IJARIIT 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

A new method of finding solutions of a class of standard quadratic congruence of prime modulus

B M Roy
roybm62@gmail.com
Jagat Arts, Commerce and Indiraben Hariharbhai Patel Science College,
Gondia, Maharashtra

ABSTRACT

In this paper, a new method of finding solutions of a class of standard quadratic congruence of comparatively large prime modulus is discussed. An algorithmic formulation is discovered. It works efficiently. It is time-saving & simple while the existed method is time-consuming & boring.

Keywords— *Quadratic congruence, Prime modulus, Middle-pair solutions*

1. INTRODUCTION

In this paper, the author wishes to discuss his new method of finding solutions to a class of standard quadratic congruence of prime modulus mathematically and analytically. The congruence of the said type is:

$$x^2 \equiv a \ (mod\ p).$$

Where, p is a comparatively large prime.

A solution of the congruence under consideration is the value of unknown x that satisfies the congruence. To find the solution literally means to find a perfect square which when divided by p, gives the remainder ‘a’.

Every reader knows that $(\pm a)^2 = a^2$ and hence we can say that a solvable quadratic congruence has at least two incongruent solutions. If the modulus p is a prime positive integer, then the quadratic congruence has exactly two incongruent solutions [2].

2. LITERATURE REVIEW

The author referred many books on Number Theory. Most of the books discussed quadratic congruence and its properties but discussed no method of finding solutions of the said congruence. But there is an existed method of solving such type of congruence in the literature of mathematics. The author does not know who the discoverer is. He knows this method from his student life. Even he could not remember the name of the book where he read it. It is also discussed in the author’s book [2].

The existed method has limited use. It cannot be used to solve the said congruence. It takes a long time (probably hours/days). $x^2 \equiv 756\ (mod\ 997)$. It cannot be solved in a day. Here is the demerit of the existed method.

3. NEED OF THIS RESEARCH

The author also found that no formula was yet discovered for the solutions of such congruence. He has a list of congruence which takes a long time to solve:

1] $x^2 \equiv 54 \ \ (mod\ 503)$
2] $x^2 \equiv 75 \ \ (mod\ 97)$
3] $x^2 \equiv 83 \ \ (mod\ 503)$
4] $x^2 \equiv 73 \ \ (mod\ 173)$
5] $x^2 \equiv 73 \ \ (mod\ 97)$
6] $x^2 \equiv 85 \ \ (mod\ 503)$ … … … ….

The remedy is the formulation. He tried his best to formulate the solutions and his efforts are presented here. To find a remedy is the need for his research.

4. PROBLEM STATEMENT

The congruence under consideration

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

is to formulate algorithmically in a shorter time.

5. PROPOSED METHOD

To solve$x^2 \equiv a\ \ (mod\ p\ )$,

(A) Construct a quadratic congruence $x^2 \equiv b\ (mod\ p\ )$ having two solutions:

$$c = \frac{p-1}{2}\ and\ d = \frac{p+1}{2}.$$

The solution pair (c, d) may be called middle-pair-solutions.

Let us try to understand the middle- pair solutions as below:

Consider a prime integer $p = 17$. Then there will be eight ($\frac{p-1}{2}$) congruence each having exactly two solutions i.e. in total eight pairs of solutions such as:

(1, 16); (2, 15); (3, 14); (4, 13); (5, 12); (6, 11); (7, 10); **(8, 9) = (c, d).**

(8, 9) is the middle pair of solutions.

We can arrange all these solutions in ascending order as below:

1, 2, 3, 4, 5, 6, 7, ***8*, *9*,** 10, 11, 12, 13, 14, 15, 16.

(B) As $c = \frac{p-1}{2}$ and is a solution of $x^2 \equiv b$ (mod p, hence $c^2 \equiv b\ (mod\ p)$.

Now,
$$\begin{aligned}(c-1)^2 &= c^2 - 2c + 1\\ &= b - 2\left(\frac{p-1}{2}\right) + 1\\ &= b - p + 2\\ &\equiv b + 2\ (mod\ p).\end{aligned}$$

Thus, $x = c - 1$ is a solution of $x^2 \equiv b + 2\ (mod\ p)$.

Also,
$$\begin{aligned}(c-2)^2 &= c^2 - 4c + 4\\ &= b - 4\left(\frac{p-1}{2}\right) + 4\\ &= b - 2p + 6\\ &\equiv b + 6\ (mod\ p).\end{aligned}$$

Thus, $x = c - 2$ is a solution of $x^2 \equiv b + 2 + 4\ (mod\ p)$.

Proceeding in this way, we get $x = c - r$ is a solution of the congruence

$$\boldsymbol{x^2 \equiv b + 2 + 4 + 6 + \cdots \ldots \ldots + 2r\ \ (mod\ p)}$$

(C) Then the required solutions are: $x \equiv c - r, d + r\ (mod\ p)$.

6. ILLUSTRATION

To elaborate the method, we solve an example using the above-proposed method.

Consider $x^2 \equiv 85\ (mod\ 503\ )$.

Here, $a = 85,\ \ p = 503, which\ is\ a\ prime\ integer.$

Let, $c = \frac{p-1}{2} = \frac{503-1}{2} = 251\ and\ d = \frac{p+1}{2} = \frac{503+1}{2} = 252.$

Then the congruence with solutions: $x \equiv 251, 252\ \ (mod\ 503)\ is\ \ x^2 \equiv 126\ (mod\ 503)$.

Now, adding a first even number to 126, we get $126 + 2 = 128$.

Then, adding next higher even integer 4 to the previous sum$i.e.\ 128 + 4 = 132$.

Proceeding, in this way: 126+2=128;$128 + 4 = 132;\ 132 + 6 = 138;\ \ 138 + 8 = 146;$

$146 + 10 = 156;\ 156 + 12 = 168;\ \ 168 + 14 = 182;\ \ 182 + 16 = 198;$

$198 + 18 = 216;\ 216 + 20 = 236;\ \ 236 + 22 = 258;\ 258 + 24 = 282;$

$282 + 26 = 308; 308 + 28 = 336;\ \ 336 + 30 = 366;\ \ 366 + 32 = 398;$

$398 + 34 = 432;\ \ \ 432 + 36 = 468;\ \ 468 + 38 = 506 \equiv 3\ (mod\ 503);$

$3 + 40 = 43;\ \ \ 43 + 42 = 85\ (mod\ 503).$

Here, r =21.

Thus, the required solutions are $x \equiv c - 21,\ \ d + 21\ \ (mod\ p)$

$i.e.\ \ x \equiv 251 - 21, 252 + 21\ \ (mod\ 503)$

$i.e.\ \ x \equiv 230,\ \ 273\ \ (mod\ 503).$

Consider one more example: $x^2 \equiv 93\ (mod\ 97)$.

In this case $c = \frac{p-1}{2} = \frac{97-1}{2} = \frac{96}{2} = 48\ \ \&\ d = \frac{p+1}{2} = \frac{97+1}{2} = \frac{98}{2} = 49.$

The middle pair solution is $(48, 49)$.

The corresponding congruence is then $x^2 \equiv 73(mod\ 97)$.

Then, $73 + 2 = 75;\ 75 + 4 = 79;\ 79 + 6 = 85;\ 85 + 8 = 93.$
Thus the solutions are: $c - 2,\ d + 2\ \ i.e.\ 48 - 4, 49 + 4\ \ i.e. 44, 53$.
Thus the required solutions are: $x \equiv 44, 53\ (mod\ 97).$
It takes at most 2 minutes.

But by the existed method:

$$\begin{aligned} x^2 &\equiv 93\ (mod\ 97) \\ &\equiv 93 + 19.97\ (mod\ 97) \\ &\equiv 1936\ (mod\ 97) \\ &\equiv 44^2\ (mod\ 97) \end{aligned}$$

Therefore, the required solutions are $x \equiv 97 \pm 44 = 44, 53\ (mod\ 97).$

To add 97, 19-times to 93 and to check every time if the sum is a perfect square or not, takes at least 30 minutes but the proposed method takes at most 2 minutes.

Consider $x^2 \equiv 17\ (mod\ 101).$
Using existed method, it can be written as

$$\begin{aligned} x^2 &\equiv 17\ (mod\ 101) \\ &\equiv 17 + 19.101\ (mod\ 101) \\ &\equiv 1936\ (mod\ 101) \\ &\equiv 44^2\ (mod\ 101) \end{aligned}$$

Thus the required solutions are given by $x \equiv \pm 44 = 44, 57\ (mod\ 101).$

We see that the existed method takes at least 30 minutes but the proposed method takes at most 2 minutes.

7. MERITS OF PROPOSED METHOD

- It takes less time to get the required Solutions.
- One need not test for perfect square at every step.
- The calculation is simple and smooth.
- Numbers never become larger than the modulus.
- This method is more suitable when the solutions are very near to **middle-pair solution** and when k in the existed method is large.

8. CONCLUSION

Here a new method of solving a solvable quadratic congruence is discussed. It is found that the proposed method is very simple, quick and easy. Thus, a quick and simple procedure is developed to find the solutions of the standard quadratic congruence:

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

Where, p is a very large positive prime integer.

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.