Formulation of Standard Quadratic Congruence of Composite Modulus as a Product of Prime-power Integer and Eight

Prof. B. M. Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon (Gondia), M. S. India.
Pin: 441801
Affiliated to R T M Nagpur University, Nagpur

***ABSTRACT*: In this paper, solutions of a special type of quadratic congruence of even composite modulus are formulated. The method is described and illustrated by giving suitable examples. Formulation of solutions is the merit of the paper. No need to use Chinese Remainder Theorem.**

Keywords & phrases: Even composite modulus, Standard quadratic-congruence, Prime- power integer.

INTRODUCTION

Quadratic congruence is a part of Mathematics (Number Theory) and Number Theory remains incomplete without the concept of congruence. Quadratic congruence is a part of it. Many ancient and modern mathematicians serve this branch of mathematics with great interest. They all made problems easier by discovering some methods of finding solutions of the congruence and they succeed. But no attempt had been made to formulate the congruence.

NEED OF RESEARCH

In the literature of Mathematics, a popular method, known as "Chinese Remainder Theorem" was described to solve quadratic congruence of composite modulus. But it is found a time-consuming, complicated method; sometimes, it becomes a boring task to use the said method. Thus, a simple, easy method was in demand of readers. For this sake, I made an effort to lessen all the above inconvenience and I succeed (I think so) and my effort is presented in this paper.

PROBLEM STATEMENT

To formulate the standard quadratic congruence of even composite modulus of the type:

$x^2 \equiv a \pmod{8p^n}$, p odd prime, $n \geq 1$. ………………………..(1)

ANALYSIS & RESULT (Formulation)

The congruence (1) must have at most eight solutions but at least two solutions [2].

We formulate these solutions.

If $a \equiv b^2$, then two obvious solutions are $\mathbf{x \equiv \pm b \equiv 8p^n \pm b \ (mod\ 8p^n)}$

If $a \neq b^2$, then adding k.8p^n to a, we get $a + k.8p^n = b^2$, then we get the above two solutions for some integer k [3].

If we consider $x = 4p^n \pm b$, then $x^2 = (4p^n \pm b)^2$

$$= 16p^{2n} \pm 8p^n b + b^2$$
$$= b^2 + 8p^n(2p^n \pm b)$$
$$\equiv b^2 \pmod{8p^n}.$$

Thus, $\mathbf{x \equiv 4p^n \pm b\ \ (mod\ 8p^n)}$ **are the two other solutions of** $\mathbf{x^2 \equiv b^2\ (mod\ 8p^n)}$.

If we consider $x = \pm(2kp^n \pm b)$, then $x^2 = (2kp^n \pm b)^2$

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

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

$$= b^2 + 4p^n(2t),\ \text{if } k.(kp^n \pm b) = 2t, \text{for iteger } t.$$

$$= b^2 + 8p^n.t$$
$$\equiv b^2 (\text{mod } 8p^n).$$

Thus, $\mathbf{x \equiv \pm(2kp^n \pm b)\ \ (mod\ 8p^n)}$ **are the other solutions of** $\mathbf{x^2 \equiv b^2\ (mod\ 8p^n)}$.

Therefore, **all the solutions are:**

$$\mathbf{x \equiv 8p^n \pm b; 4p^n \pm b;\ \ \pm(\ 2kp^n \pm b)(mod\ 8p^n), if\ k.(kp^n \pm b) = 2t\ for\ an\ integer\ t}.$$

Examples to illustrate the method:

Let us consider the congruence $x^2 \equiv 97\ (\text{mod } 7688)$[1] [**koshy-2007; p-541]**

As $7688 = 8.961 = 8.31^2$, the congruence becomes $x^2 \equiv 97(\text{mod } 8.31^2)$.

$$\equiv 97 + 6.7688\ \ (\text{mod } 7688)$$
$$\equiv 46225\ \ (\text{mod } 7688)$$
$$\equiv 215^2\ (\text{mod}7688)$$

It is of the type:

$x^2 \equiv b^2(\text{mod } 8p^n)$, p odd prime, $n = 2, p = 31, b = 215$.

The four obvious solutions are given by

$$x \equiv 8p^n \pm b;\ 4p^n \pm b\ \ (\text{mod } 8p^n).$$
$$\text{i.e. } x \equiv 7688 \pm 215; 3844 \pm 215\ (\text{mod } 7688)$$
$$\mathbf{i.e.\ \ \ x \equiv 215, 7473; 3629, 4059(mod\ 7688)}$$

Other solutions are $x \equiv \pm(2kp^n \pm b)\ (\text{mod } 8p^n)$ if $k.(kp^n \pm b) = 2t$, for integer t.

$$\equiv \pm(2kp^2 \pm b)(\text{mod } 8p^2),\ \text{ if } k(kp^2 \pm b) = 2t$$
$$\equiv \pm(2k.31^2 \pm 215)\ \ (\text{mod } 8.31^2),\ \ \text{if } k(k.31^2 \pm 215) = 2t$$
$$\equiv \pm(1922k \pm 215)\ \ (\text{mod } 7688),\ \ \text{if } k(961k \pm 215) = 2t$$

Now for $k = 1$, we have $1.(961.1 + 215) = 1176 = 2.588$

Then solutions are $x \equiv \pm(1922.1 + 215) = \pm 2137 = \mathbf{2137, 5551}$

Also for $k = 1$, we have $1.(961.1 - 215) = 746 = 2.373$

Then solutions are $x \equiv \pm(1922.1 - 215) = \pm 1707 = \mathbf{1707, 5981}$

Thus other solutions are x ≡2137, 5551; 1707, 5981 (mod 7688)

Therefore all the required eight solutions are $\mathbf{x \equiv 215, 7473; 3629, 4059; 2137, 5551;\ 1707, 5981\ \ (mod\ 7688)}$

Let us consider one more congruence $x^2 \equiv 16\ (\text{mod } 200)$.

As $200 = 8.25 = 8.5^2$, the congruence becomes $x^2 \equiv 4^2(\text{mod } 8.5^2)$.

It is of the type: $x^2 \equiv b^2(\text{mod } 8p^n)$, p odd prime, $n = 2, p = 5, b = 4$.

Therefore, the four obvious solutions are given by the formula

$$x \equiv 8p^n \pm b; 4p^n \pm b\ (\text{mod } 8p^n).$$
$$\text{i.e. } x \equiv 200 \pm 4; 100 \pm 4\ \ (\text{mod } 200)$$
$$\mathbf{i.e.\ x \equiv 4, 196; 96, 104\ (mod\ 200)}$$

Other solutions are given by $x \equiv \pm(2kp^2 \pm b)$, if $k.(kp^2 \pm b) = 2.t$ for integer t.

$$\text{i.e. } x \equiv \pm(2.k.25 \pm 4)\ \ \text{if } k.(25k \pm 4) = 2t$$
$$\text{i.e. } x \equiv \pm(50k \pm 4)\ \ \text{if } 2.(25.2 \pm 4) = 2.54 \text{ or } 2.46\ \ \text{for } k = 2.$$

$$\text{i.e.} \quad x \equiv \pm(50.2 \pm 4) = \pm 104 \ \& \ \pm 96 = \mathbf{104, 96, 96, 104}\ (\mathbf{mod\ 200}).$$

Thus, all the solutions are $\mathbf{x \equiv 4, 96, 104, 196\ \ (mod\ 200)}$.

This congruence has only four solutions.

Let us consider another example: $x^2 \equiv 20\ (\text{mod}\ 40)$. Here, 40=8.5 with p = 5, $n = 1$.

It is of the type $x^2 \equiv a\ (\text{mod}\ 8p)$.

It can be expressed as $x^2 \equiv 20\ (\text{mod}\ 40)$

$$\equiv 20 + 2.40\ (\text{mod}\ 40)$$

$$\equiv 100\ (\text{mod}\ 40)$$

$$\equiv 10^2\ \ (\text{mod}\ 40)$$

Thus, $x \equiv 40 \pm 10; 20 \pm 10\ (\text{mod}\ 40)$ i.e. $x \equiv 10,\ 40 - 10; 20 + 10, 20 - 10 \equiv \mathbf{10,\ 30; 30, 10\ (mod\ 40)}$ with b = 10.

Other solutions are given by $x \equiv \pm(2kp \pm b)$, if $k.(kp \pm b) = 2.t$ for integer t.

$$\text{i.e.}\ x \equiv \pm(2.k.5 \pm 10) \ \text{ if } \ k.(5k \pm 10) = 2t$$

$$\text{i.e.} \ \ x \equiv \pm(10k + 10) \ \text{ if } 2.(5.2 + 10) = 40 = 2.20 \ \text{ for } k = 2.$$

$$\text{i.e.} \quad x \equiv \pm(10.2 + 10) = \pm 30 = 30, 40 - 30 = \mathbf{30, 10\ (mod\ 40)}.$$

Thus, the congruence has only two solutions $\mathbf{x \equiv 10,\ 30\ \ (mod\ 40)}$.

CONCLUSION: In this paper, a special class of congruence is formulated and method is illustrated by giving three examples. The formula is tested true.

MERIT OF THE PAPER

Formulation is the merit of the paper. It saves time in finding solutions. No need to use Chinese Remainder Theorem.

References

[1] Koshy, Thomas; Elementary Number Theory with Applications; second edition, Academic press, 2007
[2] Niven, I.; Zuckerman H S.; Montgomery H L.; An Introduction to the Theory of Numbers; Fifth edition, WSE.
[3] Roy B. M., Discrete Mathematics & Number Theory, First edition, Das Ganu Prakashan, Nagpur, 2016.