RP-176: One More New Method of Solving Standard Quadratic Congruence of Comparatively Large Prime Modulus

Prof B M Roy

Head, Department of Mathematics

Jagat Arts, Commerce & I H P Science College, Goregaon

Dist- Gondia, M. S., India, Pin: 441801.

ABSTRACT

In this current paper, the author has proposed a new method of solving standard quadratic congruence of prime modulus. It may be called as "addition of successive even integer method".

There exist some quadratic congruence of prime modulus which cannot be solved easily using the existed method. Existed method is time consuming and complicated. But the author's proposed method is unbelievably easy and simple. The method is illustrated here to find solutions of such congruence.

KEY-WORDS

Existed method; proposed method; Prime modulus; Quadratic congruence.

INTRODUCTION

The readers of Number Theory know what a quadratic congruence is. The solvability condition of the congruence is also known to them. But for the other readers, a slight details are mentioned here.

General Quadratic congruence: A congruence of the type: $ax^2 + bx + c \equiv 0 \ (mod\ p)$

Is called a general quadratic congruence of prime modulus, if p is an odd prime and

$a \not\equiv 0 \ (mod\ p). e.g.\ \ 3x^2 - 4x + 7 \equiv 0 \ (mod\ 11)$ is a general quadratic congruence of prime modulus, as 11 is an odd prime.

Standard Quadratic Congruence: A general quadratic congruence can be transformed into the form $x^2 \equiv d \ (mod\ p) and$ is called standard quadratic congruence of prime modulus. $e.g.\ \ x^2 \equiv 5 \ (mod\ 11)$ is a standard quadratic congruence of prime modulus.

Quadratic Residues: The positive integers 0, 1, 2, 3, 4, 5, ………., p-1 are called residues of p $i.e.$ these are the possible remainders when any integer is divided by p. If r is any such residue of p and $r^2 \equiv a \ (mod\ p)$, then a is called the quadratic residue of p.

Solvability Condition: Any standard quadratic congruence $x^2 \equiv a \ (mod\ p)$ is called solvable, if a is a quadratic residue of p. If the congruence is solvable, then it can always be written as $x^2 \equiv r^2 \ (mod\ p)$.

Middle-pair solutions: The non-zero residues of p can be written as:

$$1, 2, 3, \dots\dots\dots.., \boldsymbol{\frac{p-1}{2}}, \boldsymbol{\frac{p+1}{2}}, \dots\dots\dots..(p-2), (p-1).$$

They can also be paired as: $(1, p-1); (2, p-2); (3, p-3); \dots\dots\dots\dots\dots..; \left(\frac{p-1}{2}, \frac{p+1}{2)}\right)$.

Every pair is a solution of a solvable standard quadratic congruence of prime modulus p.

Thus, the last pair is a solution of the quadratic congruence of prime modulus p. It is called middle-pair solutions of the congruence as it appear in the middle position of the residues in order.

PROBLEM STATEMENT

Here the problem is "To solve the standard quadratic congruence of prime modulus of the type: $x^2 \equiv a\ (mod\ p)$, p being an odd prime by the proposed method.

LITERATUR REVIEW

The standard quadratic congruence of prime modulus is studied in the universities. Every book of Number Theory discussed the said congruence in detail [1], [2], [3]. A procedure of solving the congruence known as existed method, is discussed. To illustrate the procedure consider a standard quadratic congruence of prime modulus: $x^2 \equiv a\ (mod\ p)$.

If a is a quadratic residue of p, then it can be written as $a + kp = r^2$ for a specific k and the

Congruence can be written as: $x^2 \equiv r^2\ (mod\ p)$. Then it has exactly two incongruent solutions $x \equiv \pm r\ (mod\ p)$

$$\equiv r, p - r\ (mod\ p).$$

Here, the finding of solutions become tedious when k is comparatively large.

In this case the existed method is explained numerically as under.

Consider the congruence $x^2 \equiv 132\ (mod\ 503)$.

To replace 132 by a perfect square $r^2, add\ 503\ to\ 132\ to\ get\ 132 + 503 = 535$. 535 is not a perfect square, so again adding 503 to 535 to get 535+503=1038. It is also not a perfect square. So proceeding in this way, one must get

$x^2 \equiv 132\ (mod\ 503)$

$\equiv 132 + 503 = 535\ (mod\ 503)$

$\equiv 132 + 2.503 = 1038\ (mod\ 503)$

$\equiv 132 + 3.503 = 1641\ (mod\ 503)$

$\equiv 132 + 4.503 = 2144\ (mod\ 503)$

………………………………………………………

……………………………………………………

…………………………………………………

$\equiv$132+ (123).503 = 62001 = $(249)^2$(mod 503) **[Here k =123**]

So, the congruence can be written as $x^2 \equiv 249^2\ (mod\ 503)$

Therefore the solutions are $x \equiv 249, 503 - 249\ (mod\ 503)$

$$\equiv 249, 254\ (mod\ 503).$$

Here lies the difficulty! Addition of 503, 123 times and to check if the number formed is a perfect square or not is tedious and boring. It will take at least 5 hours!!

Many more such type of time-consuming congruence are:

1) $x^2 \equiv 128\ (mod\ 503)$
2) $x^2 \equiv 113\ (mod\ 443)$
3) $x^2 \equiv 328\ (mod\ 397)$

4) $x^2 \equiv 322\ (mod\ 413)$
5) $x^2 \equiv 156\ (mod\ 503)$
1) $x^2 \equiv 79\ (mod\ 307)$
2) $x^2 \equiv 229\ (mod\ 289)$
3) $x^2 \equiv 258\ (mod\ 317)$
4) $x^2 \equiv 334\ (mod\ 413)$
5) $x^2 \equiv 126\ (mod\ 503)$

Demerit of the procedure

1) The existed method becomes impractical when k is comparatively large.
2) Every time to check if the new number formed after adding 503 is perfect square.
3) It is time-consuming and tedious method.

THE AUTHOR'S PREVIOUS CONTRIBUTIONS

The author already has discovered a time-saving method of finding solutions of standard quadratic congruence of prime modulus which are time-consuming by existed method [4].

PROPOSED METHOD

So, the author discovered a shorter method of solving such a standard quadratic congruence. In this method, the procedure starts from the congruence having middle pair solutions. Let such congruence be: $x^2 \equiv b\ (mod\ p)$.

The method can be summarised as under:

1) Consider the congruence $x^2 \equiv a\ (mod\ p), p\ being\ an\ odd\ prime\ integer.$
2) Find the middle-pair solutions (c, d) with $c = \frac{p-1}{2}$ & $d = \frac{p+1}{2}$.
3) Obtain the corresponding quadratic congruence. Let it be: $x^2 \equiv b\ (mod\ p)$.
4) Add the even positive integers successively one by one as:
   $b + 2 + 4 + 6 + 8 + 10 + \cdots \ldots \ldots \ldots \ldots . +q \equiv a\ (mod\ p)$
5) Then the required solutions are
   $$x \equiv c - \frac{q}{2}\ \&\ x \equiv d + \frac{q}{2}\ (mod\ p).$$

ANALYSYS and RESULTS

Let us consider the congruence under consideration: $x^2 \equiv a\ (mod\ p)$.

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

The congruence having solutions $x \equiv c, d\ (mod\ p)$ must be: $x^2 \equiv b\ (mod\ p)$.

Then $c^2 \equiv b\ (mod\ p)$.

Now, $(c-1)^2 = c^2 - 2c + 1$

$$\equiv b - 2c + 1\ (mod\ p)$$

$$\equiv b - 2\left(\frac{p-1}{2}\right) + 1\ (mod\ p)$$

$$\equiv b - p + 2\ (mod\ P)$$

$$\equiv b + 2\ (mod\ p).$$

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

Similarly, $(c-2)^2 = c^2 - 4c + 4$

$$\equiv b - 4c + 4\ (mod\ p)$$

$$\equiv b - 4\left(\frac{p-1}{2}\right) + 4\ (mod\ p)$$

$$\equiv b - 2p + 2 + 4\ (mod\ P)$$

$$\equiv b + 2 + 4\ (mod\ p).$$

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

Again similarly, $(c-3)^2 = c^2 - 6c + 9$

$$\equiv b - 6c + 9\ (mod\ p)$$

$$\equiv b - 6\left(\frac{p-1}{2}\right) + 9\ (mod\ p)$$

$$\equiv b - 3p + 3 + 9\ (mod\ P)$$

$$\equiv b + 12\ (mod\ p).$$

$$\equiv b + 2 + 4 + 6\ (mod\ p).$$

Then, $x \equiv c - 3\ (mod\ p)$ is a solution of $x^2 \equiv b + 2 + 4 + 6(mod\ p)$.

Proceeding in this way, one gets

$x \equiv c - \frac{q}{2}\ (mod\ p)$ is a solution of $x^2 \equiv b + 2 + 4 + 6 + \cdots \ldots. + q\ (mod\ p)$.

RESULT: Therefore, if $x^2 \equiv b + 2 + 4 + 6 + \cdots \ldots. + q\ \equiv a\ (mod\ p)$, then the congruence $x^2 \equiv a\ (mod\ p)$ Exactly has two solutions $x \equiv c - \frac{q}{2}\ , d + \frac{q}{2}\ (mod\ p)$.

ILLUSTRATIONS

Let us consider the same example solved using existed method as above.

Example-1: Consider the congruence: $x^2 \equiv 132\ (mod\ 503)$.

Then $c = \frac{503-1}{2} = 251;\ \ and\ d = \frac{503+1}{2} = 252.$

The set (251, 252) is called middle – pair of the residues of 503.

It must be called as middle-pair solutions of a standard quadratic congruence modulo 503. Let us form such quadratic congruence.

It is seen that the said congruence is $x^2 \equiv 126\ (mod\ 503)$. Here, $b = 126$.

Adding successively the even integers,

$b = 126 + 2 = 128 + 4 = 132\ (mod\ 503)$.

Therefore, the required solutions are $x \equiv c - \frac{4}{2} = 251 - 2 = 249\ and\ x \equiv d + \frac{4}{2} = 252 + 2 = 254\ (mod\ 503)$

These are the same solutions as before. How easily the solutions are obtained!

Example-2: Consider the congruence: $x^2 \equiv 15\ (mod\ 127)$.

Then $\frac{127-1}{2} = 63;\ \ and\ \frac{127+1}{2} = 64.$

The set (63, 64) is called middle – pair of the residues of 127.

It must be called as middle-pair solutions of a standard quadratic congruence of modulo 127.

Let us form such quadratic congruence.

It is seen that the said congruence is $x^2 \equiv 32\ (mod\ 127)$.

Then 32+2=34+4=38+6=44+8=52+10=62+12=74+14=88+16=104+18=122+20=142≡ $15\ (mod\ 127)$.

Then the required solutions are $c - \frac{20}{2} = c - 10 = 63 - 10 = 53$ & $d + 10 = 64 + 10 = 74$.

Thus, $x \equiv 53, 74\ (mod\ 127)$.

Example-3: Consider the congruence: $x^2 \equiv 14\ (mod\ 157)$.

Then $\frac{157-1}{2} = 78;\ \ and\ \frac{157+1}{2} = 79$.

The set (78, 79) is called middle – pair of the residues of 157.

It must be called as middle-pair solutions of a standard quadratic congruence of modulo 157.

Let us form such quadratic congruence.

It is seen that the said congruence is $x^2 \equiv 118\ (mod\ 157)$.

Then 118+2=120+4=124+6=130+8=138+10=148+12=160≡
3+14=17+16=33+18=51+20=71+22=93+24=117+26 $= 143 + 28 = 171 \equiv 14\ (mod\ 119)$.

Then the required solutions are $c - \frac{28}{2} = c - 14 = 78 - 14 = 64$ & $d + 14 = 79 + 14 = 93$.

Thus, $x \equiv 64, 93\ (mod\ 157)$.

CONCLUSION

Therefore, it can be concluded that the author's proposed method of solving standard quadratic congruence is time-saving and very simple. It is very suitable whenever the value of k in the existed method is large. The method solves the quadratic congruence very easily in a short time. This is the merit of the current paper.

REFERENCE

[1] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.

[2] David M Burton, 2012, *Elementary Number Theory*, Mc Graw Hill education (Higher Education), Seventh Indian Edition, New Dehli, India, ISBN: 978-1-25-902576-1.

[3] Zuckerman H. S., Niven I., 2008, *An Introduction to the Theory of Numbers*, Wiley India, Fifth Indian edition, ISBN: 978-81-265-1811-1.

[4] B. M. Roy, A new method of finding solutions of a solvable standard quadratic congruence of prime modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-04, Issue-03, May-Jun-18, sr. no.-87, Page-506-508.