Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-137: Solvinga Standard Quadratic Congruence of Composite Modulus Modulo a Product of two Different Odd Primes in Two Special Cases

Prof B M Roy[1] , Mr Pravin C Chavhan[2]
Head, Department of Mathematics[1]
Jagat Arts, Commerce & I H P Science College,Goregaon
DistGondia, M. S., India Pin: 441801
Student[2] NIT, New Delhi
(Now at Goregaon due to Covid-19 Pandemic)

Abstract

In this paper, a standard quadratic congruence of composite modulus modulo a product of two different odd primes in two special cases is considered for solutions. The authors established the method of finding solutions of the congruence. It is found that in both the cases, the congruence has exactly two incongruent solutions in both the cases.

Keywords: Composite modulus, Chinese Remainder Theorem, Quadratic residues.

INTRODUCTION

The congruence$x^2 \equiv a\ (mod\ pq); p, q\ are\ different\ odd\ primes$,have been formulated considering general cases only [1], [2], then it was found that the congruence have exactly four incongruent solutions; here the authors wish to find the solutions in two different special cases, not considered earlier.

PREVIOUS FORMULATION

Consider the congruence $x^2 \equiv a\ (mod\ pq); p, q\ are\ odd\ primes.$

Such types of congruence has exactly four solutions.

The congruence can be written as:$x^2 \equiv a + k.pq = b^2 (mod\ pq)$ [3].

The two obvious solutions are $x \equiv \pm b\ (mod\ pq)\ \ i.e.x \equiv b, pq - b\ (mod\ pq).$

The remaining two solutions are given by the established formula

$$x \equiv \pm(pk \pm b)(mod\ pq), \qquad if\ k(pk \pm 2b) = qt.$$

Consider two examples to illustrate this formulation.

ILLUSTRATIONS BY PREVIOUS FORMULATION

Example-1: Consider the congruence $x^2 \equiv 4$ (mod 35).

It can be written as $\mathrm{x}^2 \equiv 2^2(\mathrm{mod}\ 5.7)$.

It is of the type $\mathrm{x}^2 \equiv b^2(\mathrm{mod\ pq})$ with $\mathrm{p} = 5, \mathrm{q} = 7, \mathrm{b} = 2$.

It has four solutions. The two obvious solutions are $x \equiv \pm b\ (mod\ pq)$

$$\equiv \pm 2\ (mod\ 5.7)$$

$$\equiv 2, 33\ (mod\ 35).$$

The remaining two solutions are given by $x \equiv \pm(pk \pm b)(mod\ pq) if\ k\ (pk \pm 2b) = qt$.

$$\equiv \pm(5k \pm 2)(mod\ 5.7)\ if\ k(5k \pm 2.2) = 7t$$

$\equiv \pm(5k + 2)(mod\ 35)\ if\ k(5k + 4) = 7t.$

But it can be seen that $for\ k = 2,\ \ 1(5.2 + 4) = 7t$ and hence the solutions are given by

$$x \equiv \pm(5.2 + 2)(mod\ 35)$$

$$\equiv \pm 12\ (mod\ 35)$$

$$\equiv 12, 35 - 12 \equiv 12, 23\ (mod\ 35).$$

Therefore, all the four solutions are $x \equiv 2, 33; 12, 23\ (mod\ 35)$.

Example-2: Consider the congruence $\mathrm{x}^2 \equiv 9\ (\mathrm{mod}\ 77)$.

It can be written as $\mathrm{x}^2 \equiv 3^2(\mathrm{mod}\ 7.11)$.

It is of the type $\mathrm{x}^2 \equiv b^2(\mathrm{mod\ pq})$ with $\mathrm{p} = 7, \mathrm{q} = 11, \mathrm{b} = 3$.

It has four solutions. The two obvious solutions are $x \equiv \pm b\ (mod\ pq)$

$$\equiv \pm 3\ (mod\ 7.11)$$

$$\equiv 3, 74\ (mod\ 77).$$

The remaining two solutions are given by $x \equiv \pm(pk \pm b)(mod\ pq) if\ k\ (pk \pm 2b) = qt$.

$$\equiv \pm(7k \pm 3)(mod\ 7.11)\ if\ k(7k \pm 2.3) = 11t$$

$\equiv \pm(7k + 3)(mod\ 77)\ if\ k(7k \pm 6) = 11t.$

But it can be seen that $for\ k = 4,\ \ 4(7.4 - 6) = 11t$ and hence the solutions are given by

$$x \equiv \pm(7.4 - 3)(mod\ 77)$$

$$\equiv \pm 25\ (mod\ 77)$$

$$\equiv 25, 77 - 25 \equiv 25, 52\ (mod\ 77).$$

Therefore, all the four solutions are $x \equiv 3, 74; 25, 52\ (mod\ 77)$.

PROBLEM-STATEMENT

“To find the solutions of the congruence of the type:

$x^2 \equiv a\ (mod\ pq)$; p& q being different odd primes in two cases:

Case-I: when $a = p^2$;the congruence is then: $x^2 \equiv p^2 \ (mod\ pq)$

Case-II: when $a = q^2, the\ congruence\ is\ then\ x^2 \equiv q^2(mod\ pq)$".

LITERATURE-REVIEW

A standard quadratic congruence of composite modulus considered here for formulation of its solutions, is not formulated earlier by then mathematicians. Only CRT[4] method is permitted to find the solutions. But Roy [1] has formulated its solutions. It is found that such types of congruence have exactly four solutions. Going through the paper, it is found that two special cases are yet remain to formulate. It is also found that such congruence of composite modulus always has exactly two solutions. The aim of the present paper is to find the two solutions.

EXISTED METHOD

Existed method is popularly known as CRT method. In this method, the original congruence

Is split into two separate individual congruence as:

$x^2 \equiv p^2 \ \equiv 0 \ (mod\ p)$……………………………………………………..(A)

$x^2 \equiv p^2 \ (mod\ q)$……………………………………………..(B)

The congruence (A) has exactly one solutions and the congruence (B) has exactly two solutions [5].

Therefore, the original congruence must have exactly 1.2=2 solutions[6].

ANALYSIS & RESULTS

Consider the congruence under consideration:$x^2 \equiv b^2(mod\ pq)$.

Such congruence are always solvable as a^2 is always a quadratic residue ofpq.

Sometimes the congruence be of the form: $x^2 \equiv a \ (mod\ pq)$ with a not be a perfect square, but it can be made so as:

$$x^2 \equiv a \ (mod\ pq)$$

$$\equiv a + k.pq = b^2(mod\ pq)[3]$$

Then the solutions are $x \equiv \pm b \ (mod\ pq)$.

Case-I: Let $b = p$.

Then the congruence reduces to $x^2 \equiv p^2(mod\ pq), p < q$.

Such congruence always has exactly two solutions.

These solutions are given by $x \equiv \pm p \ (mod\ pq)$

$$\equiv p, pq - p \ (mod\ pq).$$

These are the required two solutions.

Case-II: Let $b = q$.

Then the congruence reduces to: $x^2 \equiv q^2(mod\ pq), p < q$.

Such congruence always has exactly two solutions.

These solutions are given by $x \equiv \pm q\ (mod\ pq)$

$$\equiv q, pq - q (mod\ pq).$$

These are the required two solutions.

ILLUSTRATIONS

Example-1: Consider the congruence x^2≡25 (mod 35).

It can be written as $x^2 \equiv 5^2\ (mod\ 5.7)$ with $p = 5, q = 7$.

It is of the type: $x^2 \equiv p^2 (mod\ pq), p < q$.

Such congruence always has exactly two solutions.

These solutions are given by $x \equiv \pm p\ (mod\ pq)$

$$\equiv p, pq - p (mod\ pq).$$

$$\equiv 5, 35 - 5\ (mod\ 35)$$

$$\equiv 5, 30\ (mod\ 35).$$

Example-2: Consider the congruence x^2≡14 (mod 35).

It can be written as $x^2 \equiv 14 + 35 = 49 = 7^2\ (mod\ 5.7)$ with $p = 5, q = 7$.

It is of the type: $x^2 \equiv q^2 (mod\ pq), p < q$.

Such congruence always has exactly two solutions.

These solutions are given by $x \equiv \pm q\ (mod\ pq)$

$$\equiv q, pq - q (mod\ pq).$$

$$\equiv 7, 35 - 7\ (mod\ 35)$$

$$\equiv 7, 28\ (mod\ 35).$$

CONCLUSION

Thus, it can be concluded that the congruence under consideration have two incongruent solutions$i.e.\ x^2 \equiv p^2 (mod\ pq) has\ the\ solutions\ x \equiv \pm p\ (mod\ pq)$; and the congruence

$$x^2 \equiv q^2 (mod\ pq) has\ the\ solutions\ x \equiv \pm q\ (mod\ pq) .$$

REFERENCE

[1] Roy B M, *Formulation of solutions of a solvable standard quadratic congruence of composite modulus- a product oftwo different odd primes*& also a product of twin primes, (IJCR), ISSN: 0975-8337, Vol-10, Issue-05, May-18.

[2] Roy B M, *Formulation of solutions of a standard quadratic congruence of composite modulus- a product of twin primes*, (IJTSRD), ISSN: 2456-6470, Vol-03, Issue-05, July-19.

[3] Roy B M, *Discrete Mathematics & Number Theory*, ISBN: 978-93-84336-12-7, First edition, Das GanuPrakashan, Nagpur, (India), Jan-2016

[4] Thomas Koshy, *Elementary Number Theory with Applications*, Second Edition, Academic Press (An Imprint of Elsevier), ISBN: 978-0-12-372487-8 (original), ISBN: 978-81-312-1859-4 (Indian Print), 2009.

[5] Ajay Kr Choudhury, *Introduction to Number Theory*, New Central Book Agency (P) Ltd, first edition, ISBN: 81-7381-586-0, Jan-2009.

[6]Zuckerman H. S., Niven I., Montgomery H. L., "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, Page No. 136-136, Exercise-18, ISBN: 978-81-265-1811-1. (1960: Reprint 2008).

…………………………………………………………xxx……………………………………………… ……..