iJETRM
International Journal of Engineering Technology Research & Management

RP-159: SOLVING TWO SPECIAL STANDARD QUADRATIC CONGRUENCE MODULO AN ODD PRIME MULTIPLIED BY TWO AND FOUR

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, two special standard quadratic congruence of composite modulus of modulo $2p$ *and* $4p, p$ *being an odd prime, are studied for finding solutions. The author has discussed the available suitable methods for it. It is found that the first congruence has exactly one solution while the second hasexactly two solutions in two different cases. Here, the author used his own formulation to find the solutions easily.*

KEYWORDS
Composite Modulus, Incongruent solutions, Odd primes, Quadratic Congruence.

INTRODUCTION

In [1] the standard quadratic congruence of prime modulus is prominently discussed. In {2], [3], the standard quadratic congruence of prime and composite modulus are discussed. They used the Chinese Remainder Theorem. But no formulation is presented.

It is also seen that all the solvable standard quadratic congruence of prime modulus has exactly two incongruent solutions [1]. But the congruence of composite modulus have at least four incongruent solutions [2]. Knowing these, the author started thinking of the congruence of composite modulus for a single solution; also, for a congruence of composite modulus having exactly two incongruent solutions.

In this paper, the author discussed such congruence of composite modulus. He found two such congruence.

PROBLEM-STATEMENT

Here the problem of study is "To discuss the finding of solutions of the congruence:

(1) $x^2 \equiv p \ (mod\ 2p), p$ *being an odd prime*;
(2) $x^2 \equiv p \ \ (mod\ 4p), p$ *being odd prime with* $p \equiv 1 \ (mod\ 4)$;
(3) $x^2 \equiv 3p \ \ (mod\ 4p), p$ *being odd prime with* $p \equiv 3 \ (mod\ 4)$."

LITERATURE REVIEW

In the literature of mathematics, such types of congruence are not discussed for solutions. Also, no formulation for finding solutions is seen. Even nonumerical example is found.The author already has published his research papers on the congruence of the sametype [4], [5], [6].And from these background, the author insisted to formulate the present congruence.

ANALYSIS & RESULTS

The author wishes to discuss the existed method to find the solutions of the congruence.

EXISTED METHOD

The original congruence:$x^2 \equiv p \ (mod\ 2p)$, can be split into two congruence as

$$x^2 \equiv p \ (mod\ 2) \ldots\ldots\ldots\ldots\ldots (1)$$

$x^2 \equiv p \ (mod\ p)$……(2)

iJETRM
International Journal of Engineering Technology Research & Management

Congruence (1) reduces to $x^2 \equiv 1\ (mod\ 2)\ with\ two\ solutions\ x \equiv \pm 1\ (mod\ 2)$.

$$i.e.\ x \equiv 1, 2-1\ (mod\ 2)$$
$$\equiv 1, 1\ (mod\ 2)$$
$$\equiv 1\ (mod\ 2)$$

Therefore the congruence has exactly one incongruent solution.

Congruence (2) reduces to $x^2 \equiv 0\ (mod\ p)\ with\ single\ solution\ x \equiv p\ (mod\ p)$.

$$i.e.\ x \equiv p\ (mod\ p).$$

Thus, it is easily concluded that the original congruence has exactly $(1.1 = 1)$ one incongruent solution [1].

The common solution of the congruence can now be obtained using CRT method.

(1) Now consider the second congruence:

$$x^2 \equiv p\ (mod\ 4p), p\ \ being\ odd\ prime.$$

It can also be split into two congruence: $x^2 \equiv p\ (mod\ 4)$ ... ... (3)

$x^2 \equiv p\ (mod\ p)$.....(4)

Congruence (3) has exactly two incongruent solutions while the congruence (4) has a unique solution.

Therefore, the original congruence must have $(2.1 = 2)$ two incongruent solutions. The common solutions of the congruence can now be obtained using CRT method.

Similarly, the third congruence can also be treated and solutions can be obtained only for $p \equiv 3\ (mod\ 4)$.

AUTHOR'S FORMULATION

(1) Consider the first congruence under consideration:

$$x^2 \equiv p\ (mod\ 2p), p\ being\ an\ odd\ prime.$$

For its solution, consider the expression:$p^2 - p$.

It is seen that $p^2 - p = p(p-1)$

$$= p.2t$$
$$\equiv 0\ (mod\ 2p),$$ as p odd prime, p-1 is even.

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

Therefore, $x \equiv p\ (mod\ 2p)$ satisfies the congruence $x^2 \equiv p\ (mod\ 2p)$.

Hence, it must be a solution of the said congruence.

It is also tested and found that the congruence has no other solutions. It is well understood in the following discussion.

Now consider the congruence: $x^2 \equiv p\ (mod\ 4p)$.

Let $p \equiv 1\ (mod\ 4)$. Then $p - 1 = 4t, t\ an\ integer$.

Therefore, $p^2 - p = p(p-1) = p.4t \equiv 0\ (mod\ 4p)$.

So, $x \equiv \pm p\ (mod\ 4p)$ satisfies the congruence $x^2 \equiv p\ (mod\ 4p)$.

Hence it gives two solutions of the congruence and no other possibility is found. And it is seen that such congruence always has two solutions.

Also, for the congruence $x^2 \equiv 3p\ (mod\ 4p)\ with\ p \equiv 3\ (mod\ 4)$.

Consider $x \equiv \pm p\ (mod\ 4p)$.

Then $p^2 - 3p = p(p-3) = p.4t\ \equiv 0\ (mod\ 4p)$.

Therefore, $x \equiv \pm p\ (mod\ 4p)$ are the two solutions of the congruence.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 29\ (mod\ 58)$.

As 29 is an odd prime and $58 = 2.29$, the congruence can be written as

$$x^2 \equiv 29\ (mod\ 2.29).$$

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

iJETRM
International Journal of Engineering Technology Research & Management

It has a single solution given by $x \equiv p\ (mod\ 2p)$
$\equiv 29\ (mod\ 2.29)$
$\equiv 29\ (mod\ 58)$.
Example-2: Consider the congruence $x^2 \equiv 503\ (mod\ 1006)$
It can be written as $x^2 \equiv 503\ (mod\ 4.503)$
It is of the type $x^2 \equiv p\ (mod\ 2p) with\ p = 503$.
It has exactly one solution $x \equiv p\ (mod\ 2p)$
$\equiv 503\ (mod\ 2.503)$
$\equiv 503\ (mod\ 1006)$.
Example-3: Consider the congruence $x^2 \equiv 37\ (mod\ 148)$.
It can be written as $x^2 \equiv 37\ (mod\ 4.37)$.
It is of the type $x^2 \equiv p\ (mod\ 4p) with\ p = 37$.
It has exactly two incongruent solutions:$x \equiv \pm 37\ (mod\ 148)$
$\equiv 37, 148 - 37\ (mod\ 148)$
$\equiv 37, 111\ (mod\ 148)$.
Example-4: Consider the congruence $x^2 \equiv 41\ (mod\ 164)$.
It can be written as $x^2 \equiv 41\ (mod\ 4.41)$.
It is of the type $x^2 \equiv p\ (mod\ 4p) with\ p = 41$.
The two incongruent solutions: $x \equiv \pm 41\ (mod\ 164)$
$\equiv 41,123\ (mod\ 164)$
Example-5: Consider the congruence $x^2 \equiv 33\ (mod\ 44)$.
It can be written as $x^2 \equiv 3.11\ (mod\ 4.11)$.
It is of the type $x^2 \equiv 3p\ (mod\ 4p) with\ p = 11$.
The two incongruent solutions: $x \equiv \pm 11\ (mod\ 44)$
$\equiv 11,33\ (mod\ 44)$
Example-6: Consider the congruence $x^2 \equiv 57\ (mod\ 76)$.
It can be written as $x^2 \equiv 3.19\ (mod\ 4.119)$.
It is of the type $x^2 \equiv 3p\ (mod\ 4p) with\ p = 19$.
The two incongruent solutions: $x \equiv \pm 19\ (mod\ 76)$
$\equiv 19,57\ (mod\ 76)$.

CONCLUSION

Therefore, it can be concluded that the congruence (1) has a single solution
$x \equiv p\ (mod\ 2p), p\ an\ odd\ prime,$
While the congruence (2) has exactly two solutions $x \equiv \pm p\ (mod\ 4p), p$ being an odd prime and $p \equiv 1\ (mod\ 4)$.
The third congruence also have the solutions $x \equiv \pm p\ (mod\ 4p), when\ p \equiv 3\ (mod\ 4)$.
MERIT OF THE PAPER
First time the author has presented a formulation for the solutions of the said congruence. The solutions can be obtained orally. Therefore, formulation is the merit of the paper.

REFERENCE

[1] Zuckerman H. S., Niven I., 2008, An Introduction to the Theory of Numbers, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.
[2] Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press, Second Edition, Indian print, New Delhi, India, ISBN:978-81-312-1859-4.

iJETRM
International Journal of Engineering Technology Research & Management

[3] David M Burton, 2012, Elementary Number Theory, McGraw Hill Education (India) Private Limited, New Delhi, Seventh Edition, ISBN-13: 978-1-25-902576-1.
[4] Roy B M, Formulation of a class of standard quadratic congruence of composite modulus- a positive prime multiple of four, International Journal of science and Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-11, Nov-18.
[5] Roy B M, Formulation of a class of standard quadratic congruence of composite modulus modulo double of a squared odd prime, International Journal of science and Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-10, Oct-20.
[6] Roy B M, Formulation of a class of standard quadratic congruence of composite modulus modulo a product of square of an odd prime & Four, International Journal of scientificResearch and Engineering Development (IJSRED), ISSN: 2455-2631, Vol-03, Issue-05, Oct-20.
……xxx……
……