Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 10, Issue, 05, pp.69748-69750, May, 2018

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

REVIEW ARTICLE

FORMULATION OF SOLUTIONS OF SOLVABLE STANDARD QUADRATIC CONGRUENCE OF ODD COMPOSITE MODULUS A PRODUCT OF TWO DIFFERENT ODD PRIMES AND ALSO A PRODUCT OF TWIN-PRIMES

***Prof. B. M. Roy**

Head, Dept. of Mathematics, Jagat Arts, Commerce & I H P Science college, Goregaon (Gondia) M. S. (INDIA).

ARTICLE INFO

Article History:
Received 12th February, 2018
Received in revised form
26th March, 2018
Accepted 25th April, 2018
Published online 31st May, 2018

Key words:
Composite modulus,
Chinese Remainder Theorem,
Quadratic congruence,
Twin primes.

ABSTRACT

In this paper, a new method of finding solutions of a solvable standard quadratic congruence of composite modulus which is a product of two different odd primes and also as a product of twin primes are discussed. Actually, a new 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 giving suitable numerical examples.

Citation: Roy, B. M. 2018. "Formulation of Solutions of Solvable Standard Quadratic Congruence of Odd Composite Modulus a product of two different odd primes and also a product of twin-primes", *International Journal of Current Research*, 10, (05), 69748-69750.

INTRODUCTION

Need of Research

Much more has been done on the solutions of quadratic congruence of prime and composite Modulus. Even then much more is remained to do. I have gone through books on Number Theory and I realized that much more remain to do, upon which nothing has been done. Those problems have been solved by eminent mathematicians by popular methods developed by them but they established no formula to solve the congruence easily and in comparatively less time. I tried my best to formulate some of those congruence and here I wish to present these formulations.

About the Problem

Here we consider the congruence x^2≡a (mod m) of composite modulus, when m is factorizable. If m=pq, then the congruence becomesx^2≡a (mod pq). If p, q are odd primes, then the congruence is called a congruence of odd composite modulus and has four solutions Koshy Thomus.

Corresponding author*: **Prof. B. M. Roy
Head, Dept. of Mathematics, Jagat Arts, Commerce & I H P Science college, Goregaon (Gondia) M. S. (India).

If p, q are twin primes with p > q, then, q=p-2, and the congruence is of the form: x^2≡a [mod p(p-2)] and the congruence also has four solutions. In the literature, no direct formula was found but the use of the Chinese Remainder Theorem. My effort is to discover a formula to find all the solutions.

Problem Statement

Consider a solvable standard quadratic congruence of odd composite modulusx^2≡a (mod m) (1)

Here the problem is: "To formulate the solutions of the congruence under consideration in two cases: Case-I: when m=product of two different odd primes=pq, where p,q are different primes; Case-II: when m=product of twin-primes=p(p-2),p being odd prime.

Existed Method

Consider the congruence (1). It can be explit into two congruence:

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

$x^2 \equiv a \ (mod\ q)$ .....(ii)

These standard quadratic congruence of prime modulus each having exactly two solutions [2], are solved separately to get solutions:

$x \equiv c,\ d \ \ (mod\ p)$ .....(iii)

$x \equiv e,\ f \ \ (mod\ q)$ .....(iv)

Solving these linear congruence by Chinese Remainder Theorem, four solutions can be obtained!

It is needless to state Chinese Remainder Theorem

Demerit of Existed Method

Definitely, use of "Chinese Remainder Theorem" is a time-consuming calculation. Hence it sometimes becomes a boring task.

Proposed Methed

Case-I

Consider the congruence (1) & p, q with p>q are distinct odd primes.

If $a = b^2$, then the congruence becomes $x^2 \equiv b^2(mod\ pq)$.

Two obvious solutions of the congruence are: $x \equiv pq \pm b\ (mod\ pq)$

$i.e. x \equiv pq + b, \quad pq - b \ (mod\ pq) \ \ i.e.\ x \equiv b,\ pq - b \ (mod\ pq).$

Thus, b is a solution of $x^2 \equiv b^2(mod\ pq)$ ..... (v)

If$a \neq b^2$, then we add mpq to *'a'* to get $a + mpq\ with\ such\ an\ m\ such\ that\ a + mpq = b^2$.

Then, the two obvious solutions are:$x \equiv \pm b\ (mod\ pq) \equiv b, pq - b\ (mod\ pq)$. Now, for$x \equiv \pm(pk \pm b)$, we have

$x^2 = \{\pm(pk \pm b)\}^2 = p^2k^2 \pm 2pkb + b^2 = b^2 + .k(pk \pm 2b) = b^2 + p(qt) = b^2 + (pq)t \equiv b^2\ \ (mod\ pq)$, if $k(pk \pm 2b) = qt, for\ \ integers\ k\ \&\ t.$

Thus, the other two solutions are given by:

$x \equiv \pm(pk \pm b),$
$if\ k(pk \pm 2b)\ qt, for\ some\ positive\ integers\ k\ \&\ t.$

Therefore, the congruence $x^2 \equiv b^2(mod\ pq)$ has two obvious solutions $x \equiv \pm b\ (mod\ pq)$;

other two solutions are

$x \equiv \pm(pk \pm b)(mod\ pq), when\ k(pk \pm 2b) = qt, for\ positive\ integers\ k\ \&\ t.$

Therefore, we conclude that all the four solutions are given by

$x \equiv \pm b\ , \pm(pk \pm b)\ \ mod\ (pq), for\ some\ integer\ k; if\ k(pk \pm 2b) = qt, for\ some\ integer\ t.$

Case-II

Let $p\ \&\ q$ be twin primes. Then $q = p - 2$ and the congruence becomes

$x^2 \equiv b^2(mod\ p\ (p-2))$

If $b^2 < (p-2)p$, then the four solutions are

$x \equiv \pm b\ \ (mod\ (p-2)p)$…(two obvious solutions)

& $x \equiv \pm(p-1)b\ (mod\ (p-2)p)$ ..... $(other\ two\ solutions)$

For, $[(p-1)b]^2 = (p-1)^2b^2 = (p^2 - 2p + 1)b^2 = b^2 + b^2(p-2)p \equiv b^2(mod\ (p-2)p).$

But if $b^2 > (p-2)p$, then $x \equiv \pm r\ (mod\ (p-2)p\ , if\ \ (p-1)b \equiv r\ (mod\ (p-2)p.$

Therefore, we conclude that all the four solutions are given by

$x \equiv \pm b\ , \pm((p-1)b)\ \ mod\ (p(p-2)).$

Therefore, we conclude that all the four solutions are given by

$x \equiv \pm b\ , \pm(pk \pm b)\ \ mod\ (pq), for\ some\ integer\ k; if\ k(pk \pm 2b) = qt, for\ some\ integer\ t.$

Case-II

Let $p\ \&\ q$ be twin primes. Then $q = p - 2$ and the congruence becomes

$x^2 \equiv b^2(mod\ p\ (p-2))$

If$b^2 < (p-2)p$, then the four solutions are

$x \equiv \pm b\ \ (mod\ (p-2)p)$……(two obvious solutions)

& $x \equiv \pm(p-1)b\ (mod\ (p-2)p)$ ..... $(other\ two\ solutions)$

For, $[(p-1)b]^2 = (p-1)^2b^2 = (p^2 - 2p + 1)b^2 = b^2 + b^2(p-2)p \equiv b^2(mod\ (p-2)p).$
But if $b^2 > (p-2)p$, then $x \equiv \pm r\ (mod\ (p-2)p\ , if\ \ (p-1)b \equiv r\ (mod\ (p-2)p.$

Therefore, we conclude that all the four solutions are given by
$x \equiv \pm b\ , \pm((p-1)b)\ \ mod\ (p(p-2)).$

Merit of proposed method

This method is very simple and easier. It takes less time to get the solutions of the congruence. We need not use the Chinese Remainder Theorem, which is a time-consuming method. The proposed method solves the problem directly using the established formula and one need not use Chinese Remainder Theorem for common solutions.

Illustrations

We illustrate the methods and solve the congruence by both the existed and proposed methods.

Solution by existed method

Consider the congruence $x^2 \equiv 23\ (mod\ 77)$.We see that $77 = 7.11$

Hence congruence can be explit into two congruence with solutions [3] as:

$x^2 \equiv 23\ (mod\ 7)\ \ i.e.\ \ x^2 \equiv 2\ (mod\ 7)\ \ i.e.\ x^2 \equiv 2 + 7 = 9 = 3^2\ giving\ \ x \equiv 3, 4\ (mod\ 7).$

$x^2 \equiv 23\ (mod\ 11)\ \ i.e.\ \ x^2 \equiv 1\ (mod\ 11)\ \ giving\ \ x \equiv 1, 10\ (mod\ 11).$

Thus, the solutions

are$x \equiv 3,\ 4(mod\ 7);\ \ x \equiv 1, 10\ (mod\ 11).$

Now weuse Chinese Remainder Theorem [1]:

Here $a_1 = 3,\ 4;\ \ a_2 = 1, 10\ \ with\ m_1 = 7;\ \ m_2 = 11\ \ amd\ so\ \ M = [7, 11] = 77.$

Therefore, $M_1 = 11,\ \ M_2 = 7.$

Consider $M_1x \equiv 1\ (mod\ m_1)\ i.e.\ 11x \equiv 1\ (mod\ 7)\ i.e.\ x \equiv 2\ (mod\ 7)\ giving\ x_1 = 2.$

Consider $M_2x \equiv 1\ (mod\ m_2)\ i.e.\ 7x \equiv 1\ (mod\ 11)\ i.e.\ x \equiv 8\ (mod\ 7)\ giving\ x_2 = 8.$

Then, the common solution is given by

$x_0 \equiv M_1x_1a_1 + M_2x_2a_2(mod\ M)\ \ i.e.x_0 \equiv 11.2.3 + 7.8.1 = 122 \equiv 45\ (mod\ 77)$
$x_0 \equiv M_1x_1a_1 + M_2x_2a_2(mod\ M)\ \ i.e.x_0 \equiv 11.2.4 + 7.8.1 = 144 \equiv 67\ (mod\ 77)$
$x_0 \equiv M_1x_1a_1 + M_2x_2a_2(mod\ M)\ \ i.e.x_0 \equiv 11.2.3 + 7.8.10 = 626 \equiv 10\ (mod\ 77)$
$x_0 \equiv M_1x_1a_1 + M_2x_2a_2(mod\ M)\ \ i.e.x_0 \equiv 11.2.4 + 7.8.10 = 1648 \equiv 32\ (mod\ 77)$

Thus required common solutions are$x \equiv 45, 67, 10, 67;\ (mod\ 77).$

SOLUTION BY PROPOSED METHOD

Consider the same congruence solved as in above: $x^2 \equiv 23\ (mod\ 77)$.Here $77 = 7.11\ with\ p = 11, q = 7$ Hence the above congruence is of the type $x^2 \equiv a\ (mod\ pq) with\ p, q\ odd\ primes.$ Now consider $x^2 \equiv 23\ (mod\ 77).$

It can be written as: $x^2 \equiv 23\ (mod\ 77)\ \ i.e.\ \ x^2 \equiv 23 + 77 = 100 = 10^2(mod\ 77).$ Hence two obvious solutions [3] are $x \equiv \pm 10\ (mod\ 77)\ \ i.e.\ \ x \equiv 10,\ \ 67\ (mod\ 77).$

Then $b = 10\ is\ one\ of\ the\ solution.$ Other two solutions are given by $x \equiv \pm(pk \pm b)(mod\ pq),\ \ if\ \ (pk \pm 2b)k = qt, for\ some\ integer\ t.$

Now, $(pk \pm 2b)k = qt\ becomes(11k \pm 20)k = 7t.$
For $k = 2,\ we\ have\ k(11k + 20) = 2.(11.2 + 20) = 84 = 7.12 = 7t.$

Then the other solutions are $x \equiv \pm(11.2 + 10) = \pm 32\ (mod\ 77)\ \ i.e.x \equiv 32, 45\ (mod\ 77).$

Thus required solutions are $x \equiv 10, 67; 32, 45\ (mod\ 77)$.

These are the same solutions as obtained above in existed method but with less labour and time of calculation. Consider another example of twin-prime: $x^2 \equiv 25\ (mod\ 143)\ \ i.e.x^2 \equiv 5^2(mod\ 143).$

Here, $25 < 143 = 11.13$ with$b = 5\ \&\ p = 13, q = 11 = 13 - 2$(twin primes).

Therefore, solutions are $x \equiv \pm b, \pm(p-1)b\ \ (mod\ pq)$

$i.e.x \equiv \pm 5, \pm(13-1).5\ (mod\ 11.13)$
$i.e.x \equiv \pm 5, \pm 60\ (mod\ 143)$
$i.e.x \equiv 5, 138; 60, 83(\text{mod } 143).$

We now consider one more example of twin primes: $x^2 \equiv 293\ (mod\ 5183).$

Here,$5183 = 71.73;\ \ 71\ \&\ 73$ are twin primes. We have $p = 73\ ;\ \ q = 71.$

Congruence can be written as $x^2 \equiv 293\ (mod\ 71.73).$
$\equiv 293 + 5183 = 5476 = 74^2(mod\ 5183).$

Therefore, $x \equiv \pm 74\ (mod\ 5183)$

$i.e.x \equiv 74, 5109\ (mod\ 5183)\ \ with\ b = 74,$ arethe two obvious solutions.

Other two solutions are $x \equiv \pm(p-1)b\ (mod\ (p-2)p)$

$\equiv \pm(73-1).74\ \ (mod\ 71.73)$
$\equiv \pm 5328\ (mod\ 5183)$
$\equiv \pm 145\ (mod\ 5183)$ as $5328 \equiv 145\ (mod\ 5183).$
$\equiv 145, 5083\ (mod\ 5183).$

Thus, all the four solutions are $x \equiv 74, 5109; 145, 5083\ (mod\ 5183)\ and\ also\ verified.$

Conclusion

In this paper, a simple, less time-consuming new method of finding solutions of a solvable standard quadratic congruence of odd composite modulus of the type $x^2 \equiv a\ (mod\ pq)$is developed $i.e.$ formulation of solutions is done successfully. A comparative study is made using both the methods i.e. by existed and proposed method. A direct formula was developed for the solutions of congruence of modulus of product of two-primes and also a product of twin-primes.

REFERENCES

An Introduction to The Theory of Numbers", 5/e, Wiley India (Pvt) Ltd.

B. M. ROY, Discrete Mathematics and Number Theory, 1/e, Das Ganu Prakashan. Nagpur (M S).

I.NIVEN I., ZUCKERMAN H. S., MONTGOMERY H. L. (1960, Reprint 2008),

KOSHY THOMUS, "Elementary Number Theory with Applications", 2/e, Academic press.

****