Engineering and Scientific International Journal (ESIJ)
Volume 7, Issue 1, January – March 2020
ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Reformulation of a Special Standard Quadratic Congruence of Even Composite Modulus

Prof. B. M. Roy

Head, Department of Mathematics, Jagat Arts,
Commerce & I H P Science College, Goregaon, Dist-Gondia

Abstract—A very special type of standard quadratic congruence of even composite modulus is reformulated in this paper. The formulation found in the literature of mathematics is not sufficient. The formulation found is only for an odd positive integer but nothing is said about even positive integer. So, an incomplete formulation is found in the literature. The author has taken the opportunity to find a complete formulation of the said quadratic congruence of even composite modulus and has presented a complete formulation of the congruence.

Keywords *— Composite Modulus; Quadratic Congruence; Reformulations*

1. Introduction

When the author has gone through the books of Number Theory, it is found that the congruence under consideration had not been fully discussed and formulated. Students are facing difficulties and reported. The congruence is: $x^2 \equiv a \ (mod\ 2^m); m \geq 3$. It is formulated by earlier mathematicians but not fully discussed. Here, the said congruence is considered for a complete formulation.

2. Literature Review

In the literature of mathematics, the standard quadratic congruence of even composite modulus under consideration is found formulated for odd integer a. The congruence is
$x^2 \equiv a \ (mod\ 2^m);\ m \geq 3,\ with a \equiv 1 \ (mod\ 8)$.
This is for odd positive integer.
This is the condition of solvability of the congruence for odd integer a.
Such congruence has exactly four solutions.
If $x \equiv x_0$ is a solution (how to find?), then the other three solutions are $x \equiv 2^m - x_0;\ 2^{m-1} \pm x_0$[2].
But no comment is found for even positive integer 'a'
The author already has formulated many standard quadratic congruence of prime and composite modulus [3, 4, 5, 6, 7, 8, 9, 10, 11].

3. Need of Research

This means that the said quadratic congruence has not been completely formulated and it needs a correct full formulation of solutions. The author wished to find a correct full formulation of it. This will remove the above demerit of the existed formulation. This is the need of this research.

4. Problem Statement

The problem is-"To formulate the standard quadratic congruence of even composite modulus of the type:$x^2 \equiv a \ (mod\ 2^m); m \geq 3$ in two cases for odd-even integer a.

5. Analysis and Results

Consider the congruence,
$x^2 \equiv b \ (mod\ 2^m); b \equiv 1 \ (mod\ 8)\ i.e.\ b\ is\ an\ odd\ positive\ integer$.
It is solvable as per mentioned in the literature.
The congruence can also be written as: $x^2 \equiv b + k.2^m = a^2 = (mod\ 2^m)$[1].

Case-I: Let b be odd positive integer.

Let $x \equiv 2^{m-1}k \pm a \ (mod\ 2^m), k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots$
Then $x^2 \equiv (2^{m-1}k \pm a)^2$
$\equiv (2^{m-1}k)^2 + 2.2^{m-1}k.a + a^2$
$\equiv 2^m k\{2^{m-2}k + a\} + a^2$; as a is odd positive integer.
$\equiv a^2 (mod\ 2^m)$.
Thus, $x \equiv 2^{m-1}k \pm a \ (mod\ 2^m)$ satisfies the quadratic congruence and it is a solution of it.
But for,
$k = 2,\ x \equiv 2^{m-1}.2 \pm a \ (mod\ 2^m)$,
$\equiv 2^m k \pm a \ (mod\ 2^m)$
$\equiv 0 \pm a \ (mod\ 2^m)$
$\equiv \pm a \ (mod\ 2^m)$, which is the same solution as for k=0.
But, for
$k = 3 = 2 + 1,\ x \equiv 2^{m-1}.(2 + 1) \pm a \ (mod\ 2^m)$,
$\equiv 2^m k + 2^{m-1} \pm a \ (mod\ 2^m)$
$\equiv 0 + 2^{m-1} \pm a \ (mod\ 2^m)$
$\equiv 2^{m-1} \pm a \ (mod\ 2^m)$, which is the same solution as for k=1.

DOI: **10.30726/esij/v7.i1.2020.71002**

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

Thus, it can be said that the congruence under consideration has exactly four solutions:
$x \equiv 2^{m-1}k \pm a \ (mod\ 2^m), k = 0, 1,$ as for a single value of k, it has two solutions.

Case-II: Let b be even positive integer. Then a is also even positive integer.

Let,
$x \equiv 2^{m-2}k \pm a \ (mod\ 2^m), k = 0, 1, 2, 3, 4, 5, \ldots\ldots\ldots\ldots$
Then $x^2 \equiv (2^{m-2}k \pm a)^2$
$\equiv (2^{m-2}k)^2 + 2.2^{m-2}k.a + a^2$
$\equiv 2^{m-1}k\{2^{m-2}k + a\} + a^2;$
$\equiv 2^m k\{2^{m-4}k + r\} + a^2 \ (mod\ 2^m)$, as a is even & a=2r
$\equiv a^2 (mod\ 2^m)$
Thus, $x \equiv 2^{m-2}k \pm a \ (mod\ 2^m)$ satisfies the quadratic congruence and it is a solution of it.
But for $k = 4,\ x \equiv 2^{m-2}.4 \pm a \ (mod\ 2^m),$
$\equiv 2^m k \pm a \ (mod\ 2^m)$
$\equiv 0 \pm a \ (mod\ 2^m)$
$\equiv \pm a \ (mod\ 2^m)$, which is the same solution as for k=0.
But, for
$k = 5 = 4 + 1,\ x \equiv 2^{m-2}.(4 + 1) \pm a \ (mod\ 2^m),$
$\equiv 2^m k + 2^{m-2} \pm a \ (mod\ 2^m)$
$\equiv 0 + 2^{m-2} \pm a \ (mod\ 2^m)$
$\equiv 2^{m-2} \pm a \ (mod\ 2^m)$, which is the same solution as for k=1.

Thus, the congruence under consideration has exactly eight incongruent solutions
$x \equiv 2^{m-2}k \pm a \ (mod\ 2^m), k = 0, 1, 2, 3,$ as for a single value of k, it has two solutions.
If $a = 0, (even\ positive\ integer),$ then the congruence reduces to $x^2 \equiv 0 (mod\ 2^m).$
Then it can be easily seen that $x \equiv 8k \ (mod\ 2^m); k = 0, 1, 2, 3, \ldots\ldots\ldots$ are the eight solutions of the congruence.
$i.e. all\ positive\ integer\ divisible\ by\ 8.$

Thus, it can be easily seen that for odd positive integer a, there would be 2^{m-3} congruence, each having four solutions and so total number of solutions would be $2^{m-3}x4 = 2^{m-1}.$

There remains another $2^{m-1}\ solutions$ for even positive integer a. But all mathematicians consider zero (o) as even integer and has exactly eight solutions, hence there remains only $(2^{m-1} - 8)$ solutions for nonzero even positive integer. And each congruence have exactly eight solutions. This is only possible whenever, 'a' is perfect square.

Thus, in the case when a is an even positive integer, the congruence is only solvable if 'a' is perfect square.

6. Illustrations

Consider the congruence,
$x^2 \equiv 17 \ (mod\ 2^5). As\ 17 \equiv 1 \ (mod\ 8),$ it is solvable.
It can be written as $x^2 \equiv 17 + 32 = 49 = 7^2 (mod\ 2^5).$
It is of the type
$x^2 \equiv a^2 (mod\ 2^m)\ with\ a =$
$7, odd\ positive\ integer, m = 5.$

It has exactly four solutions,
$x \equiv 2^{m-1}k \pm a \ (mod\ 2^m), k = 0, 1.$
$\equiv 2^{5-1}k \pm 7 \ (mod\ 2^5)$
$\equiv 16k \pm 7 \ (mod\ 32)$
$\equiv 0 \pm 7; 16 \pm 7 \ (mod\ 32)$
$\equiv 7, 25; 9, 23 \ (mod\ 32)$
$\equiv 7, 9, 23, 25 \ (mod\ 32).$
Consider the congruence: $x^2 \equiv 36 \ (mod\ 2^6)$. As 36 is a perfect square, it is solvable.
It can be written as $x^2 \equiv 6^2 (mod\ 2^6)$
It is of the type, .
$x^2 \equiv a^2 (mod\ 2^m)\ with\ a =$
$6, even\ positive\ integer, m = 6.$

It has exactly eight solutions,
$x \equiv 2^{m-2}k \pm a \ (mod\ 2^m), k = 0, 1, 2, 3.$
$\equiv 2^{6-2}k \pm 6 \ (mod\ 2^6)$
$\equiv 16k \pm 6 \ (mod\ 64)$
$\equiv 0 \pm 6; 16 \pm 6; 32 \pm 6; 48 \pm 6 \ (mod\ 64)$
$\equiv 6, 58; 10, 22;\ 26, 38; 42, 54 \ (mod\ 64)$
$\equiv\ 6, 10, 22, 26, 38, 42, 54, 58 \ (mod\ 64).$
Consider the congruence $x^2 \equiv 0 \ (mod\ 2^6)$
It is of the type,
$x^2 \equiv 0 (mod\ 2^m)\ with\ a =$
$0, even\ positive\ integer, m = 6.$
Its solutions are, .
$x \equiv 8k \ (mod\ 2^m); k = 0, 1, 2, 3, \ldots\ldots$
$\equiv 0, 8, 16, 24, 32, 40, 48, 56 \ (mod\ 2^6).$
Consider the congruence $x^2 \equiv 10 \ (mod\ 2^6).$
As $a = 10, not\ a\ perfect\ square,$ the congruence is not solvable. Consider the congruence $x^2 \equiv 11 \ (mod\ 2^4).$
As $11 \equiv 3 \neq 1 \ (mod\ 8),$ the congruence is not solvable.

7. Conclusion

Therefore, it can be concluded that the congruence $x^2 \equiv a^2 (mod\ 2^m)$ has exactly four solutions $x \equiv 2^{m-1}k \pm a \ (mod\ 2^m), k = 0, 1$ when a is odd positive integer $i.e.\ \ a \equiv 1 \ (mod\ 8);$ but has eight solutions $x \equiv 2^{m-2}k \pm a \ (mod\ 2^m), k = 0, 1, 2, 3$ when a is even positive integer. The congruence is only solvable if a is even perfect square. Therefore, it can be concluded that if a is odd positive integer and $a \equiv 1 \ (mod\ 8),$ the congruence has exactly four solutions. If a is even positive integer, and a perfect square, the congruence has exactly eight solutions.

DOI: 10.30726/esij/v7.i1.2020.71002

ISSN 2394-7187(Online)
ISSN 2394 - 7179 (Print)

References

[1] Roy B M, "Discrete Mathematics & Number Theory", 1/e, ISBN: 978-93-84336-12-7, Jan. 2016,Das GanuPrakashan, Nagpur, page-88.

[2] 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.

[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.

DOI: **10.30726/esij/v7.i1.2020.71002**