Research Journal of Recent Sciences ISSN 2277-2502
Vol. **10(3),** 10-11, July **(2021)** *Res. J. Recent Sci.*

Formulation of solutions of a class of standard quadratic congruence modulo aprime-multiple of even-powered even prime

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

Available online at: www.isca.in, www.isca.me
Received 18th December 2020, revised 13th March 2021, accepted 22nd May 2021

Abstract

Here the author of this paper has presented his rigorous study and the formulation of a class of quadratic congruence of composite modulus- a prime multiple of even-powered even prime. The established formula is tested and verified true by solving various numerical examples. The formulation works well. Sufficient number of solved examples are also presented. The readers must find the formulation suitable for them to find the solutions with an ease.

Keywords: Composite modulus, prime-multiple, even prime, quadratic congruence.

Introduction

Congruence is nothing but a new style of writing the mathematical statement of division Algorithm. If a is divided by $m \neq 0$, quotient q and remainder r is obtained and these fourare written as:$a = mq + r; 0 \leq r < m$. This is the mathematical statement of Division Algorithm. It is written as: $a - r = mq; 0 \leq r < m. This$ can be written in a new style as:

$a - r \equiv 0\ (mod\ m)\ or\ a \equiv r\ (mod\ m)$. If a is replaced by x^2, then it reduces to$x^2 \equiv r\ (mod\ m)$ and called as standard quadratic congruence. If m is a composite positive integer, it is congruence of composite modulus.

Here the author wishes to concentrate his study on the formulation of solutions of standard quadratic congruence of composite modulus. Such type of congruence has never studied by the earlier mathematicians. Hence the author consider it for the formulation of its solutions. This type of congruence has a large number of solutions.

Problem-Statement

To find a formula for the solutions of the congruence:
$x^2 \equiv 2^{2m}(mod\ 2^n.p);$
$p\ being\ odd\ prime\ integer, m < n, \quad n\ is\ always\ even.$

Literature Review (Existed method)

There exist no method or no formula in the literature of mathematics to find the solutions of the said congruence: $x^2 \equiv 2^{2m}(mod\ 2^n.p)$; p being odd prime integer; n is always even.

But readers can use Chinese Remainder Theorem[1].
The congruence can be split into two separate congruence:

$x^2 \equiv 2^{2m}(mod\ 2^n)$ (1)
$x^2 \equiv 2^{2m}(mod\ p)$ (2)

Solving (1) and (2), then Chinese Remainder Theorem can be used to find all the solutions.

In the book of David Burton[3], it is said that $x^2 \equiv a\ (mod\ 2^n), for\ n \geq 3, has$ a solution if $a \equiv 1\ (mod\ 8)$. Then a must be odd positive integer. Nothing is found in the literature of mathematics, if a is even positive integer. But the solutions of (1) are formulated by the author[4]. The author also has formulated the solutions of the congruence:$x^2 \equiv a\ (\mathrm{mod}\ 2^n)$[5].

The congruence (2) has exactly two solutions[2]. The finding of solutions of the individual congruence is not simple. No method is known to find the solutions of (1). Readers can only use trial and error method. It is time consuming and complicated. The author wants to overcome this difficulties and wishes to find a direct formula of the solutions of the congruence.

Analysis and results

Consider the congruence:
$x^2 \equiv 2^{2m}(mod\ 2^n.p);\ \ p\ odd\ prime\ integer.$
For its solutions, consider $x \equiv 2^{n-m-1}.pk \pm 2^m\ (mod\ 2^n.p)$

Then, $x^2 \equiv (2^{n-m-1}.pk \pm 2^m)^2\ (mod 2^n.p)$
$\equiv (2^{n-m-1}.pk\ )^2 \pm 2.\ 2^{n-m-1}.pk.2^m + (2^m)^2\ \ (mod\ 2^n.p)$
$\equiv (2^{n-m-1}.pk\ )^2 \pm 2.2^{n-1}.pk + (2^m)^2\ \ (mod\ 2^n.p)$
$\equiv 2^n.pk[2^{n-2m-2}.pk\ \pm 1] + 2^{2m}(mod\ 2^n.p).$
$\equiv 2^{2m}\ (mod\ 2^n.p)$
Therefore, it is seen that $x \equiv 2^{n-m-1}.pk \pm 2^m\ (mod\ 2^n.p)$ satisfies the said congruence and it gives solutions of the congruence for different values of k.

But if $if\ k = 2^{m+1}$, the solutions reduces to the form
$x \equiv 2^{n-m-1}.p.2^{m+1} \pm 2^m \ \ (mod\ 2^n.p)$
$\equiv 2^n.p \pm 2^m \ \ (mod\ 2^n.p)$
$\equiv 0 \pm 2^m \ (mod\ 2^n.p)$

These are the same solutions of the congruence as for $k = 0$.

Also for $k = 2^{m+1} + 1$, the solutions reduces to the form
$x \equiv 2^{n-m-1}.p.(\ 2^{m+1} + 1) \pm 2^m \ \ (mod\ 2^n.p)$
$\equiv 2^n.p + \ 2^{n-m-1}.p \pm 2^m \ \ (mod\ 2^n.p)$
$\equiv 2^{n-m-1}.p \pm 2^m \ (mod\ 2^n.p)$

These are the same solutions of the congruence as for $k = 1$.

Therefore, all the solutions are given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (mod\ 2^m.p); k =$
$0, 1, 2, 3, \dots\dots\dots\dots, (2^{m+1} - 1).$

These gives $2.2^{m+1} = 2^{m+2}$ solutions of the congruence.

Illustrations: Example-1: Let $x^2 \equiv 2^4 (mod\ 2^6.5)$ be a congruence.

It can be written as: $x^2 \equiv 2^{2.2} (mod\ 2^6.5)\ with\ m = 2, n = 6, p = 5.$

It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)$.

It has exactly 2^{m+2} *i*ncongruent solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (mod\ 2^n.p); k$
$= 0, 1, 2, 3, \dots\dots\dots\dots, (2^{2+1} - 1).$
$\equiv 2^{6-2-1}.5k \pm 2^2 (mod\ 2^6.5); k = 0, 1, 2, 3, 4, 5, 6, 7\ .$
$\equiv 40k \pm 4\ (mod\ 320); k = 0, 1, 2, 3, \quad 4, 5, 6, 7.$
$\equiv 0 \pm 4; 40 \pm 4; 80 \pm 4; 120 \pm 4\ ; 160 \pm 4; 200 \pm 4; 240$
$\pm 4; 280 \pm 4\ (mod\ 320)$
$\equiv 4, 316; 36, 44; 76, 84; 116, 124; 156, 164; 196, 204;$
$236, 244; 276, 284\ (mod\ 320).$

Example-2: Consider the congruence: $x^2 \equiv 2^{2.2}\ (mod\ 2^6.7)$
It is of the type: $x^2 \equiv 2^{2m} (\text{mod}\ 2^n.p)$ with $m = 2, n = 6, p = 7.$
It has exactly 2^{m+2} *i* ncongruent solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (\text{mod}\ 2^n.p); k$
$= 0, 1, 2, 3, \dots\dots\dots\dots, (2^{m+1} - 1).$
$\equiv 2^{6-3-1}.7k \pm 2^2 (\text{mod}\ 2^6.7); k$
$= 0, 1, 2, 3\ \dots\dots\dots\dots, (2^3 - 1)$
$\equiv 56k \pm 4\ (\text{mod}\ 448); k = 0, 1, 2, 3, 4, 5, 6, 7.$
$\equiv 0 \pm 4; 56 \pm 4; 112 \pm 4; 168 \pm 4\ ; 224 \pm 4; 280 \pm 4;$
$336 \pm 4; 392 \pm 4\ (\text{mod}\ 448)$
$\equiv 4, 444; 52, 60; 108, 116; 164, 172; 220, 228; 276, 284;$
$332, 340; 388, 396\ (\text{mod}\ 448).$
These are sixteen incongruent solutions of the congruence.

Example-3: Consider the congruence: $x^2 \equiv 2^{2.3}\ (\text{mod}\ 2^{10}.3)$
It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)$ with $m = 3, n = 10, p = 3.$

It has exactly 2^{m+2} *i*ncongruent solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (\text{mod}\ 2^n.p); k$
$= 0, 1, 2, 3, \dots\dots\dots\dots, (2^{m+1} - 1).$
$\equiv 2^{10-3-1}.3k \pm 2^3 (mod\ 2^{10}.3); k$
$= 0, 1, 2, 3\ \dots\dots\dots\dots, (2^4 - 1)$
$\equiv 192k \pm 8\ (mod\ 3072); k = 0, 1, 2, 3, \dots\dots\dots\dots\dots, 15.$
$\equiv 0 \pm 8; 192 \pm 8; 384 \pm 8; 576 \pm 8; 768 \pm 8; 960 \pm$
$8; 1152 \pm 8; 1344 \pm 8; 1536 \pm 8; 1728 \pm 8; 1920 \pm$
$8; 2112 \pm 8; 2304 \pm 8; 2496 \pm 8; 2688 \pm 8; 2880 \pm$
$8;\ (mod\ 3072)$
$\equiv 8, 3064; 84, 200; 376, 392; 568, 584; 760, 776; 952,$
$968; 1144, 1160; 1336, 1352;$
$1528, 1544; 1720, 1736; 1912, 1928; 2104, 2120;$
$2296, 2312; 2488, 2504;$
$2680, 2696; 2872, 2888;\ \ (mod\ 3072).$
These are thirty two incongruent solutions of the congruence.

Conclusion

Therefore, here in this case, it is concluded that the congruence under consideration:
$x^2 \equiv 2^{2m} (\text{mod}\ 2^n.p)$ has 2^{m+2} incongruent solutions given by $x \equiv 2^{n-m-1}.pk \pm 2^m (\text{mod}\ 2^n.p); k = 0, 1, 2, 3, \dots\dots, (2^{m+1} - 1)$ as for a single value of k, the formula gives exactly two solutions.

References

1. Zuckerman et al, (2008). An Introduction to The Theory of Numbers. Willey India (Pvt) Ltd, Fifth edition (Indian Print), ISBN: 978-81-265-1811-1, pp 1-70.

2. Thomas Koshy (2009). Elementary Number Theory with Applications. Academic Press, second edition, ISBN: 978-81-312-1859-4, page-497.

3. David M Burton (2012). Elementary Number Theory. Mc Graw Hill education, Seventh edition, ISBN: 978-1-25-902576-1, page-194.

4. Roy B. M. (2020). Formulation of solutions of a very special class of standard quadratic congruence of composite modulus modulo an even prime of even power. *International Journal for research Trends and Innovations*, 5(12).

5. Roy B. M. (2020). Reformulation of a special standard quadratic congruence of even composite modulus. *Research Journal of Mathematical and Statistical Science*, 7(2).