RP-134: Reformulation of Solutions of a Class of Standard Quadratic Congruence of Composite Modulus - A Product of an Odd Prime and Eight

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, the solvable standard quadratic congruence of composite modulus- a Product of an odd prime-power integer and eight is reformulated. A new single formula is established for its solutions. Now, it becomes finding the solutions orally without using pen & paper. Reformulation of the solutions is the merit of the paper. The author's previous formulation was different and was not a single formula.**

***Keywords*: Composite modulus, C R T method, Prime Integer, Quadratic congruence.**

INTRODUCTION

The congruence under consideration $i.e. x^2 \equiv a \ (mod\ 8p), p\ being\ an\ odd\ prime$ is formulated earlier by the author [4]. But it is now found that the then established formulae are not so easy to remember. Hence, the author wishes to find a single formula to find all the solutions. This is also the need of the reformulation of the solutions of the congruence under consideration.

PROBLEM-STATEMENT

Here the problem is

"To reformulate the solutions of the standard quadratic congruence of the type:

$x^2 \equiv a \ (mod\ 8p), p\ being\ an\ odd\ prime\ positive\ integer\ in\ two\ cases$:

$Case - I$: $If\ a\ is\ an\ odd\ positive\ integer.$

$Case - II$: $If\ a\ is\ an\ even\ positive\ integer$ ".

LITERATURE REVIEW

It is well-known to us that the congruence under consideration: $x^2 \equiv a \ (mod\ 8p)$, $p\ an\ odd\ prime$ Can be solved using CRT Method. No other method or no other formulation is found in the literature of mathematics. Only the author's first formulation is available. So, let us discuss the existed method here.

EXISTED METHOD

In this existed method, Chinese Remainder Theorem (C R T) is used. At first, the congruence is split into two separate individual congruence; these are solved. Using these solutions, common solutions are obtained by CRT [1].

So, the two individual congruence are:

$x^2 \equiv a \ (mod\ 8)$…… (A)

$x^2 \equiv a \ (mod\ p)$ … … … … … … … … … … (B)

If a is an odd positive integer and $a \equiv 1 \ (mod\ 8)$, then (A) has exactly four solutions [2].

The congruence (B) has exactly two solutions [2]. Sometimes, it becomes impractical to solve the congruence (B) because it takes more than 10 hours.

The congruence under consideration as discussed above must have $4.2 = 8$ incongruent solutions, if $a \equiv 1 \ (mod\ 8)$.

But if a is an even positive integer and a perfect square (it is an observation after the rigorous study $i.e.\ a \equiv 0, 4 \ (mod\ 8)$), it has exactly two solutions. It can also be concluded from this study that the congruence is not solvable, if $a \equiv 2, 3, 5, 6, 7 \ (mod\ 8)$.

Therefore, the congruence under consideration must have $2.2 = 4$ incongruence solutions, if a is an even perfect square.

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv a \ (mod\ 8p), p\ an\ odd\ prime.$

If a is an odd perfect square, then the congruence reduces to: $x^2 \equiv a^2 \ (mod\ 8p)$.

If not, then it can be written as: $x^2 \equiv a + k.8p = b^2 \ (mod\ 8p)$ for some k [3].

The congruence then reduces to the form: $x^2 \equiv b^2 \ (mod\ 8p)$.

Case-I: Let a be an odd positive integer. Then b is also an odd positive integer.

For its solutions, consider: $x \equiv 2pk \pm b \ (mod\ 8p)$.

Then, $x^2 \equiv (\ 2pk \pm b)^2 \ (mod\ 8p)$

$\equiv (2pk)^2 \pm 2.2p^m k.b + b^2 \ \ (mod\ 8p)$

$\equiv 4p^2k^2 \pm 4pk.b + b^2 \ (mod\ 8p)$
$\equiv 4pk(\ pk \pm b) + b^2 \ (mod\ 8p)$
$\equiv 4pk(2t) + b^2 \ (mod\ 8p)$
$\equiv 8pkt + b^2 (mod\ 8p)$
$\equiv b^2 \ (mod\ 8p)$

Therefore, $x \equiv 2pk \pm b \ (mod\ 8p)$ satisfies the said congruence and hence it can be considered as a solution.
But if $k = 4, then\ \ x \equiv 2p.4 \pm b \ (mod\ 8p)$
$\equiv 8p \pm b \ (mod\ 8p)$
$\equiv 0 \pm b \ (mod\ 8p)$.
It is the same solution as for $k = 0$.
Similarly, for $k = 5,6$ ... ... the solutions repeats as for $k = 1, 2$ ....
Hence all the solutions are given by $x \equiv 2pk \pm b \ (mod\ 8p); k = 0, 1, 2, 3.$
These are the eight solutions of the congruence under consideration for an odd positive integer b.

Case-II: Let a be an even perfect square.
Then the congruence becomes $x^2 \equiv a^2 \ (mod\ 8p)$.
For its solutions, consider: $x \equiv 4pk \pm a \ (mod\ 8p)$.
Then, $x^2 \equiv (\ 4pk \pm a)^2 \ (mod\ 8p)$
$\equiv (4pk)^2 \pm 2.4p^mk.a + a^2 \ \ (mod\ 8p)$
$\equiv 16p^2k^2 \pm 8pk.a + a^2 \ (mod\ 8p)$
$\equiv 8pk(\ 2pk \pm a) + a^2 \ (mod\ 8p)$
$\equiv 8pk(t) + a^2 \ (mod\ 8p)$
$\equiv 8pkt + a^2 (mod\ 8p)$
$\equiv a^2 \ (mod\ 8p)$

Therefore, $x \equiv 4pk \pm a \ (mod\ 8p)$ satisfies the said congruence and hence it can be considered as a solution.
But if $k = 2, then\ \ x \equiv 4p.2 \pm a \ (mod\ 8p)$
$\equiv 8p \pm a \ (mod\ 8p)$
$\equiv 0 \pm a \ (mod\ 8p)$.
It is the same solution as for $k = 0$.
Similarly, for $k = 3,4$ ... ... the solutions repeat as for $k = 1, 2$ ....
Hence all the solutions are given by $x \equiv 4pk \pm a \ (mod\ 8p); k = 0, 1.$
These are the four solutions of the congruence under consideration for an even positive integer a.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 25 \ (mod\ 4024)$.
It can be written as $x^2 \equiv 5^2 \ (mod\ 8.503)$
It is of the type $x^2 \equiv a^2 \ (mod\ 8p)$ with $p = 503$ & $a = 5, an\ odd\ positive\ integer$.
It has exactly eight solutions given by
$x \equiv 2pk \pm a \ (mod\ 8p);\ k = 0, 1, 2, 3.$
$\equiv 2.503k \pm 5 \ (mod\ 8.503)$
$\equiv 1006 \pm 5 \ (mod\ 4024)$
$\equiv 0 \pm 5; 1006 \pm 5; 2012 \pm 5; 3018 \pm 5 \ (mod\ 4024).$
$\equiv 5, 4019; 1001, 1011; 2007, 2017; 3013, 3023 \ (mod\ 4024)$
These are the required solutions.

N.B.: The above solutions of example-1 can also be obtained orally using the author's formulation. But if one uses the CRT method, it will take more than 10 hours).

Example-2: Consider the congruence $x^2 \equiv 16 \ (mod\ 4024)$.
It can be written as $x^2 \equiv 4^2 \ (mod\ 8.503)$
It is of the type $x^2 \equiv a^2 \ (mod\ 8p)$ with $p = 503$ & $a = 4, an\ even\ positive\ integer$.
It has exactly four solutions given by
$x \equiv 4pk \pm a \ (mod\ 8p);\ k = 0, 1.$
$\equiv 4.503k \pm 4 \ (mod\ 8.503)$
$\equiv 2012 \pm 4 \ (mod\ 4024)$
$\equiv 0 \pm 4; 2012 \pm 4 \ (mod\ 4024).$
$\equiv 4, 4020; 2008, 2016 \ (mod\ 4024)$
These are the required solutions.

CONCLUSION

Thus it can be concluded that the congruence: $x^2 \equiv a^2 \ (mod\ 8p)$, p an odd prime has exactly eight incongruent solutions $x \equiv 2pk \pm a \ (mod\ 8p);\ k = 0, 1, 2, 3$ if a is an odd positive integer.
But the congruence has exactly four incongruent solutions $x \equiv 4pk \pm a \ (mod\ 8p)$;

$k = 0, 1$, if a is an even positive integer.

REFERENCES

[1] Koshy Thomas, 2009, *Elementary Number Theory with Applications*, Academic Press, An Imprint of Elsevier, 2nd Edition, (Indian reprint-2009), ISBN: 978-81-312-1859-4.

[2] Zuckerman at el, 2008, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

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

[4] Roy B M, *Formulation of solutions of a class of 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 Sep-18.