RP-143: Formulation of a class of standard quadratic congruence of composite modulus modulo double of a powered 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 author has formulated the solutions of a standard quadratic congruence of composite modulus modulo double of a powered odd prime.**

Such type of congruence always has 2p solutions, where p is an odd prime.

Author's formulation made the finding of solutions very easy. The formulation provided a very simple formula for solutions. Oral calculation of solutions is also possible. Formulation is the merit of the paper.

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

INTRODUCTION

Standard quadratic congruence of composite modulus is seldom studied in mathematics. The focus is converged to study the standard quadratic congruence of prime modulus only. The author of this paper pained so much and started studying these congruence of composite modulus and formulated many such standard quadratic congruence [1], [2], [3]. Here, is one more such congruence found unformulated yet and tried his best to formulate.

PROBLEM-STATEMENT

Here the problem is "To formulate the solutions of the congruence

$x^2 \equiv p^2 \ (mod\ 2p^n), n \geq 3, p\ an\ odd\ prime$".

LITERATURE-REVIEW

The above standard quadratic congruence of composite modulus is seen unformulated in the literature of mathematics. No special method is found to solve the problem but one can use Chinese Remainder Theorem [4], [5], [6]. It is a long process and one must know the method of solving the individual congruence. The literature of mathematics is kept nearly silent.

ANALYSIS & RESULT

Consider the congruence $x^2 \equiv p^2 \ (mod\ 2p^n), n \geq 3, p\ an\ odd\ prime$.

For its solutions, let us consider that $x \equiv 2p^{n-1}k \pm p \ (mod\ 2p^n)$.

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

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

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

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

$$\equiv 0 + p^2 \ (mod\ 2p^n)$$

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

Thus, it can be said that $x \equiv 2p^{n-1}k \pm p \ (mod\ 2p^n), n \geq 3, p\ an\ odd\ prime$ gives the solutions of the congruence. But for $k = p$, the solutions reduce to the form

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

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

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

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

Also, for $k = p - 1$, the solutions formula reduces to

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

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

Therefore, $x \equiv 2p^{n-1}.k \pm p \ (mod\ 2p^n)$ gives all the solutions of the congruence under consideration for$k = 0, 1, 2, \dots \dots \dots \dots, (p-1)$.

Hence the congruence has exactly 2p solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 9 \ (mod\ 54)$.

It can be written as $x^2 \equiv 3^2 (mod\ (2.27)\ \ i.e.\ x^2 \equiv 3^2 (mod\ 2.3^3)$.

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

It has exactly $2p = 2.3 = 6$ incongruent solutions.

These solutions are given by $x \equiv 2p^{n-1}k \pm p \ (mod\ 2p^n); k = 0, 1, 2, \dots \dots, (p-1)$.

$$\equiv 2.3^2k \pm 3 \ (mod\ 2.3^3); k = 0, 1, 2.$$
$$\equiv 18k \pm 3 \ (mod\ 54); k = 0, 1, 2.$$
$$\equiv \pm 3; 18 \pm 3, 36 \pm 3 \ (mod\ 54)$$
$$\equiv 3, 51; 15, 21; 33, 39 \ (mod\ 54).$$

These are the six solutions.

Example-2: Consider the congruence $x^2 \equiv 25 \ (mod\ 1250)$.

It can be written as $x^2 \equiv 5^2 (mod\ 2.5^4)$

It is of the type $x^2 \equiv p^2 (mod\ 2.p^n)\ with\ n = 4, p = 5$.

It has exactly $2p = 2.5 = 10$ incongruent solutions.

These solutions are given by

$$x \equiv 2p^{n-1}k \pm p \ (mod\ 2p^n); k = 0, 1, 2, \dots \dots, (p-1).$$
$$\equiv 2.5^3k \pm 5 \ (mod\ 2.5^4); k = 0, 1, 2, 3, 4.$$
$$\equiv 250k \pm 5 \ (mod\ 1250); k = 0, 1, 2, 3, 4.$$
$$\equiv \pm 5; 250 \pm 5, 500 \pm 5; 750 \pm 5; 1000 \pm 5 \ \ (mod\ 1250)$$
$$\equiv 5, 1245; 245, , 255; 495, 505; 745, 755; 995, 1005 \ (mod\ 1250).$$

These are the ten solutions.

Example-3: Consider the congruence $x^2 \equiv 121 \ (mod\ 2662)$

It can be written as $x^2 \equiv 11^2 (mod\ 2.11^3)$

It is of the type $x^2 \equiv p^2 (mod\ 2.p^n)\ with\ n = 3, p = 11$.

It has exactly $2p = 2.11 = 22$ incongruent solutions.

These solutions are given by

$$x \equiv 2p^{n-1}k \pm p \ (mod\ 2p^n); k = 0, 1, 2, \dots \dots, (p-1).$$
$$\equiv 2.11^2k \pm 11 \ (mod\ 2.11^3); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.$$

$\equiv 242k \pm 11\ (mod\ 2662); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10.$

$\equiv 0 \pm 11; 242 \pm 11, 484 \pm 11; \ldots\ldots\ldots\ldots\ldots\ldots.; 2178 \pm 11; 2420 \pm 11\ (mod\ 2662)$

$\equiv 11, 2651; 231, 253; 473, 495; \ldots\ldots\ldots\ldots; 2167, 2189; 2409, 2431\ (mod\ 1250).$

These are the twenty-two solutions.

CONCLUSION

Therefore, it can be concluded that the standard quadratic congruence:

$x^2 \equiv p^2\ (mod\ 2p^n), n \geq 3, p\ an\ odd\ prime$, has exactly $2p -$ incongruent solutions given by $x \equiv 2p^{n-1}k \pm p\ (mod\ 2p^n); n \geq 3, p\ odd\ prime\ with\ \ k = 0, 1, 2, \ldots\ldots\ldots\ldots, (p-1)$.

MERIT OF THE PAPER

This formulation gives all the incongruent solutions directly. These solutions can also be calculated orally. First time a formulation is provided by the author. This is the merit of the paper.

REFERENCES

[1] Roy B M, Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime-power integer by two or four, (IJRTI), ISSN: 2456-3315, Vol-3, Issue-05, May-18.

[2] Roy B M, Formulation of solutions of a class of standard quadratic congruence of even composite modulus, (IJSDR), ISSN: 2455-2631, Vol-03, Issue-08, Aug-18.

[3] Roy B M, Formulation of a class of solvable standard quadratic congruence of even composite modulus, (IJRTI), ISSN: 2456-3315, Vol-04, Issue-03, March-19.

[4] Roy B M,2016, Discrete Mathematics & Number Theory, First edition, Das Ganu Prakashan, Nagpur, India, ISBN: 978-93-84336-12-7.

[5] Burton David M, 2012, Elementary Number Theory, Seventh Indian edition, Mac Graw Hill publication, ISBN: 13: 978-1-25-902576-1.

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