# RP-181: Formulation of Standard Quadratic Congruence of Even Composite Modulus modulo an Even Prime Raised to the Power n 

Prof. B M Roy<br>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

The paper presented here, is a standard quadratic congruence of composite modulus, studied rigorously and found the formulation incomplete. It was partially formulated by the earlier mathematicians. The present authors realised that the earlier formulation need a completion and a reformulation of the solutions is done along with two more results. The author considered the problem for reformulation, studied and reformulated the solutions completely. A partial formulation is found in a books of Number Theory by Zuckerman at el. There the formulation is only for an odd positive integer but nothing is said about even positive integer. The authors have provided a complete formulation of the said quadratic congruence and presented here.


Keywords: Composite Modulus, Quadratic Congruence, Reformulation.

## I. 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: $x^{2} \equiv a\left(\bmod 2^{n}\right)$;
$n \geq 3$. It is formulated by earlier mathematicians but not fully discussed. Hence, the said congruence is considered for a complete formulation.

## II. REVIEW OF BACKGROUND LITERATURE

The congruencee 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 the problem completely.
The congruence $x^{2} \equiv a\left(\bmod 2^{n}\right) ; n \geq 3, a \equiv 1(\bmod 8)$ 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.
Here the author's formulation needs no previously known $x_{0}$.
The author's formulation on the similar types of congruence are: [3], [4], [5], [6], [7], [8], [9], [10], [11].

## A. Problem-Statement

The problem of study is stated here in the form of theorems:

1) Theorem-1: The solutions of the congruence: $x^{2} \equiv 2^{n-1}\left(\bmod 2^{n}\right) ; m, n$ positive integer has exactly solutions: $\mathrm{x} \equiv 2^{\frac{n-1}{2}} k+$ $2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2,3, \ldots \ldots, 2^{\frac{n+1}{2}}$.
2) Theorem-2: The solutions of the congruence: $x^{2} \equiv 2^{n-3}\left(\bmod 2^{n}\right) ; m, n$ positive integer has exactly solutions: $x \equiv 2^{\frac{n-1}{2}} k+$ $2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2,3, \ldots \ldots . .2^{\frac{n+1}{2}}$.
3) Theorem-3: The solutions of the standard quadratic congruence: $x^{2} \equiv a\left(\bmod 2^{n}\right)$ has exactly four incongruent solutions given by $x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right)$, if $b$ is an odd positive integer; $a \equiv 1(\bmod 8) \& \mathrm{k}=0,1$.
4) Theorem-4: The solutions of the standard quadratic congruence: $x^{2} \equiv a\left(\bmod 2^{n}\right)$ has exactly eight incongruent solutions given by $x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right)$, if $b$ is an even positive integer; $a$ is a perfect square, $a=b^{2} \& \mathrm{k}=0,1,2,3$.

## III. ANALYSIS \& RESULTS

1) Proof of theorem-1: Consider the congruence: $x^{2} \equiv 2^{n-1}\left(\bmod 2^{n}\right) ; n$ an odd positive integer.
For its solutions let $x \equiv 2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-1}{2}}\left(\boldsymbol{\operatorname { m o d }} 2^{n}\right)$.
Then $x^{2} \equiv\left(2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-1}{2}}\right)^{2}\left(\bmod 2^{n}\right)$

$$
\begin{aligned}
& \equiv\left(2^{\frac{n-1}{2}} k\right)^{2}+2.2^{\frac{n-1}{2}} k \cdot 2^{\frac{n-1}{2}}+\left(2^{\frac{n-1}{2}}\right)^{2}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-1} k^{2}+2^{n} k+2^{n-1}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-1} k^{2}+2^{n-1}\left(\bmod 2^{n}\right) ; k \text { being an integer. }
\end{aligned}
$$

Therefore, $x \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right)$ gives solutions of the congruence.
But for $k=2^{\frac{n+1}{2}}$, the formula reduces to

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} \cdot 2^{\frac{n+1}{2}}+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n}+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 0+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right)
\end{aligned}
$$

This is the same solution as for $k=0$.
Also, for $k=2^{\frac{n-1}{2}}+1$, the formula reduces to
$x \equiv 2^{\frac{n-1}{2}} \cdot\left(2^{\frac{n+1}{2}}+1\right)+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right)$
$\equiv 2^{n}+2^{\frac{n-1}{2}}+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right)$

$$
\equiv 2^{\frac{n-1}{2}}+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right)
$$

This is the same solution as for $k=1$.
Therefore it is concluded that the solutions formula becomes

$$
x \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2, \ldots \ldots \ldots,\left(2^{\frac{n+1}{2}}-1\right)
$$

It gives all the solutions.
2) Proof of Theorem-2: Consider the congruence:
$x^{2} \equiv 2^{n-3}\left(\bmod 2^{n}\right) ; n$ an odd positive integer.
For its solutions let $x \equiv 2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-3}{2}}\left(\boldsymbol{\operatorname { m o d }} 2^{n}\right)$.
Then $x^{2} \equiv\left(2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-3}{2}}\right)^{2}\left(\bmod 2^{n}\right)$

$$
\begin{aligned}
& \equiv\left(2^{\frac{n-1}{2}} k\right)^{2}+2.2^{\frac{n-1}{2}} k \cdot 2^{\frac{n-3}{2}}+\left(2^{\frac{n-3}{2}}\right)^{2}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-1} k^{2}+2^{n-1} k+2^{n-3}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-1} k(k+1)+2^{n-3}\left(\bmod 2^{n}\right) ; k \text { being an integer. } \\
& \equiv 2^{n} t+2^{n-3}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-3}\left(\bmod 2^{n}\right)
\end{aligned}
$$

Therefore, $x \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right)$ gives solutions of the congruence.
But for $k=2^{\frac{n+1}{2}}$, the formula reduces to

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} \cdot 2^{\frac{n+1}{2}}+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 2^{n}+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 0+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right)
\end{aligned}
$$

This is the same solution as for $k=0$.
Also, for $k=2^{\frac{n+1}{2}}+1$, the formula reduces to

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} \cdot\left(\left(^{\frac{n+1}{2}}+1\right)+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right)\right. \\
\equiv & \equiv 2^{n}+2^{\frac{n-1}{2}}+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) \\
& \equiv 2^{\frac{n-1}{2}}+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right)
\end{aligned}
$$

This is the same solution as for $k=1$.
Therefore it is concluded that the solutions formula becomes

$$
x \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2, \ldots \ldots \ldots,\left(2^{\frac{n+1}{2}}-1\right) .
$$

It gives all the solutions.
3) Proof of Theorem-3:

Let us consider that $a \equiv 1(\bmod 8)$; i.e. $a$ is an odd positive integer.
Here the congruence under study is: $x^{2} \equiv a\left(\bmod 2^{n}\right)$ with $a \equiv 1(\bmod 8)$.
If $a$ is an odd perfect square, then $a=b^{2}$.
The congruence reduces to: $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$.
If not, then the congruence can be written as: $x^{2} \equiv a+k .2^{n}=b^{2}\left(\bmod 2^{n}\right)$ [2].
For odd positive integer $b$,
Let $x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right), k=0,1,2,3, \ldots \ldots \ldots \ldots \ldots$

$$
\text { Then } \begin{aligned}
x^{2} & \equiv\left(2^{n-1} k \pm b\right)^{2} \\
& \equiv\left(2^{n-1} k\right)^{2}+2 \cdot 2^{n-1} k . b+b^{2} \\
& \equiv 2^{n} k\left\{2^{n-2} k+b\right\}+b^{2} ; \text { as } \mathbf{b} \text { is odd positive integer. } \\
& \equiv b^{2}\left(\bmod 2^{n}\right) .
\end{aligned}
$$

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

$$
\equiv 2^{n} k \pm b\left(\bmod 2^{n}\right)
$$

$$
\equiv 0 \pm b\left(\bmod 2^{n}\right)
$$

$$
\equiv \pm b\left(\bmod 2^{n}\right) \text {, which is the same solution as for } \mathrm{k}=0 .
$$

But, for $k=3=2+1, x \equiv 2^{n-1} \cdot(2+1) \pm b\left(\bmod 2^{n}\right)$,

$$
\begin{aligned}
& \equiv 2^{n} k+2^{n-1} \pm b\left(\bmod 2^{n}\right) \\
& \equiv 0+2^{n-1} \pm b\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-1} \pm b\left(\bmod 2^{n}\right), \text { which is the same solution as for } \mathrm{k}=1 .
\end{aligned}
$$

Thus, it can be said that the congruence under consideration has exactly four solutions:
$x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right), k=0,1$, if $a \equiv 1(\bmod 8)$, as for a single value of k , it has two solutions.

## 4) Proof of Theorem -4:

Let $a$ be an even perfect square.
Then, $a=b^{2}, b$ even positive integer.
For the solutions, consider $x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right)$
Then, $x^{2} \equiv\left(2^{n-2} k \pm b\right)^{2}$

$$
\begin{aligned}
& \equiv\left(2^{n-2} k\right)^{2}+2 \cdot 2^{n-2} k \cdot b+b^{2} \\
& \equiv 2^{n-1} k\left\{2^{n-3} k+b\right\}+b^{2} \\
& \equiv 2^{n-1} k\left\{2^{n-3} k+2 t\right\}+b^{2} \text { as } \mathbf{b} \text { is even positive integer. } \\
& \equiv \equiv 2^{n} k\left\{2^{n-4} k+t\right\}+b^{2} \\
& \equiv b^{2}\left(\bmod 2^{n}\right) .
\end{aligned}
$$

Thus, $x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right)$ satisfies the quadratic congruence and it is a solution of it.
But, for $k=4=2^{2}, x \equiv 2^{n-2} \cdot 2^{2} \pm b\left(\bmod 2^{n}\right)$,

$$
\equiv 2^{n} k \pm b\left(\bmod 2^{n}\right)
$$

$$
\equiv 0 \pm b\left(\bmod 2^{n}\right)
$$

$\equiv \pm b\left(\bmod 2^{n}\right)$, which is the same solution as for $\mathrm{k}=0$.
But, fork $=5=2^{2}+1, x \equiv 2^{n-2} \cdot\left(2^{2}+1\right) \pm b\left(\bmod 2^{n}\right)$,

$$
\begin{aligned}
& \equiv 2^{n} k+2^{n-2} \pm b\left(\bmod 2^{n}\right) \\
& \equiv 0+2^{n-2} \pm b\left(\bmod 2^{n}\right) \\
& \equiv 2^{n-2} \pm b\left(\bmod 2^{n}\right), \text { which is the same solution as for } \mathrm{k}=1 .
\end{aligned}
$$

Thus, it can be said that the congruence under consideration has exactly eight solutions: $x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right), k=0,1,2,3$; as for a single value of k , it has two solutions.

## IV. ILLUSTRATIONS

1) Example-1: Consider the congruence $x^{2} \equiv 16(\bmod 32)$.

It can be written as: $x^{2} \equiv 2^{4}\left(\bmod 2^{5}\right)$.
It is of the type: $x^{2} \equiv 2^{n-1}\left(\bmod 2^{n}\right)$ with $n=5$, an odd positive integer.
Its solutions are given by

These are the eight solutions of the congruence.
2) Example-2: Consider the congruence $x^{2} \equiv 64(\bmod 128)$.

It can be written as: $x^{2} \equiv 2^{6}\left(\bmod 2^{7}\right)$.
It is of the type: $x^{2} \equiv 2^{n-1}\left(\bmod 2^{n}\right)$ with $n=7$, an odd positive integer.
Its solutions are given by

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2, \ldots \ldots \ldots .,\left(2^{\frac{n+1}{2}}-1\right) . \\
& \equiv 2^{3} k+2^{3}\left(\bmod 2^{7}\right) ; k=0,1,2, \ldots \ldots, 15 . \\
& \equiv 8 k+8(\bmod 128) \\
& \equiv \mathbf{8}, \mathbf{1 6}, \mathbf{2 4}, \mathbf{3 2}, \mathbf{4 0}, \ldots \ldots \ldots \ldots ., \mathbf{1 2 8} .
\end{aligned}
$$

These are the sixteen solutions of the congruence.
3) Example-3: Consider the congruence $x^{2} \equiv 16(\bmod 128)$.

It can be written as: $x^{2} \equiv 2^{4}\left(\bmod 2^{7}\right)$.
It is of the type: $x^{2} \equiv 2^{n-3}\left(\bmod 2^{n}\right)$ with $n=7$, an odd positive integer.
Its solutions are given by

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2, \ldots \ldots \ldots .,\left(2^{\frac{n+1}{2}}-1\right) . \\
& \equiv 2^{3} k+2^{2}\left(\bmod 2^{7}\right) ; k=0,1,2, \ldots \ldots, 15 . \\
& \equiv 8 k+4(\bmod 128) \\
& \equiv 4,12,20,28,36, \ldots \ldots \ldots \ldots, 124 .
\end{aligned}
$$

These are the sixteen solutions of the congruence.
4) Example-4: Consider the congruence $x^{2} \equiv 64(\bmod 512)$.

It can be written as: $x^{2} \equiv 2^{6}\left(\bmod 2^{9}\right)$.
It is of the type: $x^{2} \equiv 2^{n-3}\left(\bmod 2^{n}\right)$ with $n=9$, an odd positive integer.
Its solutions are given by

$$
\begin{aligned}
x & \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-3}{2}}\left(\bmod 2^{n}\right) ; k=0,1,2, \ldots \ldots \ldots .,\left(2^{\frac{n+1}{2}}-1\right) . \\
& \equiv 2^{4} k+2^{3}\left(\bmod 2^{9}\right) ; k=0,1,2, \ldots \ldots, 31 . \\
& \equiv 16 k+\mathbf{8}(\bmod 152)
\end{aligned}
$$

$$
\equiv 4,12,20,28,36
$$

$\qquad$ 504.

These are the thirty-two solutions of the congruence.

$$
\begin{aligned}
& \boldsymbol{x} \equiv 2^{\frac{n-1}{2}} k+2^{\frac{n-1}{2}}\left(\bmod 2^{n}\right) ; \boldsymbol{k}=\mathbf{0}, 1,2, \ldots \ldots \ldots .,\left(2^{\frac{n+1}{2}}-1\right) \text {. } \\
& \equiv 2^{2} k+2^{2}\left(\bmod 2^{5}\right) ; k=0,1,2, \ldots ., 7 . \\
& \equiv 4 k+4(\bmod 32) \\
& \equiv 4,8,12,16,20,24,28,32 .
\end{aligned}
$$

5) Example-5: Consider the congruence $x^{2} \equiv 25\left(\bmod 2^{5}\right) . A s 25 \equiv 1(\bmod 8)$, it is solvable.

It can be written as $x^{2} \equiv 25=5^{2}\left(\bmod 2^{5}\right)$.
It is of the type $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$ with $b=5$, odd positive integer, $n=5$.
It has exactly four solutions $x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right), k=0,1$.

$$
\begin{aligned}
& \equiv 2^{5-1} k \pm 5\left(\bmod 2^{5}\right) \\
& \equiv 16 k \pm 5(\bmod 32) \\
& \equiv 0 \pm 5 ; 16 \pm 5(\bmod 32) \\
& \equiv 5,27 ; 11,21(\bmod 32)
\end{aligned}
$$

6) Example-6: Consider the congruence: $x^{2} \equiv 17\left(\bmod 2^{6}\right)$.

It is of the type: $x^{2} \equiv a\left(\bmod 2^{n}\right)$.
As 17 is odd positive integer and $17 \equiv 1(\bmod 8)$, it is solvable.
It can be written as $x^{2} \equiv 17+64=18=9^{2}\left(\bmod 2^{6}\right)$
It is of the type $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$ with $b=9$, odd positive integer, $n=6$.
It has exactly four solutions: $x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right), k=0,1$.

$$
\begin{aligned}
& \equiv 2^{6-1} k \pm 9\left(\bmod 2^{6}\right) \\
& \equiv 32 k \pm 9(\bmod 64) \\
& \equiv 0 \pm 9 ; 32 \pm 9(\bmod 64) \\
& \equiv 9,55 ; 23,41(\bmod 64)
\end{aligned}
$$

7) Example-7: Consider the congruence $x^{2} \equiv 19\left(\bmod 2^{6}\right)$. As $a=19 \not \equiv 1(\bmod 8)$, the congruence is not solvable.
8) Example-8: Consider the congruence: $x^{2} \equiv 36\left(\bmod 2^{6}\right)$.

It can be written as $x^{2} \equiv 6^{2}\left(\bmod 2^{6}\right)$
It is of the type $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$ with $b=6$, even positive integer, $n=6$.
As 36 is even perfect square positive integer, it is solvable.
It has exactly eight incongruent solutions: $x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right), k=0,1,2,3$.

$$
\begin{aligned}
& \equiv 2^{6-2} k \pm 6\left(\bmod 2^{6}\right) \\
& \equiv 16 k \pm 6(\bmod 64) \\
& \equiv 0 \pm 6 ; 16 \pm 6 ; 32 \pm 6 ; 48 \pm 6(\bmod 64) \\
& \equiv 6,58 ; 10,22 ; 28,38 ; 42,54(\bmod 64)
\end{aligned}
$$

9) Example-9: Consider the congruence $x^{2} \equiv 10\left(\bmod 2^{6}\right)$.

As $a=10$, not an even perfect square, the congruence is not solvable.
10) Example-10: Consider the congruence: $x^{2} \equiv 0(\bmod 256)$.

It can be written as: $x^{2} \equiv 0\left(\bmod 2^{8}\right)$.
It is of the type: $x^{2} \equiv 0\left(\bmod 2^{n}\right)$ with $n=8$, an even positive integer.
Its solutions are given by:

$$
\begin{aligned}
x & \equiv 2^{\frac{n}{2}} k\left(\bmod 2^{n}\right) ; k=1,2,3, \ldots \ldots, 2^{\frac{n}{2}} \\
& \equiv 2^{4} k\left(\bmod 2^{8}\right) ; k=1,2,3, \ldots \ldots \ldots, 2^{4} . \\
& \equiv 16 k(\bmod 256) ; k=1,2,3, \ldots \ldots \ldots .16 . \\
& \equiv 16,32,48,64,80,96,112,128,144,160,176,192,208,224,240,256(\bmod 256) .
\end{aligned}
$$

These are the sixteen incongruent solutions of the congruence.

## V. CONCLUSION

The congruence: $x^{2} \equiv 2^{n-1}\left(\bmod 2^{n}\right)$, $n$ always an odd positive integer has exactly
$2^{\frac{n+1}{2}}$ solutions given by $\boldsymbol{x} \equiv 2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-1}{2}}\left(\boldsymbol{\operatorname { m o d }} 2^{\boldsymbol{n}}\right) ; \boldsymbol{k}=\mathbf{0}, \mathbf{1}, 2, \ldots \ldots \ldots,\left(2^{\frac{n+1}{2}}-\mathbf{1}\right)$.
The congruence: $x^{2} \equiv 2^{n-3}\left(\bmod 2^{n}\right)$, $n$ always an odd positive integer has exactly
$2^{\frac{n+1}{2}}$ solutions given by $\boldsymbol{x} \equiv 2^{\frac{n-1}{2}} \boldsymbol{k}+2^{\frac{n-3}{2}}\left(\boldsymbol{\operatorname { m o d }} 2^{\boldsymbol{n}}\right) ; \boldsymbol{k}=\mathbf{0}, \mathbf{1}, 2, \ldots \ldots \ldots,\left(2^{\frac{n+1}{2}}-\mathbf{1}\right)$.
The congruence $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$ has exactly four solutions:
$x \equiv 2^{n-1} k \pm b\left(\bmod 2^{n}\right), k=0,1$, when $a \equiv 1(\bmod 8)$
i.e. $a$ is an odd positive integer.

The congruence $x^{2} \equiv b^{2}\left(\bmod 2^{n}\right)$ has exactly eight solutions:
$x \equiv 2^{n-2} k \pm b\left(\bmod 2^{n}\right), k=0,1,2,3$ when $a$ is an even perfect square.

## 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 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 (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.

do
cross ${ }^{\text {ref }}$
10.22214/IJRASET


IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL.

IMPACT FACTOR:
7.429

## INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE \& ENGINEERING TECHNOLOGY
Call : 08813907089 @ (24*7 Support on Whatsapp)

