A Comparative Study of Existed Method & Proposed Method of Solving Standard Quadratic Congruence of Prime Modulus

Prof. B M ROY

Head, Department of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon (GONDIA)
Pin- 441801
Affiliated to R T M Nagpur University, Nagpur

***ABSTRACT*: In this paper, two methods of solving standard quadratic congruence of prime modulus is described; one is existed method found in literature and the other is the proposed new method by the author. Existed method sometimes becomes impractical but proposed method is found very short, practical.**

***Keywords*: middle-pair solutions, perfect-square, quadratic congruence.**

INTRODUCTION

Congruence is nothing more than a statement about divisibility and expressed in a convenient notation. It is a concept of Number Theory. Many earlier mathematician studied quadratic congruence and proposed many methods to solve a standard quadratic congruence of prime modulus. Here, one such method is described. It is found that the said method is very long and complicated. It takes a long time to find the solutions. Such a problem cannot be solved in the examination for time-shake. The method is not fair for students. This struck my heart deeply and I am pained so much to find a new fair method. I tried my best and what I found was **published in the International Journal IJISRT (INDIA), Volume-3, Issue-5, May-2018.**

For the awareness of the method, I am comparing the two methods of solving the congruence.

PROBLEM STATEMENT

Consider a standard quadratic congruence of prime modulus $x^2 \equiv a \ (mod\ p)$ ……..(1)

Such congruence always has two incongruent solutions [2].

Let us consider that p is a comparatively large prime integer.

Here the problem is "To find all the solutions of (1) using existed method and a new method proposed by the author".

SOLUTION BY EXISTED METHOD

To find solutions of (1), we find a perfect-square b^2 which is congruent to a modulo p.

If $a = b^2$, then the congruence becomes $x^2 \equiv b^2 \ (mod\ p)$ and it has two solutions given by $x \equiv \pm b \ (mod\ p)$.

If a is not a perfect square, then we add p to a to get the congruence $x^2 \equiv a + p \ (mod\ p)$. If $a + p$ is a perfect square, $a + p = b^2$, then the solutions are as in above. If $a + p$ is not a perfect square, then we again add p to $a + p$ to get $a + 2p$. If it is a perfect square, then we are done; otherwise, we continue to add p to get a perfect square [1]. Thus at last the congruence becomes $x^2 \equiv a + k.p \ (mod\ p)$

$$\equiv b^2 \ (mod\ p) \quad if\ a + k.p = b^2\ for\ a\ fixed\ positive\ integer\ k.$$

Then the solutions are as in above.

ILLUSTRATION

To illustrate the existed method, Let us consider an example $x^2 \equiv 43 \ (mod\ 503)$.

43 is not a perfect-square, so we add 503 to 43 to get $x^2 \equiv 43 + 503 = 546 \ (mod\ 503)$.

WE see that 546 is not a perfect square, so we again add 503 to 546 to get $x^2 \equiv 546 + 503 = 1049 \ (Mod\ 503)$. 1049 is not a perfect square. Proceeding in this way we get

$x^2 \equiv 43$ (Mod 503)

$x^2 \equiv 43 + 503.1 = 546$ (Mod 503)

$x^2 \equiv 43 + 503.2 = 1049$ (Mod 503)

$x^2 \equiv 43 + 503.3 = 1552$ (Mod 503)

…….

……

$x^2 \equiv 43 + 503.106 = 53361 = 231^2$ (Mod 503)

Hence the solutions are $x \equiv \pm 231\ (mod\ 503)\ i.e. x \equiv 231, 503 - 231\ (mod\ 503)$

$$i.e.\ \boldsymbol{x \equiv 231, 272\ (mod\ 503)}.$$

In this problem, 503 is added 106-times to get a perfect square!!! Isn't it tedious and time-consuming?

Such types of many more congruence are: 1. $x^2 \equiv 73\ (mod\ 97)$

2. $x^2 \equiv 83\ (mod\ 503)$
3. $x^2 \equiv 83\ (mod\ 503)$
4. $x^2 \equiv 54\ (mod\ 503)$ and many more.

DRABACKS OF EXISTED METHOD

The existed method has a serious drawback and hence it is not a fair method for reader/ students. It sometimes becomes impractical. Also, one has to check at every step whether the number obtained is a perfect square or not. Here lies the difficulty.

PROPOSED METHOD

To solve the said congruence $x^2 \equiv a\ (mod\ p)$, we construct another standard quadratic congruence$x^2 \equiv b\ (mod\ p)$ having two solutions $c = \frac{p-1}{2}\ and\ d = \frac{p+1}{2}$. We call these two solutions as **middle-pair-solutions [3].**

[It is known to all Mathematicians fond of Number Theory, that for a prime P, the numbers

$$1, 2, 3, 4, \ldots . c = \frac{\boldsymbol{p-1}}{\boldsymbol{2}}, \boldsymbol{d} = \frac{\boldsymbol{p+1}}{\boldsymbol{2}}, \ldots \ldots \ldots (p-2), (p-1)$$

are the integers less than p and all are solutions of some quadratic congruence of prime modulus p. we see that c, d are the middle-pair of these solutions.]

Let the required solutions be $x \equiv c - n\ (mod\ p) and\ x \equiv d + n (mod\ p)$ … … … … … … … (2).

Only we have to find n.

For this, we consider the formula [3]: $b + n(n+1) = a + k.p$ ……..(3)

$$i.e.\quad n(n+1) = a - b + k.p\ \ with\ k = 0, 1, 2, \ldots \ldots \ldots$$

We solve this equation (3) for n. Then from (2), required solutions can be obtained.

[**Formula was published in IJISRT**].

ILLUSTRATION

Consider the same congruence as in above: $x^2 \equiv 43\ (mod\ 503)\ with\ a = 43, P = 503$

Let us find c, d as $c = \frac{p-1}{2} = \frac{503-1}{2} = 251\ \ \&\ d = \frac{p+1}{2} = 252.$

Then the congruence with solutions $x \equiv 251, 253\ (mod\ 503)$ must be$x^2 \equiv 126\ (mod\ 503)$.

Hence $b = 126$.

Putting the values in (3) we get $126 + n(n+1) = 43 + k.503$

$$i.e.\ \ n(n+1) = 503k - 83.$$

For k=1, we have $n(n+1) = 503 - 83 = 420 = 20.21\ \ giving\ n = 20.$

Then the solutions are $x \equiv 251 - 20 = 231(Mod\ 503) \& x \equiv 252 + 20 = 272(mod\ 503)$.

These are the same solutions obtained as before.

MERIT OF THE METHOD

Following are the merits of the paper:

1) One need not test every time for a perfect square.
2) Method is simple and smooth.
3) Calculation takes less time.
4) A fair method for all.
5) Overall time for solutions is very affordable.

CONCLUSION

In this paper, two methods are described in detail and found that existed method is time-consuming, complicated and very long while the proposed method by the author is very simple, easy and non-time-consuming. A better method is proposed which resolved the difficulty in solving the congruence.

REFERENCE

1] Roy B M, *Discrete Mathematics & number Theory*, first edition, Jan. 2016, Das Ganu prakashan, Nagpur.
2] Zuckerman & at el, *An Introduction to the Theory of Numbers*, fifth edition, 2008, Wiley India, (pvt) Ltd.
3] *Roy B M, IJISRT (INDIA)*, Volume-3, Issue-5, May-2018.