RESEARCH ARTICLE OPEN ACCESS

RP-157: A Revised Formulation of Special Standard Quadratic Congruence Modulo nth Power of an Odd Prime Multiplied by Two

Prof B M Roy

Head, Department of Mathematics

Jagat Arts, Comerce& I H P Science College, Goregaon

Dist-Gondia, M. S., India, PIN: 441801

ABSTRACT

In this revised formulation, the author has revised the formulation of the solutions of the standard quadratic congruence of even multiple of odd prime-power modulus.Previously, it was formulated by the author for a single case. Now a complete formulation is presented here.The formulae are established for the solutions in different cases. It is found that in first case, the congruence has a single solution; in the second case, it has exactly p incongruent solutions; in the third case, the congruence has $2p$ incongruent solutions, where p is an odd prime positive integer present in the congruence.The formulae are tested using numerical examples and verified true. Such formulations are not found in the literature of mathematics. First time, a formulation is obtained.

KEY-WORDS : Incongruent solutions, Odd prime, Prime-power modulus, Quadratic congruence.

INTRODUCTION

In this paper, the author wishes to find the solutions of a very special type of standard quadratic congruence of an even multiple of an odd prime power modulus. The congruence can be written as:$x^2 \equiv p^2 (mod\ 2p^n); p\ odd\ prime, n \geq 1$.The author already has formulated the congruence only for $n \geq 3$ [1].Now the author formulated the said congruence foe different cases.After a rigorous study, the author understood that the said congruence has different number of solutions for different powers of p $i.e. for\ different\ values\ of\ n\ such\ as\ n = 1, n = 2, n \geq 3$.

PROBLEM STATEMENT

Here to formulate the solutions of the very special type of standard quadratic congruence:

$x^2 \equiv p^2 (mod\ 2p^n); p\ odd\ prime, n \geq 1$in three different cases, for n=1, n=2, n≥ 3.

LITERATURE REVIEW

Going through the books of Number Theory to find some literature of the said congruence, nothing is found about the solutions. Yet no mention of the congruence is seen. No other method is found to find all the solutions directly except the Chinese Remainder Theorem (CRT) [2].Some related congruence are also formulated by the author [3], [4].

EXISTED METHODS

In using CRT, one has to split the given congruence in two separate congruence:

$$x^2 \equiv p^2 (mod\ 2)\ i.e. x^2 \equiv 1\ (mod\ 2)\ i.e. x \equiv \pm 1\ (mod\ 2)\ i.e. x \equiv 1\ (mod\ 2).$$

The congruence: $x^2 \equiv p^2 (mod\ p^n)$ can be solved by iterative method [5]. But it is not so simple. Some congruence is time-consuming. The congruence has different number of solutions. Only the author's formulation saves time [2]. It gives solutions very easily in a short time.

ANALYSIS & RESULTS

Consider the congruence: $x^2 \equiv p^2 (mod\ 2p^n); p\ odd\ prime, n \geq 1.$

Case-I: Let $n = 1$. Then the congruence reduces to: $x^2 \equiv p^2 (mod\ 2p); p\ odd\ prime.$

The study revealed that the congruence has just exactly one incongruent solution:

$x \equiv \pm p\ \ (mod\ 2p)$; for $x^2 \equiv p^2 (mod\ 2p)$, the solutions are $x \equiv \pm p\ (mod\ 2p)$

$$\equiv p, -p\ (mod\ 2p)$$

To have a positive solution, one have to add 2p to –p $i.e. x \equiv p, 2p - p\ (mod\ 2p)$

$$\equiv p, p\ (mod\ 2p)$$

$$\equiv p\ (mod\ 2p).$$

Thus, the congruence has a single solution$x \equiv p\ (mod\ 2p)$.

Case-II: Let $n = 2$. Then the congruence reduces to: $x^2 \equiv p^2 (mod\ 2p^2); p\ odd\ prime.$

The similar study revealed that the congruence has exactly p incongruent solutions.For these solutions, consider $x \equiv 2pk + p\ (mod\ 2.p^2); p\ odd\ prime.$

Then $x^2 \equiv (2.pk + p)^2 (mod\ 2.p^2)$

$$\equiv (2.pk)^2 + 2.2.pk.p + p^2\ (mod\ 2p^2)$$

$$\equiv 4p^2k^2 + 4p^2k + p^2\ (mod\ 2p^2)$$

$$\equiv 4p^2k\ (\ k + 1) + p^2\ (mod\ 2p^2)$$

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

Thus, $x \equiv 2.pk + p\ (mod\ 2.p^2)$ satisfies the congruence under consideration and so it must be considered as solutions of the congruence.

But for$k = p$, the formula becomes $x \equiv 2.p.p + p\ (mod\ 2.p^2)$

$$\equiv 2p^2 + p\ (mod\ 2p^2)$$

$\equiv p\ (mod\ 2p^2).$

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

Also for $k = p + 1$, it can be seen that $x \equiv 2.p.(p + 1) + p\ (mod\ 2.p^2)$

$$\equiv 2p^2 + 2p + p\ (mod\ 2p^2)$$

$\equiv 2p + p (mod\ 2p^2).$

This is the same solutions as for $k = 1$.

Therefore, all the solutions are given by

$$x \equiv 2.pk + p \ (mod\ 2.p^2); p\ odd\ prime\ with\ k = 0, 1, 2, \dots \dots .. (p-1).$$

Case-III: Let $n \geq 3$.For the solutions of the congruence $x^2 \equiv p^2 (mod\ 2p^n); n \geq 3$, consider $x \equiv 2p^{n-1}k \pm p\ (mod\ 2p^n)$.

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

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

$$\equiv 4p^{2n-2}k^2 \pm 4p^n k + p^2\ (mod\ 2p^n)$$

$$\equiv 4p^n k(p^{n-2}k \pm 1) + p^2 (mod\ 2p^n)$$

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

Therefore, $x \equiv 2p^{n-1}k \pm p\ (mod\ 2p^n)$ satisfies the congruence and hence it gives the solutions. But it is seen that for $k = p$, the solutions formula reduces to

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

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

$\equiv 0 \pm p\ (mod\ 2p^n)$.

These are the same solutions as for $k = 0$.

Also for $k = p + 1$, the solutions formula again becomes

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

$$\equiv 2p^n + 2p^{n-1} \pm p\ (mod\ 2p^n)$$

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

These are the same solutions as for $k = 1$.

Therefore all the solutions are given by

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

These gives exactly $2p -$ incongruent solutions.

ILLUSTRATIONS

Example -1: Consider the congruence $x^2 \equiv 49\ (mod\ 14)$.

It can be written as: $x^2 \equiv 7^2 (mod\ 2.7)$.

It is of the type: $x^2 \equiv p^2 (mod\ 2p)\ with\ p = 7, n = 1$.

It has exactly one solution which is given by

$$x \equiv \pm p\ (mod\ 2.p).$$

$$\equiv \pm 7\ (mod\ 2.7)$$

$$\equiv 7, -7\ (mod\ 14)$$

$$\equiv 7, 14-7\ (mod\ 14)$$

$$\equiv 7, 7\ (mod\ 14)$$

$$\equiv 7\ (mod\ 14).$$

Example-2: Consider the congruence $x^2 \equiv 49\ (mod\ 98)$.

It can be written as: $x^2 \equiv 7^2 (mod\ 2.7^2)$.

It is of the type: $x^2 \equiv p^2 (mod\ 2p^n)\ with\ p = 7, n = 2$.

It has exactly p=7 solutions which are given by

$$x \equiv 2.p^{2-1}k + p\ (mod\ 2.p^2); k = 0, 1, 2, 3, 4, 5, 6.$$

$$\equiv 2.7k + 7\ (mod\ 2.7^2)$$

$$\equiv 14k + 7\ (mod\ 98)$$

$$\equiv 0 + 7, 14 + 7, 28 + 7, 42 + 7, 56 + 7, 70 + 7, 84 + 7\ (mod\ 98)$$

$$\equiv 7, 21, 35, 49, 63, 77, 91\ (mod\ 98).$$

These are the seven solutions of the congruence.

Example-3: Consider the congruence $x^2 \equiv 49\ (mod\ 686)$.

It can be written as: $x^2 \equiv 7^2 (mod\ 2.7^3)$.

It is of the type: $x^2 \equiv p^2 (mod\ 2p^n)\ with\ p = 7, n = 3$.

It has exactly 2p=2.7=14 solutions which are given by

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

$$\equiv 2.7^2k \pm 7\ (mod\ 2.7^3)$$

$$\equiv 98k \pm 7\ (mod\ 686)$$

$$\equiv 0 \pm 7, 98 \pm 7, 196 \pm 7, 294 \pm 7, 392 \pm 7, 490 \pm 7, 588 \pm 7\ (mod\ 686)$$

$$\equiv 7, 679;\ 91, 105;\ 189, 203; 287, 301;\ 385, 399\ ; 483, 497; 581,595\ (mod\ 686).$$

These are the fourteen solutions of the congruence.

CONCLUSION

Therefore, it can be concluded that the congruence: $x^2 \equiv p^2 (mod\ 2p^2); p\ odd\ prime$, has p incongruent solutions:$x \equiv 2.pk + p\ (mod\ 2.p^2); k = 0,1, 2, 3, \dots \dots \dots \dots (p-1)$.

But the congruence $x^2 \equiv p^2 (mod\ 2p^n); p\ odd\ prime, n \geq 3$, has exactly $2p$ incongruent solutions:$x \equiv 2.pk \pm p\ (mod\ 2.p^2); k = 0,1, 2, 3, \dots \dots \dots \dots (p-1)$ as for a single value of k, the congruence has exactly two solutions. Also, the congruence: $x^2 \equiv p^2\ (mod\ 2p)$as for $n = 1$, has a single solution $x \equiv p\ (mod\ 2p)$.

REFERENCE

[1] Roy B M,*Formulation of solutions of a very special standard quadratic congruence of prime-power modulus*,International Journal of Trends in Scientific Research and Development(IJTSRD), ISSN: 2456-6470, Vol-04, Issue-05, July-20.

[2]Zuckerman H. S.,Niven I., 2008, *An Introduction to the Theory of Numbers,* Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.

[3] Roy B M,*Formulation of a very special type of standard quadratic congruence of composite modulus modulo a product of a powered odd prime integer and four***,** International Journal for Scientific Development and Research (IJSDR), ISSN:2455-2631, Vol-05, Issue-07,July-20.

[4] Roy B M,*Formulation of solutions of standard quadratic congruence of composite modulus- a product of an odd prime power integer and eight*, International Journal for Scientific Development and Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-08, Aug-20.

[5] Thomas Koshy, 2009, *Elementary number Theory with Applications*, Academic Press, An Imprint of Elsevier, New Delhi, Second edition, ISBN:978-81-312-1859-4, page-537.