International Journal of
Recent Innovations in Academic Research

Volume-2, Issue-2, June 2018, Page No: 1-3 ISSN : 2635-3040

FORMULATION OF SOLUTIONS OF STANDARD QUADRATIC CONGRUENCE OF COMPOSITE MODULUS AS A PRODUCT OF TWO ODD PRIMES AND FOUR

Prof. B. M. Roy
Head, Dept. of Mathematics, Jagat Arts, Commerce and I.H.P. Science College, Goregaon (Gondia), Pin: 441801
Affiliated to RTM Nagpur University, Nagpur, India
Corresponding author E-mail: roybm62@gmail.com

Abstract : In this paper, a formula for solutions of a solvable standard quadratic congruence of even composite modulus as a product of two odd primes and Four is discovered. It solves the problem directly. It saves time in calculation. No need to use Chinese Remainder Theorem. This is the merit of the paper.
Keywords: Chinese Remainder Theorem, even composite modulus, Quadratic Congruence.

Citation: **Roy, B.M.** 2018. Formulation of Solutions of Standard Quadratic Congruence of Composite Modulus as a Product of Two Odd Primes and Four**.** Int. J. Rec. Innov. Acad. Res., 2 (2): 1-3

Introduction

Congruence $x^2 \equiv a\ (mod\ m)$ is a standard quadratic congruence in an unknown x.

If m is a prime positive integer, then the congruence is called a congruence of prime modulus. If m is a composite integer, then the congruence is called a standard quadratic congruence of composite modulus. Here we consider the congruence $x^2 \equiv a\ (mod\ 4pq)$and it has eight incongruent solutions (Thomas Koshy, 2007).

Need of Research

The only method for solutions of the said congruence found in the literature is by using ***Chinese Remainder Theorem;*** it takes a long time to find all the solutions. It is not a fair method for students. No formulation is found in the literature of mathematics. Thus to save the time in the calculation for solution, we need another method of solution which must be easier. It must be the formulation. Here lies the need of this research. I tried my best to formulate the solutions and my effort is presented in this paper.

Problem-Statement

To formulate the standard quadratic congruence of even composite modulus:

$x^2 \equiv a\ (mod\ 4pq)$ ……..(1)

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

Discussion of existed Method (Thomas Koshy, 2007)

Consider the congruence (Niven *et al.*, 1960)

It can be separated into three congruence:

$x^2 \equiv a\ (mod\ 4)$ .....(i)

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

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

These standard quadratic congruence can be solved separately to get solutions as

$x \equiv b, c\ \ (mod\ 4)$ .....(iv)

$x \equiv\ \ d, e\ \ (mod\ p)$ .....(v)

$x \equiv\ f, g\ \ (mod\ q)$ .....(vi)

as "every solvable quadratic congruence of positive odd prime modulus has exactly two solutions (Thomas Koshy, 2007).

Solving these, **eight solutions** can be obtained using Chinese Remainder Theorem.

Demerits of the existed method:

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

Discussion of Proposed method (Formulation)

Consider the congruence (Niven *et al.*, 1960)

If $a = b^2$, then the congruence becomes $x^2 \equiv b^2(mod\ 4pq)$.

Two obvious solutions of the congruence are: $x \equiv 4pq \pm b\ (mod\ 4pq)$.

$i.e.\ \ x \equiv 4pq + b,$
$4pq - b\ \ (mod\ 4pq)\ \ i.e.\ x \equiv b,\ \ 4pq - b\ \ (mod\ \ 4pq)$.

Thus, b is a solution of $x^2 \equiv b^2(mod\ 4pq)$.

If $a \neq b^2$, then we add "$4kpq$" to **a** to get $a + 4kpq\ with\ such\ a\ \boldsymbol{k}\ such\ that\ a + 4kpq = b^2$.

Then, the two obvious solutions are as before.

Also, for $x = 2pq \pm b$, we have $x^2 = (2pq \pm b)^2$

$$= 4p^2q^2 \pm 4pqb + b^2$$
$$= b^2 + 4pq(pq \pm b)$$
$$\equiv b^2\ (mod\ 4pq)$$

So, two other solutions are $x \equiv 2pq \pm b\ (mod\ 4pq)$.

Thus, the four obvious solutions are given by $\boldsymbol{x \equiv 4pq \pm b}$; $\boldsymbol{2pq \pm b\ (mod\ 4pq)}$.

Now, for the remaining four solutions, let $x = \pm(2pk \pm b)$,

Then we have $x^2 = \{\pm(2pk \pm b)\}^2$

$$= 4p^2k^2 \pm 4pkb + b^2$$
$$= b^2 + 4pk(pk \pm b)$$
$$= b^2 + 4p(qt)$$
$$= b^2 + (4pq).t\ ,\ \text{if}\ \ k(pk \pm b) = qt, for\ an\ integer\ t.$$
$$\equiv b^2\ \ (mod\ 4pq),$$

if
$k(pk \pm b) =$
$qt\ for\ two\ different\ values\ of\ k.$

Thus, the other four solutions are given by:

$$\boldsymbol{x \equiv \pm(2pk \pm b),}$$
$$\boldsymbol{if\ k(pk \pm b)}$$
$$\boldsymbol{= qt, for\ some\ positive\ integer\ t.}$$

Therefore, the congruence $x^2 \equiv b^2(mod\ 4pq)$ has four obvious solutions

$x \equiv \pm b \ (mod\ 4pq); 2pq \pm b;$ and other four solutions are $x \equiv \pm(2pk \pm b)(mod\ 4pq)$,

$when\ k(pk \pm b) = qt, for\ positive\ integer\ t.$

Illustration of the method by examples

We illustrate the method by giving an example and solving the congruence by the formula established. Consider the congruence:

$x^2 \equiv 4\ (mod\ 84).$

Here, $84 = 4.3.7\ with\ p = 7, q = 3.$

Thus, the congruence is of the type: $x^2 \equiv b^2\ (mod\ 4pq).$

It can be written as:

$x^2 \equiv 4 = 2^2 (mod\ 84)$

giving solutions $x \equiv \pm 2\ (mod\ 84)$

$i.e.\ x \equiv 2, 82\ \ (mod\ 84).$

Therefore, $b = 2$ is a solution.

Other two obvious solutions are given by $x \equiv 2pq \pm b\ (mod\ 4pq)$

$\equiv 2.7.3 \pm 2\ (mod\ 4.7.3)$

$\equiv 42 \pm 2\ (nod\ 84)$

$\equiv 40, 44\ (mod\ 84\ )$

Other four solutions are given by

$x \equiv \pm(2pk \pm b)(mod\ 4pq), \quad if\ k(pk \pm b) = qt, for\ some\ integer\ t.$

So, $x \equiv \pm(2.7.k \pm 2)(mod\ 84),\ if\ k(7k \pm 2) = 3t$

$i.e.\ x \equiv \pm(14k \pm 2)\ \ (mod\ 42)\ if k(\ 7k \pm 2) = 3t.$

But $1.(7.1 + 2) = 9 = 3.3\ giving\ \boldsymbol{k = 1.}$

Also,$2.(7.2 - 2) = 24 = 3.8\ giving\ \boldsymbol{k = 2}.$

Other four solutions are

$x \equiv \pm(14.1 + 2) = \pm 16\ (mod\ 84)\ i.e.\ x \equiv 16, 26\ (mod\ 84).$

& $x \equiv \pm(14.2 - 2) \equiv (Mod\ 84) \equiv \pm 26$ (mod 84)$\equiv 26, 58\ (mod 84)$

Therefore, all the eight solutions are $x \equiv 2, 82;\ 40; 44;\ 16, 26; 26, 58\ (mod\ 84).$

Conclusion

Thus a simpler, less time-consuming new method of finding solutions (directly by formula) of a solvable quadratic congruence of even composite modulus of the type $x^2 \equiv a^2\ (mod\ 4pq)$ $with\ p, q\ are\ odd\ primes,$ is established. The congruence $x^2 \equiv b^2 (mod\ 4pq)$ has four obvious solutions

$x \equiv 4pq \pm b; 2pq \pm b\ (mod\ 4pq)$

and other four solutions are

$x \equiv \pm(2pk \pm b)(mod\ 4pq)$,

$when\ k(pk \pm b) = qt, for\ positive\ integer\ t.$

No need to use Chinese Remainder Theorem. ***This is the merit of this paper.***

References

Niven, I., Zuckerman, H.S. and Montgomery H.L. **1960,** Reprint 2008. An Introduction to the Theory of Numbers. 5/e, Wiley India (Pvt) Ltd.

Thomas Koshy, **2007.** Elementary Number Theory with Applications, 2nd Edition, Academic press.