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 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 of following congruence:

Case –I: \( x^2 \equiv a^2 \pmod{2^p} \), \( n \geq 1 \).
Case-II: \( x^2 \equiv a^2 \pmod{4^p} \), \( n \geq 2 \).

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.

ANALYSIS & RESULT:

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

Case-I: Let us consider the congruence \( x^2 \equiv a^2 \pmod{2^p} \), where \( p \) is a prime integer.
For \( x = 2^p \pm a \), we have \( x^2 = (2^p \pm a)^2 \)

\[
= 4p^2 \pm 4^p a + a^2
= 4^p (p^2 \pm a) + a^2
= 4p^n t + a^2, \text{ for an integer } t,
\equiv a^2 \pmod{4^p}.
\]

The congruence must not have any other solution.

Thus, it is proved that this congruence has only two solutions given by \( x \equiv 2^p \pm a \pmod{2^p} \).
Let us consider an example of this type as below:

Consider \( x^2 \equiv 41 \pmod{50} \). Here \( 50 = 2 \cdot 25 = 2 \cdot 5^2 \) so \( p = 5 \).

It can be written as \( x^2 \equiv 41 \pmod{50} \)
\[ \equiv 1 + 8 \cdot 50 \pmod{50} \]
\[ \equiv 441 \pmod{50} \]
\[ \equiv 21^2 \pmod{2 \cdot 5^2} \]

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

It has only two solutions. The two solutions are \( x \equiv 2p^n \pm a \equiv 2 \cdot 5^2 \pm 21 = 21, 50 - 21 (\pmod{50}) \).

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

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 \( x \equiv \pm a \pmod{4p^n} \) is 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 \( 500 = 4 \cdot 125 = 4 \cdot 5^3 \) so \( p = 5 \).

It can be written as \( x^2 \equiv 125 \pmod{500} \)
\[ \equiv 125 + 1.500 \pmod{500} \]
\[ \equiv 625 \pmod{500} \]
\[ \equiv 25^2 \pmod{4 \cdot 5^3} \]

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 \cdot 5^3 \pm 25; \ 2 \cdot 5^3 \pm 25 = 500 \pm 25; \ 250 \pm 25 \pmod{500} \).

Thus the congruence has four solutions \( x \equiv 25, 500 - 25; \ 250 - 25, 250 + 25 \pmod{500} \)
\[ \equiv 25, 475; \ 225, 275 \pmod{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:

