International Journal of Scientific Engineering and Research (IJSER)
ISSN (Online): 2347-3878
Index Copernicus Value (2015): 56.67 | Impact Factor (2017): 5.156

Formulation of Solvable Standard Quadratic Congruence of Odd Composite Modulus as a Product of Three Odd Primes

B M Roy

Head and Professor, Dept. of Mathematics, Jagat Arts, Commerce & I H P Science college, Goregaon (GONDIA),M. S.
Affiliated to RTM Nagpur University, Nagpur (India)

Abstract: ***In this paper, a class of solvable standard quadratic congruence of composite modulus is formulated. The formula is also verified with solved examples. This formula saves time to find the solutions directly without using Chinese remainder theorem. There is no other method found in the literature of mathematics.This research is for formulation of solutions. This is the merit of this paper.***

Keywords: composite modulus, Chinese Remainder Theorem, Prime integer, quadratic congruence

1. Introduction

In my research papers, I have formulated many quadratic congruence and congruence of higher degree. Here is another quadratic congruence I have considered for the formulation. I found that no attempt had been taken for formulation of the congruence under consideration. They used Chinese Remainder Theorem to solve the congruence, which takes a long time. For the time saving purpose, I promised myself to formulate the congruence and I tried my best to do so. I am presenting my effort in this paper.

2. Need of Research

Intentionally, I have gone through the literature of number theory and found no formula to solve the said congruence directly; but a method using Chinese Remainder Theorem. Then I prepared myself strongly to formulate the congruence and I succeed (as I think).

Existed Method:
The method of finding solutions of quadratic congruence of composite modulus, found in the literature of mathematics is as under:

Consider the congruence $x^2 \equiv b^2\ (mod\ m)$, (b, m) =1 with m composite integer.

Let us consider for simplicity that $m = pqr;\ \ p, q, r,$ $are\ \ different\ odd\ positive\ prime\ integers.$

Then the congruence can be split into three equivalent congruence [2]:
$x^2 \equiv b^2(mod\ p)\ ;\ \ x^2 \equiv b^2(mod\ q) \& x^2 \equiv b^2(mod\ r).$
Each has two solutions[3].

Let the solutions be $x \equiv b_1,\ b_2$ (mod p); $x \equiv b_3,$ $b_4(mod\ q) \&\ x \equiv b_5,\ b_6$ (mod r).
Using "Chinese Remainder Theorem" [1], the common solutions can be obtained.

If the congruence $x^2 \equiv a\ (mod\ m)\ with\ (a, m) = 1$ is solvable, then it must be written in the form:
$x^2 \equiv b^2(mod\ m)$by adding m to a k-times $i.e\ .a + km = b^2\ \ with\ two\ obvious$
$solutions\ \ x \equiv \pm b$ (mod pqr) [3].
[**Here Chinese Remainder Theorem is needless to state**.]

Demerit of the Existed Method:
Use of Chinese Remainder Theorem, is a long process and takes long time to find common solutions.
To save time in calculation, I tried to formulate the solutions in this paper.

3. Problem Statement

In this paper, I want to formulate the class of quadratic congruence of composite modulus of the type
$x^2 \equiv a^2\ (mod\ pqr)$ .....(1)
$with\ p, q, r\ are\ different\ odd\ primes.$ Such congruence has eight solutions [1].

The solutions are given by a formula developed by the author as below:
$x = \pm a;\ \pm(pk \pm a), if\ k.(pk \pm 2a)$
$= qrt\ for\ integers\ t\ \&\ k\ where\ p\ is\ the\ largest\ prime.$

4. Analysis & Result [Formulation]

Let us consider the congruence under consideration (1).
We see that $x \equiv \pm a\ (mod\ pqr)$ are the two obvious solutions. Yet six solutions are remained to find.
Let us take $x = \pm(pk \pm a)$.Then,

$$x^2 = \{\pm(pk \pm a)\}^2 = p^2k^2 \pm 2pka + a^2$$
$$= p\ k(pk \pm 2a) + a^2$$

$= pk.qrt + a^2\ \ if\ \ k.(pk\ \pm 2a) =$ qrt for an integer t & k.

$$\equiv a^2(mod\ pqr).$$

Thus the solutions are $x = \pm(pk \pm a),\ if\ k.(pk \pm 2a) = qrt\ for\ integers\ t\ \&\ k.$
These are the six other solutions can be obtained choosing different values of k.
Let us consider an example.
Consider the congruence $x^2 \equiv 1\ (mod\ 165).$
Here $165 = 3.5.11\ \ with\ p = 11, q = 5, r = 3\ \&\ a = 1.$
Such a congruence always has eight solutions.

Two obvious solutions are $x \equiv \pm 1 = 1, 165 - 1 = 1, 164\ (mod\ 165)$.

The other solutions are given by

$$x \equiv \pm(kp \pm a)\ if\ k.(kp \pm 2a) = q\ rt\ for\ integer\ t\ \&\ k.$$

$$i.e.\ \ x \equiv \pm(11k \pm 1)\ if\ (11k \pm 2.1).k = 5t\ or\ 3t\ for\ integer\ t.$$

For $k = 5$, $11k \pm 2.a = (11.5 + 2.1).5 = 57.5 = 3.5.19$

Thus other two solutions are

$$x \equiv \pm(11.5 + 1) = \pm 56 = 56, 165 - 56 = 56, 109\ (mod\ 165).$$

For $k = 3$, $(11.3 + 2.1).3 = 35.3 = 5.7.3$

Thus other two solutions are

$$x \equiv \pm(11.3 + 1) = \pm 34 = 34, 165 - 34 = 34, 131\ (mod\ 165).$$

For $k = 7$, $(11.7 \pm 2.1).7 = (77 - 2).7 = 75.7 = 5.15.7$

Thus other two solutions are $x \equiv \pm(11.7 - 1) = \pm 76 = 76, 165 - 76 = 76,\ 89\ (mod\ 165)$.

The required solutions are $x \equiv 1, 164;\ 34, 131;\ 56, 109; 76, 89\ (mod\ 165)$.

Here is another example.

Consider $x^2 \equiv 16\ (mod\ 105)$.

It can also be written as $x^2 \equiv 4^2\ (mod\ 105)$

Here $105 = 3.5.7\ with\ p = 7, q = 5, r = 3\ \&\ a = 4$.

Such a congruence has eight solutions.

Two obvious solutions are $x \equiv \pm 4 = 4, 105 - 4 = 4, 101\ (mod\ 105)$.

Other solutions are given by $x \equiv \pm(pk \pm a),\ if\ k.(pk \pm 2a = qrt\ for\ integers\ t\ \&\ k$

$$i.e.\ x \equiv \pm(7k \pm 4)\ if\ k.(7k \pm 2.4) = 5.3.t$$

For $k = 1$, $1.(7.1 + 2.4) = 15 = 15.1$

Thus two other solutions are

$x \equiv \pm(7.1 + 4) = \pm 11 = 11, 105 - 11 = 11, 94\ (mod\ 105)$.

For $k = 5$, $5.(7.5 - 2.4) = 5.27 = 5.3.9 = 15.9$

Thus two other solutions are

$x \equiv \pm(7.5 - 4) = \pm 31 = 31, 105 - 31 = 31, 74\ (mod\ 105)$.

For $k = 6$, $6.(7.6 + 2.4) = 6.(42 + 8) = 6.50 = 2.3.5.10 = 15.20$

Thus two other solutions are

$x \equiv \pm(7.6 + 4) = \pm 46 = 46, 105 - 46 = 46, 59\ (mod\ 105)$.

All the solutions are $x \equiv 4, 101;\ 11, 94;\ 31, 74;\ 46, 59\ (mod\ 105)$.

Merit of the Paper

The method developed has the merits as under:

1) The Chinese Remainder Theorem takes a long time to find solutions. We get rid of the use of Chinese remainder theorem.
2) It gives a Formula for solutions to get the same directly and quickly.
3) The method saves time in calculation.

5. Conclusion

Thus, solutions of a standard quadratic congruence of composite modulus of the type $x^2 \equiv a^2(mod\ pqr)$ with p, q, r are different odd primes, is formulated. It is a very quick method to find all the solutions. One need not use the Chinese Remainder Theorem.

References

[1] Koshy, Thomas; Elementary Number Theory with Applications; 2/e; Academic press.
[2] Niven, I.; Zuckerman H S.; Montgomery H L.; An Introduction to the Theory of Numbers; 5/e; WSE.
[3] Roy B. M., Discrete Mathematics and Number Theory, 1/e, Das Ganu Prakashan, Nagpur.
[4] Burton David, Elementary Number Theory, 7/e, Mac Graw Hills, Indian edition.