RP-67: Formulation of a Class of Solvable Standard Quadratic Congruence of Even Composite Modulus

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, a class of solvable standard quadratic congruence of even composite modulus, is formulated. Formula is tested and found true, by solving different examples. The formula is proved time-saving and simple. It is now become possible to find all the solutions orally. No need to use Chinese Remainder Theorem. Formulation is the merit of the paper.

Keywords: Chinese Remainder Theorem, Quadratic congruence, Composite modulus.

INTRODUCTION

Number Theory is a special branch of mathematics and congruence is a very important chapter of it. The said chapter finds its application in the development of industries. This branch of mathematics is not much rich in its theory. It must be made popular among the readers /users. The author formulated a lot of standard quadratic congruence such as

$x^2 \equiv a^2 \pmod{4p}$ [5]

$x^2 \equiv a^2 \pmod{8p}$ [6]

Here is another congruence considered for formulation.

The congruence under consideration can be stated as: $x^2 \equiv a^2 \pmod{2^m p}, m \geq 4, p$ an odd positive prime integer.

EXISTED METHOD

The said congruence can be solved by splitting it into two separate congruence as:

$$x^2 \equiv a^2 \pmod{2^m} \& \; x^2 \equiv a^2 \pmod{p}.$$

The first congruence has four solutions while the second has only two solutions. Hence the original congruence may have $4.2 = 8$ solutions [4].

These eight common solutions are obtained using Chinese Remainder Theorem, popularly known as (CRT).

DEMERITS OF CRT

The theorem suffers from some demerits. These are:

(1) It takes a long time to find all the solutions.
(2) It is not a simple but complicated method.
(3) If prime factors of the modulus are comparatively large, then finding solutions of individual congruence are nearly impossible.

LITERATURE REVIEW

The author referred many books of Number Theory and found discussions on standard quadratic congruence of prime modulus [3] but no formulation of the solutions of the said congruence but a method, popularly known as CRT (Chinese Remainder Theorem) [1]. Solving the above two congruence and using Chinese Remainder Theorem, all the solutions can be obtained.

NEED OF RESEARCH

Use of Chinese Remainder Theorem is time-consuming and complicated. Readers always try to get rid of the use of the theorem. They always remain in search of a time-saving and simple method. Everyone prefers to use a method which is time-saving and

simple. Formulation is the only remedy or correct alternative for the readers. The author understood the need and tried his best to establish a formulation for the solutions of the said congruence and his effort is presented in this paper.

PROBLEM-STATEMENT

The solvable standard quadratic congruence under consideration of the type:

$x^2 \equiv a^2 \pmod{2^m.p}, m \geq 4$, p being an odd prime, is to formulate.

ANALISIS & RESULT

Consider the congruence under consideration:

$x^2 \equiv a^2 \pmod{2^m p}; m \geq 4$, p an odd prome.

The solutions can be formulated in two cases.

Case-I: Let a be an odd positive integer.

It is seen that $x = 2^m p \pm a \equiv a, 2^m p - a \pmod{2^m p}$ are the two obvious Solutions [2].

Also, for $x = 2^{m-1}.p \pm a$, $x^2 = (2^{m-1}p \pm a)^2$

$= 2^{2m-2}p^2 \pm 2.2^{m-1}p.a + a^2$

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

$\equiv a^2 \pmod{2^m p}$.

Thus, $x \equiv 2^{m-1}p \pm a \pmod{2^m p}$ are the other two solutions.

Therefore, it is seen that $x \equiv 2^m p \pm a;\ 2^{m-1}p \pm a \pmod{2^m p}$ are the four obvious solutions of the congruence.

Also, for $x = \pm(2kp \pm a)$, $x^2 = (2kp \pm a)^2$

$= 4k^2p^2 \pm 4kpa + a^2$

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

$= 2^2 p.2^{m-2}t + a^2$; if $k.(kp \pm a) = 2^{m-2}t$, **if a is odd.**

Thus the other four solutions are $x \equiv \pm(2kp \pm a) \pmod{2^m p}$, if $k(kp \pm a) = 2^{m-2}t$.

Therefore, for an odd a, the congruence has eight solutions.

Case-II: let a be an even positive integer.

Then as shown above, the congruence has four obvious solutions given by

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

But for even a, the next four solutions do not exist and the congruence has only four solutions.

Sometimes the congruence under consideration can be stated as: $x^2 \equiv b \pmod{2^m p}$.

It can be written as: $x^2 \equiv b \pmod{2^m p}$

$\equiv a + kp \pmod{2^m p}$ for some suitable positive integer k.

$\equiv a^2 \pmod{2^m p}$, if for such k, $b + kp = a^2$ [2].

This method sometimes becomes more lengthy and difficult. It may take hours / days.

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 9 \pmod{80}$.

It can be written as $x^2 \equiv 3^2 \pmod{16.5}$ i.e. $x^2 \equiv 3^2 \pmod{2^4.5}$

It is of the type $x^2 \equiv a^2 \pmod{2^m.p}$ with $m = 4, a = 3, p = 5$.

Such congruence has eight solutions as $a = 3$, an odd positive integer.

The four obvious solutions are given by $x \equiv 2^m.p \pm a;\ 2^{m-1}p \pm a \pmod{2^m p}$

$$\equiv 2^4.5 \pm 3;\ 2^{4-1}.5 \pm 3 \pmod{2^4.5}$$

$$\equiv 80 \pm 3; 40 \pm 3 \pmod{80}$$

$$\equiv 3, 77; 37, 43 \pmod{80}$$

Other four solutions are given by $x \equiv \pm(2kp \pm a)$, if $k.(kp \pm a) = 2^{m-2}.t$

$$\equiv \pm(10k \pm 3), \text{ if } k.(5k \pm 3) = 2^{4-2}.t$$

$$\equiv \pm(10k \pm 3), \text{ if } k.(5k \pm 3) = 4t.$$

It is seen that for $k = 1,\ 1.(5.1 + 3) = 8 = 4.2$

Thus the two solutions are $x \equiv \pm(10.1 + 3) \pmod{80} \equiv \pm 13 \equiv 13,67 \pmod{80}$.

Also for $k = 3,\ 3.(3.5 - 3) = 3.(15 - 3) = 36 = 4.9$

Thus the two other solutions are $x \equiv \pm(10.3 - 3) \equiv \pm 27 \equiv 27, 53 \pmod{80}$.

Therefore, all the eight solutions are $x \equiv 3, 77; 37, 43; 13, 67; 27, 53 \pmod{80}$.

Consider the congruence $x^2 \equiv 16 \pmod{80}$.

It can be written as $x^2 \equiv 4^2 \pmod{16.5}$ i.e. $x^2 \equiv 4^2 \pmod{2^4.5}$

It is of the type $x^2 \equiv a^2 \pmod{2^m.p}$ with $m = 4, a = 4, p = 5$.

Such congruence has only four obvious solutions as $a = 4$, an even positive integer.

The four obvious solutions are given by $x \equiv 2^m.p \pm a;\ 2^{m-1}p \pm a \pmod{2^m p}$

$$\equiv 2^4.5 \pm 4;\ 2^{4-1}.5 \pm 4 \pmod{2^4.5}$$

$$\equiv 80 \pm 4; 40 \pm 4 \pmod{80}$$

$$\equiv 4, 76; 36, 44 \pmod{80}.$$

Let us consider the congruence $x^2 \equiv 132 \pmod{544}$.

It can be written as $x^2 \equiv 132 \pmod{32.17}$ i.e. $x^2 \equiv 132 + 544 = 676 = 26^2 \pmod{2^5.17}$

with $m = 5, p = 17,\ a = 26$.

As a is even, it has only four solutions.

These are $x \equiv 544 \pm 26; 272 \pm 26 \equiv 26, 518; 246, 298 \pmod{544}$.

CONCLUSIONS

Thus, from the above study it is concluded that the standard solvable quadratic congruence of even composite modulus of the type: $x^2 \equiv a^2 \pmod{2^m.p}$ is formulated. If a is even positive integer, the congruence has only four solutions .On the other hand, for an odd a, the congruence has eight solutions. The formula is tested true.

MERIT OF THE PAPER

In this paper, the author presented his efforts to formulate the said congruence. Formula works efficiently. Formulation is the merit of the paper. It is time-saving and simple.

REFERENCE

[1] Burton D M, "Elementary Number Theory", 2/e, 2003, Universal Book Stall.
[2] Roy B M, "Discrete Mathematics & Number Theory", 1/e, Jan. 2016, Das Ganu Prakashan, Nagpur.
[3] Thomas Koshy, "Elementary Number Theory with Applications", 2/e (Indian print, 2009), Academic Press.
[4] Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "An Introduction to The Theory of Numbers", 5/e, Wiley India (Pvt) Ltd.
[5] Roy, B. M., Formulation of a class of Solvable standard quadratic congruence of even modulus, International Journal of Science & Engineering Development Research (IJSDR), Vol-03, Issue-11, Nov-18, ISSN: 2455-2631.
[6] Roy, B. M. , Formulation of solutions of a class of solvable standard quadratic congruence of composite modulus- a power of prime positive integer multiple of Eight, International Journal of Mathematics Trends and Technology (IJMTT), Vol − 61, Issue − 04, Sep − 18, ISSN: 2231 − 5373.