International Journal of Scientific Research and Engineering Development-– Volume 3 Issues 2 Mar- Apr 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-109: Formulation of Solutions of a Standard Quadratic Congruence of Composite Modulus- an odd prime multiple of Power of an Odd Prime

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 new generalised method of solving standard quadratic congruence of composite modulus – an odd prime multiple of power of an odd prime, is discovered. The developed method is algorithmic which works very astonishingly.The author already has proposed a new method, may be called as "**Middle-pair Solution"** method of solving standard quadratic congruence of prime-power modulus. This study is a generalisation of that method. It may be called a very simple and time-saving method.

Key-words: Algorithmic formulation, Legendre's symbol, Middle-pair solution.

INTRODUCTION

The author already has developed three different time-saving efficient methods of solving standard quadratic congruence of prime modulus of the type $x^2 \equiv a\ (mod\ p)$;

$(a,p) = 1;\ p\ being\ an\ odd\ prime\ positive\ integer$,and it is published in different reputed international journals. Also, some formulations of solutions of standard quadratic congruence of composite modulus have been published in different international journals by the author[5], [6], [7], [8]. Here is author's one more generalised method of solving standard quadratic congruence of composite modulus - an odd prime multiple of power of an odd **prime,** of the type: $\boldsymbol{x^2 \equiv a\ (mod\ p^n q);\ q\ being\ an\ odd\ prime}$.

It has exactly four incongruent solutions [4].

The idea of solving congruence arises when the author faced some problems of the types:

(1) $x^2 \equiv 25\ (mod\ 3.5^3)$
(2) $x^2 \equiv 100\ (mod\ 3.5^3)$
(3) $x^2 \equiv 1901\ (mod\ 13^3)$
(4) $x^2 \equiv 116\ (mod\ 7.5^2)$
(5) $x^2 \equiv 49\ (mod\ 3.5^2)$

(6) $x^2 \equiv 882\ (mod\ 7^4)$.

$in\ the\ book\ of\ Thomas\ Koshy$[3], and tried to find their solutions by existed method but failed because the existed method takes a very long time proving that the existed method is time-consuming. It is not a fair method for the readers.

LITERATURE-REVIEW

In the book of Number Theory [2], the author found a method to solve the said congruence. In the existed method, the readers have to add the modulus repeatedly to a to make it a perfect square. Sometimes it takes a long time. It will take hours or days. It is not fair method for readers.

Thomas Koshy has posed two questions as:

(1) When is the congruence $x^2 \equiv a\ (mod\ p^n)$ solvsble?
(2) When it is solvable, how do we find the solutions? [3]

But he did not mention any direct method or formula to find the solutions. His suggested method is very long and tedious. Koshy has mentioned the said problem in an exercise of his book as a computer problem [3].

NEED OF RESEARCH

Such a time-consuming method is in existence. It is not a suitable method for the readers.

They are in need of a simple and time-saving method or formula so that they can find the solutions easily. Thus, a simple and easy method of solving the said congruence is in need.

To have a time-saving method of solutions, the author tried his best and presented his great effort in this paper. This is the need of the paper.

PROBLEM-STATEMENT

Herethe problem is:

"To discover an efficient formulation of solutions of the standard quadratic congruence of the type: $x^2 \equiv a\ (mod\ p^n q); (p,a) = (q,a) = 1,\ n\ is\ a\ positive\ integer;\ p,q\ are\ odd$

$primes$in four cases:

Case-I: when a is a perfect square and $a = p^2$;

Case-II: when a is a perfect square and $a = (mp)^2$;

Case-III: when a is any other perfect square;

Case-IV: when a is not a perfect square.

ANALYSIS & RESULT

Case-I: when a is a perfect square and $a = p^2$; the congruence reduces to the form:

$$x^2 \equiv p^2(mod\ p^n q), n\ any\ positive\ integer, q\ an\ odd\ prime.$$

Let $x \equiv p^{n-1}qk \pm p\ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots\ldots$

Then it is seen that $x^2 \equiv (p^{n-1}qk \pm p)^2\ (modp^n q)$

$\equiv p^2\ (mod\ p^n q)$, expanding and simplifying.

Thus, the value of x satisfies the congruence and hence it is a solution of the congruence.

But, if $k = p$, then it is seen that $x \equiv p^n qk + p^2\ (mod\ p^n q)$

$$\equiv p^2(mod\ p^n q)$$

Which is the same solution as for $k = 0$.

Similarly for $k = p + 1, p + 2, \ldots\ldots$; the solutions repeat as for $k = 1, 2, \ldots\ldots$

Therefore, it can be said that the congruence has in total 2p solutions as for every value of k, the congruence has exactly two solutions. Those are given by

$$x \equiv p^{n-1}qk \pm p\ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p-1).$$

Case-II: When a is a perfect square and $a = (mp)^2$, then the congruence reduces to the form: $x^2 \equiv (mp)^2(mod\ p^n q)$.

Let $x \equiv p^{n-1}qk \pm mp\ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots\ldots$

Then it is seen that $x^2 \equiv (p^{n-1}qk \pm mp)^2\ (modp^n q)$

$\equiv (mp)^2\ (mod\ p^n q)$, expanding and simplifying.

Thus, the value of x satisfies the congruence and hence it is a solution of the congruence.

But, if $k = p$, then it is seen that $x \equiv p^n qk + (mp)^2\ (mod\ p^n q)$

$$\equiv (mp)^2(mod\ p^n q)$$

Which is the same solution as for $k = 0$.

Similarly for $k = p + 1, p + 2, \ldots\ldots$; the solutions repeat as for $k = 1, 2, \ldots\ldots$

Therefore, it can be said that the congruence has in total 2p solutions as for every value of k, the congruence has exactly two solutions. Those are given by

$$x \equiv p^{n-1}qk \pm mp\ (mod\ p^n q); k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p-1).$$

Case-III: When a is any other perfect square.

Then the said congruence reduces to $x^2 \equiv a^2(mod\ p^n q)$. It has four solutions.

The one pair of solutions is $x \equiv \pm a \ (mod\ p^n q)$

$\equiv a, p^n q - a \ (mod\ p^n q)$.

For the remaining pair of solutions, the reader can proceed as below:

(1) Find $c = \frac{p^n q-1}{2}$ & $d = \frac{p^n q+1}{2}$. (c, d) is called **middle-pair** solution.
(2) Find the corresponding standard quadratic congruence : $x^2 \equiv b \ (mod\ p^n q)$.
(3) Find r from the equation: $r(r+1) = a - b + p^n qk,\ for\ k = 0, 1, 2, \ldots\ldots$
(4) Then the required solutions are $x \equiv c - r, d + r \ (mod\ p^n q)$..
This gives the other pair of solutions of the congruence.

Case-IV: when a is not a perfect square.

Then the said congruence is $x^2 \equiv a \ (mod\ p^n q)$.

Such types of congruence are not always solvable. They are solvable if and only if the Legendre's symbol:$\left(\frac{a}{p}\right) = 1$ [1]. If the congruence is solvable, then for the solutions,

the readers have to perform the following steps(developed by the author):

1. Test for solvability of the problem.
2. Find $c = \frac{p^n q-1}{2}$ & $d = \frac{p^n q+1}{2}$. (c, d) is called **middle-pair** solution.
3. Find the corresponding standard quadratic congruence : $x^2 \equiv b \ (mod\ p^n q)$.
4. Find r from the equation: $r(r+1) = a - b + p^n qk,\ for\ k = 0, 1, 2, \ldots\ldots$
5. Then the required solutions are $x \equiv c - r, d + r \ (mod\ p^n q)$.
For one value of k, one-pair of solution can be obtained. For the other pair, another value of k must be determined.

Formulation is obtained by the author scientifically & mathematically. Mathematical calculation is not shown here. **The method is already published in IJARIIT[9]**.

ILLUSTRATION

Consider the quadratic congruence $x^2 \equiv 25(mod\ 375)$

It can be written as $x^2 \equiv 25 = 5^2(mod\ 3.5^3)$.

Here, $a = 25 = 5^2; and\ p = 5$.

This congruence must have 2p=2.5=10 incongruent solutions.

These are given by the formula:

$$x \equiv p^{n-1} qk \pm p \ (mod\ p^n q); k = 0, 1, 2, 3, 4.$$

$$\equiv 5^{3-1}.3k \pm 5 \ (mod\ 5^3.3)$$

$$\equiv 75k \pm 5\ (mod\ 375)$$

$$\equiv 0 \pm 5; 75 \pm 5; 150 \pm 5; 225 \pm 5; 300 \pm 5\ (mod\ 375)$$

$\equiv 5, 370; 70, 80; 145, 155; 220, 230; 295, 305\ (mod\ 375)$.

These are the required 10 incongruent solutions of the congruence.

Consider the quadratic congruence $x^2 \equiv 100(mod\ 375)$

It can be written as $x^2 \equiv 10^2(mod\ 3.5^3)$.

Here,$(a, p) = (10, 5) = 5 = p$.

This congruence must have 2p=2.5=10 incongruent solutions.

These are given by the formula:

$$x \equiv p^{n-1}qk \pm a\ (mod\ p^n q); k = 0, 1, 2, 3, 4.$$

$$\equiv 5^{3-1}.3k \pm 10\ (mod\ 5^3.3)$$

$$\equiv 75k \pm 10\ (mod\ 375)$$

$$\equiv 0 \pm 10; 75 \pm 10; 150 \pm 10; 225 \pm 10; 300 \pm 10\ (mod\ 375)$$

$\equiv 10, 365; 65, 85; 140, 160; 215, 235; 290, 310\ (mod\ 375)$.

These are the required 2.5=10 incongruent solutions of the congruence.

Consider one more problem as $x^2 \equiv 49\ (mod\ 75)$

It can be written as $x^2 \equiv 7^2(mod\ 75)$ with $a = 49 = 7^2, p = 5, q = 3$.

Then one pair of solutions are $x \equiv \pm 7\ (mod\ 75)$

$$\equiv 7, 75 - 7\ (mod\ 75)$$

$\equiv 7, 68\ (mod\ 75)$.

For the other pair of solutions, proceed as below:

Here, $\frac{p^n q-1}{2} = \frac{75-1}{2} = 37 = c$ & $\frac{p^n q+1}{2} = \frac{75+1}{2} = 38 = d$.

$(c, d) = (37, 38)$is the middle pair solutions of the said congruence.

The corresponding quadratic congruence is then $x^2 \equiv 19\ (mod\ 75)$

$$giving\ b = 19.$$

To find r, let us consider the equation: $r(r + 1) = p^n qk + a - b$

$$= 375k + 49 - 19$$

$$= 375k + 30$$

$= 30\ for\ k = 0\&$

$$= 5.6\ giving\ \ r = 5\,.$$

Then the required solutions pair is $x \equiv c - r, d + r\ (mod\ p^n q)$

$$\equiv 37 - 5, \qquad 38 + 5\ (mod 75)$$

$$\equiv 32, 43\ (mod\ 75).$$

Therefore all the four solutions are $x \equiv 7, 68;\ 32, 43\ (mod\ 75)$.

Consider one more problem: $x^2 \equiv 116\ (mod\ 175)$

Here, $a = 116, p = 5, q = 7.$

$$c = \frac{175 - 1}{2} = 87\ and\ \ d = \frac{175 + 1}{2} = 88.$$

Corresponding quadratic congruence $x^2 \equiv 44\ (mod\ 175)$ giving $b = 44$

For the pairs of solutions, consider: $r(r + 1) = p^n qk + a - b$

$$= 175k + 116 - 44$$

$$= 175k + 72$$

$$= 175.0 + 72$$

$$= 8.9\ giving\ \ r = 8\,.$$

Then the required one solutions pair is $x \equiv c - r, d + r\ (mod\ p^n q)$

$$\equiv 87 - 8, \qquad 88 + 8\ (mod\ 175)$$

$$\equiv 79, 96\ (mod\ 175).$$

The other pair is given by: $r(r + 1) = p^n qk + a - b$

$$= 175k + 116 - 44$$

$$= 175k + 72$$

$= 175.6 + 72$

$$= 1122 = 33.34\ giving\ r = 33.$$

Therefore, the other pair of solutions is $x \equiv c - r, d + r\ (mod\ p^n q)$

$$\equiv 87 - 33, \qquad 88 + 33 \ (mod\ 175)$$

$$\equiv 54, 121 \ (mod\ 175).$$

Therefore, all the required four solutions are

$$x \equiv 79, 96, 54, 121 \ (mod\ 175).$$

CONCLUSION

Therefore, it can be concluded that the author's proposed algorithmic method of solving standard quadratic congruence of prime modulus of the type $x^2 \equiv a \ (mod\ p)$ is generalised to solve the standard quadratic congruence of prime-power modulus of the type:

$x^2 \equiv a \ (mod\ p^n q)$,p, q being an odd prime integers. The method works efficiently when the required solutions are near to middle-pair solution.

MERIT OF THE PAPER

The proposed algorithmic method works efficiently. It solves the congruence in a least time. Thus, author's method is proved time-saving. This is the merit of the paper.

REFERENCE

1. Burton D M, "*Elementary Number Theory*", 2/e, 2003, Universal Book Stall.
2. Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016, Das GanuPrakashan, Nagpur.
3. Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.
4. Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.
5. Roy B M, Formulation of a Class of Solvable Standard Quadratic Congruence of Even Composite Modulus, (IJRTI), ISSN: 2456-3315, Vol-04, Issue-03, Mar-19.
6. Roy B M, Formulation of standard quadratic congruence of composite modulus- a product of twin primes, (IJTSRD), ISSN: 2456-6470, Vol-03, Issue-05, July-19.
7. Roy B M, Formulation of a Class of Standard Quadratic Congruence modulo an Integer-multiple of The Power of a Composite Integer, (IJSDR), Vol-04, Issue-03, Aug-19.
8. Roy B M, Formulation of Solutions of a Very Special Class of Standard Quadratic Congruence of a Multiple of Prime-power Modulus, (IJSRED), ISSN: 2581-7175, Vol-02, Issue-06, Nov-Dec-19.
9. Roy B M, An Algorithmic Formulation of solving Standard Quadratic Congruence of Prime- power Modulus, (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-06,Dec-19.

……..xxx…….

