RP-104: Formulation of Standard Quadratic Congruence of Composite modulus- an Integer-multiple of the Power of the Modulus

Prof B M Roy

Head, department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist- GONDIA, M S, INDIA Pin: 441801
(Affiliated to R T M Nagpur University)

***Abstract*: In this paper, a class of standard quadratic congruence modulo an integer-multiple of the power of composite integer, is considered for formulation. Author's keen interest and hard labour successfully formulate the congruence. Such congruence have large numbers of solutions. Solutions can be obtained easily instantly. It is also possible to find the solutions orally. Thus the formulation of solutions of the said congruence is the merit of the paper. The formulation of the congruence increases the interest of the study of quadratic congruence. A large numbers of solutions can be calculated mentally. This is one more merit of the paper.**

***Keywords*: Binomial expansion formula, Composite-power modulus, Formulation, Quadratic congruence.**

INTRODUCTION

A congruence is of the type: $x^2 \equiv a^2 \ (mod\ m)$; m being a Prime or Composite integer, is called a standard quadratic congruence of prime or composite modulus. 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 quadratic congruence of composite modulus, then it may have more than two solutions [2]. Here, the author wishes to formulate the standard quadratic congruence modulo a multiple of an integer and the power of a composite integer of the type* $x^2 \equiv a^2 \ (mod\ b.a^n)$; *n*≥ 2, *a being positive composite integer and b any positive 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. Earlier mathematicians (it seems) were not much interested in it. The author's successful efforts opens the gate of entry to the solutions of the 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: $x^2 \equiv a^2 \ (mod\ b.a^n); a, b\ are$ positive integers, $n \geq 2$".

ANALYSIS & RESULTS

Consider the congruence $x^2 \equiv a^2 \ (mod\ b.a^n); a, b\ are$ positive integers, $n \geq 2$.

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

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

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

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

$a\ is$ Positive integers, $n \geq 2$.

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

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

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

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

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

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

ILLUSTRATIONS

Consider the congruence $x^2 \equiv 49 \ (mod\ 147); n \geq 2, a\ an\ integer.$

It can be written as $x^2 \equiv 7^2 (mod\ 3.7^2)$ with $a = 7, b = 3\ and\ n = 2.$

Such congruence always has $2a = 2.7 = 14$ solutions.

Those solutions are given by $x \equiv b.a^{n-1}k \pm a\ (mod\ b.a^n); k = 0, 1, 2, 3, 4, 5, 6.$

$$i.e.\ x \equiv 3.7^{2-1}k \pm 7 \ \equiv 21k \pm 7 \ (mod\ 3.7^2); k = 0, 1, 2, 3, 4, 5, 6.$$

$$i.e.\ x \equiv 21k \pm 7 \ (mod\ 147); k = 0, 1, 2, 3, 4, 5, 6.$$

$$i.e.\ x \equiv 0 \pm 7; 21 \pm 7; 42 \pm 7; 63 \pm 7; 84 \pm 7; 105 \pm 7; 126 \pm 7 \ (mod\ 147)$$

$$i.e.\ x \equiv 7, 140; 14, 28; 35, 49; \ 56, 70; 77, 91; 99, 112; 119, 133 \ (mod\ 147).$$

These are the fourteen solutions of the congruence under consideration.

Consider the congruence $x^2 \equiv 16 \ (mod\ 192); n \geq 2, a\ an\ integer.$

It can be written as $x^2 \equiv 4^2 (mod\ 3.4^3)$ with $a = 4, b = 3\ and\ n = 3.$

Such congruence always has $2a = 2.4 = 8$ solutions.

Those solutions are given by $x \equiv b.a^{n-1}k \pm a\ (mod\ b.a^n); k = 0, 1, 2, 3.$

$$i.e.\ x \equiv 3.4^{3-1}k \pm 4 \ \equiv 48k \pm 4 \ (mod\ 3.4^3); k = 0, 1, 2, 3.$$

$$i.e.\ x \equiv 48k \pm 4 \ (mod\ 192); k = 0, 1, 2, 3.$$

$$i.e.\ x \equiv 0 \pm 4; 48 \pm 4; 96 \pm 4; 144 \pm 4 \ (mod\ 192)$$

$$i.e. x \equiv 4, 188; 44, 52; 92, 100; 140, 148 \ (mod\ 192).$$

These are the eight solutions of the congruence under consideration.

Consider the congruence $x^2 \equiv 36 \ (mod\ 6480); n \geq 2, a\ an\ integer.$

It can be written as $x^2 \equiv 6^2 (mod\ 5.6^4)$ with $a = 6, b = 5\ and\ n = 4.$

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

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

$$i.e.\ x \equiv 5.6^{4-1}k \pm 6 \ \equiv 1080k \pm 6 \ (mod\ 5.6^4); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 1080k \pm 6 \ (mod\ 6480); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 0 \pm 6; 1080 \pm 6; 2160 \pm 6; 3240 \pm 6; 4320 \pm 6;$$

$$5400 \pm 6 \ (mod 6480\ )$$

$$i.e. x \equiv 6, 6474; 1074, 1086; 2154, 2166; 3234, 3246;$$

$$4314, 4326; 5394, 5406 \ (mod\ 6480).$$

These are the eight solutions of the congruence under consideration.

CONCLUSION

In the conclusion it can be said that the congruence $x^2 \equiv a^2 \ (mod\ b.a^n); a, b\ are$ positive integers, $n \geq 2$, is formulated successfully. The congruence has exactly $2a\ solutions$ which are given by

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

MERIT OF THE PAPER

Formulation of the congruence made the study of the congruence interesting and easy. Solutions can be calculated mentally. This is the merit of the paper.

REFERENCES

[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, *An Algorithmic 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.