Volume-3, Issue-2, February-2019: 134-137
International Journal of Recent Innovations in Academic Research ISSN: 2635-3040

Formulation of Some Classes of Standard Solvable Bi-Quadratic Congruence of Even Composite Modulus-A Generalisation

Prof. B.M. Roy

Head, Department of Mathematics, Jagat Arts, Commerce and I.H.P. Science College, Goregaon (Gondia), Pin: 441801, India.
(Affiliated to RTM Nagpur University, Nagpur)
Corresponding Author E-mail: roybm62@gmail.com

Received: February 3, 2019; **Accepted:** February 10, 2019; **Published:** February 14, 2019

Abstract: In this paper, some classes of standard solvable bi-quadratic congruence of even composite modulus are formulated. The formulae established are tested true using some suitable examples. Formulation makes it easy to find all the solutions. It is time-saving and simple. Formulation is the merit of the paper. No need to use Chinese Remainder Theorem. Formulation is the merit of the paper.
Keywords: Bi-quadratic congruence, Binomial Theorem, Bi-quadratic residues, Chinese Remainder Theorem.

Citation: Roy, B.M. 2019. Formulation of Some Classes of Standard Solvable Bi-Quadratic Congruence of Even Composite Modulus- A Generalisation. International Journal of Recent Innovations in Academic Research, 3(2): 134-137.

Introduction
A solvable standard bi-quadratic congruence of prime modulus is a congruence of the type: $x^4 \equiv a^4 \ (mod\ p)$, p being a prime positive integer. Its solutions are the values of x that satisfy the congruence. If the congruence has solution, then a is called a bi-quadratic residue of p [3]. Much material has not been found in the literature of mathematics. It seems that earlier mathematicians had given a little attention to the topic and no research had been done on it.

Literature-Review
The author referred many books of Number Theory and found no formulation about standard bi-quadratic congruence in the literature of mathematics. Only a definition and two problems of finding bi-quadratic residues are seen [4]. There is no formulation and no suitable method found in the literature except the Chinese Remainder Theorem, which has its own demerits [1]. Thus, the author takes the responsibility to do some research on it and have started his journey in the ocean of research with standard solvable bi-quadratic congruence of composite modulus. The author also formulated many standard quadratic congruence of composite modulus and published in different international journals.
The author already formulated the congruence: (1) $x^4 \equiv a^4 \ (mod\ 4^n)$; (2) $x^4 \equiv a^4 \ (mod\ 4^n.b); b \neq 4l$ [3].

Here, in this paper, the generalisation of the above paper is considered.

Need of Research

To get an easy and simple method of finding solutions, the author tried his best to formulate the congruence and presented his efforts in this paper. It lessens the time of calculation. Now it becomes an interesting topic of study for the readers. The negligence of earlier mathematicians insists the author to consider it for research. The only method available is the Chinese Remainder Theorem which is a long and complicated method. A remedy is in demand.

Problem-Statement

The problem is "To formulate some classes of standard solvable bi-quadratic congruence of composite modulus of the types:
(1) $x^4 \equiv a^4 (mod\ 4^n. b^m)$; b m, n are positive integers.
(2) $x^4 \equiv a^4\ (mod\ r. b^m. 4^n); r \neq 4l, r \neq bt; r, b, m, n\ are\ positive\ integers.$

Analysis and Result

The congruence under consideration is: $x^4 \equiv a^4\ (mod\ b^m. 4^n); b \neq 4l; l\ being\ a\ positive\ integer.$

Then, for $x = b^m. 4^{n-1}k \pm a,\ \ k = 0, 1, 2, 3, 4, \dots \dots$
$x^4 = (b^m. 4^{n-1}k \pm a)^4$

Expanding using binomial theorem, one get

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

Thus, $x = b^m. 4^{n-1}k \pm a$ satisfies the congruence and hence is a solution of it.
For $k = 4,\ \ x = b^m. 4^{n-1}. 4 \pm a = b^m. 4^n \pm a \equiv \pm a\ (mod\ b^m. 4^n)$ 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.
In this case, it can be easily seen that $b \neq 4l$, for an integer l.
Because then, $b^m = 4l$.
The congruence under consideration is: $x^4 \equiv a^4\ (mod\ r. b^m. 4^n); r, b \neq 4l; r \neq b; l\ being\ a\ positive\ integer.$
Then, for $x = r. b^m. 4^{n-1}k \pm a,\ \ k = 0, 1, 2, 3, 4, \dots \dots$

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

Expanding using binomial theorem, one get

$$x^4 = (r. b^m. 4^{n-1}k)^4 \pm 4. (r. b^m. 4^{n-1}k)^3. a + \frac{4.3}{1.2}(r. b^m. 4^{n-1}k)^2 a^2 \pm \frac{4.3.2}{1.2.3}(r. b^m. 4^{n-1})^1 a^3 + a^4$$
$$= a^4 + r. b^m. 4^n(\dots \dots . .)$$
$$\equiv a^4\ (mod\ r. b^m. 4^n)$$

Thus, $x = r.b^m.4^{n-1}k \pm a$ satisfies the congruence and hence is a solution of it.
For $k = 4$, $x = r.b^m.4^{n-1}.4 \pm a = r.b^m.4^n \pm a \equiv \pm a \ (mod\ r.b^m.4^n)$ 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.
In this case, it can be easily seen that $r, b \neq 4l$, for an integer l.
Because then, $b^m = 4l\ and\ r.b^m.4^n = r.(4l)^m.4^n = r.l^m.4^{m+n}$
which is same as $r.b^m.4^n$. Similar result for $r = 4l$.
Sometimes the said bi-quadratic congruence is given as: $x^4 \equiv b\ (mod\ r.4^n.b^m)$
Then it can be solved as: $x^4 \equiv b + t.r.4^n.4^m \equiv a^4\ (mod\ \ r.b^m.4^n)$[**2.**]

Illustrations

Consider the congruence $x^4 \equiv 16\ (mod\ 1728)$.
Here $1728 = 27.64 = 3^3.4^3$.
The congruence can be written as $x^4 \equiv 2^4\ (mod\ 3^3.4^3)$.
It is of the type: $x^4 \equiv a^4 (mod\ b^m.4^n)\ \ with\ a = 2, b = 3, m = 3, n = 3$.
Then the solutions are given by $x \equiv b^m.4^{n-1}k \pm a\ (mod\ b^m.4^n) for\ k = 0, 1, 2, 3$.

$$\equiv 3^3.4^2.k \pm 2\ (mod\ 3^3.4^3)$$
$$\equiv 432k \pm 2\ (mod\ 1728)$$
$$\equiv \pm 2; 430, 434; 862, 866; 1294, 1298\ (mod\ 1728).$$

These are the required solutions of the above congruence.
Consider the congruence: $x^4 \equiv 16\ (mod\ 3456)$
Here $3456 = 2.27.64 = 2.3^3.4^3$.
The congruence can be written as $x^4 \equiv 2^4\ (mod 2.3^3.4^3)$.
It is of the type: $x^4 \equiv a^4 (mod\ r.b^m.4^n)\ \ with\ a = 2, r = 2, b = 3, m = 3, n = 3$.
Then the solutions are given by $x \equiv r.b^m.4^{n-1}k \pm a\ (modr.b^m.4^n) for\ k = 0, 1, 2, 3$.

$$\equiv 2.3^3.4^2.k \pm 2\ (mod 2.3^3.4^3)$$
$$\equiv 864k \pm 2\ (mod\ 3456)$$
$$\equiv \pm 2; 864 \pm 2; 1728 \pm 2; 2592 \pm 2\ (mod\ 3456).$$
$$\equiv 2, 3454; 862, 866; 1726, 1730; 2590, 2594\ (mod\ 3456).$$

These are the eight required solutions of the congruence.
Consider the congruence $x^4 \equiv 96\ (mod\ 1200)$.
It can be written as $x^4 \equiv 96 + 1200 \equiv 1296 \equiv 6^4\ (mod\ 1200)\ with\ a = 6$.
But $1200 = 3.16.25 = 3.4^2.5^2)\ \ with\ r = 3, b = 5, m = 2, n = 2$.
Then the congruence becomes of the type: $x^4 \equiv a^4\ (mod\ 3.4^2.5^2)$.
The solutions are given by $x \equiv r.4^{n-1}.b^m k \pm a\ (mod\ r.4^n.b^m)$

$$\equiv 3.4^1.5^2 k \pm 6\ (mod\ 3.4^2.5^2)$$
$$\equiv 300k \pm 6\ (mod\ 1200)$$
$$\equiv \pm 6; 300 \pm 6; 600 \pm 6; 900 \pm 6\ (mod\ 1200).$$
$$\equiv 6, 1194; 294, 306; 594, 606; 894, 906\ (1200).$$

These are the required eight solutions of the above congruence.

Conclusion

It can be concluded that the congruence under consideration:

$x^4 \equiv a^4 \ (mod\ b^m.4^n)$;
$x^4 \equiv a^4 \ (mod\ r.b^m.4^n), r, b \neq 4l$,
has exactly eight incongruent solutions given by
$x \equiv b^m.4^{n-1}k \pm a \ (mod\ b^m.4^n); k = 0, 1, 2, 3$
And, $x \equiv r.b^m.4^{n-1}k \pm a \ (mod\ r.b^m.4^n); k = 0, 1, 2, 3$.

Merit of the Paper

Here, in this paper, some classes of standard solvable bi-quadratic congruence are formulated. These are the generalisation of the author's last paper on the formulation of standard solvable bi-quadratic congruence of composite modulus. Formulation is the merit of the paper.

References

1. Burton, D.M. 2003. Elementary Number Theory. 2nd Edition, Universal Book Stall.

2. Roy, B.M. 2016. Discrete Mathematics and Number Theory. 1st Edition, Das Ganu Prakashan, Nagpur.

3. Roy, B.M. 2019. Formulations of solutions of some classes of standard bi-quadratic congruence of composite modulus. International Journal of Engineering Technology Research and Management, 3(2): 7-10.

4. Thomas Koshy, 2009. Elementary Number Theory with Applications. 2nd Edition, (Indian print, 2009), Academic Press.