INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

IJARIIT

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 4)
Available online at: www.ijariit.com

Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes and eight

Bikashchandra Mukunda Roy
roybm62@gmail.com
Jagat Arts, Commerce & Indiraben Hariharbhai Patel Science College,
Goregaon, Maharashtra

ABSTRACT

In this paper, a formula for finding solutions of a standard quadratic congruence of even composite modulus as a product of two different odd primes & eight is established. It solves the problem directly. It saves the time of calculation. The formulation is the merit of the paper.

Keywords: *Chinese Remainder Theorem, even composite modulus, Quadratic Congruence*

1. INTRODUCTION

Many mathematicians tried to solve the quadratic congruence of the composite modulus. They proposed a method to find the solutions by using only Chinese Remainder Theorem [1]. Even then many more is remained to do. No formulation is found in the literature. Here, a special type of quadratic congruence of even composite modulus as a product of two odd primes & eight is considered. The formula for solutions is established & tested true by solving examples.

Here we consider the congruence

$$x^2 \equiv a \ (mod\ 8pq) \qquad (1)$$

2. NEED OF RESEARCH

The congruence under consideration can be solved 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. Here lies the need for a research for a formulation. I tried my best to formulate the congruence and the effort is presented in this paper.

3. PROBLEM-STATEMENT

To formulate the solutions of a standard quadratic congruence of the composite modulus of the type: $x^2 \equiv a(mod\ 8pq)$, p & q being different odd positive primes.

4. DISCUSSION OF THE EXISTED METHOD [1]

Consider the congruence (1).

It can be split into three congruence

$$x^2 \equiv a \ (mod\ 8)\ ; \ x^2 \equiv a \ (mod\ p)\ ; \ \ x^2 \equiv a \ (mod\ q)$$

This standard quadratic congruence can be solved separately to get solutions:

$$x \equiv \ 1, 3, 5, 7 \ \ (mod\ 8) \ \text{ if } a \equiv 1 \ (mod\ 8);$$ (<u>otherwise, has only two solutions</u>)

$$x \equiv \ \ d, e \ \ (mod\ p)\ ; \ x \equiv \ \ f, g \ \ (mod\ q)$$

As "every solvable quadratic congruence of positive odd prime modulus has exactly two solutions [2].

Solving these**, sixteen (otherwise <u>eight</u>) solutions** can be obtained using **Chinese Remainder Theorem.**

4.1 Demerits of the proposed method

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

4.2 Discussion of the Proposed method (Formulation)

Consider the congruence (1).

If $a = b^2$, then the congruence becomes: $x^2 \equiv b^2 (mod\ 8pq)$

Two obvious solutions of the congruence are: $x \equiv 8pq \pm b\ (mod\ 8pq)$

$$i.e.\ \ x \equiv 8pq + b, \quad 8pq - b\ \ (mod\ 2pq)\ \ i.e.\ x \equiv b,\ \ 8pq - b\ \ (mod\ \ 8pq)$$

Thus, b is a solution of $x^2 \equiv b^2 (mod\ 8pq)$.

If $a \neq b^2$, we add "$k.8pq$" to a to get $a + k.8pq\ with\ such\ \ k\ such\ that\ a + k.8pq = b^2$[3]

Then, the two obvious solutions are as before.

Two other obvious solutions are $x \equiv 4pq \pm b\ \ (mod\ 8pq)$

Because, $x^2 = (4pq \pm b)^2 = 16p^2q^2 \pm 8pqb + b^2 = 8pq(2pq \pm b) + b^2 \equiv b^2\ (mod\ 8pq)$

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

We have
$$\begin{aligned} x^2 &= \{\pm(2pk \pm b)\}^2 \\ &= 4p^2k^2 \pm 4pkb + b^2 \\ &= b^2 + 4pk(pk \pm b) \\ &= b^2 + 4pk(2qt) \\ &= b^2 + t(8pq)\ ,\ \text{if } k(pk\ \pm b) = 2qt, for\ an\ integer\ t. \\ &\equiv b^2\ \ (mod\ 8pq),\ \text{if } k(pk\ \pm b) = 2qt. \end{aligned}$$

Thus, the other solutions are given by:

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

Therefore, the congruence $x^2 \equiv b^2 (mod\ 8pq)$ always has four obvious solutions $x \equiv 8pq \pm b; 4pq \pm b\ (mod\ 8pq)$; and other four solutions: $x \equiv \pm(2pk \pm b)(mod\ 8pq)$, $When\ k(pk \pm b) = 2qt, for\ positive\ integer\ t.$

4.3 Illustration of the method by an Example

Consider the congruence: $x^2 \equiv 4 = 2^2\ (mod\ 120)$.

Here, $120 = 8.3.5\ with\ p = 5, q = 3; a \neq 1\ (mod\ 8)$

Thus, the congruence is of the type: $x^2 \equiv a^2\ (mod\ 8pq)$. $\boldsymbol{It\ has\ eight\ solutions.}$

- **Solution by existed Method**:

Consider $x^2 \equiv 4\ (mod\ 120)$.

We see that $120 = 8.3.5$

So, the congruence can be explit into the following congruence:

$$x^2 \equiv 4\ (mod\ 8)\ i.e.\ x^2 \equiv 4\ (mod\ 8)\ giving\ solutions\ \ x \equiv 2, 6\ (mod\ 8)$$
$$x^2 \equiv 4\ (mod\ 3)\ i.e.\ x^2 \equiv 1\ \ (mod\ 3)\ giving\ solutions\ x \equiv 1, 2\ (mod\ 3)$$
$$x^2 \equiv 4\ (mod\ 5)\ i.e.\ x^2 \equiv 4\ (mod\ 5)\ giving\ solutions\ x \equiv 2, 3\ \ (mod\ 5)$$

We consider the congruence for Chinese Remainder Theorem.

Thus, we have $x \equiv 2, 6\ (mod\ 8); \equiv 1, 2\ (mod\ 3)\ ; x \equiv 2, 3\ (mod\ 5)$.

So, $a_1 = 2\ or\ 6;\ \ a_2 = 1\ \ or\ \ 2\ ;\ \ \ a_3 = 2\ \ or\ \ 5;\ \ m_1 = 8;\ \ \ m_2 = 3;\ \ m_3 = 5.$

We have, $M = [8, 3, 5] = 120; M_1 = 15;\ \ \ M_2 = 40;\ \ \ M_3 = 24.$

Now, $M_1x \equiv 1\ (mod\ m_1)\ \ \ i.e. 15x \equiv 1\ (mod\ 8)\ \ i.e.\ \ x \equiv 7\ (mod\ 8) giving\ x_1 = 7.$

$$M_2x \equiv 1\ (mod\ m_2)\ \ \ i.e. 40x \equiv 1\ (mod\ 3)\ \ \ i.e.\ \ x \equiv 1\ (mod\ 3) giving\ x_2 = 1.$$
$$M_3x \equiv 1\ (mod\ m_3)\ \ \ i.e. 24x \equiv 1\ (mod\ 5)\ \ \ i.e.\ \ x \equiv 4\ (mod\ 5) giving\ x_3 = 4.$$

The common solutions are given by $x_0 \equiv a_1M_1x_1 + a_2M_2x_2 + a_3M_3x_3 (mod\ M)$.

Putting values one must get $x_0 \equiv 2, 22, 38, 58, 62, 82, 98, 118 (mod\ 120)$

[Calculations not shown] ***Isn't a time-consuming method?***

- **Solution by Formulation**:

Consider $x^2 \equiv 4\ (mod\ 120)$.

It can be written as: $x^2 \equiv 4 = 2^2 (mod\ 120)$ giving solutions $x \equiv 8pq \pm b\ (mod\ 8pq)$

$$i.e.\ \ x \equiv 120 \pm 2\ (mod\ 120)$$
$$\boldsymbol{i.e.\ \ x \equiv 2, 118\ (mod\ 120)}$$

Therefore, $b = 2$ is a solution.

Also, the other two solutions are $x \equiv 4pq \pm b\ (mod\ 8pq)$

$$\equiv 60 \pm 2\ (mod\ 120)$$
$$\equiv \boldsymbol{58, 62\ (mod\ 120)}$$

Other solutions are given by $x \equiv \pm(2pk \pm b)(mod\ 8pq),\ if\ k(pk \pm b) = 2qt, for\ some\ integer\ t.$
So, $x \equiv \pm(2.5.k \pm 2)(mod\ 120),\ if\ k(5k \pm 2) = 6t$
$i.e.\ x \equiv \pm(10k \pm 2)\ (mod\ 120)\ if k(5k \pm 2) = 6t.$
But $2.(5.2 + 2) = 24 = 6.4\ giving\ k = 2$

Thus, the two solutions are $x \equiv \pm(10.2 + 2) = \pm 22\ (mod\ 120)$
$$\boldsymbol{i.e. x \equiv 22, 98\ (mod\ 120)}.$$
Also, $4(5.4 - 2) = 72 = 6.12\ giving\ k = 4$
Thus, the two solutions are $x \equiv \pm(10.4 - 2) = \pm 38\ (mod\ 120)$
$$\boldsymbol{i.e. x \equiv 38, 82\ (mod\ 120)}.$$

Thus all the solutions are $\boldsymbol{x \equiv 2, 118; 22, 98; 38, 82; 62, 58\ (mod\ 120)}$
These are the same solutions obtained as in above by existing method but easily and in comparatively less time.
Let us consider another example: $x^2 \equiv 1\ (mod\ 280)$.
Now, $280 = 8.5.7\ \ with\ \ p = 7, q = 5;\ \ a \equiv 1(mod\ 8)$.
It is also of the type $x^2 \equiv b^2\ (mod\ 8pq)\ with\ b = 1$ **& has sixteen solutions.**
Four obvious solutions are $x \equiv 8pq \pm b;\ 4pq \pm b$
$\equiv 280 \pm 1; 140 \pm 1.$
$\equiv \boldsymbol{1, 279;\ 139, 141\ (mod\ 280)}$

Other possible solutions are given by:
$x \equiv \pm(2pk \pm b)$ (mod 8pq), if k.(p k $\pm b) = 2qt$ for some positive integer t.
$i.e. x \equiv \pm(2.7.k \pm 1)(mod\ 280)$, if k (7k$\pm$1) $= 2.5.t$
$i.e. x \equiv \pm(14k \pm 1)(mod\ 280)$, if k (7k$\pm$1) $= 10t$

For $k = 2, we\ have\ 2.(7.2 + 1) = 30 = 10.3$
Thus the other two solutions are $x \equiv \pm 14.2 + 1) \equiv \pm 29 \equiv \boldsymbol{29, 251\ (mod\ 280)}$.
Also for $k = 3,\ we\ have\ \ 3.(7.3 - 1) = 3.(21 - 1) = 60 = 10.6$
So, other the two solutions are $x \equiv \pm 14.3 - 1) \equiv \pm 41 \equiv \boldsymbol{41, 239(mod\ 280)}$.
Also for $k = 5,\ we\ have\ \ 5.(7.5 + 1) = 5.(35 + 1) = 5.36 = 180 = 10.18$
So, the two solutions are $x \equiv \pm(14.5 + 1) \equiv \pm 71 \equiv \boldsymbol{71, 209(mod\ 280)}$.
Also for $k = 5,\ we\ have\ 5.(7.5 - 1) = 5.(35 - 1) = 5.34 = 170 = 10.17$
So, the two solutions are $x \equiv \pm(14.5 - 1) \equiv \pm 69 \equiv \boldsymbol{69, 211(mod\ 280)}$.
Also for $k = 7,\ we\ have\ 7.(7.7 + 1) = 7.(49 + 1) = 7.50 = 350 = 10.35$
So, the two solutions are $x \equiv \pm(14.7 + 1) \equiv \pm 99 \equiv \boldsymbol{99, 181(mod\ 280)}$.
Also for $k = 8,\ we\ have\ 8.(7.8 - 1) = 8.(56 - 1) = 8.55 = 440 = 10.44$
So, the two solutions are $x \equiv \pm(14. -1) \equiv \pm 111 \equiv \boldsymbol{111, 169(mod\ 280)}$.
Thus all the sixteen solutions are: $\boldsymbol{x \equiv 1, 279, 139, 141, 29, 251, 41, 239, 71, 209, 69, 211, 99, 181, 111, 169\ (mod\ 280)}$**.**

5. CONCLUSION

Thus a simpler, less time-consuming new method of finding solutions (directly) of a solvable quadratic congruence of the even composite modulus of the type:
$$x^2 \equiv a\ (mod\ 8pq)$$
$with\ p, q\ are\ different\ odd\ primes$, is developed.
The solutions are given by $x \equiv 8pq \pm b; 4pq \pm b;\ \pm(2pk \pm b)$ (mod 8pq), if k.(p k $\pm b) = 2qt$, for some positive integer t.

6. MERIT OF THE PAPER

It is seen that correct solutions are obtained by using the established formula in a less effort and in a short time. No need to use the Chinese Remainder Theorem. ***This is the merit of this paper.***

7. REFERENCES

[1] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), *"An Introduction to the Theory of Numbers"*, 5/e, Wiley India (Pvt) Ltd.
[2] Koshy Thomas, *Elementary Number Theory with Applications*, 2/e, 2007, Academic Press.
[3] ROY B. M., *Discrete Mathematics & Number Theory, First edition*, 2016, Das Ganu Prakashan, Nagpur(INDIA).

