International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 3 Issue 5, August 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-105: Formulation of Standard Quadratic Congruence of Composite Modulus- A Product of Twin Primes

Prof B M Roy

Head, Department of Mathematics, Jagat Arts, Commerce and I H P Science College,
Goregaon Gondia, Maharashtra, India

How to cite this paper: Prof B M Roy "RP-105: Formulation of Standard Quadratic Congruence of Composite Modulus- A Product of Twin Primes" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-3 | Issue-5, August 2019, pp.896-898, **https://doi.org/10.31142/ijtsrd26492**

IJTSRD26492

ABSTRACT

In this paper, a standard quadratic congruence of composite modulus- a product of twin primes, is formulated. Actually a formula is discovered to find all the solutions of the congruence. It is found that the method is simple and takes less time as compared to the existed method. A comparative study is made by solving a problem using existed method and Author's formulation. Formulation is proved time-saving. Solutions can be obtained orally. This is the merit of the paper.

KEYWORDS: *Composite modulus, Chinese Remainder Theorem, Quadratic congruence, Twin primes*

INTRODUCTION

Congruence is a topic of Elementary Number Theory. It has been studied in undergraduate classes. No detailed discussion is found. Quadratic congruence is discussed prominently. But no formulation was found. Merely a method, popularly known as Chinese Remainder Theorem (CRT) is used.

A standard quadratic congruence is of the form: $x^2 \equiv a \ (mod\ m);$ $m\ being\ a\ prime\ or\ composite\ integer.$ If $m = p$ is a prime integer, then the standard quadratic congruence $x^2 \equiv b^2 \ (mod\ p)$ has exactly two solutions given by $x \equiv \pm b \ (mod\ p)\ i.e.\ \ x \equiv b, p-b \ (mod\ p)\ [1].$

But if m is a composite integer, then the congruence has more than two solutions. In exceptional cases, it has only two solutions.

LITERATURE REVIEW

The quadratic congruence of prime and composite modulus are studied in the books of Number Theory. The author already formulated many standard quadratic congruence of prime and composite modulus [3], [4], [5], [6], [7]. Even then he found one more congruence to formulate. These problems have been solved by earlier mathematicians using popular methods developed by them but no formula was established to solve the congruence easily and in comparatively less time.

PROBLEM-STATEMENT

Here the problem is-
"To establish a formula for the solutions of the standard quadratic congruence:

$$x^2 \equiv a \ (mod\ pq),$$

where p, q are distinct odd primes with $q < p$.

EXISTED METHOD OF SOLUTIONS

Consider the congruence $x^2 \equiv a \ (mod\ pq)$; p, q are distinct odd primes with $q < p$.

It can be split into two congruence:

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

Each of these congruence have exactly two solutions [1] and are solved separately to get a system of linear congruence of the solutions. Then solving these linear congruence by CRT [2], the common solutions are obtained.

ILLUSTRATION BY EXISTED METHOD

Consider the congruence $x^2 \equiv 293 \ (mod\ 5183).$

Here, $5183 = 71.73$

The congruence can be separated as

$x^2 \equiv 293 \ (mod\ 71);\ x^2 \equiv 293 \ (mod\ 73).$

$i.e. x^2 \equiv 9 \ (mod\ 71);\ x^2 \equiv 1 \ (mod\ 73).$

The solutions are then:

$x \equiv \pm 3 \ (mod 71) \ \ and \ \ x \equiv \pm 1 \ (mod\ 73).$

The solutions set in congruence form is:

$x \equiv 3, 68 \ \ (mod 71);$

$x \equiv 1, 72 \ \ (mod\ 73).$

Now this system of congruence can be solved by using CRT method.

$$M = m_1.m_2 = 71.73 = 5183 \ \ as\ (71,73) = 1.$$

Here, $a_1 = 3, 68 \quad m_1 = 71, \quad M_1 = 73,$

$\qquad a_2 = 1, 72 \quad m_2 = 73 \quad M_2 = 71.$

Consider the congruence
$M_1x \equiv 1\ (mod\ m_1)$ i.e. $73x \equiv 1\ (mod\ 71) i.e.\ \ 2x \equiv 1\ (mod\ 71) i.e.\ \ x \equiv 36\ (mod\ 71)$
$So, \quad x_1 = 36.$

Consider the congruence
$M_2x \equiv 1\ (mod\ m_2)\ \ i.e.\ \ 71x \equiv 1\ (mod\ 73)\ i.e.\ \ x \equiv 36\ (mod\ 73).\ How?$
Here lies the difficulty. This difficulty is removed in the paper of the author [8].
$So, \quad x_2 = 36.$

Then the common solutions are given by
$x_0 \equiv M_1a_1x_1 + M_2a_2x_2\ (mod\ M)$
$\equiv 73.3.36 + 71.1.36 = 74;$
$\equiv 73.68.36 + 71.1.36 = 5083;$
$\equiv 73.3.36 + 71.72.36 = 145;$
$\equiv 73.68.36 + 71.72.36 =$5109.

Thus, $x_0 = 74, 145, 5083, 5109\ (mod\ 5183)$
These are the required solutions.
It takes at least 50 minutes!!

DEMERIT OF THE EXISTED METHOD
Though the existed method is very popular among the readers, it has its own demerits.

Those are:
The existed method is time-consuming.
It takes a long time to get all the solutions of the original congruence.

Sometimes it becomes impractical and boring.

PROPOSED METHOD (Formulation)
Consider the congruence $x^2 \equiv a\ (mod\ pq),\ \ with\ p > q, both\ are\ twin\ primes.$

If $a = b^2, and\ \ q = p - 2,$ then the congruence becomes $x^2 \equiv b^2\ \ (mod\ p(p-2)).$

Let us now consider the other case when p, q are twin-primes. Then also the congruence $x^2 \equiv b^2\ \ (mod\ pq)$ has four solutions.

The first two solutions are $x \equiv b, pq - b\ \ (mod\ pq)$ as usual.

For the other two solutions, consider
$x = \pm(p-1)b\ (mod\ pq);\ \ \ q = p - 2.$
Then, $x^2 = [\pm(p-1).b]^2$
$= (p-1)^2b^2$
$= (p^2 - 2p + 1)b^2$
$= p(p-2).b^2 + b^2$
$\equiv b^2\ \ (mod\ p(p-2)$
$\equiv b^2\ \ (mod\ pq)\ as\ q = p - 2.$

Thus, it is established that $x \equiv \pm(p-1).b\ \ \ (mod\ pq)$ are the two solutions of the said congruence.

But if $b = p$, then $x \equiv \pm(p-1).b = (p-1).p$
As $(p-1).p > p(p-2) = pq$, hence one must have $x \equiv \pm(p-1).p - (p-2).p$

$\equiv \pm[p(p-1-(p-2)]$

$\equiv \pm p\ (mod\ pq).$

Thus it is seen that if $b = p, then$ the quadratic congruence under consideration has only two solutions $x \equiv \pm p\ (mod\ pq).$

ILLUSTRATIONS
Consider the congruence $x^2 \equiv 293\ (mod\ 5183).$
It is seen that
$5183 = 71.73\ \ with\ p = 73\ \&q = 71, both\ are\ twin -\ \ primes.$

It can also be written as:
$x^2 \equiv 293 + 5183 = 5476 = 74^2.$

Therefore, the solutions are
$x \equiv \pm 74;\ \pm(73-1).74\ \ (mod\ 71.73)$
$\equiv \pm 74; 72.74\ (mod\ 5183)$
$\equiv \pm 74;\ \pm 5328\ \ \equiv \pm 74;\ \pm 145\ (mod\ 5183)$
$\equiv 74, 5183 - 74;\ \ 145, 5183 - 145\ (mod\ 5183)$
$\equiv 74, 5109;\ \ 145, 5083\ (mod\ 5183).$
≡74, 145, 5083, 5109 (mod 5183).

These are the same solutions obtained in existed method. It takes at most 5 minutes.
Consider one more problem $x^2 \equiv 146\ (mod\ 5183)$
It can be written as $x^2 \equiv 146 + 5183 = 5329 = 73^2$ (mod 5183)

Therefore, its two obvious solutions are $x \equiv \pm 73\ (mod\ (5183)$
$\equiv 73, 5183 - 73\ (mod\ 5183)$
$\equiv 73, 5110\ (mod\ 5183)$

Here, $b = p = 73.$

Hence, the other two solutions are as per formula:
$x \equiv \pm(p-1).p\ (mod\ (p-2).p)$
$\equiv \pm(73-1).73 - (73-2).73\ \ (mod\ 71.73)$
$\equiv \pm 73[(73-1) - (73-2)]\ \ (71.73)$

$\equiv \pm 73 \ (mod\ 71.73)$
$\equiv \ \pm 73 \ (mod\ 5183)$.
≡73, 5183-73 $\equiv 73, 5110 \ (mod\ 5183)$

These solutions are the same as before.
Thus, the congruence has exactly two solutions.

CONCLUSION

As p, q are twin primes, then $q = p - 2$ and solutions are given by
$x \equiv b, pq - b; \pm(p-1)b \ (mod\ pq)$.

But if $b = p$, the congruence has only two solutions $x \equiv \pm p \ (mod\ pq)$.

MERIT OF THE PAPER

Here the standard quadratic congruence
$x^2 \equiv a \ (mod\ pq)$,
$with\ p, q, both\ are\ twin\ primes$ $q = p - 2$ is formulated. The formulation is the merit of the paper. It takes only five minutes to solve the congruence.

REFERENCE

[1] H S Zuckerman at el, 2008, *An Introduction to The Theory of Numbers*, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

[2] Thomas Koshy, 2009, "*Elementary Number Theory with Applications*", 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.

[3] Roy B M, 2018, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & four, International Journal of Recent Innovations In Academic Research (IJRIAR), ISSN:2635-3040, Vol-2, Issue-2, Jun-18.*

[4] Roy B M, 2018, *Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & eight,* International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-4, July-18.

[5] Roy B M, 2019, Formulation of Some Classes of Solvable Standard Quadratic Congruence modulo a Prime Integer - Multiple of Three & Ten, International Journal of Scientific Research and Engineering development (IJSRED), ISSN: 2456-2631, Vol-02, Issue-02, Mar-19.

[6] Roy B M, 2018, Formulation of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- an Odd Prime Positive Integer Multiple of Seven, International Journal of Science and Engineering development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-11, Nov-18.

[7] Roy B M, 2018, Formulation of Solutions of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- a Prime Positive Integer Multiple of Five, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-03, Issue-10, Sep-18.

[8] Roy B M, 2019, *An Algorithmic Formulation of solving Linear Congruence of Prime & Composite Modulus of Degree One, International Journal for research Trends and Innovations (IJRTI), ISSN: 2456-3315, vol-04, Issue-04, April-19.*