International Journal of Scientific Research and Engineering Development-– Volume 3 Issue 3, May – June 202

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-61: Formulation of Solutions of a Standard Quadratic Congruence of Even Composite modulus- a Product of a Powered Odd Prime with Eighth-multiple of another Odd Prime

Prof. B. M. Roy
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

The solutions of a standard quadratic congruence of even composite modulus-a product of a powered oddprime & eight-multiple of another odd prime is formulated. The author has made a thorough study of the problem stated and the formulation of the solutions of the said congruence is established in different cases. Formulation is the merit of the paper.

Keywords: 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:

$x^2 \equiv a\ (mod\ 8p^n q)$ for its formulation of solutions.

The said congruence is not always solvable. If a is a **quadratic residue** of $8p^n q$, 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]. If the congruence is solvable, then the congruence can be written as: $x^2 \equiv b^2 (mod\ 8p^n q)$.

PROBLEM STATEMENT

"To formulate of the solutions of the standard quadratic congruence:

$x^2 \equiv a\ (mod\ 8p^n q)$ ……(1)

$where\ p, q$ are positive odd primes and n is a positive integer in four cases:

Case-I: $if\ a = b^2$,

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

Case-III: if $a = p^2$.

Case-IV: if $a = (mp)^2$.

LITERATURE-REVIEW

The standard quadratic congruence under consideration is not formulated earlier. It can be solved using the Chinese Remainder Theorem (C R T); no other method is found in the literature of mathematics accept the author's formulation.

EXISTED METHOD

In existed method, the solutions of such congruence are obtained by separating into three individual congruence as: $x^2 \equiv a\ (mod\ 8)$, $x^2 \equiv a\ (mod\ p^n)$&$x^2 \equiv a\ (mod\ q)$, and solving these three individual congruence separately, required solutions are obtained using Chinese Remainder Theorem. The use of **Chinese Remainder Theorem [2]** is a time-consuming procedure as finding solutions of the individual congruence sometimes takes a long time to find the solutions. This is the demerit of the existed method. This is also the need of this research.

The author tried his best to formulate solutions of some other standard quadratic congruence of composite modulus of this sequence [4],[5], [6], [7], [8], [9].

ANALYSIS & RESULT

Consider the congruence $x^2 \equiv a\ (mod\ 8p^nq)$.

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

Then the congruence can be written as $x^2 \equiv b^2(\ mod\ 8p^nq\ )$.

It has exactly eight solutions.

For its solutions, consider $x \equiv 4p^nqk \pm b\ (mod\ 8p^nq)$.

Then $x^2 \equiv (4p^n qk)^2 \pm 2.4p^n qk.b + b^2 (\ mod\ 8p^n q\ )$.

$$\equiv 8p^n qk(\ 2p^n qk \pm b) + b^2\ (mod\ 8p^n q)$$

$$\equiv b^2\ (mod\ 8p^n q)$$

Therefore, $x \equiv 4p^n qk \pm b\ (mod\ 8p^n q)$ is a solution of it. But for $k = 2$, the solution is the same as for $k = 0$.

Thus, $x \equiv 4p^n qk \pm b\ (mod\ 8p^n q); k = 0, 1$ gives the four solutions of the congruence.

Also consider $x \equiv \pm(4p^n k \pm b)\ (mod\ 8p^n q)$

Then $x^2 \equiv (4p^n k \pm b)^2 (mod\ 8p^n q)$

$$\equiv (4p^n k)^2 \pm 2.4p^n k.b + b^2\ (mod\ 8p^n q)$$

$$\equiv 8p^n qt + b^2, \qquad if\ (2p^n k \pm b) = qt.$$

$$\equiv b^2 (mod\ 8p^n q).$$

Therefore, the other four solutions are $x \equiv \pm(4p^n k \pm b)(mod\ 8p^n q),\ if\ (2p^n k \pm b) = qt.$

Therefore, the said congruence has eight solutions.

Case-II: Let $a \neq b^2$. Then the congruence can be written as

$$x^2 \equiv a + k.8p^n q = b^2 (\ mod\ 8p^n q\ )\ [3].$$

It also has exactly eight solutions.

These solutions are given as in case-I.

Case-III: Let $a = p^2$.

Then the congruence under consideration becomes$x^2 \equiv p^2 (\ mod\ 8p^n q\ )$.

Let $x \equiv 2p^{n-1} qk \pm p\ (mod\ 8p^n q\ )$.

Then, $x^2 \equiv (2p^{n-1} qk \pm p)^2$ (mod $8p^n q\ )$

$$\equiv (2p^{n-1} qk)^2 \pm 2.2p^{n-1} qk.p + p^2 (mod\ 8p^n q\ )$$

$$\equiv (2p^{n-1} qk)^2 \pm 4.p^n qk + p^2 (mod\ 8p^n q\ )$$

$$\equiv 4p^n qk\ (p^{n-2} qk \pm 1) + p^2\ ((mod\ 8p^n q\ )\ as\ p^{n-2} qk \pm 1\ is\ always\ even,$$

$\equiv p^2 (mod\ 8p^n q\ )$.

Therefore, $x \equiv 2p^{n-1} qk \pm p\ (mod\ p^n q\ )$ is a solution of the said congruence. But if $k = 4p$, the solution reduces to $x \equiv 2p^{n-1} q.4p \pm p\ (mod\ 8p^n q\ )$

$$\equiv 8p^n q \pm p\ \ (mod\ 8p^n q\ )$$

$$\equiv \pm p\ \ (mod\ 8p^n q\ )$$

Which is the same solutions as for $k = 0$. Therefore, the congruence has exactly 8p solutions:

$$x \equiv 2p^{n-1} qk \pm p\ (mod\ 8p^n q\ ); k = 0, 1, 2, \ldots\ldots\ldots\ldots 4p - 1.$$

Case-IV: Let $a = (mp)^2$.

Then the congruence under consideration becomes$x^2 \equiv (mp)^2 (\ mod\ 8p^n q\ )$.

Let $x \equiv 4p^{n-1}qk \pm mp\ (mod\ 8p^nq\ )$.

Then, $x^2 \equiv (4p^{n-1}qk \pm mp)^2$ (mod $8p^nq$)

$$\equiv (4p^{n-1}qk)^2 \pm 2.4p^{n-1}qk.mp + (mp)^2(mod\ 8p^nq\ )$$

$$\equiv (4p^{n-1}qk)^2 \pm 8.p^nqkm + (mp)^2(mod\ 8p^nq\ )$$

$$\equiv 8p^nqk\ (2p^{n-2}qk \pm m) + (mp)^2\ ((mod\ 8p^nq\ )$$

$\equiv (mp)^2(mod\ 8p^nq\ )$.

Therefore, $x \equiv 4p^{n-1}qk \pm mp\ (mod\ p^nq\ )$ is a solution of the said congruence. But if $k = 2p$, the solution reduces to $x \equiv 4p^{n-1}q.2p \pm mp\ (mod\ 8p^nq\ )$

$$\equiv 8p^nq \pm mp\ \ (mod\ 8p^nq\ )$$

$$\equiv \pm mp\ \ (mod\ 8p^nq\ )$$

Which is the same solutions as for $k = 0$. Therefore, the congruence has exactly 4p- solutions:

$$x \equiv 4p^{n-1}qk \pm mp\ (mod\ 8p^nq\ ); k = 0, 1, 2, \dots\dots\dots\dots 2p - 1.$$

ILLUSTRATIONS

Let us consider an example$x^2 \equiv 4\ (mod\ 360)$.

It can be written as: $x^2 \equiv 2^2(mod\ 8.3^2.5)$

Here, $360 = 8.9.5 = 8.3^2.5$ with $p = 3, b = 2,\ n = 2$ & $q = 5$.

So, the congruence is of the type $x^2 \equiv b^2(mod\ 8p^nq)$ and has only eight solutions.

The four solutions are given by $x \equiv 4p^nqk \pm b\ (mod\ 8p^nq\ ); k = 0, 1$.

$$\equiv 4.9.5k \pm 2\ (mod\ 8.3^2.5\ ); k = 0, 1.$$

$$\equiv 180 \pm 2\ (mod\ 360)$$

$$\equiv 0 \pm 2; 180 \pm 2\ (mod\ 360).$$

≡2, 358; 178, 182 (mod 360).

The remaining four solutions are given by

$x \equiv\ \pm(4p^nk \pm b),\ if\ 2p^nk \pm b = qt$, for some values of k.

$\equiv \pm(4.9.k \pm 2)$, if 2.9k$\pm$2 $= 5t$

$$\equiv \pm(36k \pm 2);\ \ if\ 18k \pm 2 = 5t$$

$$\equiv \pm(36.1 + 2);\ \ if\ 18.1 + 2 = 5t$$

$$\equiv \pm(38); if\ 20 = 5t.$$

$\equiv 38, 322\ (mod\ 360)$

Also,$x \equiv\ \pm(4p^nk \pm b),\ if\ (2p^nk \pm b)k = qt$, for some values of k.

$\equiv \pm(4.9.k \pm 2)$, if (2.9k$\pm$2)$k = 5t$

$$\equiv \pm(36k \pm 2);\ \ if\ (18k \pm 2)k = 5t$$

$$\equiv \pm(36.4-2);\ \ if\ (18.4-2).4=5t$$

$$\equiv \pm(142); if\ 70.4=5t.$$

$$\equiv 142, 218\ (mod\ 360).$$

Thus all the eight solutions are: $x \equiv 2, 38, 142, 178, 182, 218, 322, 358\ \ (mod\ 360)$.

Let us consider an example$x^2 \equiv 25\ (mod\ 600)$.

It can be written as: $x^2 \equiv 5^2 (mod\ 8.5^2.3)$

Here, $600 = 8.25.3 = 8.5^2.3$ with $p=5, b=5,\ n=2$ & $q=3$.

So, the congruence is of the type $x^2 \equiv p^2 (mod\ 8p^n q)$ and has only 8p=40- solutions.

These solutions are given by

$$x \equiv 2p^{n-1}qk \pm p\ (mod\ 8p^n q\ ); k=0,1,2,\ldots.4p-1.$$

$$\equiv 2.5^1.3k \pm 5\ (mod\ 8.5^2.3\ ); k=0,1,2,3,4,\ldots\ldots..,18,19.$$

$$\equiv 30k \pm 5\ (mod\ 600)$$

$$\equiv 0 \pm 5; 30 \pm 5; 60 \pm 5, 90 \pm 5; 120 \pm 5; 150 \pm 5; 180 \pm 5; 210 \pm 5;$$

$$240 \pm 5; 270 \pm 5; 300 \pm 5; 330 \pm 5; 360 \pm 5; 390 \pm 5; 420 \pm 5; 450 \pm 5;$$

$$480 \pm 5; 510 \pm 5; 540 \pm 5; 570 \pm 5\ (mod\ 600).$$

≡5, 595; 25, 35; 55, 65; 85, 95; 115, 125; 145, 155; 175, 185; 205, 215;

235, 245; 265, 275; 295, 305; 325, 335; 355, 365; 385, 395; 415, 425; 445, 455;

475, 485; 505, 515; 535, 545; 565, 575 (mod 600).

Thus all the forty solutions are: $x \equiv 5, 10, 20, 25, 35, 40, 50, 55, 65, 70, \ldots\ldots.575\ (mod\ 600)$.

Let us consider another example:$x^2 \equiv 225\ (mod\ 600)$.

It can be written as: $x^2 \equiv 15^2 (mod\ 8.5^2.3)$

Here, $600 = 8.25.3 = 8.5^2.3$ with $p=5, b=15, an\ odd\ multiple\ of\ p,\ n=2$ & $q=3$.

So, the congruence is of the type $x^2 \equiv (mp)^2 (mod\ 8p^n q)$ and has only 4p=20- solutions.

These solutions are given by

$$x \equiv 4p^{n-1}qk \pm mp\ (mod\ 8p^n q\ ); k=0,1,2,\ldots.2p-1.$$

$$\equiv 4.5^1.3k \pm 15\ (mod\ 8.5^2.3\ ); k=0,1,2,\ldots\ldots\ldots.8,9.$$

$$\equiv 60k \pm 15\ (mod\ 600)$$

$$\equiv 0 \pm 15; 60 \pm 15; 120 \pm 15; 180 \pm 15; 240 \pm 15; 300 \pm 15; 360 \pm 15;$$

$$420 \pm 15; 480 \pm 15;\ 540 \pm 15\ (mod\ 600).$$

≡15, 585; 45, 75; 105, 135; 165, 195; 225, 255; 285, 315; 345, 375; 405, 435;

465, 495; 525, 555 (mod 600).

Thus all the twenty solutions are: $x \equiv 15, 45, 75, 105, 135, , \ldots\ldots.525, 555, 585\ (mod\ 600)$.

Let us consider an example$x^2 \equiv 100\ (mod\ 600)$.

It can be written as: $x^2 \equiv 10^2 (mod\ 8.5^2.3)$

Here, $600 = 8.25.3 = 8.5^2.3$ with $p = 5, b = 10, an\ even\ multiple\ of\ 5,\ n = 2\ \&\ q = 3$.

So, the congruence is of the type $x^2 \equiv (mp)^2 (mod\ 8p^n q)$ and has only 4p = 20- solutions.

These solutions are given by

$$x \equiv 4p^{n-1}qk \pm mp\ (mod\ 8p^n q\ ); k = 0, 1, 2, \ldots . 4p - 1.$$

$$\equiv 4.5^1.3k \pm 10\ (mod\ 8.5^2.3\ ); k = 0, 1, 2, 3, 4, \ldots \ldots . , 18, 19.$$

$$\equiv 60k \pm 10\ (mod\ 600)$$

$$\equiv 0 \pm 10; 60 \pm 10, 120 \pm 10; 180 \pm 10; 240 \pm 10; 300 \pm 10; 360 \pm 10; 420 \pm 10;$$

$$480 \pm 10; 540 \pm 10\ (mod\ 600).$$

≡10, 590; 50, 70; 110, 130; 170, 190; 230, 250; 290, 310; 350, 370; 410, 430;

470, 490; 530, 550 (mod 600).

These are all the twenty solutions.

Let us consider an example$x^2 \equiv 25\ (mod\ 1080)$.

It can be written as: $x^2 \equiv 5^2 (mod\ 8.3^3.5)$

Here, $1080 = 8.27.5 = 8.3^3.5$ with $p = 3, b = 5,\ n = 3\ \&\ q = 5$.

So, the congruence is of the type $x^2 \equiv q^2 (mod\ 8p^n q)$ and has only eight solutions.

These solutions are given by $x \equiv 2.p^n qk \pm q\ (mod\ 8p^n q\ ); k = 0, 1, 2, 3.$

$$\equiv 2.27.5k \pm 5\ (mod\ 8.3^3.5\ ); k = 0, 1, 2, 3.$$

$$\equiv 270 \pm 5\ (mod\ 1080)$$

$$\equiv 0 \pm 6; 270 \pm 5; 540 \pm 5; 810 \pm 5\ (mod\ 1080).$$

≡5, 1075; 265, 275; 535, 545; 805, 815 (mod 1080).

Thus all the eight solutions are: $x \equiv 5, 265, 275, 535, 545, 805, 815, 1075\ \ (mod\ 1085)$.

Consider the congruence $x^2 \equiv 225 (mod\ 360)$

It can be written as: $x^2 \equiv 15^2 (mod\ 8.3^2.5)$

Here, $360 = 8.9.5 = 8.3^2.5$ with $p = 3, b = 15,\ n = 2\ \&\ q = 5$.

So, the congruence is of the type $x^2 \equiv (mq)^2 (mod\ 8p^n q)$ and has only eight solutions.

These solutions are given by $x \equiv 2p^n qk \pm mq\ (mod\ 8p^n q\ ); k = 0, 1, 2, 3.$

$$\equiv 2.9.5k \pm 15\ (mod\ 8.3^2.5\ ); k = 0, 1, 2, 3.$$

$$\equiv 90 \pm 15\ (mod\ 360)$$

$$\equiv 0 \pm 15; 90 \pm 15; 180 \pm 15; 270 \pm 15\ \ (mod\ 360).$$

≡ 15, 345; 75, 105; 165, 195; 255, 285 (mod 360).

Thus all the eight solutions are: $x \equiv \ (mod\ 360)$.

CONCLUSION:

The congruence: $x^2 \equiv b^2(mod\ 8p^nq)$ has exactly 8- solution; four are given by

$$x \equiv 4p^nqk \pm b\ (mod\ 8p^nq);\ k = 0, 1.$$

The remaining four are given by $x \equiv \pm(4p^nk \pm b)(mod\ 8p^nq);\ if\ (2p^nk \pm b).k = qt.$

The congruence: $x^2 \equiv p^2(mod\ 8p^nq)$ has exactly 8p - solution are given by

$$x \equiv 2p^{n-1}qk \pm p\ (mod\ 8p^nq);\ k = 0, 1, 2, \dots\dots\dots..4p - 1.$$

The congruence: $x^2 \equiv (mp)^2(mod\ 8p^nq); m \geq 2$, has exactly 2p-solution,given by

$$x \equiv 4p^{n-1}qk \pm mp\ (mod\ 8p^nq), k =, 1, 2, \dots\dots\dots.2p - 1.$$

MERIT OF THE PAPER

In this paper, the quadratic congruence under consideration is formulated. Using the formulation, the solutions can be obtained easily. This is the merit of the paper.

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*, Das Ganu Prakashan, Nagpur, India, ISBN: 978-93-84336-12-7, 1/e, 2016.

[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 standard quadratic congruence of even composite modulus- a prime multiple of a powered odd prime*, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, May-20, Vol-05, Issue-05.

[8] Roy B M, *Formulation of standard quadratic congruence of even composite modulus- a product of twice an odd prime&another powered odd prime*, International Journal for Research and Innovation (IJRTI), ISSN: 2456-3315,May-20, Vol-05, Issue-05.

[9] Roy B M, Formulation of standard quadratic congruence of even composite modulus- a product of powered odd prime& four-times of another odd prime, International Journal of Scientific Research and Engineering Development(IJSRED), ISSN: 2581-7175, May-20, Vol-03, Issue-03.

……xxx…….

