RP-138: Formulation of solutions of standard quadratic congruence of composite modulus- a product of an odd prime power integer and eight

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
(Affiliated to R T M Nagpur University)

***Abstract*: In this paper, the author considered a class of standard quadratic congruence of composite modulus- a product of an odd prime power integer and eight for formulation of its solutions. After a rigorous study, the solutions of the said congruence, the author succeed to establish the formula for its solutions. Formulation is the merit of the paper.**

***Keywords*: Composite modulus, CRT method, Quadratic Congruence, Quadratic residue.**

INTRODUCTION

A standard quadratic congruence under consideration is of the type $x^2 \equiv a\ (mod\ 8p^n)$. It is said to be solvable, if a is quadratic residue of $8p^n$. The author already has reformulated and published the standard quadratic congruence: $x^2 \equiv a\ (mod\ 8p)$ [1], [2].It is found that the said congruence has exactly eight incongruent solutions if a is an odd positive integer & $a \equiv 1\ (mod\ 8)$; $but\ if\ a\ is\ an\ even\ perfect\ square, it\ has\ exactly\ four\ incongruent\ solutions$.

Now the author wishes to generalise the formulation for an odd prime power integer in the form: $x^2 \equiv a\ (mod\ 8p^n); a \neq p$. The congruence is considered for two different cases.

LITERATURE REVIEW

The present problem is not found in the literature of mathematics. Zukerman [3] had discussed only for standard quadratic congruence of prime modulus and Koshy [4] had started the discussion of the standard quadratic congruence of composite modulus but mentioned no specific method or formula to find the solutions. The author take the responsibility to formulate the solutions of the congruence. There is a method popularly known as Chinese Remainder Theorem (CRT) method [5], can be used to find the solutions of this congruence but problem arises when the individual congruence such as

$x^2 \equiv a\ (mod\ p^n)$ is to solve. Sometimes it takes more than 10 hours to solve the congruence [6].

PROBLEM-STATEMENT

Here the problem is-

"Formulation of standard quadratic congruence of composite modulus:

$x^2 \equiv a\ (mod\ 8p^n); a \neq p\ ,\ p\ an\ odd\ prime\ integer, n\ any\ positive\ integer\ in$

$two\ general\ cases$".

ANALYSIS & RESULT

Let us consider the two general cases as

Case-I: $a\ is\ an\ odd\ positive\ integer\ \&\ a \equiv 1\ (mod\ 8)$;

Case-II: $a\ is\ an\ even\ perfect\ square\ positive\ integer$.

Consider the case-I $i.e.\ a\ is\ odd\ positive\ integer\ \&\ a \equiv 1\ (mod\ 8)$.

Consider the congruence: $x^2 \equiv a\ (mod\ 8p^n)$. If a is quadratic residue, then the congruence can be written as $x^2 \equiv a^2\ (mod\ 8p^n)$.

Case-I: Let $a \neq p$ be an odd positive integer.

Let $x \equiv 2p^n k \pm a\ (mod\ 8p^n)$.

Then, $x^2 \equiv (2p^n k \pm a)^2\ \ (mod\ 8p^n)$

$\equiv (2p^n k)^2\ \pm 2.2p^n k.a + a^2 (mod\ 8p^n)$

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

$\equiv 4p^n k\ (p^n k \pm a) + a^2 \ (mod\ 8p^n)$

$\equiv 4p^n k.\{2t\} + a^2 \ (mod\ 8p^n)$

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

$\equiv a^2 \ (mod\ 8p^n).$

Thus, $x \equiv 2p^n k \pm a \ (mod\ 8p^n)$ are the solutions of the congruence. But for $k = 4$, the solutions reduce to: $x \equiv 2p^n.4 \pm a \ (mod\ 8p^n)$

$\equiv 8p^n + a \ (mod\ 8p^n)$

$\equiv 0 + a \ (mod\ 8p^n).$

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

Similarly, for $k = 5, 6, 7,$ the solutions repeats as for $k = 1, 2, 3$.

Therefore, all the solutions are given by: $x \equiv 2p^n k \pm a \ (mod\ 8p^n); k = 0, 1, 2, 3.$

This gives the eight solutions of the said congruence, if a is an odd positive integer &

$a \equiv 1 \ (mod\ 8)$.

Case-II: Let a be an even perfect square positive integer.

For the solutions, consider $x \equiv 4p^n.k \pm a \ (mod\ 8p^n)$

Then, $x^2 \equiv (4p^n.k \pm a)^2 \ (mod\ 8p^n)$

$\equiv (4p^n.k\ )^2 \pm 2.4p^n k.a + a^2 \ (mod\ 8p^n)$

$\equiv 16.p^{2n}k^2 \pm 8p^n k.a + a^2 \ (mod\ 8p^n)$

$\equiv 8p^n k(\ 2p^n k \pm a) + a^2 \ (mod\ 8p^n)$

$\equiv a^2 \ (mod\ 8p^n).$

Therefore, $x \equiv 4p^n.k \pm a \ (mod\ 8p^n)$ are the solutions for different values of k.

But if $k = 2$, the solutions reduces to $x \equiv 4p^n.2 \pm a \ (mod\ 8p^n)$

$\equiv 8p^n \pm a \ (mod\ 8p^n)$

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

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

Similarly, for $k = 3$, the solutions are the same as for $k = 1$.

Hence, the said congruence has exactly four solutions given by $x \equiv 4p^n.k \pm a \ (mod\ 8p^n)$;

$k = 0, 1.$

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 9 \ (mod\ 1000)$

It can be written as: $x^2 \equiv 3^2 \ (mod\ 8.5^3)$

It is of the type: $x^2 \equiv a^2 \ (mod\ 8.p^n)$ with $a = 3, p = 5, n = 3.$

The congruence has exactly eight solutions, given by

$x \equiv 2p^n k \pm a \ (mod\ 8p^n); k = 0, 1, 2, 3.$

$\equiv 2.5^3 k \pm 3 \ (mod\ 8.5^3)$

$\equiv 250k \pm 3 \ (mod\ 1000); k = 0, 1, 2, 3.$

$\equiv 0 \pm 3; 250 \pm 3; 500 \pm 3; 750 \pm 3 \ \ (mod\ 1000)$

$\equiv 3, 997; 247, 253; 497, 503; 747, 753 \pmod{1000}$.

Example-2: Consider the congruence $x^2 \equiv 65 \pmod{2744}$

It can be written as: $x^2 \equiv 65 + 2744 = 2809 = 53^2 \pmod{8.7^3}$

It is of the type: $x^2 \equiv a^2 \pmod{8.p^n}$ with $a = 53, p = 7, n = 3$.

The congruence has exactly eight solutions, given by

$x \equiv 2p^n k \pm a \pmod{8p^n}; k = 0, 1, 2, 3.$

$\equiv 2.7^3 k \pm 53 \pmod{8.7^3}$

$\equiv 686k \pm 53 \pmod{2744}; k = 0, 1, 2, 3.$

$\equiv 0 \pm 53; 686 \pm 53; 1372 \pm 53; 2058 \pm 53 \pmod{2744}$

$\equiv 53, 2691; 633, 739; 1319, 1425; 2005, 2111 \pmod{2744}$).

Example-3: Consider the congruence $x^2 \equiv 4 \pmod{200}$

It can be written as: $x^2 \equiv 2^2 \pmod{8.5^2}$

It is of the type: $x^2 \equiv a^2 \pmod{8.p^n}$ with $a = 2, p = 5, n = 2$.

The congruence has exactly four solutions, given by

$x \equiv 4p^n k \pm a \pmod{8p^n}; k = 0, 1.$

$\equiv 4.5^2 k \pm 2 \pmod{8.5^2}$

$\equiv 100k \pm 2 \pmod{200}; k = 0, 1.$

$\equiv 0 \pm 2; 100 \pm 2 \pmod{200}$

$\equiv 2, 198; 98, 102 \pmod{200}$.

Example-4: Consider the congruence $x^2 \equiv 6 \pmod{200}$. Though $a = 6$, an even positive integer, but it is not a perfect square; hence it has no solutions.

Example-5: Consider the congruence $x^2 \equiv 3 \pmod{200}$. Though $a = 3$, an odd positive integer, but ; $a \not\equiv 1 \pmod{8}$; hence it has no solutions.

CONCLUSION

Therefore, it can be concluded that the congruence under consideration

$x^2 \equiv a^2 \pmod{8.p^n}; a \neq p$ has exactly eight incongruent solutions if a is an odd positive integer & $a \equiv 1 \pmod{8}$.

Also the same congruence has exactly four incongruent solutions if a is an even perfect square positive integer.

MERIT OF THE PAPER

Here, the congruence $x^2 \equiv a \pmod{8.p^n}; a \neq p$ is formulated successfully and it also becomes possible to find the solutions orally. No need to use papers and pens. This is the merit of the paper.

REFERENCES

[1] Roy B M, *Formulation of solutions of a class of standard solvable standard quadratic congruence of composite modulus- an odd prime positive integer multiple of eight*, International Journal of Mathematics Trends & Technology (IJMTT), ISSN: 2231-5373, Vol-61, Issue-04, and Aug-18.

[2] Roy B M, *Reformulation of solutions of a class of standard quadratic congruence of composite modulus- a product of an odd prime and eight*, (IJRTI), ISSN: 2456-3315, Vol- 05, Issue-08 , Aug-20.

[3] Zuckerman H. S., Niven I., Montgomery H. L., "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, Page No. 136-136, Exercise-18, ISBN: 978-81-265-1811-1. (1960: Reprint 2008).

[4] Thomas Koshy, *Elementary Number Theory with Applications*, ISBN: 978-81-312-1859-4, Academic Press, An Imprint of Elsevier, second edition, 2009 (Indian print).

[5] Ajay Kumar Choudhury, *Introduction to Number Theory*, ISBN: 978-81-7381-586-7, New Central Book Agency (P) Ltd, Kolkata, W. B., India.

[6] Roy B M, *An algorithmic formulation of solving standard quadratic congruence of prime-power modulus*, International Journal of Advanced Research, Ideas, and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-06, Nov-Dec-18.