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

Prof B M Roy
Head, department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- GONDIA, M S, INDIA

ABSTRACT
In this study, a special class of standard quadratic congruence of composite modulusis formulated successfully. These types of congruence have a large numbers of solutions. These solutions can be obtained very easily in a short- time. Oral calculation of solutions are possible. It is the merit of the paper. Formulation made the study of quadratic congruence very interesting. Such standard quadratic congruence are not formulated by earlier Mathematicians.

Keywords: *Composite modulus, Formulation, Quadratic congruence.*

INTRODUCTION

A standard quadratic congruence is a congruence of the type: $x^2 \equiv a^2 (mod\ m)$; m being a

Prime or Composite integer. The solutions are the values of x that satisfy the congruence. If m is a prime positive integer, the congruence is called a standard quadratic congruence of prime modulus. But if m is a composite integer, then it is called a standard quadratic congruence of composite modulus. Such types of congruence are always solvable.

If it is a standard quadratic congruence of prime modulus, then it has exactly two solutions [1]. *But if it is a standard quadratic congruence of composite modulus, then it may have more than two solutions [2]. Here, the author wishes to formulate the standard quadratic congruence of compositemodulus of the type:*

$x^2 \equiv a^2 (mod\ a^n)$; *n*≥ 3*, a positivecomposite integer.*

LITERATURE-REVIEW

In the literature of mathematics, a standard quadratic congruence of prime modulus is discussed prominently. A little discussion is found on quadratic congruence of prime-power modulus or composite modulus. The author's successful efforts opens the gate of entry to the solutions of the said congruence directly. He (the author) already formulated many standard quadratic congruence of prime and composite modulus [3] to [12].

NEED OF RESEARCH

Though the author formulated many standard quadratic congruence of prime and composite modulus, even he found one more such special congruence yet remained to formulate. Here in this paper, the author considered such congruence for formulation and his efforts are presented here. This is the need of the paper.

PROBLEM-STATEMENT

Here the problem is-

"To formulate the solutions of the special quadratic congruence:
$x^2 \equiv a^2 (mod\ a^n); a\ is\ an\ odd\ positive\ integer, n \geq 3$".

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv a^2 (mod\ a^n); n \geq 3$.

Let us consider that $x \equiv a^{n-1}k \pm a \quad (mod\ a^n)$.

Then, $x^2 \equiv (a^{n-1}k \pm a)^2$ (mod a^n)

$$\equiv (a^{n-1}k)^2 \pm 2.a^{n-1}k.a + a^2\ (mod\ a^n)$$

$\equiv a^2 + a^{2n-2}k^2 \pm 2a^n k\ (mod\ a^n)$

$$\equiv a^2 + a^n(a^{n-2}k^2 \pm 2k)$$

$\equiv\ a^2\ (mod\ a^n)$, by binomial expansion formula.

Thus, $x \equiv a^{n-1}k \pm a\ \ (mod\ a^n)$ is a solution of the said congruence$x^2 \equiv a^2(mod\ a^n);\ n \geq 3$.

But, if we consider $k = a$, then $x \equiv a^{n-1}.a \pm a\ \ (mod\ a^n)$

$$\equiv a^n \pm a\ \ (mod\ a^n)$$

$$\equiv 0 \pm a \equiv \pm a\ (mod\ a^n)$$

Which is the same solution as for $k = 0$.

Similarly, for higher values of k, the solutions repeats as for $k = 1, 2, 3, \dots..$

Therefore, all the required solutions are given by

$$x \equiv a^{n-1}k \pm a\ (mod\ a^n); k = 0, 1, 2, \dots \dots \dots (a-1).$$

These are $2a$ incongruent solutions for all values of k. The congruence has two solutions for every value of k and k has a different values.

ILLUSTRATIONS

Consider the congruence$x^2 \equiv 225\ (mod\ 3375)$

It can be written as $x^2 \equiv 15^2(mod\ 15^3)$ with $a = 15\ and\ n = 3$.

Such congruence always has $2a = 2.15 = 30$ solutions.

Those solutions are given by

$$x \equiv a^{n-1}k \pm a\ (mod\ a^n); k = 0, 1, 2, 3, 4, \dots \dots \dots .. ,29.$$

$$i.e.\ \ x \equiv 5^{4-1}k \pm 5\ \ \equiv 125k \pm 5\ (mod\ 5^4); k = 0, 1, 2, 3, 4.$$

$$i.e.\ \ x \equiv 0 \pm 5; 125 \pm 5; 250 \pm 5; 375 \pm 5; 500 \pm 5\ (mod\ 625)$$

$$i.e. x \equiv 5, 620; 120, 130; 245, 255; 370, 380; 495, 505\ (mod\ 625).$$

These are the ten solutions of the congruence under consideration.

Consider the congruence $x^2 \equiv 36\ (mod\ 1296)$.

It can be written as $x^2 \equiv 6^2(mod\ 6^4)$ with $a = 6\ and\ n = 4$.

Such congruence always has $2a = 2.6 = 12$ solutions.

Those solutions are given by

$$x \equiv a^{n-1}k \pm a\ (mod\ a^n); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 6^{4-1}k \pm 6\ \equiv 216k \pm 6\ (mod\ 6^4); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 0 \pm 6; 216 \pm 6; 432 \pm 6; 648 \pm 6; 864 \pm 6; 1080 \pm 6\ (mod\ 1296)$$

$$i.e. x \equiv 6, 1290; 210, 222; 426, 438; 642, 654; 858, 870; 1074, 1086\ (mod\ 1296).$$

These are the twelve solutions of the congruence under consideration.

Consider the congruence $x^2 \equiv 36\ (mod\ 1296)$.

It can be written as $x^2\ \equiv 6^2 (mod\ 6^4)$ with $a = 6\ and\ n = 4$.

Such congruence always has $2a = 2.6 = 12$ solutions.

Those solutions are given by

$$x \equiv a^{n-1}k \pm a\ (mod\ a^n); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 6^{4-1}k \pm 6\ \equiv 216k \pm 6\ (mod\ 6^4); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 0 \pm 6; 216 \pm 6; 432 \pm 6; 648 \pm 6; 864 \pm 6; 1080 \pm 6\ (mod\ 1296)$$

$$i.e. x \equiv 6, 1290; 210, 222; 426, 438; 642, 654; 858, 870; 1074, 1086\ (mod\ 1296).$$

These are the twelve solutions of the congruence under consideration.

CONCLUSION

Thus, it can be concluded that the congruence under consideration $x^2\ \equiv a^2 (mod\ a^n)$,

$n \geq 3$is formulated successfully and has $2a$ solutions which can be given by

$$x \equiv a^{n-1}k \pm a\ (mod\ a^n); k = 0, 1, 2, \dots \dots \dots (a - 1).$$

If a is an even positive integer, then one must have: $a^n\ = 2^n.p^n$; p being a prime and the congruence becomes: $x^2\ \equiv a^2 (mod\ 2^n.p^n)$.

It is already formulated by the author.

MERIT OF THE PAPER

Formulation is the merit of the paper. It made the finding of solutions very easy. This formulation is time-saving and very simple. Sometimes the solutions can be obtained orally. It is one more merit of the paper.

REFERENCE

[1] H S Zuckerman at el, 2008, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.

[2] Thomas Koshy, 2009, "Elementary Number Theory with Applications", 2/e Indian print, Academic Press, ISBN: 978-81-312-1859-4.

[3] Roy B M, 2018, A new method of finding solutions of a solvable standard quadratic congruence of comparatively large prime modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-3, May-Jun-18.

[4] Roy B M, 2018, Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & four, International Journal of Recent Innovations In Academic Research (IJRIAR), ISSN:2635-3040, Vol-2, Issue-2, Jun-18.

[5] Roy B M, 2018, Formulation of solutions of standard quadratic congruence of even composite modulus as a product of two odd primes & eight, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-4, July-18.

[6] Roy B M, 2018, Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime-power integer by two or four, International Journal for Research Trends and Innovations(IJRTI), ISSN:2456-3315, Vol-3, Issue-5, May-18.

[7] Roy B M, 2018, Formulation of solutions of some classes of standard quadratic congruence of composite modulus as a product of a prime-power integer by two or four, International Journal for Research Trends and Innovations(IJRTI), ISSN:2456-3315, Vol-3, Issue-5, May-18.

[8] Roy B M, 2018, Formulation of Standard Quadratic Congruence of Composite modulus as a product of prime-power integer and eight, International Journal of Science & Engineering Development Research (IJSDR),ISSN: 2455-2631, Vol-3, Issue-7, Jul-18.

[9] Roy B M, 2018, Formulation of solutions of a class of standard quadratic congruence of even composite modulus, International Journal of Science & Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-3, Issue-8, Jul-18.

[10] Roy B M, 2018, AnAlgorithmic Formulation of solving Standard Quadratic Congruence of Prime- power Modulus, International Journal of Advanced Research, Ideas and Innovations in Technology (IJARIIT), ISSN: 2454-132X, Vol-4, Issue-6, Dec-18.

[11] Roy B M, 2019, Formulation of a Class of Solvable Standard Quadratic Congruence of Even Composite Modulus, International Journal for Research Trends and Innovations (IJRTI), ISSN: 2456-3315, Vol-4, Issue-3, Mar-19.

[12] Roy B M, 2019,Formulation of Some Classes of Solvable Standard Quadratic Congruence modulo a Prime Integer - Multiple of Three & Ten, International Journal of Scientific Research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-2, Issue-2, Mar-19.

[13] Roy B M, 2018, Formulation of Solutions of a Class of Solvable Standard Quadratic Congruence of Composite Modulus- a Prime Positive Integer Multiple of Eight, International Journal of Mathematics Trends and Technology (IJMTT), ISSN: 2231-5373, Vol-61, Issie-4,Sep-18.