INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 6)
Available online at: www.ijariit.com

An algorithmic formulation of solutions of solvable standard quadratic congruence of prime- power modulus

B M Roy
roybm62@gmail.com
Jagat Arts Commerce Indraben Hariharbhai Patel Science College,
Goregaon, Maharashtra

ABSTRACT

In this paper, a new generalised method of solving the standard quadratic congruence of prime-power modulus is discovered. An algorithmic formula is developed. It works efficiently. It is the generalisation of author's proposed Middle-pair solution method of solving standard quadratic congruence of prime modulus. It is very simple and time-saving.

Keywords— *Algorithmic formulation, Legendre's symbol, Middle-pair solution, Prime- power modulus*

1. INTRODUCTION

The author discovered three different efficient methods of solving standard quadratic congruence of the prime modulus of the type $x^2 \equiv a\ (mod\ p); (a,p) = 1;\quad p\ being\ an\ odd\ prime\ positive\ integer,$ and is published in different reputed international journals. Here is author's one more method (an **algorithmic formulation**) to discuss for the solutions of standard quadratic congruence of **prime-power modulus** of the type: $\boldsymbol{x^2 \equiv a\ (mod\ p^n)}$.

It has exactly two incongruent solutions [4].

2. LITERATURE-REVIEW

The author referred many books on Number Theory and found a method to solve the said congruence. In the existed method, the readers have to add the modulus repeatedly to a to make it a perfect square [2]. Sometimes it takes a long time. It will take hours or days. It is not fair method for readers.

Thomas Koshy has posed two questions as:

(1) When is the congruence $x^2 \equiv a\ (mod\ p^n)$ solvsble?
(2) When it is solvable, how do we find the solutions? [3]

But he did not mention any direct method or formula to find the solutions. His suggested method is very long and tedious. Koshy has mentioned the said problem in an exercise of his book as a computer problem [3].

3. NEED OF RESEARCH

- Such a time-consuming method is in existence. It is not a suitable method for the readers.
- They are in need of a simple and time-saving method or formula so that they can find the solutions easily. Thus, a simple and easy method of solving the said congruence is in need.
- To have a time-saving method of solutions, the author tried his best and presented his great effort in this paper.

4. PROBLEM-STATEMENT

The problem of the paper is:

"To discover an efficient algorithmic formulation of solutions of the standard quadratic congruence: $x^2 \equiv a\ (mod\ p^n)$, $where\ p\ is\ a\ prime, n\ is\ positive\ integer$".

5. ANALYSIS AND RESULT

The said congruence $x^2 \equiv a\ (mod\ p^n),\ n\ any\ positive\ integer\ \&\ (a,p) = 1$, is solvable if and only if $\left(\frac{a}{p}\right) = 1$ [1]. If the congruence is solvable, then for the solutions,

Perform the following steps:

(1) Test for the solvability of the problem.
(2) Find $c = \frac{p^n-1}{2}\ \&\ d = \frac{p^n+1}{2}$. (c,d) is called middle-pair solutions.
(3) Find the corresponding standard quadratic congruence : $x^2 \equiv b\ (mod\ p^n)$.
(4) Find r from the equation: $r(r+1) = a - b + p^n k,\ for\ k = 0, 1, 2, \ldots \ldots$
(5) Then the required solutions are $x \equiv c - r, d + r\ (mod\ p^n)$.

The formulation is obtained by the author scientifically and mathematically. Mathematical calculation is not shown here. The method is already published in IJARIIT.

6. ILLUSTRATION

Consider the congruence $x^2 \equiv 363(mod\ 11^3)\ with\ a = 363, p^n = 11^3$.
It can be written as $x^2 \equiv 363\ (mod\ 1331)$. Here $11^3 = 1331$.
So, $c = \frac{p^n-1}{2} = \frac{1331-1}{2} = 665;\quad d = \frac{p^n+1}{2} = 666$.
Therefore, the middle pair solution is $(c,d) = (665, 666)$.

The corresponding quadratic congruence is then $x^2 \equiv 333\ (mod\ 1331)\ giving\ b = 333$.

To find r, let us consider the equation: $r(r+1) = p^n k + a - b$
$= 1331k + 363 - 333$
$= 1331k + 30$
$= 0 + 30\ for\ k = 0$
$= 30 = 5.6\ giving\ r = 5$.
Then the required solutions pair is $x \equiv c - r, d + r\ (mod\ p^n)$
$\equiv 665 - 5, 666 + 5\ (mod\ 1331)$
$\equiv 660, 671\ (mod\ 1331)$.

How easily the solutions are obtained!
But by the existed method, one can solve as under:

Consider the same congruence $x^2 \equiv 363\ (mod\ 11^3)$.
It can be written as $x^2 \equiv 363\ (mod\ 1331)$.
$\equiv 363 + 1.1331 = 1694\ (mod\ 1331)$
$\equiv 363 + 2.1331 = 3025\ (mod\ 1331)$
.....
.....
$\equiv 363 + 327.169 = 435600\ (mod\ 1331)$
$\equiv 660^2\ (mod\ 1331)$.

Thus required solutions are $x \equiv \pm 660 = 660, 671\ (mod\ 1331)$.

Thus we can see that the existed method takes **at least 12 hours** because the reader has to add 1331, 327 times and has to check every time if the new sum is a perfect square or not(which is not so easy) while the proposed method takes **at most five minutes**.

Consider congruence $x^2 \equiv 882\ (mod\ 7^4)$.
It can be written as $x^2 \equiv 882\ (mod\ 2401)$. Here $a = 882,\ p^n = 7^4 = 2401$.
So, $c = \frac{p^n-1}{2} = \frac{2401-1}{2} = 1200;\quad d = \frac{p^n+1}{2} = 1201$.

Therefore, the middle pair solution is $(c,d) = (1200, 1201)$.

The corresponding quadratic congruence is then $x^2 \equiv 1801\ (mod\ 2401)$
$giving\ b = 1801$.

To find r, let us consider the equation: $r(r+1) = p^n k + a - b$
$= 2401k + 882 - 1801$
$= 2401k - 919$
$= 2401 - 919\ for\ k = 1$
$= 1482 = 38.39\ giving\ r = 38$.

Then the required solutions pair is $x \equiv c - r, d + r \ (mod\ p^n)$
$\equiv 1200 - 38, \quad 1201 + 38 \ (mod\ 2401)$
$\equiv 1162, 1239 (mod\ 2401).$

Using existed method one can solve the congruence as under:
Consider the same congruence $x^2 \equiv 882 \ (mod\ 7^4)$.
It can be written as $x^2 \equiv 882 \ (mod\ 2401)$.
$\equiv 882 + 1.2401 = 3283 \ (mod\ 2401)$
$\equiv 882 + 2.2401 = 5684 \ (mod\ 2401)$
.....
.....
$\equiv 882 + 562.2401 = 1350244 \ (mod\ 343)$
$\equiv 1162^2 \ (mod\ 2401).$

Thus the required solutions are $x \equiv \pm 1162 = 1162, 1239 \ (mod\ 2401)$.
Thus we can see that the existed method takes **at least ten hours** while the proposed method takes **at most ten minutes**.

Let us consider one more problem: $x^2 \equiv 196 \ (mod\ 7^3)$.
It can be written as $x^2 \equiv 196 \ (mod\ 343)$. Here $a = 196, \ p^n = 7^3 = 343$.
So, $c = \frac{p^n - 1}{2} = \frac{343 - 1}{2} = 171; \quad d = \frac{p^n + 1}{2} = 172.$

Therefore, the middle pair solution is $(c, d) = (171, 172)$.

The corresponding quadratic congruence is then $x^2 \equiv 86 \ (mod\ 343)$
$giving\ b = 86.$

To find r, let us consider the equation: $r(r + 1) = p^n k + a - b$
$= 343k + 196 - 86$
$= 2401k + 110$
$= 0 + 110\ for\ k = 0$
$= 110 = 10.11\ giving\ \ r = 10.$

Then the required solutions pair is $x \equiv c - r, d + r \ (mod\ p^n)$
$\equiv 171 - 10, 172 + 10 \ (mod\ 343)$
$\equiv 161, 182 (mod\ 343).$

Some other congruences for practice are:

(1) $x^2 \equiv 124 \ (mod\ 17^2)\ i.e. x^2 \equiv 124 \ (mod\ 289)$ ……??.
(2) $x^2 \equiv 163 \ (mod\ 7^3)\ i.e. x^2 \equiv 163 \ (mod\ 343)$
(3) $x^2 \equiv 1901 \ (mod\ 13^3)\ i.e. x^2 \equiv 1901 \ (mod\ 2197)$
(4) $x^2 \equiv 124 \ (mod\ 5^3)\ i.e. x^2 \equiv 124 \ (mod\ 125)$
(5) $x^2 \equiv 23 \ (mod\ 7^3)\ i.e. x^2 \equiv 23 \ (mod\ 343)$
(6) $x^2 \equiv 23 \ (mod\ 7^4)$.

7. CONCLUSION

Therefore, it can be concluded that the author's proposed algorithmic method of solving standard quadratic congruence of the prime modulus of the type $x^2 \equiv a \ (mod\ p)$ is generalised to solve the standard quadratic congruence of prime-power modulus of the type $x^2 \equiv a \ (mod\ p^n)$, p being an odd prime integer. The method works efficiently when the required solutions are near to middle-pair solution.

8. MERIT OF THE PAPER

The proposed algorithmic method works efficiently. It solves the congruence in the least time. Thus, the author's method is proved time-saving. This is the merit of the paper.

9. REFERENCES

[1] Burton D M, "*Elementary Number Theory*", 2/e, 2003, Universal Book Stall.
[2] Roy B M, "*Discrete Mathematics & Number Theory"*, 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.
[3] Thomas Koshy, "*Elementary Number Theory with Applications",* 2/e (Indian print, 2009), Academic Press.
[4] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd.

