International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 3, May – June 2020

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Rp-52: Formulation Of Solutions Of A Standard Quadratic Congruence Of Even Composite Modulus- A Product Of Power Of An Odd Prime& Four Times Of Another Odd Prime

Prof. B. M. Roy
M. Sc. (Maths); Ph. D. (Hon); D.Sc. (Hon).
Head, Dept. of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon (Gondia).
Dist. - GONDIA, M. S., India, Pin-441801
(Affiliated to R T M Nagpur University)

ABSTRACT

In this current paper, the finding of solutions of a standard quadratic congruence of even composite modulus-a product of four times an odd prime & power of another odd prime is discussed and formulated in different cases.Here, the formulation is established and a detailed study is done solving different numerical examples. The solutions obtained by formulation are tested and verified true. Formulation is the merit of the paper. It is found that the said congruence has exactly eight incongruent solutions in one case; in another case, it has only four solutions whereas in another case the congruence has $4p-$ solutions, p being an odd prime.

Keywords: Composite modulus; Chinese Remainder Theorem,Legendre's symbol, Quadratic congruence, Quadratic residue.

INTRODUCTION

Here, the author considered a **quadratic congruence** of even **composite modulus** of the type: $x^2 \equiv a \pmod{4p^n q}$ for its formulation of solutions.

The said congruence is not always solvable. If a is a **quadratic residue** of $4p^n q$, then it is solvable.

The quadratic reciprocity is tested by **Legendre's symbol**: $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = 1$ [1].

Then, the congruence can be written as: $x^2 \equiv b^2 \pmod{4p^n q}$ and is always solvable.

PROBLEM STATEMENT

The problem is:

"To formulate of the solutions of the standard quadratic congruence of even composite modulus:

$x^2 \equiv a \pmod{4p^n . q}$ ……………………………………….(1)

where p, q are positive odd primes and n is a positive integer infourcases:

Case-I: if $a = b^2$& $b \neq p \neq q$,

Case-II: if $a \neq b^2$, $b \neq p \neq q$,

Case-III: if $b = q$,

Case-IV: if $b = p$.

LITERATURE-REVIEW

The standard quadratic congruence under consideration is not previously formulated. It can be solved using the Chinese Remainder Theorem (C R T);no other method is found in the literature of mathematics. This is the only existed method found.

EXISTED METHOD

In existed method, the solutions of such congruence are obtained by separating into threeindividual congruence as:

$$x^2 \equiv a \pmod 4 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots. (2)$$

$x^2 \equiv a \pmod{p^n}$ ………………………………………….(3)

$$x^2 \equiv a \pmod q \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (4).$$

and solving these three individual congruence separately, required solutions are obtained using Chinese Remainder Theorem.

The congruence (2), (3) & (4) each has exactly two solutions and hence the congruence (1) has exactly (2)(2)(2)= 8 solutions [2].

The use of **Chinese Remainder Theorem [2]** is a time-consuming procedure. This is the demerit of the existed method. Therefore, the author wished to formulate the said congruence.

The use of C R T is not suitable to find the solutions of the individual congruence because some congruence takes a long time to find the solutions. The author tried his best to formulate the solutions of the said congruence. The author's other research papers are also seen in the literature [4] [5], [6], [7], [8].

ANALYSIS & RESULT

Case-I: Let $a = b^2$.

The congruence under consideration becomes$x^2 \equiv b^2 (\bmod 4p^n q)$.

Such type of congruence always has eightincongruent solutions as seen above.

Now consider $x \equiv (2p^n qk \pm b) \pmod{4p^n q}$

Then, $x^2 \equiv (2p^n qk \pm b)^2 \pmod{4p^n q}$

$$\equiv (2p^n qk)^2 \pm 2.2p^n qk.b + b^2 \pmod{4p^n q}$$

$$\equiv b^2 + 4p^n q\,(p^n qk^2 \pm kb) \pmod{4p^n q}$$

$$\equiv b^2 \pmod{4p^n q}\ .$$

Therefore $x \equiv (2p^n qk \pm b) \pmod{4p^n q}$is a solution of the congruence.

But for $k = 2$, the solution becomes $x \equiv (2p^n q.2 \pm b) \pmod{4p^n q}$

$$\text{i.e. } x \equiv (4p^n q \pm b) \pmod{4p^n q}$$

$$\text{i.e. } x \equiv \pm b \pmod{4p^n q}$$

which is the same solutions as for $k = 0$.

Therefore, this formulation gives only four solutions for $k = 0, 1$.

For the remaining four solutions, let us consider thatx $\equiv \pm(2p^n k \pm b) \pmod{4p^n q}$, then

$$x^2 \equiv (2p^n k \pm b)^2 \pmod{4p^n q}$$

$$\equiv 4p^{2n}k^2 \pm 2.2kp^n b + b^2 \pmod{4p^n q}$$

$$\equiv b^2 + 4p^n k(p^n k \pm b) \pmod{4p^n q}$$

$$\equiv b^2 + 4p^n qt, \pmod{4p^n q} \qquad \text{if } (p^n k \pm b)k = qt$$

$$\equiv b^2 + 4p^n qt \pmod{4p^n q}$$

$\equiv b^2 \pmod{4p^n q}$.

Thus, $x \equiv \pm(2p^n k \pm b) \pmod{p^n q}$ gives the other four solutions for some values of k.

Case-II: Let $a \neq b^2$.

Then, it can be written as: $x^2 \equiv 4p^n qk + a = b^2 \pmod{4p^n q}$ [3].

All the eight solutions can be obtained as in case-I.

Case-III: Let $b = q$. Then the congruence becomes $x^2 \equiv q^2 \pmod{4p^n q}$.

Separating the individual congruence, it can be seen that the said congruence has exactly four solutions.These solutions are given by $x \equiv (2p^n qk \pm q) (mod\ 4p^n q)$.

Case-IV: Let $b = p$. Then the congruence becomes $x^2 \equiv p^2 (mod\ 4p^n q)$.

It also can be seen that the said congruence must have (1)(2p)(2) = 4p solutions.

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

$$x^2 \equiv (2p^{n-1}qk \pm p)^2 \ (mod\ 4.p^n q)$$

$$\equiv p^2 (mod\ 4p^n q).$$

But for $k = 2p$, the solution is the same as for $k = 0$.

Therefore. All the 4p-solutions are given by

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

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 4\ (mod\ 180)$.

Here, $b^2 = 4,\ 180 = 4.9.5 = 4.3^2.5$ with$p = 3,\ n = 2\ \&\ q = 5$.

So, the congruence is of the type $x^2 \equiv b^2 (mod\ 4p^n q)$ and has only eight solutions.

Its four solutions are given by $x \equiv (2p^n qk \pm b)\ (mod\ 4\ p^n q)$

$$i.e.\ x \equiv (2.3^2.5k \pm 2)(mod\ 4.9.5); k = 0,1.$$

$$i.e.\ x \equiv 0 \pm 2; 90 \pm 2\ (mod\ 180)$$

$$i.e.\ x \equiv 2, \quad 178; 88, 92\ (mod\ 180).$$

Other four solutions are given by

$x \equiv \pm(2p^n k \pm b)(mod\ 4p^n q)$, if$(p^n k \pm b)k = qt$

$$i.e.\ x \equiv \pm(18k \pm 2)(mod\ 4.9.5)\ , \quad if\ (9k \pm 2)k = 5t$$

$$i.e.\ x \equiv \pm(18.2 + 2)(mod\ 180), \quad if\ (9.2 + 2).2 = 5t\ for\ k = 2.$$

$$i.e.\ \equiv \pm 38\ (mod\ 180)$$

$$i.e.\ \equiv 38, 142\ (mod\ 180)$$

Then for $k = 4$, $x \equiv \pm(54 - 2)(mod\ 180)$ $as\ (9.3 - 2).2 = 5t$ for $k = 3$.

$$\equiv \pm 52\ (mod\ 180)$$

$$\equiv 52, \quad 180 - 52\ (mod\ 180)$$

$$\equiv 52, \quad 128\ (mod\ 180).$$

Therefore, all the solutions are $x \equiv 2, 178; 88, 92; 38, 142; 52, 128\ (mod\ 180)$.

Let us consider an example$x^2 \equiv 1\ (mod\ 300)$.

It can be written as: $x^2 \equiv 1^2(mod\ 4.5^2.3)$

Here, $p = 5, b = 1,\ n = 2\ \&\ q = 3$.

So, the congruence is of the type $x^2 \equiv b^2(mod\ 4p^n q)$ and has only eight solutions.

Its four solutions are: $x \equiv (2p^n qk \pm b)(mod\ 4p^n q); k = 0, 1$.

$$i.e.\ \ x \equiv (2.25.3k \pm 1\ (mod\ 4.5^2.3)$$

$$i.e.\ \ x \equiv (150k \pm 1\ (mod\ 300)$$

$$i.e.\ \ x \equiv 0 \pm 1, \quad 150 \pm 1\ (mod\ 300)$$

$$i.e.\ \ x \equiv 1, 299; 149, 151\ (mod\ 300).$$

Other four solutions are given by

$x \equiv \pm(2p^n k \pm b)\ (mod\ p^n q)$ if$(p^n k \pm b)k = qt$

$$i.e.\ x \equiv \pm(2.5^2 k \pm 1)(mod\ 4.5^2.3)\ , \quad if\ (5^2 k \pm 1)k = 3t$$

$$i.e.\ \ x \equiv \pm(50k \pm 1)(mod\ 300), \quad if\ (25k \pm 1)k = 3t.$$

Then for $k = 1$, $x \equiv \pm(50.1 - 1)(mod\ 300)$ $as\ (25.1 - 1).1 = 24 = 3t$

$$x \equiv \pm 49\ \ (mod\ 300)$$

$$x \equiv 49, \quad 300 - 49\ (mod\ 300)$$

$$x \equiv 49, 251\ (mod\ 300).$$

Then for $k = 2$, $x \equiv \pm(50.2 + 1)(mod\ 300)$ $as\ (25.2 + 1).2 = 102 = 3t$

$$x \equiv \pm 101\ \ (mod\ 300)$$

$$x \equiv 101, \quad 300 - 101\ (mod\ 300)$$

$$x \equiv 101, 199\ (mod\ 300).$$

Thus, the two solutions are: $x \equiv 101, 199\ (mod\ 300)$.

Therefore all the eight solutions are $x \equiv 1, 299; 149, 151; 49, 251; 101, 199\ (mod\ 300)$.

Consider the congruence: $x^2 \equiv 25\ \ (mod\ 540)$.

It can also be written as: $x^2 \equiv 5^2\ (mod\ 4.3^3.5)$.

It is of the type: $x^2 \equiv q^2\ (\mathrm{mod}\ 4.\mathrm{p^n}.\mathrm{q})$.

It has exactly four solutions.

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

$$\equiv 2.3^3.5\mathrm{k} \pm 5\ (\mathrm{mod}\ 4.3^3.5)$$

$$\equiv 270 \pm 5\ (\mathrm{mod}\ 540)$$

$$\equiv 0 \pm 5; 270 \pm 5\ (\mathrm{mod}\ 540); \mathrm{k} = 0, 1.$$

$$\equiv 5, 535; 265, 275\ (\mathrm{mod}\ 540).$$

Therefore all the four solutions are $\mathrm{x} \equiv 5, 535; 265, 275\ (\mathrm{mod}\ 540)$.

Consider one more congruence: $\mathrm{x}^2 \equiv 9\ \ (\mathrm{mod}\ 540)$.

It can be written as: $\mathrm{x}^2 \equiv 3^2(\mathrm{mod}\ 4.3^3.5)$.

It is of the type: $\mathrm{x}^2 \equiv \mathrm{p}^2(\mathrm{mod}\ 4.\mathrm{p^n}.\mathrm{q})$ with $\mathrm{p} = 3, \mathrm{q} = 5,\ \mathrm{b} = \mathrm{p}, \mathrm{n} = 3.$

It has twelve (4p=4.3=12)solutions.

These solutions are given by

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

$$\equiv 2.3^2.5\mathrm{k} \pm 3\ (\mathrm{mod}\ 4.3^3.5); \mathrm{k} =, 1, \ldots\ldots 5.$$

$$\equiv 90k \pm 3 \pmod{540}$$

$$\equiv 0 \pm 3; 90 \pm 3; 180 \pm 3; 270 \pm 3; 360 \pm 3; 450 \pm 3 \pmod{540}$$

≡3, 537; 87, 93; 177, 183; 267, 273; 357, 363; 447, 453 (mod 540).

CONCLUSION

The solutions of the congruence: $x^2 \equiv b^2 \pmod{4p^n q}$; p, q odd primes

has eight solutions which are given by $x \equiv (2p^n qk \pm b) \pmod{4p^n q}; k = 0, 1$

and also $x \equiv \pm(2p^n k \pm b) \pmod{4p^n q}$, if $(p^n k \pm b)k = qt$.

If $b = p$, the congruence has $4p -$ solutions; if $b = q$, then it has four solutions.

MERIT OF THE PAPER

In this paper, the quadratic congruence under consideration is fully formulated. Using the formulation, the solutions can be obtained easily. This is the merit of the paper. No need to use Chinese Remainder Theorem.

REFERENCE:

[1]Koshy, Thomas, Elementary Number Theory with Applications; 2/e; Academic press.ISBN: 978-81-312-1859-4.

[2] Niven, I., Zuckerman H S.; Montgomery H L, An Introduction to the Theory of Numbers; 5/e; WSE, ISBN: 978-81-265-1811-1.

[3] Roy B M, Discrete Mathematics &Number Theory, 1/e, Das Ganu Prakashan, Nagpur (India), ISBN: 978-93-84336-12-7.

[4]Roy B M, Formulation of solutions of a standard quadratic congruence of composite modulus-an odd prime multiple of power of an odd prime, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-02, Mar-20.

[5] Roy B M, Formulation of a special class of standard quadratic congruence of prime-power modulus, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-06, Nov-Dec-19.

[6] Roy B M, A review and reformulation of solutions of standard quadratic congruence of even composite modulus-a power of an odd prime, International Journal of Engineering Research & Technology (IJETRM), ISSN: 2456-2348, Vol-04, Issue-02,Feb-20.

[7] Roy B M, Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of prime-power integer by two or four, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-03, Issue-05, May-18.

[8] Roy B M, Formulation of solutions of a standard quadratic congruence of composite modulus- an odd multiple of prime-power of an odd prime,International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-02, Mar-April 20.

……xxx……..

