© 2018 IJRTI | Volume 3, Issue 5 | ISSN: 2456-3315

Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime –power integer & two or four

Prof. B M Roy

Head & Assistant Professor
Department of Mathematics,
Jagat Arts, Commerce & I H P Science College, Goregaon (GONDIA)
Affiliated to R T M Nagpur University, M. S.), INDIA

***ABSTRACT*: In this paper, some classes of standard quadratic congruence of composite modulus is formulated when modulus is a product of prime-power integers by two & four. The formulae are tested by giving examples. No need to use Chinese Remainder Theorem. This is the merit of the paper.**

***KEYWORDS*: Chinese Remainder Theorem, composite modulus, quadratic congruence, prime-power modulus.**

INTRODUCTION

In the literature of mathematics, only a method of solving these above said congruence by the use of the Chinese Remainder Theorem is mentioned. It takes a long time to find all the solutions. This struck my mind & I mentally get decided to establish a formula for all the solutions. I worked on the matter and I succeed (I think so).

Let us consider those standard quadratic congruence of the type

Case –I: $x^2 \equiv a^2 \pmod{2p^n}$, n ≥1.
Case-II: $x^2 \equiv a^2 \pmod{4p^n}$, n >≥.

where p is a prime positive integer with an index n which is a positive integer. Here modulus is a composite number which is a product of a prime and two & four.

NEED OF THIS RESEARCH

In the literature, only a method to find all the solutions are present, using Chinese remainder theorem; no direct formulae are found. No attempt had been taken. This is the main reason, I have selected the topic for my research to get a direct formula for solutions. **Here is the merit of my research.**

PROBLEM STATEMENT:

The congruence in case-I has only two solutions while the congruence in case-II has four solutions [1]. My aim is to find all these solutions by establishing formulae for solutions offollowing congruence:
Case –I: $x^2 \equiv a^2 \pmod{2p^n}$, n ≥1.
Case-II: $x^2 \equiv a^2 \pmod{4p^n}$, n >≥.

ANALYSIS & RESULT:

We consider these congruence stated above, one by one in the following discussion.

Case-I: Let us consider the congruence $x^2 \equiv a^2 \pmod{2p^n}$, where p is a prime integer.

For $x = 2p^n \pm a$, we have $x^2 = (2p^n \pm a)^2$

$$= 4p^{2n} \pm 4p^n a + a^2$$

$$= 4p^n(p^n \pm a) + a^2$$

$$= 4p^n.t + a^2, \text{ for an integer t,}$$

$$\equiv a^2 \pmod{4p^n}.$$

The congruence must not have any other solution.

Thus, it is proved that this congruence has only two solutions given by $x \equiv 2p^n \pm a \pmod{2p^n}$.

Let us consider an example of this type as below:

Consider $x^2 \equiv 41 \pmod{50}$. Here $50 = 2.25 = 2.5^2$ so $p = 5$.

It can be written as $x^2 \equiv 41 \pmod{50}$

$$\equiv 1 + 8.50 \pmod{50}$$

$$\equiv 441 \pmod{50}$$

$$\equiv 21^2 \pmod{2.5^2}$$

It is of the type $x^2 \equiv a^2 \pmod{2p^n}$

It has only two solutions.

The two solutions are $x \equiv 2p^n \pm a \equiv 2.5^2 \pm 21 = 50 \pm 21 = \mathbf{21, 50 - 21} \ (\mathbf{mod\ 50})$.

Thus the congruence has two solutions $\mathbf{x \equiv 21,\ 29\ (mod\ 50)}$.

It is also checked that it has no other solutions.

Case-II: Let us consider the congruence $x^2 \equiv a^2 \pmod{4p^n}$ where p is an odd prime integer.

We see that $x \equiv \pm a \pmod{4p^n} \equiv 4p^n \pm a \pmod{4p^n}$ are the two obvious solutions of the congruence.

Let $x = (2p^n \pm a)$. Then, as in case-I

$$x^2 = (2p^n \pm a)^2$$

$$\equiv a^2 \pmod{4p^n}$$

Thus, we see that $x = (2p^n \pm a) \pmod{4p^n}$ are the two other solutions.

Therefore, we can conclude that the solutions are:

$x \equiv 4p^n \pm a;\ 2p^n \pm a \pmod{4p^n}$

But the congruence have only four solutions given by $x \equiv 4p^n \pm a;\ 2p^n \pm a \pmod{4p^n}$.

It has no other solutions.

Consider $x^2 \equiv 125 \pmod{500}$ Here $500 = 4.125 = 4.5^3$ so $p = 5$.

It can be written as $x^2 \equiv 125 \pmod{500}$

$$\equiv 125 + 1.500 \pmod{500}$$

$$\equiv 625 \pmod{500}$$

$$\equiv 25^2 \pmod{4.5^3}$$

It is of the type $x^2 \equiv a^2 \pmod{4p^n}$

It has only four solutions.

The two solutions are $x \equiv 4p^n \pm a; 2p^n \pm a \pmod{4p^n}$

$$\equiv 4.5^3 \pm 25; 2.5^3 \pm 25 = \mathbf{500 \pm 25;\ 250 \pm 25\ (mod\ 500)}.$$

Thus the congruence has four solutions $\mathbf{x \equiv 25, 500 - 25;\ 250 - 25, 250 + 25\ (mod\ 500)}$

$$\mathbf{\equiv 25, 475;\ 225, 275\ (mod\ 500)}.$$

It is also checked that it has no other solutions.

CONCLUSION:

Thus we have formulated the said congruence and the result is also verified by siting many examples.We have seen that the congruence $x^2 \equiv a^2 \pmod{2p^n}$ has two solutions. The congruence $x^2 \equiv a^2 \pmod{4p^n}$ has four solutions.

MERIT OF THE PAPER:

In the literature, such types of quadratic congruence are solved by using Chinese remainder theorem but no formula was found in the literature. First-time, formulae are established to find the solutions of the congruence correctly. It takes less time than the use of the said theorem.

Here lies the merit of this paper.

REFERENCE:

[1] Niven I., Zuckerman H. S., Montgomery H. L., An Introduction to the Theory of Numbers, 5/e, Wiley India Edition, 2008.
[2] Koshy T., Elementary Number Theory with Applications, 2/e, Academic press, India, 2009.
[3] Roy B. M., Discrete Mathematics and Number Theory, 1/e, Das Ganu Prakashan, Nagpur, 2016.