International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 5, July-August 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-132: Formulation of Solutions of a Very Special Standard Quadratic Congruence of Prime-Power Modulus

Prof B M Roy

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

ABSTRACT

In this paper, the author considered a very special type of standard quadratic congruence of prime–power modulus for his study and after a rigorous study, the congruence is formulated for its solutions. Now the finding of solutions become very easy and the solutions can be obtained orally; no need to use pen & paper. Formulation is the merit of the paper. It is found that the congruence has $2p$ solutions for an odd prime p.

KEYWORDS: *Formulation, Prime-power Modulus, Standard Quadratic Congruence*

How to cite this paper: Prof B M Roy "RP-132: Formulation of Solutions of a Very Special Standard Quadratic Congruence of Prime-Power Modulus" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-5, August 2020, pp.528-529, URL: www.ijtsrd.com/papers/ijtsrd31877.pdf

IJTSRD31877

INTRODUCTION

The author already has formulated the solutions of the standard quadratic congruence of prime- power modulus of the type:$x^2 \equiv a \ (mod\ p^m)$, p being an odd prime and a any positive integer [3]. Such types of standard quadratic congruence of composite modulus has exactly two solutions [1]. Now the author considered the standard quadratic congruence of composite modulus the type: $x^2 \equiv p^2 \ (mod\ p^m)$, p an odd prime for its formulation of solutions.

PROBLEM-STATEMENT

Here the problem is
"To formulate the solutions of the standard quadratic congruence:
$x^2 \equiv p^2 \ (mod\ p^m)$; p an odd prime & m a positive integer".

LITERATURE-REVIEW

In the literature of mathematics *and* in the books of Number Theory, no formulation for solutions of the congruence under consideration is found, though some methods are mentioned [1]. These methods are complicated and time-consuming. It is not suitable for the readers. These are the demerits of the existed methods.

EXISTED METHODS

Method-I: Consider the congruence: $x^2 \equiv p^2 \ (mod\ p^m)$. It can be written as
$x^2 \equiv p^2 + k.p^m = a^2 (mod\ p^m)$, for some suitable values of k [2].

Here, lies the difficulty to find k.It is also time-consuming. This method is not always suitable here.

METHOD-II:

In this case the congruence can be solved iteratively.

At first, the congruence: $x^2 \equiv p^2 \ (mod\ p)$ is solved. Then using these solutions, the congruence: $x^2 \equiv p^2 \ (mod\ p^2)$ is solved. Then, $x^2 \equiv p^2 \ (mod\ p^3)$. Proceeding in this way, the solutions of the congruence: $x^2 \equiv p^2 \ (mod\ p^m)$ is obtained [1].

Definitely, it is boring and not suitable for the readers.

ANALYSIS & RESULTS (Formulation)

Consider the congruence: $x^2 \equiv p^2 \ (mod\ p^m)$; p odd prime, $m \geq 3$.

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

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

Thus, it is seen that $x \equiv p^{m-1}k \pm p \ (mod\ p^m)$ satisfies the said congruence and hence it can be considered as a solution of it.

But for $k = p$, this solutions reduces to
$x \equiv p^{m-1}.p \pm p \ (mod\ p^m)$
$\equiv p^m \pm p \ (mod\ p^m)$
$\equiv \pm p \ (mod\ p^m)$

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

Also, for the other higher values of k such as $k = p+1, p+2, \ldots \ldots$ the solutions repeat as for $k = 1, 2, \ldots ..$

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

Thus the congruence under consideration must have $2p - solutions$.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 25 \ (mod\ 625)$.
It can be written as: $x^2 \equiv 5^2 (mod\ 5^4)$.

It is of the type: $x^2 \equiv p^2 (mod\ p^m)$with $p = 5, an\ odd\ prime; m = 4$.

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

These solutions are given by
$x \equiv p^{m-1}.k \pm p \ (mod\ p^m); k = 0, 1, 2, \ldots.., (p-1)$.
$\equiv 5^{4-1}k \pm 5 \ (mod\ 5^4); k = 0, 1, 2, 3, 4$.
$\equiv 125k \pm 5 \ (mod\ 625); k = 0, 1, 2, 3, 4$.
$\equiv 0 \pm 5; 125 \pm 5; 250 \pm 5; 375 \pm 5; 500 \pm 5 \ (mod\ 625)$.
≡5, 620; 120, 130; 245, 255; 370, 380; 595, 505 (mod 625).

These are the required ten solutions.

Example-2: Consider the congruence $x^2 \equiv 49 \ (mod\ 343)$.
It can be written as: $x^2 \equiv 7^2 (mod\ 7^3)$.

It is of the type: $x^2 \equiv p^2 (mod\ p^m)$with $p = 7, an\ odd\ prime; m = 3$.

It has exactly $2p = 2.7 = 14$ solutions.

These solutions are given by
$x \equiv p^{m-1}.k \pm p \ (mod\ p^m); k = 0, 1, 2, \ldots.., (p-1)$.
$\equiv 7^{3-1}k \pm 7 \ (mod\ 7^3); k = 0, 1, 2, 3, 4, 5, 6$.
$\equiv 49k \pm 7 \ (mod\ 343); k = 0, 1, 2, 3, 4, 5, 6$.
$\equiv 0 \pm 7; 49 \pm 7; 98 \pm 7; 147 \pm 7; 196 \pm 7; 245 \pm 7; 294 \pm 7 \ (mod\ 343)$.
≡7, 336; 42, 56; 91, 105; 140, 154; 189,203; 238, 252; 287, 301 (mod 343).

These are the required fourteen solutions.

Example-3: Consider the congruence $x^2 \equiv 121 \ (mod\ 1331)$.
It can be written as: $x^2 \equiv 11^2 (mod\ 11^3)$.

It is of the type: $x^2 \equiv p^2 (mod\ p^m)$with $p = 11, an\ odd\ prime; m = 3$.

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

These solutions are given by
$x \equiv p^{m-1}.k \pm p \ (mod\ p^m); k = 0, 1, 2, \ldots.., (p-1)$.
$\equiv 11^{3-1}k \pm 11 \ (mod\ 11^3); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$.
$\equiv 121k \pm 11 \ (mod\ 1331); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$.
$\equiv 0 \pm 11; 121 \pm 11; 241 \pm 11; 363 \pm 11; 484 \pm 11; 605 \pm 11; 726 \pm 11; 847 \pm 11; 968 \pm 11; 1089 \pm 11; 1210 \pm 11 \ (mod\ 1331)$.
≡11, 1320; 110, 132; 230, 252; 352, 374; 473, 495; 594, 616; 715, 737; 836, 858; 957, 979; 1078, 1100; 1199, 1221 (mod 1331).

These are the required twenty two solutions.

CONCLUSION

Therefore, it can be concluded that the congruence under consideration:
$x^2 \equiv p^2 \ (mod\ p^m)$has exactly $2p$ solutions given by
$x \equiv p^{m-1}.k \pm p \ (mod\ p^m); k = 0, 1, 2, \ldots.., (p-1)$.

MERIT OF THE PAPER

The congruence is formulated for its solutions. The solutions can be obtained orally. Thus, formulation of the solutions of the congruence is the merit of the paper.

REFERENCE

[1] Koshy Thomas, *Elementary Number Theory with Applications*, Academic Press (An Imprint of Elsevier), Second edition, ISBN: 978-81-312-1859-4, 2007

[2] Roy B M, *Discrete Mathematics & Number Theory*, Das GanuPrakashan, (Nagpur, India), First edition, ISBN: 978-93-84336-12-7, Jan. 2016.

[3] Roy B M, *A New method of finding solutions of a solvable standard quadratic congruence of comparatively large prime modulus*, International Journal of Advanced Research, Ideas, and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue03, May-Jun-18.

[4] 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, Issue06, Nov-Dec--18.