International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-144: Formulation of Solutions of a Very Special Class of Standard Quadratic Congruence of Composite Modulus modulo a Multiple of Powered Even Prime by a Powered Odd Prime

Prof B M Roy

Head, Department of Mathematics, Jagat Arts,
Commerce & I H P Science College, Goregaon, Gondia, Maharashtra, India

ABSTRACT

In this paper, the author considered a very special type of standard quadratic congruence of composite modulus for its formulation of solutions. It is found that such a congruence has exactly 4p- solutions, p being an odd prime present in the modulus of the congruence. These solutions are formulated by the author. First time a formula is derived and hence the solutions can be obtained orally. The literature of mathematics remains silent in case of formulation of such congruence. Formulation is the merit of the paper.

KEYWORDS: *Chinese Remainder Theorem, Powered odd prime, Quadratic congruence*

How to cite this paper: Prof B M Roy "RP-144: Formulation of Solutions of a Very Special Class of Standard Quadratic Congruence of Composite Modulus modulo a Multiple of Powered Even Prime by a Powered Odd Prime" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1661-1663, URL: www.ijtsrd.com/papers/ijtsrd35718.pdf

IJTSRD35718

INTRODUCTION

The standard quadratic congruence of prime modulus is a congruence of the type:
$x^2 \equiv a\ (mod\ p)$, p being an odd prime. It has exactly two incongruent solutions [1].

But if the standard quadratic congruence is of composite modulus of the type:
$x^2 \equiv a\ (mod\ m), m$ being a composite integer, then it has more than two solutions [3].

The author already has formulated many standard quadratic congruence of composite modulus, even he found one more such type standard quadratic congruence of a special class of standard quadratic congruence of composite modulus to formulate.

PROBLEM-STATEMENT

The problem is "To formulate the solutions of the standard quadratic congruence of the type:
$x^2 \equiv p^2(mod\ 2^m.p^n); n \geq 2, m \geq 4$.

LITERATURE REVIEW

The literature of mathematics is full of standard quadratic congruence of prime modulus A slight discussion is found for standard quadratic congruence of composite modulus.

Most of the problems are solved using Chinese Remainder theorem [1], [2], [3]. But no direct formulation is there. The author has taken the responsibility to formulate these congruence of composite modulus. Previously he has formulated many such congruence [4], [5], [6].

ANALYSIS & RESULT

Consider the congruence$x^2 \equiv p^2(mod\ 2^m.p^n), n \geq 1, m \geq 4$.

Let us consider that $n = 1$.

In this case the congruence reduces to the form $x^2 \equiv p^2(mod\ 2^m.p)$.

For solutions, consider that $x \equiv 2^{m-1}pk \pm p\ (mod\ 2^mp)$.

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

Thus, $x \equiv 2^{m-1}pk \pm p \ (mod\ 2^m p)$ satisfies the congruence and hence it gives the solutions of the congruence.

But for $k = 2$, the solution formula reduces to $x \equiv 2^{m-1}p.2 \pm p \ (mod\ 2^m p)$

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

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

This is the same solutions as for $k = 0$.

Therefore, the required solutions are given by $x \equiv 2^{m-1}p.2 \pm p \ (mod\ 2^m p); k = 0, 1$.

These are the four solutions of the congruence.

Now let us consider that $n \geq 2$.
In this case the congruence reduces to the form $x^2 \equiv p^2 (mod\ 2^m.p^n)$.

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

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

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

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

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

Hence, $x \equiv 2^{m-1}p^{n-1}k \pm p \ (mod\ 2^m p^n)$ can be considered as solutions of the said congruence. But if $k = 2p$, then

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

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

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

These are the same solutions as for $k = 0$.
Therefore, the congruence must have $4p -$ solutions given by
$x \equiv 2^{m-1}p^{n-1}.k \pm p \ (mod\ 2^m p^n); k = 0, 1, 2, \ldots \ldots \ldots, (2p - 1)$.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 25 \ (mod\ 2000)$.
It can be written as $x^2 \equiv 5^2 (mod\ 2^4.5^3)$.

It is of the type: $x^2 \equiv p^2 (mod\ 2^m.p^n)\ with\ p = 5, m = 4, n = 3$.

It has exactly $4p = 4.5 = 20$ incongruent solutions given by
$x \equiv 2^{m-1}p^{n-1}k \ \pm p \ (mod\ 2^m p^n); k = 0, 1, 2, 3, \ldots \ldots \ldots .., (2p - 1)$.

$\equiv 2^3 5^2 k \pm 5 \ (mod\ 2^4.5^3); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots .., 9$.

$\equiv 200k \pm 5 \ (mod\ 2000)$

$\equiv 0 \pm 5; 200 \pm 5; 400 \pm 5; 600 \pm 5; 800 \pm 5; 1000 \pm 5; 1200 \pm 5; 1400 \pm 5;$

$1600 \pm 5; 1800 \pm 5 \ (mod\ 2000)$.

$\equiv 5, 1995; 195, 205; 395, 405; 595, 605; 795, 805; 995, 1005; 195, 1205; 1395, 1405; 1595, 1605; 1795, 1805 \ (mod\ 2000)$.

These are the twenty solutions.

Example-2: Consider the congruence $x^2 \equiv 49 \ (mod\ 1568)$.

It can be written as $x^2 \equiv 7^2 (mod\ 2^5.7^2)$.

It is of the type: $x^2 \equiv p^2 (mod\ 2^m.p^n)\ with\ p = 7, m = 5, n = 2$.

It has exactly $4p = 4.7 = 28$ incongruent solutions given by
$x \equiv 2^{m-1}p^{n-1}k \ \pm p \ (mod\ 2^m p^n); k = 0, 1, 2, 3, \ldots \ldots \ldots .., (2p - 1)$.

$\equiv 2^4.7k \pm 7 \ (mod\ 2^5.7^2); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots .., 13$.

$\equiv 112k \pm 7 \ (mod\ 1568)$

$\equiv 0 \pm 7; 112 \pm 7; 224 \pm 7; 336 \pm 7; 448 \pm 7; 560 \pm 7; 672 \pm 7; 784 \pm 7;\ 896 \pm 7; 1008 \pm 7; 1120 \pm 7; 1232 \pm 7; 1344 \pm 7; 1456 \pm 7 \ (mod\ 1568)$.

≡7, 1561; 105, 119; 217, 231; 329, 343; 441, 455; 553, 567; 665, 679; 767, 791; 889,906; 1001, 1015; 1113, 1127; 1225,1239; 1337,1351; 1449,1463 (mod 2000).

These are the twenty-eight solutions.

Example-3: consider the congruence $x^2 \equiv 121 \ (mod\ 352)$.

It can be written as: $x^2 \equiv 11^2 \ (mod\ 2^5.11)$.

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

It has exactly four solutions given by

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

$\equiv 2^4.11 \pm 11 \ (mod\ 2^5.11)$

$\equiv 176k \pm 11 \ (mod\ 352); k = 0, 1$.

$\equiv 0 \pm 11; 176 \pm 11 \ (mod\ 352)$.

$\equiv 11, 341; 165, 187 \ (mod\ 352)$.

These are the required four solutions.

CONCLUSION

Thus, the congruence $x^2 \equiv p^2 (mod\ 2^m.p)\ has\ exactly\ four\ incongruent$ solutions given by $x \equiv 2^{m-1}p.k \pm p \ (mod\ 2^m p), m \geq 4; k = 0, 1$.

But the congruence $x^2 \equiv p^2 (mod\ 2^m.p^n); m \geq 4, n \geq 2$ has exactly $4p -$ solutions given by $x \equiv 2^{m-1}p^{n-1}k \pm p \ (mod\ 2^m p^n)\ ; k = 0, 1, 2, \ldots \ldots \ldots .., (2p - 1)$.

MERIT OF THE PAPER

A direct formula for all the solutions is established. Sometimes the solutions can be obtained orally. Formulation is the merit of the paper. No need to use Chinese Remainder Theorem. Formulation is time-saving and Labour-saving.

REFERENCE

[1] Thomas Koshy, *Elementary Number Theory with Applications*, Second Edition, Academic Press (An Imprint of Elsevier), ISBN: 978-0-12-372487-8 (original), ISBN: 978-81-312-1859-4 (Indian Print), 2009.

[2] Ajay Kr Choudhury, *Introduction to Number Theory*, New Central Book Agency (P) Ltd, first edition, ISBN: 81-7381-586-0, Jan-2009.

[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] Roy B M, *Formulation of a very special type of standard quadratic congruence of composite modulus modulo a product of a powered odd prime integer and four*, International Journal of science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-07, July-20.

[5] 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, Aug-20.

[6] Roy B M, *Reformulation of solutions of standard quadratic congruence of even composite modulus - a product of powered even prime with a powered odd prime,* International Journal of science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-05, Issue-06, June-20.