RP-148: Formulation of solutions of standard quadratic congruence modulo a powered even-prime-multiple of square of an odd prime.

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- Gondia, M. S., India. Pin: 441801

Abstract: In this paper, the standard quadratic congruence of composite modulus modulo a multiple of powered even prime & square of an odd prime is formulated. It is the generalisation of the author's previous papers. It is found that the such congruence always have $4p-$ incongruent solutions. A suitable formula is presented here, which helps to find the solutions orally. Formula is tested true by solving suitable numerical examples.

Keywords: Chinese Remainder Theorem, Powered even-prime, Powered odd-prime, Quadratic congruence,

INTRODUCTION

The author already has formulated the standard quadratic congruence of composite modulus of the type:

$$x^2 \equiv p^2 \pmod{2p^2}\ [4];$$
$$x^2 \equiv p^2 \pmod{4p^2}\ [5];$$
$$x^2 \equiv p^2 \pmod{8p^2}\ [6].$$

Now the author has intended to generalise these congruence. For that he consider the congruence: $x^2 \equiv p^2 \pmod{2^m p^2}; m \geq 2; p$ being an odd prime.

PROBLEM-STATEMENT

Here the problem is-

"To formulate solutions of $x^2 \equiv p^2 \pmod{2^m p^2}; m \geq 2;$ p being an odd prime".

LITERATURE REVIEW

The author has gone through many books of Number Theory and found that most of the books contains discussion on standard quadratic congruence of prime modulus but no discussion is found for congruence of composite modulus except Thomas Koshy [1]. In his book, he started a discussion on the congruence of composite modulus but stops abruptly. Some problems were given in the exercise. Chine Remainder Theorem [2], [3] finds its important use in solving the congruence. The author nowhere found the method of solutions or any formulation of solutions of the congruence considered here.

ANALYSIS & RESULTS

Consider the congruence: $x^2 \equiv p^2 \pmod{2^m p^2}$, p an odd prime.

For the solutions, let $x \equiv 4pk \pm p \pmod{2^m p^2}$.

Then, $x^2 \equiv (4pk \pm p)^2 \pmod{2^m p^2}$

$$\equiv (4pk)^2 \pm 2.4pk.p + p^2 \pmod{4p^2}$$

$$\equiv 16p^2k^2 \pm 8pk + p^2(\pmod{8p^2}$$

$$\equiv 8pk(2pk \pm 1) + p^2 \pmod{8p^2}$$

$$\equiv p^2 \pmod{8p^2}$$

Therefore, $x \equiv 4pk \pm p \pmod{8p^2}$ satisfies the said congruence and hence it must be consider as solutions of the congruence. But if $k = 2p$, the solution formula reduces to the form, $x \equiv 4p.2p \pm p \pmod{8p^2}$

$$\equiv 8p^2 \pm p \pmod{8p^2}$$

$$\equiv 0 \pm p \pmod{8p^2}.$$

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

Also for $k = 2p + 1$, the solution formula reduces to the form: $x \equiv 4p \pm p \pmod{8p^2}$.

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

Therefore, all the solutions are given by:

$$x \equiv 4pk \pm p \pmod{8p^2};\ k = 0, 1, 2, \ldots\ldots, (2p - 1).$$

These are $4p -$ incongruent solutions as for a single value of k, it has exactly two solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 9 \pmod{144}$.

It can be written as $x^2 \equiv 3^2 \pmod{16.3^2}$.

It is of the type $x^2 \equiv p^2 \pmod{2^4p^2}$ with $p = 3$.

It has exactly $4p = 4.3 = 12$ incongruent solutions given by

$$x \equiv 2^{m-1}pk \pm p \pmod{2^mp^2};\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (2p - 1).$$

$$\equiv 2^{4-1}.3k \pm 3 \pmod{16.9}$$

$$\equiv 24k \pm 3 \pmod{144};\ k = 0, 1, 2, 3, 4, 5.$$

$$\equiv 0 \pm 3; 24 \pm 3; 48 \pm 3; 72 \pm 3; 96 \pm 3; 120 \pm 3 \pmod{144}.$$

$$\equiv 3, 69; 21, 27; 45, 51; 69, 75; 93, 99; 117, 123 \pmod{144}$$

These are the required twelve solutions.

Example-2: Consider the congruence $x^2 \equiv 25 \pmod{800}$.

It can be written as $x^2 \equiv 5^2 \pmod{32.5^2}$ i.e. $x^2 \equiv 5^2 \pmod{2^5.5^2}$.

It is of the type $x^2 \equiv p^2 \pmod{2^m.p^2}$ with $p = 5$.

It has exactly $4p = 4.5 = 20$ incongruent solutions given by

$$x \equiv 2^{m-1}pk \pm p \pmod{2^mp^2};\ k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (2p - 1).$$

$$\equiv 16.5k \pm 5 \pmod{32.25}$$

$$\equiv 80k \pm 5 \pmod{800};\ k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9.$$

$$\equiv 0 \pm 5; 80 \pm 5; 160 \pm 5; 240 \pm 5; 320 \pm 5; 400 \pm 5; 480 \pm 5;$$

$$560 \pm 5; 640 \pm 5; 720 \pm 5 \pmod{800}.$$

$$\equiv 5, 795; 75, 85; 155, 165; 235, 245; 315, 325; 395, 405; 475, 485;$$

$$555, 565; 635, 645; 715, 725 \pmod{800}$$

These are the required twenty solutions.

CONCLUSION

Therefore, it is concluded that the standard quadratic congruence of composite modulus of the type: $x^2 \equiv p^2 \pmod{2^mp^2}$ has exactly $4p$ incongruent solutions given by

$$x \equiv 2^{m-1}.p.k \pm p \pmod{2^mp^2};\ k = 0, 1, 2, \ldots\ldots\ldots, (2p - 1).$$

MERIT OF THE PAPER

Formulation of the solutions is the merit of the paper.

REFERENCES

[1] Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic press, Second edition, ISBN: 978-81-312-3859-4.

[2] Zuckerman H. S., Niven I., Montgomery H. L., 2008, "An Introduction to The Theory of Numbers", fifth edition, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.

[3]David M Burton, 2012, Elementary Number Theory, Mc Graw Hill education, Seventh Indian Edition, ISBN: 978-1-25-902576-1.

[4] Roy B M, Formulation of a class of standard quadratic congruence of composite modulus modulo double of a powered odd prime, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-05, Issue-10, oct-20.

[5] Roy B M, Formulation of solutions of standard quadratic congruence of composite modulus modulo a product of square of an odd prime & four, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-03, Issue-05, Oct-20.

[6]] 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.