Formulation of Solutions of a Special Class of Standard Quadratic Congruence of Even Composite Modulus

Prof. B. M. Roy

Head, Dept. of Mathematics
Jagat Arts, commerce & I H P Science College, Goregaon (Gondia), M. S., India.
Affiliated to R T M Nagpur University, Nagpur.

***ABSTRACT*: In this paper, solutions of a special class of standard quadratic congruence of even composite modulus are formulated. The method is described and illustrated by giving suitable examples.**

The formula is verified true. No need of Chinese Remainder Theorem.

Keywords & phrases: Composite modulus, quadratic-congruence, Chinese Remainder Theorem.

INTRODUCTION

Congruence plays an important role in Number Theory, and without it, the said theory becomes a juiceless fruit. Congruence is written as $x \equiv a \pmod m$ with a, m integers and x is unknown. The values of x satisfying the congruence are called its solutions.

$x^2 \equiv a \pmod m$ is a standard quadratic congruence. Methods of finding solutions are found in the literature of mathematics**.** The use of Chinese Remainder Theorem is the only method suggested **but no formulation is found**. Here, lies the need of my research. In this paper, I have considered a special type of standard quadratic congruence of even composite modulus and tried my best to formulate the solutions.

PROBLEM STATEMENT

Consider a class of standard quadratic congruence of even composite modulus of the type:

$$x^2 \equiv b^2 (\text{mod } 2^m p^n),\ \ m \geq 4, n \geq 1 \text{ integers};\ p \text{ is odd prime integer.}$$

Formulation of the solutions is the aim of the paper.

ANALYSIS & RESULT (Formulation of Solution)

Given congruence is $x^2 \equiv b^2 (\text{mod } 2^m p^n)$, p odd prime, $m \geq 4, n \geq 1$.Solutions in different cases are discussed here.

Case-I: Let b be an even positive integer.

By rule, this congruence must have in total 8 incongruent solutions [2]

It is seen that $x \equiv \pm b \ (\text{mod } 2^m p^n)$ are the two obvious solutions and are written as

$$x \equiv 2^m p^n \pm b \ (\text{mod } 2^m p^n)$$

i.e. $\mathbf{x \equiv b,\ 2^m p^n - b\ (mod\ 2^m p^n)}$**…………………………………………………..(A)**

are the two obvious solutions.

If $x = 2^{m-1}p^n \pm b$, then $x^2 = (2^{m-1}p^n \pm b)^2$

$$= 2^{2m-2}p^{2n} \pm 2^m p^n b + b^2$$

$$= b^2 + 2^m p^n (2^{m-2}p^n \pm b)$$

$$\equiv b^2 (\text{mod } 2^m p^n).$$

Thus, $\mathbf{x \equiv 2^{m-1}p^n \pm b\ \ (mod\ 2^m p^n)}$ **……………………………………………………..(B)**

are the two other solutions of $x^2 \equiv b^2 \ (\text{mod } 2^m p^n)$.

If $x = \pm(2^{m-2}p^n \pm b)$, then $x^2 = (2^{m-2}p^n \pm b)^2$

$$= 2^{2m-4}p^{2n} \pm 2^{m-1}p^n b + b^2$$

$$= b^2 + 2^{m-1}p^n(2^{m-3}p^n \pm b)$$

$$= b^2 + 2^{m-1}p^n(2t), \text{ as b is an even integer.}$$

$$\equiv b^2 \pmod{2^m p^n}.$$

Thus, $x \equiv \pm(2^{m-2}p^n \pm b) \pmod{2^m p^n}$ are the four other solutions ……………………(C)

Therefore, all the eight solutions are given by

$x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b\ \&\ x \equiv \pm(2^{m-2}p^n \pm b) \pmod{2^m p^n}$ ….…………………(D)

Case-II: Let b be an odd positive integer.

Then as per (A) & (B), four solutions are

$$x \equiv 2^m p^n \pm b;\quad 2^{m-1}p^n \pm b \pmod{2^m p^n}.$$

Formula (C) does not hold as b is not even integer.

So, the remaining four solutions will be obtained by some other way.

Now, if $x = \pm(2kp^n \pm b$, then $x^2 = (2kp^n \pm b)^2$

$$= 4k^2p^{2n} \pm 4kp^n b + b^2$$

$$= b^2 + 4p^n.k(kp^n \pm b)$$

$$= b^2 + 4p^n(2^{m-2}t)\ ;\ \text{if } (kp^n \pm b).k = 2^{m-2}t$$
$$= b^2 + 2^m p^n.t \text{ for an integer t.}$$

$$\equiv b^2 \pmod{2^m p^n}$$

Thus, $\mathbf{x \equiv \pm(2kp^n \pm b)(mod\ 2^m p^n)}$ **if** $\mathbf{(kp^n \pm b).k = 2^{m-2}t}$ **……………………..(E)**

are the four remaining solutions for some k.

Therefore, all the four pairs of solutions are:

$x \equiv 2^m p^n \pm b;\ \ 2^{m-1}p^n \pm b;\ \pm(2kp^n \pm b) \pmod{2^m p^n}$, b odd & k integers ….……..(F)

Therefore, we can have the summery as under:

The congruence $x^2 \equiv b^2 \pmod{2^m p^n}$ with $m \geq 4, n \geq 1$; p odd prime integer has the solutions

Case-I: $x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b\ \&\ x \equiv \pm(2^{m-2}p^n \pm b) \pmod{2^m p^n}$, if b is even integer.

Case-II: $x \equiv 2^m p^n \pm b;\ \ 2^{m-1}p^n \pm b \pmod{2^m p^n}\ \&\ x \equiv \pm(2kp^n \pm b) \pmod{2^m p^n}$,

if b is an odd integer with $(kp^n \pm b).k = 2^{m-2}.t$

Illustration of the method by suitable examples

Let us consider the congruence $x^2 \equiv 16 \pmod{320}$.

As $320 = 64.5 = 2^6.5$, the congruence becomes $x^2 \equiv 4^2 \pmod{2^6.5}$.

It is of the type: $x^2 \equiv b^2 \pmod{2^m p^n}$, p odd prime with $n = 1, m = 6, p = 5, b = 4$ with b even integer.

It has four pairs of solutions. These solutions are given by the formulae:

$$x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b\ ;\ \ \pm(2^{m-2}p^n \pm b) \pmod{2^m p^n}.$$

$$\equiv 2^6.5^1 \pm 4;\ 2^{6-1}.5^1 \pm 4\ ;\ \ \pm(2^{6-2}.5^1 \pm 4) \pmod{2^6.5^1}.$$

$$\text{i.e. } x \equiv 320 \pm 4; 160 \pm 4; \pm(80 \pm 4) \pmod{320}$$

$$\text{i.e. } x \equiv 4, 316; 156, 164; 76, 84; 244, 236 \pmod{320}$$

Thus, all the 8 solutions are $\mathbf{x \equiv 4, 76, 84, 156, 164, 236, 244, 316\ (mod\ 320)}$.

Let us consider the congruence $x^2 \equiv 49 \pmod{320}$.

As $320 = 64.5 = 2^6.5$, the congruence becomes $x^2 \equiv 7^2 \pmod{2^6.5}$.

It is of the type: $x^2 \equiv b^2 \pmod{2^m p^n}$, p odd prime with $n = 1, m = 6, p = 5, b = 7$

with b odd integer.

It has four pairs of solutions. These solutions are given by the formulae:

$$x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b;\ \pm(2kp^n \pm b)\ (\text{mod } 2^m p^n).$$

$$\equiv 2^6.5^1 \pm 7;\ 2^{6-1}.5^1 \pm 7;\ \pm(2k.5^1 \pm 7)\ (\text{mod } 2^6.5^1).$$

i.e. $x \equiv 320 \pm 7; 160 \pm 7; \pm(10k \pm 7)\ (\text{mod } 320)$

i.e. $x \equiv 320 \pm 7; 160 \pm 7; \pm(50+7);\ \pm(110-7)(\text{mod } 320)$ for $k = 5\ \&\ k = 11$.

i.e. $x \equiv 7, 313; 153, 167; 57, 263; 103, 217\ (\text{mod } 320)$

Thus, all the 8 solutions are $x \equiv 4, 57, 103, 153, 167, 217, 263, 313\ (\text{mod } 320)$.

Let us consider the congruence $x^2 \equiv 9\ (\text{mod } 432)$.

As $432 = 16.27 = 2^4.3^3$, the congruence becomes $x^2 \equiv 9\ (\text{mod } 2^4.3^3)$.

It is of the type: $x^2 \equiv b^2(\text{mod } 2^m p^n)$, p odd prime with $n = 3, m = 4, p = 3, b = 3$

with b odd integer.

It has four pairs of solutions. These solutions are given by the formulae:

$$\mathbf{x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b\ \&\ \pm(2kp^n \pm b)(mod\ 2^m p^n),\qquad if\ (kp^n \pm b).k = 2^{m-2}.t}$$

$$\equiv 2^4.3^3 \pm 3;\ 2^{4-1}.3^3 \pm 3;\ \pm(2k.3^3 \pm 3)(\text{mod } 2^4.3^3)\ \text{ if } (k.3^3 \pm 3).k = 2^2.t$$

i.e. $x \equiv 432 \pm 3; 216 \pm 3; \pm(54k \pm 3)(\text{mod } 432)$ if $(27k \pm 3).k = 4t$

i.e. $x \equiv 3, 429; 213, 219; \pm(54-3);\ \pm(162+3)(\text{mod } 432)$ for $k = 1\ \&\ k = 3$.

i.e. $x \equiv 3, 429; 213, 219;\ \pm 51, \pm 165\ (\text{mod } 432)$

i.e. $x \equiv 3, 429; 213, 219; 51, 381; 165, 267\ (\text{mod } 432)$

Thus, all the 8 solutions are $x \equiv 3, 51, 165, 213, 219, 267, 381, 429\ (\text{mod } 432)$.

Let us consider one more example as per our need**:**

Let us consider the congruence $x^2 \equiv 9\ (\text{mod}96)$.

As $96 = 32.3 = 2^5.3$, the congruence becomes $x^2 \equiv 9\ (\text{mod } 2^5.3^1)$.

It is of the type: $x^2 \equiv b^2(\text{mod } 2^m p^n)$, p odd prime with $n = 1, m = 5, p = 3, b = 3$

with b odd integer.

It has four pairs of solutions. These solutions are given by the formulae:

$$\mathbf{x \equiv 2^m p^n \pm b;\ 2^{m-1}p^n \pm b\ \&\ \pm(2kp^n \pm b)(mod\ 2^m p^n),\qquad if\ (kp^n \pm b).k = 2^{m-2}.t}$$

i.e. $x \equiv 96\pm 3; 48 \pm 3; \&\ \pm(2.k.3 \pm 3)\ (\text{ mod } 96)$, if $(k.3 \pm 3).k = 2^3 t$

i.e. $x \equiv 3, 93; 45, 51; \pm(6k \pm 3)\ (\text{mod } 96)$, if $(3k \pm 3).k = 8t$

i.e. $x \equiv 3, 93, 45, 51;\ \pm(6-3);\ \pm(42+3)\ (\text{mod } 96)$for $k = 1, 7$

i.e. $x \equiv 3,93,45, 51;\ \pm 3;\ \pm 45\ (\text{mod } 96)$

i.e. $x \equiv 3, 93; 45, 51\ (\text{mod } 96)$.

Thus it has only four solutions.

CONCLUSION

In this paper, some special classes of congruence are formulated and method is illustrated by giving four examples, considering different conditions.

REFERENCE

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.