International Journal of Scientific Research and Engineering Development-– Volume 4 Issue 2, Mar- Apr 2021

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

RP-117: A Review & Reformulation of the Solutions of the Standard Quadratic Congruence of Even Composite Modulus-an Integer- Power of Two

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

Here in the current paper, a special type of congruence of composite modulus-a power of an even – prime is reviewed and found that it was partially formulated for its solutions. The author realised that the earlier formulation is incomplete and a reformulation of the solutions is needed. The author considered the problem for reformulation and reformulated. Apartial formulation is found in a books of Number Theory. There the formulation is only for an odd positive integer but nothing is said about even positive integer. So, an incomplete formulation is in the literature of mathematics. The author reviewed the problemand provide a complete formulation of the said quadratic congruence and has presented here.

Key-words: Composite Modulus, Quadratic Congruence, Review andReformulation.

INTRODUCTION

In the book of Number Theory [1], it is found that the congruence under consideration had not been fully discussed and formulated. This is the said congruence: $x^2 \equiv a\ (mod\ 2^n); n \geq 3$. It is formulated by earlier mathematicians but not fully discussed.Hence, the said congruence is considered for a complete formulation $i.e. reformulation$.

REVIEW OF BACKGROUND LITERATURE

The congruence of even composite modulus under consideration is found formulated for odd integer only.

No discussion is found for even positive integer. The author wished to formulate for even positive integer a.

Thecongruence$x^2 \equiv a\ (mod\ 2^n);\ n \geq 3, a \equiv 1\ (mod\ 8) is\ found\ formulated.$

Such congruence have exactly four solutions.

If $x \equiv x_0$ is a solution,then the other three solutions are: $x \equiv 2^n - x_0;\ 2^{n-1} \pm x_0$[1].

But how to find x_0, is not mentioned and this creates the difficulties in finding the solutions.

The author's formulation on the similar types of congruence [3], [4], [5], [6], [7], [8], [9], [10], [11].

NEED OF RESEARCH

Thus, the quadratic congruence of composite modulus under consideration has not been completely formulated and it needs a review and a correctreformulation of its solutions. The author has found a correctreformulation of it. This removes the above demerit of the existed formulation.

PROBLEM-STATEMENT

Here the problemis-

"To review and reformulate the solutions of the congruence of the type:$x^2 \equiv a\ (mod\ 2^n); n \geq 3$ with

$a \equiv 1\ (mod\ 8)$.

ANALYSIS & RESULTS

Here the congruence under study is: $x^2 \equiv a\ (mod\ 2^n); a \equiv 1\ (mod\ 8);\ i.e.\ a\ is\ anodd\ positive\ integer.$

The congruence can also be written as: $x^2 \equiv a + k.2^n = b^2 (mod\ 2^n)$[2].

Let b be odd positive integer.

Let $x \equiv 2^{n-1}k \pm b\ (mod\ 2^n), k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots$

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

$$\equiv (2^{n-1}k)^2 + 2.2^{n-1}k.b + b^2$$

$\equiv\ 2^n k\{2^{n-2}k + b\} + b^2$; **as b is odd positive integer.**

$$\equiv b^2 (mod\ 2^n).$$

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

But,for$k = 2,\ x \equiv 2^{n-1}.2 \pm b\ (mod\ 2^n)$,

$$\equiv 2^n k \pm b\ (mod\ 2^n)$$

$$\equiv 0 \pm b\ (mod\ 2^n)$$

$\equiv \pm b\ (mod\ 2^n)$, which is the same solution as for k=0.

But, for$k = 3 = 2 + 1,\ x \equiv 2^{n-1}.(2 + 1) \pm b\ (mod\ 2^n)$,

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

$$\equiv 0 + 2^{n-1} \pm b\ (mod\ 2^n)$$

$\equiv 2^{n-1} \pm b\ (mod\ 2^n)$, which is the same solution as for k=1.

Thus, it can be said that the congruence under consideration has exactly four solutions:

$x \equiv 2^{n-1}k \pm b\ (mod\ 2^n), k = 0, 1,$ as for a single value of k, it has two solutions.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 25\ (mod\ 2^5)$. $As\ 25 \equiv 1\ (mod\ 8)$, it is solvable.

It can be written as $x^2 \equiv 25 = 5^2 (mod\ 2^5)$.

It is of the type $x^2 \equiv b^2 (mod\ 2^n)\ with\ b = 5, odd\ positive\ integer, n = 5$.

It has exactly four solutions $x \equiv 2^{n-1}k \pm b\ (mod\ 2^n), k = 0, 1$.

$$\equiv 2^{5-1}k \pm 5\ (mod\ 2^5)$$

$$\equiv 16k \pm 5\ (mod\ 32)$$

$$\equiv 0 \pm 5; 16 \pm 5\ (mod\ 32)$$

$$\equiv 5, 27; 11, 21\ (mod\ 32)$$

Example-2: Consider the congruence:$x^2 \equiv\ 17 (mod\ 2^6)$.

It is of the type: $x^2 \equiv a\ (mod\ 2^n)$.

As 17 is oddpositive integer and $17 \equiv 1\ (mod\ 8)$, it is solvable.

It can be written as $x^2 \equiv 17 + 64 = 18 = 9^2 (mod\ 2^6)$

It is of the type $x^2 \equiv b^2 (mod\ 2^n)\ with\ b = 9, odd\ positive\ integer, n = 6$.

It has exactly four solutions: $x \equiv 2^{n-1}k \pm b\ (mod\ 2^n), k = 0, 1$.

$$\equiv 2^{6-1}k \pm 9\ (mod\ 2^6)$$

$$\equiv 32k \pm 9\ (mod\ 64)$$

$$\equiv 0 \pm 9; 32 \pm 9\ (mod\ 64)$$

$$\equiv 9, 55;\ 23, 41\ (mod\ 64)$$

Example-3: Consider the congruence $x^2 \equiv 19\ (mod\ 2^6)$.As$a = 19\ \not\equiv 1\ (mod\ 8)$, the congruence is not solvable.

CONCLUSION

The congruence $x^2 \equiv b^2 (mod\ 2^n)$ has exactly four solutions:$x \equiv 2^{n-1}k \pm b\ (mod\ 2^n), k = 0, 1,$ when $a \equiv 1\ (mod\ 8)$. A very simple and suitablereformulation of the solutions of the congruence is presented. It isfully discussed,tested and asingle formula for all the solutions is presented.

REFERENCES

1. Niven I., Zuckerman H. S., Montgomery H. L. (1960, Reprint 2008), "*An Introduction to The Theory of Numbers*", 5/e, Wiley India (Pvt) Ltd, page-148, problem-11.
2. Roy B M, 2016, *Discrete Mathematics & Number Theory*, Das GanuPrakashan, Nagpur, India, ISBN: 978-93-84336-12-7.
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 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.
8. 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.
9. 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.
10. 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.
11. 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.

……xxx……..

