RP-133: Formulation of solutions of a very special type of standard quadratic congruence of composite modulus- an eighth multiple of an odd prime-power integer

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- Gondia, M. S., India, Pin: 441801
(Affiliated to R T M Nagpur University)

***Abstract*: In this paper, a very special type of standard quadratic congruence of composite modulus – an eighth multiple of an odd prime-power integer is studied for its formulation. After a rigorous study, the author succeed to establish a formulation for its solutions. The formula is tested and verified by illustration a number of numerical examples. Formulation is the merit of the paper. Chinese Remainder Theorem finds no place here for the solutions.**

***Keywords*: Composite Modulus, Formulation, Quadratic Congruence, Prime-power Integer.**

INTRODUCTION

In this paper, the author considered a very special type of standard quadratic congruence of composite modulus- an eighth multiple of an odd prime-power integer for its formulation. After a constant rigorous study of the congruence under consideration, the author succeed to establish the required formulation. This effort is presented here in this paper.

The congruence under consideration is of the type: $x^2 \equiv p^2 \ (mod\ 8.p^m); m \geq 2,$

$p\ an\ odd\ prime$ Integer.

Recently the author has formulated the congruence $x^2 \equiv a\ (mod\ 8p)$ [1] and

Also the congruence $x^2 \equiv a\ (mod\ 8p^m); m \geq 2; a \neq p$ [2].

PROBLEM-STATEMENT

Here the problem is-

"To formulate the standard quadratic congruence of the type:

$$x^2 \equiv p^2\ (mod\ 8.p^m); m \geq 2, p\ an\ odd\ prime\ positive\ integer".$$

LITERATURE-REVIEW

The author already has formulated the congruence: $x^2 \equiv a^2\ (mod\ 8.p^m); a \neq p$. Here p is an odd prime integer. So, the case $a = p$ is remained unformulated. In the literature of mathematics, there found no earlier formulation of the congruence under consideration.

There readers used to apply the Chinese Remainder Theorem (C R T) [3]. In this method the original congruence is split into individual congruence as under:

$x^2 \equiv p^2\ (mod\ 8)$……(1)

$x^2 \equiv p^2\ (mod\ p^m)$ … … … … … … … … (2)

Solving (1) & (2) separately, the common solutions are obtained using C R T.

Sometimes solutions of the congruence (2) creates much trouble. But the author has also formulated the said congruence [4]. Then, the number of common solutions are the product of the number of solutions of the individual congruence [5].

ANALYSIS & RESULTS

Consider the said congruence: $x^2 \equiv p^2\ (mod\ 8p^m)$.

For its solutions, consider: $x \equiv 2.p^{m-1}k \pm p\ \ (mod\ 8p^m)$.

Then, $x^2 \equiv (2.p^{m-1}k \pm p)^2$ (mod $8p^m$)

$$\equiv (2.p^{m-1}k\,)^2 \pm 2.2p^{m-1}k.p + p^2 \ (mod\ 8p^m)$$

$$\equiv 4.p^{2m-2}k^2 \pm 4p^m k + p^2 \ (mod\ 8p^m)$$

$$\equiv 4p^m k(p^{m-2}k \pm 1) + p^2 \ (mod\ 8p^m)$$

$$\equiv 4p^m k.(2t) + p^2 \ (mod\ 8p^m)$$

$$\equiv 8p^m kt + p^2 (mod\ 8p^m)$$

$$\equiv p^2 \ (mod\ 8p^m)$$

Therefore, it can be said that: $x \equiv 2.p^{m-1}k \pm p \ \ (mod\ 8p^m)$ gives the solutions of the congruence under consideration for different values of k.

But for $k = 4p$, the solutions formula established reduces to

$$x \equiv 2.p^{m-1}.4p \pm p \ \ (mod\ 8p^m)$$

$$\equiv 8p^m \pm p \ (mod\ 8p^m)$$

$$\equiv 0 \pm p \ (mod\ 8p^m).$$

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

Also for$k = 4p + 1$, the formula reduces to:

$$x \equiv 2.p^{m-1}.(4p + 1) \pm p \ \ (mod\ 8p^m)$$

$$\equiv 8p^m + 2.p^{m-1}.1 \pm p \ (mod\ 8p^m)$$

$$\equiv 2.p^{m-1}1 \pm p \ (mod\ 8p^m).$$

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

Similarly, for$k = 4p + 2$, it can be seen that the solutions are the same as for $k = 2$.

Therefore, it is concluded that: $x \equiv 2.p^{m-1}.k \pm p \ \ (mod\ 8p^m)$;

$k = 0, 1, 2, \dots\dots\dots, (4p - 1)$ gives all the solutions of the said congruence. These are $2(4p) = 8p$ −solutions as for one value of k, it gives two incongruent solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 25 \ (mod\ 1000)$

It can be written as $x^2 \equiv 5^2 \ (mod\ 8.5^3)\ with\ p = 5$.

It must have $8p = 8.5 = 40$ incongruent solutions.

These solutions are given by

$$x \equiv 2.p^{m-1}.k \pm p \ \ (mod\ 8p^m); k = 0, 1, 2, \dots\dots\dots, (4p - 1).$$

$$\equiv 2.5^{3-1}k \pm 5 \ (mod\ 8.5^3); k = 0, 1, 2, 3, 4, \dots\dots\dots\dots.19.$$

$$\equiv 50k \pm 5 \ (mod\ 1000)$$

$$\equiv 0 \pm 5; 50 \pm 5; 100 \pm 5; 150 \pm 5; 200 \pm 5; 250 \pm 5; 300 \pm 5; 350 \pm 5;$$

$$400 \pm 5; 450 \pm 5; 500 \pm 5; 550 \pm 5; 600 \pm 5; 650 \pm 5; 700 \pm 5; 750 \pm 5; 800 \pm 5;$$

$$850 \pm 5; 900 \pm 5; 950 \pm 5 \ (mod\ 1000)$$

$$\equiv 5, 995; 45,55; 95, 105; 145, 155; 195, 205; 245, 255; 295, 305; 345, 355; 395, 405;$$

$$445, 455; 495, 505; 545, 555; 595, 605; 645, 655; 695, 705; 745, 755; 795, 805; 845,855;$$

$$895, 905; 945, 955 \ (mod\ 1000)$$

These are the forty solutions of the congruence.

Example-2: Consider the congruence $x^2 \equiv 49\ (mod\ 2744)$

It can be written as $x^2 \equiv 7^2\ (mod\ 8.7^3)\ with\ p = 7$.

It must have $8p = 8.7 = 56$ incongruent solutions.

These solutions are given by

$$x \equiv 2.p^{m-1}.k \pm p\ \ (mod\ 8p^m); k = 0, 1, 2, \dots\dots\dots, (4p-1).$$

$$\equiv 2.7^{3-1}k \pm 7\ (mod\ 8.7^3); k = 0, 1, 2, 3, \dots\dots\dots\dots.26, 27.$$

$$\equiv 98k \pm 7\ (mod\ 2744)$$

$$\equiv 0 \pm 7; 98 \pm 7; 196 \pm 7; 294 \pm 7 \dots\dots\dots\dots, 2548 \pm 7; 2646 \pm 7\ (mod\ 2744)$$

≡7, 2737; 91, 105; 189, 203; 287, 301; ……; 2541, 2555; 2639, 2653 $(mod\ 2744))$

These are the fifty-six solutions of the congruence.

CONCLUSION

Therefore, it can be conclude that the standard quadratic congruence of composite modulus of the type

$x^2 \equiv p^2\ (mod\ 8p^m)\ , p\ being\ an\ odd\ prime,$ has exactly $8p$ solutions given by

$$x \equiv 2.p^{m-1}.k \pm p\ \ (mod\ 8p^m); k = 0, 1, 2, \dots\dots\dots, (4p-1).$$

MERIT OF THE PAPER

Using the formula established, the solutions can be obtained orally. A single formula gives a large number of solutions. Formulation is the merit of the paper. No need to use the CRT.

REFERENCES

[1] Roy B M, *Reformulation of solutions of a class of standard quadratic congruence of composite modulus- a product of an odd prime and eight*, International Journal for research trends and innovation (IJRTI), ISSN: 2456-3315, Vol-05, Issue-08, August-20.

[2] 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 of science & Engineering development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-08, August-20.

[3] Roy B M, *Discrete mathematics & Number Theory*, ISBN: 978-93-84336-12-7, Das Ganu Prakashan (Nagpur), India, 1/e, Jan-2016.

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

[5] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "An Introduction to The Theory of Numbers", 5/e, Wiley India (Pvt) Ltd, ISBN: 978-81-265-1811-1.