RP-87: An Algorithmic Method of Finding Solutions of Standard Bi-quadratic Congruence of Prime 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: **Author discussed the method of finding solutions of a class standard bi-quadratic congruence of prime modulus. A little study material is available in the literature. Author tried his best with sincere effort to study the solutions of such congruence. A very simple algorithmic method of finding solutions is developed. It makes the finding of the solutions easy. This is the merit of the paper.**

***Keywords*: Bi-quadratic congruence, Legendre's Symbol, Prime-modulus, Quadratic congruence.**

INTRODUCTION

The standard bi-quadratic congruence is found a much neglected topic of number theory. No discussion is seen in the literature of Mathematics. It is a very interesting topic for study. Earlier mathematicians showed a little interest in it and had done nothing. Bi-quadratic residue is a term associated with it. A quadratic residue is known to the readers of congruence. The square of a quadratic residue modulo a prime integer is a bi-quadratic residue of the prime [8].

LITERATURE-REVIEW

A little material about the said congruence is available on internet. Works of Gauss and Dirichlet are found in terms of Gaussian Integers but are very insufficient [1]. So, the author has tried his best to find solutions of the said standard bi-quadratic congruence of prime modulus and his sincere effort is presented in this paper. Following papers have been published by the author in different International Journals which are the formulation of:

(1) $x^4 \equiv a^4 (mod\ 4^n)$,
(2) $x^4 \equiv a^4 (mod\ 4^n . b)$[2]
(3) $x^4 \equiv a^4 (mod\ 4^n . b^m)$,
(4) $x^4 \equiv a^4\ (mod\ r.4^n . b^m), b \neq 4l, r \neq b$ [3]
(5) $x^4 \equiv a^4 (mod\ 4p^n),\ p\ an\ odd\ prime$.
(6) $x^4 \equiv a^4 (mod\ 8p^n),\ p\ an\ odd\ prime$ [4]
(7) $x^4 \equiv a^4 (mod 2^m . p^n), m \geq 4,\ p\ an\ odd\ prime.$ [5]

Now, the author wishes to find a simple method of finding solutions of a standard bi-quadratic congruence of prime modulus of the type: $x^4 \equiv b\ (mod\ p)$.

NEED OF RESEARCH

As no material of study of standard bi-quadratic congruence of prime and composite modulus is found in the literature of mathematics, readers feel uneasy and are in a search of a very simple and easy method or a formulation of the congruence. Hence the author tried his best to develop a simple method of solutions of the said congruence and wished to present his effort here. This is the need of the research.

PROBLEM-STATEMENT

The problem is

"To find solutions of standard bi-quadratic congruence of prime modulus of the type:

$x^4 \equiv b\ (mod\ p),\ \ p\ being\ an\ odd\ positive\ prime\ integer, in\ two\ different\ cases$:

$Case\ I$: $p \equiv 1\ (mod\ 4)$; and,

$Case\ II$: $p \equiv 3\ (mod\ 4)$."

ANALYSIS & RESULT

Consider the congruence $x^4 \equiv b\ (mod\ p); p$ being a prime integer.

If b is quadratic residue of p, then it can be written as:

$b = a^2$ or $b + k.p \equiv a^2\ (mod\ p)$[6].

Then the congruence becomes $x^4 \equiv a^2\ (mod\ p)$.

It can be written as: $x^4 - a^2 \equiv 0\ (mod\ p)\ \ i.e.\ (x^2 - a)(x^2 + a) \equiv 0(mod\ p)$.

Then, $x^2 - a \equiv 0\ (mod\ p);\quad x^2 + a \equiv 0\ (mod\ p)$.

$i.e.\ \ x^2 \equiv a\ (mod\ p)\ \ \&\ \ x^2 \equiv -a\ (mod\ p)$.

Thus, the bi-quadratic congruence is reduced to two quadratic congruence of prime modulus.

Case-I: If $p \equiv 1\ (mod\ 4), then\ p - 1 = 4k\ \ i.e.\ \frac{p-1}{2} = 2k, an\ even\ positive\ integer.$

Consider the congruence: $x^2 \equiv a\ (mod\ p)$.

Then, by Legendre's symbol: $if\ \left(\frac{a}{p}\right) = 1$, the congruence is solvable.

It has exactly two solutions.

And the congruence: $x^2 \equiv -a\ (mod\ p)$ is also solvable and has exactly two solutions

as $\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right).\left(\frac{a}{p}\right) = -1^{p-1/2}.1 = 1.$

Thus the congruence under consideration has exactly four solutions.

Thus, it can be concluded that the bi-quadratic congruence $x^4 \equiv b\ (mod\ p)$ has exactly four solutions if it is solvable and $p \equiv 1\ (mod\ 4)$.

Case-II: Let $p \equiv 3\ (mod\ 4)$. Then p-3 = 4k i.e. p-1= 4k+2

i.e. $\frac{p-1}{2} = 2k + 1, an\ odd\ integer.$

Now consider $x^2 \equiv a\ (mod\ p)$.

Using Legendre's symbol, if we have: $\left(\frac{a}{p}\right) = 1,$ the congruence is solvable [7].

The solutions are: $x \equiv \pm a\ (mod\ p)\ i.e.\ x \equiv a,\ p - a\ (mod\ p)$.

And the congruence $x^2 \equiv -a\ (mod\ p)$ is not solvable as then

$(\frac{-a}{p}) = (\frac{-1.a}{p}) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k+1} = -1.$

Similarly, if $x^2 \equiv a\ (mod\ p)$ is not solvable, then test $x^2 \equiv -a\ (mod\ p)$ for solvability.

Hence, if $p \equiv 3\ (mod\ 4), the\ bi - quadratic\ congruence$ has exactly two solutions.

Thus, the congruence $x^4 \equiv b\ (mod\ p); p \equiv 3\ (mod\ 4)$ may have exactly two solutions.

Some bi-quadratic congruence may not be solvable even though b is a quadratic residue of p.

An example is given in the illustration.

ALGORITHMIC METHOD

From the above discussion, we can summarise the method as under:

(1) Consider the congruence: $x^4 \equiv b \ (mod\ p)$.

(2) Test if b is quadratic residue of p i.e. $\left(\frac{b}{p}\right) = 1\ or - 1$.

(3) If $\left(\frac{b}{p}\right) = -1$, the congruence has no solution. Otherwise, write the congruence as

$$x^4 \equiv b + kp = a^2 \ \ (mod\ p) for\ some\ suitable\ k.$$

(4) Reduce into two quadratic congruence: $x^2 \equiv a \ (mod\ p)$& $x^2 \equiv -a \ (mod\ p)$.

(5) Test for p: $If\ p \equiv 1\ (mod\ 4) \quad or \quad p \equiv 3\ (mod\ 4)$.

(6) If $p \equiv 1\ (mod\ 4)$, then both the quadratic congruence is solvable and have exactly four solutions. If $p \equiv 3\ (mod\ 4)$, then, one of the two quadratic congruence is solvable and has exactly two solutions.

(7) Solve the congruence.

ILLUSTRATIONS

Consider the congruence: $x^4 \equiv 13\ (mod\ 17)$.

Using Legendre's symbol, it is seen that $\left(\frac{13}{17}\right) = 1$; hence 13 is a quadratic residue of 17.

It can be written as: $x^4 \equiv 13 + 4.17 \equiv 81 \equiv 9^2\ (mod\ 17)\ \ with\ \ 17 \equiv 1\ (mod\ 4)$.

Therefore, the given bi-quadratic congruence is solvable and has exactly four solutions.

Now, consider $x^4 \equiv 9^2\ (mod\ 17)$.

Its equivalent quadratic congruence are: $x^2 \equiv 9\ (mod\ 17)\ \ and\ x^2 \equiv -9 \equiv 5^2\ (mod\ 17)$

as $x^2 \equiv -9 \equiv -9 + 2.17 = 25 \equiv 5^2\ (mod\ 17)$.

Then, the solutions are: $x \equiv \pm 3, \pm 5\ (mod\ 17)$.

$$\equiv 3, 14; 5, 12\ (mod\ 17)$$

$$\equiv 3, 5, 12, 14\ (mod\ 17).$$

Consider the congruence $x^4 \equiv 1\ (mod\ 23)\ \ with\ p = 23 \equiv 3\ (mod\ 4)$.

It is always solvable and the bi-quadratic congruence has exactly two solutions.

Corresponding quadratic congruence are: $x^2 \equiv 1\ (mod\ 23)$ & $x^2 \equiv -1\ (mod\ 23)$.

As the congruence $x^2 \equiv -1\ (mod\ 23)$ has no solutions because then

$\left(\frac{-1}{23}\right) = (-1)^{11} = -1$ and the congruence is not solvable.

The congruence $x^2 \equiv 1\ (mod\ 23)$ is solvable and the solutions are

$$x \equiv \pm 1\ (mod\ 23)$$

$$i.e. \quad x \equiv 1, 23 - 1$$

$$i.e. \quad \equiv 1, 22\ (mod\ 23.$$

Therefore the bi-quadratic congruence $x^4 \equiv 1\ (mod\ 23)$ has only two solutions

$x \equiv 1, 22\ (mod\ 23)$.

Consider the congruence $x^4 \equiv 4\ (mod\ 13)$.

It can be written as $x^4 \equiv\ 2^2 (mod\ 13)$.

It is always solvable.

The two separated quadratic congruence are: $x^2 \equiv 2(mod\ 13)$ & $x^2 \equiv -2(mod\ 13)$.

It can be easily seen that no one is solvable. Thus the bi-quadratic congruence has no solution.

From this example it is concluded that the bi-quadratic congruence $x^4 \equiv b\ (mod\ p)$ may have no solution even if b is a quadratic residue of p.

CONCLUSION

Thus, it can be concluded that a very simple method of solving the standard bi-quadratic congruence of prime modulus is developed.

The algorithmic method works well. Condition of solvability is discussed.

The original congruence is separated into two quadratic congruence of the type:

$x^2 \equiv a\ (mod\ p)$ & $x^2 \equiv -a\ (mod\ p)$.

It is found that if $p \equiv 1\ (mod\ 4), and\ if\ x^4 \equiv b\ (mod\ p) is\ solvable,$ the congruence has exactly four solutions & both the congruence are solvable;

if $p \equiv 3\ (mod\ 4)$ & $x^4 \equiv b\ (mod\ p)\ is\ solvable, then\ any\ one\ of\ the\ two\ congruence$ is solvable & has exactly two solutions.

MERIT OF THE PAPER

A formulation is obtained for the solutions of the standard bi-quadratic congruence of prime modulus. Such a formulation is not found in the literature of mathematics. First time a formulation for solutions is made available and it made the finding solutions easy. This is the merit of the paper.

REFERENCES

[1] https://en. Wikipedia.org/wiki/quartic reciprocity.
[2] Roy, B. M.,2019, Formulation of Solutions of Some Classes of Standard Bi-quadratic Congruence of Composite modulus, International Journal of Engineering Technology Research & Management,ISSN:2456-9348, Vol-03, Issue-02, Feb-19.
[3] Roy, B. M.,2019, Formulation of Solutions of Some Classes of Standard Solvable Bi-quadratic Congruence of Even Composite modulus-a Generalisation, International Journal of Recent Innovations in Academic Research, ISSN:2659-1561, Vol-03, Issue-02, Feb-19, Page no. 1-4.
[4] Roy, B. M., 2019, Formulation of Solutions of Some Classes of Standard Bi-quadratic Congruence of Prime-Power modulus, International Journal of Scientific Research and Engineering Development, ISSN:2581-7175, Vol-03, Issue-02, Feb-19.
[5] Roy, B. M., 2019, Formulation of Solutions of a Class of Standard solvable Bi-quadratic Congruence of even composite modulus-a power of prime integer, International Journal of Science and Engineering Development Research, ISSN: 2455-2631, Vol-04, Issue-02, Feb-19.
[6] Roy, B. M., 2016, Discrete Mathematics and Number Theory, Das Ganu Prakashan, Nagpur, India, ISBN: 978-93-84336-12-7, Page-no. 88.
[7] Zuckerman, H. S., et al, 2008, An Introduction to The Theory of Numbers, fifth edition, ISBN: 978-81-265-1811-1, Wiley India Edition, page no: 132.
[8] Thomas Koshy, 2009, "*Elementary Number Theory with Applications",* 2/e (Indian print), Academic Press.