RP-147: Formulation of solutions of standard quadratic congruence modulo an eighth multiple of square of an odd prime in a special case

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 author has formulated the solutions of a standard quadratic congruence modulo an eighth multiple of square of an odd prime in a special case. Such type of congruence always has 4p - incongruent solutions, where p is the prime in the modulus. Various numerical examples are solved using the established formula; solutions are tested and verified true. The formulation made the calculation of solutions orally. This is the merit of the paper.**

***Keywords*: Composite modulus, Eighth multiple, Formulation, Quadratic congruence.**

INTRODUCTION

The author has first time attempted to formulate some special type of standard quadratic congruence of composite modulus. In this connection, in continuation of the previous formulation, one more standard quadratic congruence of such type is considered here for formulation the congruence of the type: $x^2 \equiv p^2 \pmod{8p^2}$, p an odd prime. It is found that it has a different type of formulation. No special method or formulation is found in the literature of mathematics.

PROBLEM-STATEMENT

Here the problem is – "To formulate the standard quadratic congruence of the type:

$$x^2 \equiv p^2 \pmod{8p^2}, \text{p an odd prime"}.$$

LITERATURE-REVIEW

The author already has formulated many standard quadratic congruence of composite modulus [1], [2], [3], [4], [5]. Literature of mathematics shows no consent of the said congruence. Thomas Koshy [6] and David M. Burton [7] discussed the standard quadratic congruence of composite modulus. In these books, the method of solving the congruence

$x^2 \equiv a \pmod{p^n}, n \geq 1,$ p an odd prime, is discussed. The method described is an iterative method which takes a long time to get the solutions by iterations. No formulation is given for the solutions. Also, in the book of Number Theory, Zuckerman [8] discussed the solutions of the congruence $x^2 \equiv a \pmod{2^n}, n \geq 3,$ and presented a formulation for solutions.

But the books remain silent about the present congruence. Hence, the author wishes to formulate the congruence.

NEED OF RESEARCH

The congruence considered here for formulation, has a huge number of solutions. These solutions can only be obtained if appropriate formulation is known. Without formulation, it is nearly impossible to find all those solutions. Thus formulation of solutions is needed.

ANALYSIS & RESULT

Consider the congruence: $x^2 \equiv p^2 \pmod{8p^2}$, p an odd prime.

For the solutions, let $x \equiv 4pk \pm p \pmod{8p^2}$.

Then, $x^2 \equiv (4pk \pm p)^2 \pmod{8p^2}$

$\equiv (4pk)^2 \pm 2.4pk.p + p^2 \pmod{8p^2}$

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

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

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

Therefore, $x \equiv 4pk \pm p \pmod{8p^2}$ satisfies the said congruence and hence it must be considered as the solutions of the said congruence. But if $k = 2p$, the solution formula reduces to the form, $x \equiv 4p.2p \pm p \pmod{48}$

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

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

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 $x^2 \equiv 49 \pmod{392}$.

It can be written as $x^2 \equiv 7^2 (\mathrm{mod}\ 8.7^2)$.

It is of the type $x^2 \equiv p^2 (\mathrm{mod}\ 8p^2)$ with $p = 7$.

It has $4p = 4.7 = 28$ incongruent solutions given by

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

$$\equiv 4.7k \pm 7 \pmod{8.49};\ k = 0, 1, 2, 3, 4, 4, 6, 7, 8, 9, 10, 11, 12, 13.$$

$$\equiv 28k \pm 7 \pmod{196};\ k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.$$

$$\equiv 0 \pm 7; 28 \pm 7; 56 \pm 7; 84 \pm 7; 112 \pm 7; 140 \pm 7; 168 \pm 7; 196 \pm 7; 224 \pm 7;$$

$$252 \pm 7; 280 \pm 7; 308 \pm 7; 336 \pm 7; 364 \pm 7 \pmod{392}.$$

$$\equiv 7, 189; 21, 35; 49, 63; 77, 91; 105, 119; 133, 147; 161, 175; 189, 203; 217, 231;$$

$$245, 259; 273, 287; 301, 315; 329, 343; 357, 371 \pmod{392}.$$

These are the twenty-eight solutions of the congruence.

Example-2: Consider the congruence $x^2 \equiv 9 \pmod{72}$.

It can be written as $x^2 \equiv 3^2 (\mathrm{mod}\ 8.3^2)$.

It is of the type $x^2 \equiv p^2 (\mathrm{mod}\ 8.p^2)$ with $p = 3$.

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

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

$$\equiv 4.3k \pm 3 \pmod{8.9};\ k = 0, 1, 2, 3, 4, 5.$$

$$\equiv 12k \pm 3 \pmod{72};\ k = 0, 1, 2, 3, 4, 5.$$

$$\equiv 0 \pm 3; 12 \pm 3; 24 \pm 3; 36 \pm 3; 48 \pm 3; 60 \pm 3; \pmod{72}.$$

$$\equiv 3, 69; 9, 15; 21, 27; 33, 39; 45, 51; 57, 63 \pmod{72}.$$

$$\equiv 3, 9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69 \pmod{72}.$$

These are the twelve incongruent solutions of the congruence.

Example-3: Consider the congruence $x^2 \equiv 961 \pmod{7688}$.

It can be written as $x^2 \equiv 31^2 (\mathrm{mod}\ 8.31^2)$.

It is of the type $x^2 \equiv p^2 (\mathrm{mod}\ 8.p^2)$ with $p = 31$.

It has $4p = 4.31 = (124!!)$ incongruent solutions given by

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

$\equiv 4.31k \pm 31 \pmod{8.961}; k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots\ldots.., 61.$

$\equiv 124k \pm 31 \pmod{72}; k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots.., 61.$

$\equiv 0 \pm 31; 124 \pm 31; 248 \pm 31; 372 \pm 31; \ldots\ldots\ldots.; 7564 \pm 31 \pmod{7688}.$

$\equiv 31, 7657; 93, 155; 217, 279; \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots.; 7533, 7595 \pmod{7688}.$

These are the one hundred & twenty-four incongruent solutions of the congruence.

CONCLUSION

Therefore, the congruence $x^2 \equiv p^2 \pmod{8.p^2}$ has 4p-incongruent solutions given by

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

These solutions are tested by trial and error method and found true.

MERIT OF THE PAPER

A formula is established for solutions of the said congruence. Now it becomes possible to find a huge number of solutions of the congruence under consideration directly and also orally. This is the merit of the paper.

REFERENCES

[1] Roy B M, Formulation of solutions of a very special standard quadratic congruence of prime-power modulus, (IJTSRD), ISSN: 2456-6470, vol-04, Issue-05, July-20.

[2] 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, (IJSDR), ISSN: 2455-2631, vol-05, Issue-07, July-20.

[3] Roy B M, Formulation of solutions of a very special type of standard quadratic congruence of composite modulus – an eighth multiple of an odd prime-power integer, (IJSDR), ISSN: 2455-2631, vol-05, Issue-08, Aug-20.

[4] Roy B M, Formulation of solutions of a class of standard quadratic congruence of composite modulus modulo double of a squared odd prime, (IJSDR), ISSN: 2581-7175, vol-03, Issue-05, 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, (IJSRED), ISSN: 2455-2631, vol-05, Issue-10, Oct-20.

[6] Thomas Koshy, 2009, Elementary Number Theory with Applications, second edition, Academic Press, ISBN: 978-81-312-1859-4.