Research Journal of Mathematical and Statistical Sciences _____ISSN 2320-6047
Vol. **10(1),** 9-10, January **(2022)** *Res. J. Mathematical and Statistical Sci.*

Short Review paper

A review and reformulation of solutions of the standard quadratic congruence of even composite modulus

B.M. Roy
Department of Mathematics, Jagat Arts, Commerce & I H P Science College, Goregaon, Dist-Gondia, MS, India
roybm62@gmail.com

Available online at: www.iscamaths.com , www.isca.in , www.isca.me
Received 11th December 2020, revised 8th July 2021, accepted 15th September 2021

Abstract

A very special type of standard quadratic congruence of composite modulus modulo a power of an even –prime integer 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. In the literature of mathematics, an insufficient partial formulation is found in a book 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 problem and provide a complete formulation of the said quadratic congruence and has presented here.

Keywords: Composite modulus, quadratic congruence, review and Reformulation.

Introduction

In the book of Number Theory[1,2], 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. $i.e. reformulation$

Literature-Review

In the literature of mathematics, the standard quadratic congruence of even composite modulus under consideration is found formulated for odd integer a only.

The congruence is $x^2 \equiv a(\mathrm{mod}\ 2^n); n \geq 3, \text{with } a \equiv 1(\mathrm{mod}\ 8)$
This is for odd positive integer a.
This is the condition of solvability of the congruence for odd integer a.
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. No method is yet detectedin the literature of mathematics. Here lies the difficulties.

The author already has formulated many standard quadratic congruence of prime and composite modulus[3-11].

Need of research: Thus, the quadratic congruence of composite modulus under consideration has not been completely formulated and it needs a review and a correct reformulation of its solutions. The author has found a correct reformulation of it. This removes the above demerit of the existed formulation. This is the need of this research.

Problem-statement: Here the problem of study is - To review and reformulate the standard quadratic congruence of composite modulus-a power of an even prime integer, of the type :$x^2 \equiv a\ (mod\ 2^n); n \geq 3$ with $a \equiv 1\ (mod\ 8)$.

Results and discussion

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

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

Merit of the paper: Here in this paper, the author has provided are formulation of the solutions of the congruence under consideration. It is discussed and a single formula is presented. This is the merit of the paper.

References

1. Niven I., Zuckerman H. S. and Montgomery H. L. (2008). An Introduction to The Theory of Numbers. 1960, Reprint 2008, 5/e, Wiley India (Pvt) Ltd, problem-11, pp-148,.

2. Roy B. M. (2016). Discrete Mathematics & Number Theory. Das Ganu Prakashan, 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*, 4(3).

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*, 2(2).

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*, 4(4).

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*, 3(5).

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*, 3(7).

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*, 3(8).

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*, 4(6).

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*, 4(3).

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*, 2(2).