
$\equiv 80 \pm 3\ (mod\ 320); k = 0, 1, 2, 3.$
$\equiv 0 \pm 3; 80 \pm 3; 160 \pm 3; 240 \pm 3\ (mod\ 320)$
$\equiv 3, 317; 77, 83; 157, 163; 237, 243\ (mod\ 320).$

Example-6: Consider $x^4 \equiv 1296\ (mod\ 5120).$
It can be written as $x^4 \equiv 6^4\ (mod\ 5.4^5)$
It is of the type $x^4 \equiv a^4\ (mod\ b.4^n)\ with\ b = 5, n = 5.$
It has exactly thirty two solutions. The solutions are given by
$x \equiv b.4^{n-2}k \pm a\ (mod\ b.4^n)\ with\ n = 5, b = 5.$
$\equiv 5.4^3k \pm 6\ (mod\ 5.4^5)$
$\equiv 320 \pm 6\ (mod\ 5120); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, 15.$
$\equiv 0 \pm 6; 320 \pm 6; 640 \pm 6; 960 \pm 6; \ldots\ldots\ldots; 4800 \pm 6\ (mod\ 5120)$
$\equiv 6, 5114; 314, 326; 634, 646; 954, 966; \ldots\ldots\ldots; 4794, 4806\ (mod\ 5120).$

Example-7: Consider $x^4 \equiv 256\ (mod\ 5120)$.
It can be written as $x^4 \equiv 4^4\ (mod\ 5.4^5)$
It is of the type $x^4 \equiv 4^4\ (mod\ b.4^n)\ with\ b = 5, n = 5$.
It has exactly one hundred and twenty-eight solutions. The solutions are given by
$x \equiv b.4^{n-3}k \pm 4\ (mod\ b.4^n)\ with\ n = 5, b = 5.$
$\equiv 5.4^2k \pm 4\ (mod\ 5.4^5)$
$\equiv 80 \pm 4\ (mod\ 5120); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, 63.$
$\equiv 0 \pm 6; 320 \pm 6; 640 \pm 6; 960 \pm 6; \ldots\ldots\ldots; 4800 \pm 6\ (mod\ 5120)$
$\equiv 6, 5114; 314, 326; 634, 646; 954, 966; \ldots\ldots\ldots; 4794, 4806\ (mod\ 5120).$

CONCLUSION

Therefore for the first congruence, it is concluded that the standard bi-quadratic congruence:
$x^4 \equiv a^4\ (mod\ 4^n); a\ is\ odd\ positive\ integer$ has exactly $2.4 = 8$ Incongruent solutions given by $x \equiv 4^{n-1}k \pm a\ (mod\ 4^n); k = 0, 1, 2, 3.$
Also the standard bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ 4^n); a\ is\ even\ positive\ integer$ has exactly $2.4^2 = 2.16 = 32$ incongruent solutions given by
$x \equiv 4^{n-2}k \pm a\ (mod\ 4^n); k = 0, 1, 2, 3, \ldots\ldots\ldots, 15.$
Also the standard bi-quadratic congruence: $x^4 \equiv 4^4\ (mod\ 4^n)$ has exactly $2.4^3 = 2.64 = 128$ incongruent solutions given by $x \equiv 4^{n-3}k \pm 4\ (mod\ 4^n); k = 0, 1, 2, 3, \ldots\ldots\ldots, 63.$
For the second congruence, it is concluded that the standard bi-quadratic congruence:
$x^4 \equiv a^4\ (mod\ b.4^n); b \neq 4l, positive\ integer; a\ is\ odd\ positive\ integer,$ has exactly $2.4 = 8$ incongruent solutions given by $x \equiv b.4^{n-1}k \pm a\ (mod\ b.4^n); k = 0, 1, 2, 3.$
Also the standard bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ b.4^n); b \neq 4l, positive\ integer;$
$a\ is\ even\ positive\ integer,$ has exactly $2.4^2 = 2.16 = 32$ incongruent solutions given by $x \equiv b.4^{n-2}k \pm a\ (mod\ b.4^n); k = 0, 1, 2, 3, \ldots\ldots\ldots, 15.$
Also the standard bi-quadratic congruence: $x^4 \equiv a^4\ (mod\ b.4^n); b \neq 4l, a = 4,$ has exactly
$2.4^3 = 2.64 = 128$ Incongruent solutions given by
$x \equiv b.4^{n-3}k \pm a\ (mod\ b.4^n); k = 0, 1, 2, 3, \ldots\ldots\ldots, 63.$

REFERENCES

[1] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Delhi, India, ISBN: 978-81-312-1859-4.
[2] David M Burton, 2012, *Elementary Number Theory*, Mc Graw Hill education (Higher Education), Seventh Indian Edition, New Delhi, India, ISBN: 978-1-25-902576-1.
[3] Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.
[4] B M Roy, *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] B M Roy, *An Algorithmic Method of Finding Solutions of Standard Bi-quadratic Congruence of Prime Modulus*, IJSDR/2455-2631, Vol-04, Issue-04, April-19.
[6] B M Roy, *Formulation Solutions of a special standard bi-quadratic congruence- modulo a powered odd prime*, (IJETRM), ISSN: 2456-9348, Vol-05, Issue-04, April-21.