International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-129: Formulation of a Special Type of Standard Quadratic Congruence of Composite Modulus– a Product of Two Powered Odd Primes

Prof B M Roy

M. Sc. (maths); Ph. D. (Hon); D. Sc. (Hon), Head, Department of Mathematics,
Jagat Arts, Commerce & I H P Science College, Goregaon, Maharashtra, India

ABSTRACT

In this current study, a very special type of standard quadratic congruence of composite modulus- a product of two powered odd primes is considered for finding solutions. It is studied and solved in different cases. The author's effort made an easy way to find the solutions of the congruence under consideration. Such types of congruence are not formulated earlier. First time the author's effort came in existence. This is the merit of the paper.

KEYWORDS: *Composite modulus, CRT method, Legendre's symbol, Quadratic congruence*

How to cite this paper: Prof B M Roy "RP-129: Formulation of a Special Type of Standard Quadratic Congruence of Composite Modulus– a Product of Two Powered Odd Primes" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.326-328, URL: www.ijtsrd.com/papers/ijtsrd30964.pdf

IJTSRD30964

INTRODUCTION

The author formulated many standard quadratic congruence of prime and composite modulus.

Here he found one more standard quadratic congruence of composite modulus- a product of two powered primes yet remained unformulated. He consider the problem for his study and found a formulation for its solutions. His efforts are presented in this current paper.

PROBLEM-STATEMENT

In this paper, the problem is:
"To find the solutions of the standard quadratic congruence of composite modulus of the type $x^2 \equiv b\ (mod\ p^n q^m); p\ , q\ are\ odd\ primes, if\ b = a^2, p^2, q^2, (mp)^2\ or\ (mq)^2$

LITERATURE-REVIEW

In the literature of mathematics, a standard quadratic congruence of prime modulus of discussed prominently. But a very little material of solving standard quadratic congruence of composite modulus is found. Only a method known as Chinese Remainder Theorem (CRT) can be used [3]. The author's formulations of solutions of standard quadratic congruence of composite modulus are found [4], …….[8].

ANALYSIS & RESULTS

Consider the congruence under consideration: $x^2 \equiv b\ (mod\ p^n q^m); p\ , q\ are\ odd\ primes.$

Its individual congruence are:

$$x^2 \equiv b\ (mod\ p^n) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (I)$$
$$x^2 \equiv b\ (mod\ q^m)\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (II)$$

Case-I: For $b = a^2$, the congruence (I) has exactly two solutions and the congruence (II) also has exactly two solution. Therefore, the congruence under consideration has exactly four incongruent solutions [1].

It is generally known that the standard quadratic congruence of the type:
$x^2 \equiv a^2\ (mod\ m)$ has at least two solutions $x \equiv \pm a \equiv a, m - a\ (mod\ m)$ [2].

Therefore, the two obvious solutions of the said congruence are given by:
$x \equiv \pm a \equiv a, p^m q^m - a\ (mod\ p^m q^m)$.

For other two solutions, consider $x \equiv \pm(p^n k \pm a (mod\ pnqm)$.

Then $x^2 \equiv (p^n k \pm a)^2$

$\equiv (p^n k)^2 \pm 2.p^n k.a + a^2 \ (mod\ p^n q^m)$
$\equiv a^2 + p^n k\ (p^n k \pm 2a)\ (mod\ p^m q^m)$
$\equiv\ a^2 + p^n.q^m t, if\ k(p^n k \pm 2a) = q^m t.$
$\equiv a^2\ (mod\ p^n q^m)$

Therefore, the other two solutions are given by: $x \equiv \pm(p^n k \pm a)(mod\ p^n q^m)$,
$if\ k(p^n k \pm 2a) = q^m t.$

Sometimes the congruence may be of the type: $x^2 \equiv b\ (mod\ p^n q^m)$. Then at first the solvability condition must be tested to know if the congruence is solvable.

If the Legendre's symbols are $(\frac{b}{p}) = \left(\frac{b}{q}\right) = 1$, then it is said that the congruence is solvable [1].

Then the congruence must be written as: $x^2 \equiv b + k.p^n q^m = a^2\ (mod\ p^n q^m)$ for a certain value of k [2]. Then the four solutions are given by as in above.

Case-II: For $b = q^2$, the congruence (I) has exactly two solutions and the congruence (II) also has exactly q-solution. Therefore, the congruence under consideration has exactly 2q- solution. Therefore, the congruence $x^2 \equiv q^2\ (mod\ p^n q^m)$ has exactly 2q- solutions.

These are given by $x \equiv p^n q^{m-1} k \pm q\ (mod\ p^n q^m)\ with\ k = 0, 1, 2, \ldots\ldots, q1.$

Case-III: *For* $b = p^2$, the congruence (I) has exactly p-solutions and the congruence (II) also has exactly two solution. Therefore, the congruence under consideration has exactly 2p solution. Therefore, the congruence $x^2 \equiv p^2\ (mod\ p^n q^m)$ has exactly 2p- solutions.
These are given by $x \equiv p^{n-1} q^m k \pm q\ (mod\ p^n q^m)\ for\ k = 0, 1, 2, \ldots\ldots\ldots, p-1.$

ILLUSTRATIONS

Example-1: Consider the congruence: $x^2 \equiv 49\ (mod\ 1125)$.
It can be written as: $x^2 \equiv 7^2\ (mod\ 5^3.3^2)$.
It is of the type: $x^2 \equiv a^2\ (mod\ p^n q^m)\ with\ p = 5, q = 3.$
It has four Solutions.

Two of the solutions are given by
$x \equiv \pm a\ \equiv a, p^n q^m - a\ (mod\ p^n q^m).$
$\equiv \pm 7\ \equiv 7, 1125 - 3\ (mod\ 1125)$
$\equiv 7, 1118\ (mod\ 1125).$

Other two solutions are given by
$x \equiv \pm(p^n k \pm a), if\ k(p^n k \pm 2a) = q^m.t$
$\equiv \pm(125k \pm 7), if\ k(125k \pm 2.7) = 3^2 t$
$\equiv \pm 125k \pm 7), if\ k(125k \pm 14) = 9t.$

But for $k = 4, x \equiv \pm(125.4 - 7)$ *as* $4.(125.4 - 14) = 4.(500 - 14) = 216.9$
$\equiv \pm 493\ (mod\ 1125)$
$\equiv 493, 632\ (mod\ 1125).$
Therefore, $x \equiv 7, 1118; 493, 632\ (mod\ 1125).$

Example -2: Consider the congruence: $x^2 \equiv 31\ (mod\ 225)$.
It can be written as: $x^2 \equiv 31 + 225 = 256 = 16^2\ (mod\ 5^2.3^2)$.
It is of the type: $x^2 \equiv a^2\ (mod\ p^n q^m)\ with\ p = 5, q = 3.$
It has four Solutions.

Two of the solutions are given by
$x \equiv \pm a\ \equiv a, p^n q^m - a\ (mod\ p^n q^m).$
$\equiv \pm 16\ \equiv 16, 225 - 16\ (mod\ 1125)$
$\equiv 16, 209\ (mod\ 225).$
Other two solutions are given by
$x \equiv \pm(p^n k \pm a), if\ k(p^n k \pm 2a) = q^m.t$
$\equiv \pm(25k \pm 16), if\ k(25k \pm 2.16) = 3^2 t$
$\equiv \pm(25k \pm 16), if\ k(25k \pm 32) = 9t.$

But for $k = 2, x \equiv \pm(25.2 - 16)$ *as* $2.(25.2 - 32) = 2.(50 - 32) = 2.18 = 36 = 9.4$
$\equiv \pm(25.2 - 16)\ (mod\ 225)$
$\equiv 34, 191\ (mod\ 225).$
Therefore, $x \equiv 16, 209; 34, 191\ (mod\ 225).$

Example-3: Consider the congruence: $x^2 \equiv 25\ (mod\ 6125)$.
It can be written as: $x^2 \equiv 5^2\ (mod\ 7^2.5^3)$.
It is of the type: $x^2 \equiv q^2\ (mod\ p^n q^m)\ with\ p = 7, q = 5.$
It has 2.5=10 solutions.

The solutions are given by
$x \equiv\ p^n q^{m-1} k \pm q\ (mod\ p^n q^m); k = 0, 1, 2, 3, 4.$
$\equiv 7^2.5^2 k \pm 5\ (mod\ 7^2.5^3)$
$\equiv 1225k \pm 5\ (mod\ 6125).$
5, 6120; 1220, 1230; 2445, 2455; 3670, 3680; 4895,4905 (*mod* 6125)

Example-4: Consider the congruence:
$x^2 \equiv 121\ (mod\ 41503)$.

It can be written as: $x^2 \equiv 11^2\ (mod\ 121.343)$ i.e. $x^2 \equiv 11^2\ (mod\ 11^2.7^3)$.

It is of the type: $x^2 \equiv p^2\ (mod\ p^n q^m)\ with\ p = 11, q = 7.$
It has twenty two solutions.

The solutions are given by
$x \equiv\ p^{n-1} q^m k \pm p\ (mod\ p^n q^m); k = 0, 1, 2, \ldots\ldots\ldots, 10.$
$\equiv 11.7^3 k \pm 11\ (mod\ 11^2.7^3).$
$\equiv 3773k \pm 11\ (mod\ 41503)$
$\equiv\ \pm 11; 3773 \pm 11; 7546 \pm 11; 11319 \pm 11; 15092 \pm 11; 18865 \pm 11;$
$22638 \pm 11; 26411 \pm 11; 30184 \pm 11; 33957 \pm 11; 37730 \pm 11\ (mod\ 77).$
$\equiv 11, 41492; 3762, 3784; 7535, 7557;$
$11308, 11330; \ldots\ldots\ldots; 37719, 37741\ (mod\ 41503).$

Example-5: Consider the congruence:
$x^2 \equiv 625\ (mod\ 2025)$.
It can be written as: $x^2 \equiv 625\ (mod\ 25.81)\ i.e.\ x^2 \equiv (25)^2\ (mod\ 5^2.3^4)$.
It is of the type: $x^2 \equiv (mp)^2\ \left(mod\ p^n q^m\right)\ with\ p = 5, q = 3.$

It has exactly ten solutions given by
$x \equiv\ p^{n-1} q^m k \pm mp\ (mod\ p^n q^m); k = 0, 1, 2, 3, 4.$
$\equiv 5^1.3^4 k \pm 5.5\ (mod\ 5^2.3^4)$
$\equiv 405k \pm 25\ (mod\ 2025); k = 0, 1, 2, 3, 4.$
$\equiv 0 \pm 25; 405 \pm 25; 810 \pm 25; 1215 \pm 25; 1620 \pm 25\ (mod\ 2025)$
$\equiv 25, 2000; 380,430; 785, 835; 1190, 1240; 1595, 1645\ (mod\ 2025)$

CONCLUSION

Therefore, it is concluded that the congruence: $x^2 \equiv a^2\ (mod\ p^n.q^m)$ has exactly four solutions, two of them are given by $x \equiv \pm a\ \equiv a, p^n.q^m - a\ (mod\ p^n.q^m)$.

Remaining two are given by
$x \equiv \pm(p^n k \pm p)\ (mod\ p^n.q^m), if\ k(p^n k \pm 2a) = q^m.t$
It is also concluded that the congruence $x^2 \equiv p^2\ (mod\ p^n.q^m)$ has exactly 2p-solutions given by $x \equiv p^{n-1}.q^m k \pm p; k = 0, 1, 2, \dots\dots, p-1$.

It is also concluded that the congruence $x^2 \equiv q^2\ (mod\ p^n.q^m)$ has exactly 2q-solutions given by $x \equiv p^n.q^{m-1} k \pm q; k = 0, 1, 2, \dots\dots, q-1$.

REFERENCE

[1] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "An Introduction to The Theory of Numbers", 5/e, Wiley India (Pvt) Ltd.

[2] Roy B M, "Discrete Mathematics & Number Theory", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.

[3] Thomas Koshy, "Elementary Number Theory with Applications", 2/e (Indian print, 2009), Academic Press.

[4] Roy B M, *Formulation of solutions of Solvable standard quadratic congruence of odd composite modulus-a product of two odd primes and also a product of twin primes*, International Journal of Current Research (IJCR), ISSN: 0975-833X, Vol-10, Issue-05, May-18.

[5] Roy B M, *Formulation of solutions of a class of solvable standard quadratic congruence of composite modulus-an odd prime positive integer multiple of five*, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-03, Issue-9, Sep-18.

[6] Roy B M, *Formulation of solutions of a class of solvable standard quadratic congruence of composite modulus-an odd prime positive integer multiple of seven*, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-11, Nov-18.

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

[8] 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-Apr-20.