International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Formulation of a Class of Standard Quadratic Congruence of Composite Modulus modulo Even-Multiple of an Odd Prime

Prof B M Roy

Assistant Professor, Department of Mathematics, Jagat Arts, Commerce & I H P Science College, Goregaon, Gondia, Maharashtra, India

ABSTRACT

The author here in this paper presented formulation of solutions of a class of standard quadratic congruence of composite modulus modulo an even-multiple of an odd prime. The established formula is tested and verified true by solving various numerical examples. The formulation works well and proved time-saving.

KEYWORDS: *Composite modulus, even-multiple, odd prime, Quadratic Congruence*

How to cite this paper: Prof B M Roy "Formulation of a Class of Standard Quadratic Congruence of Composite Modulus modulo Even-Multiple of an Odd Prime" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.1372-1374, URL: www.ijtsrd.com/papers/ijtsrd38228.pdf

IJTSRD38228

INTRODUCTION

Congruence is a mathematical statement of division algorithm in another way without the use of quotient. If a is divided by $m \neq 0$, quotient q and remainder r is obtained and these four integers are written as: $a = mq + r; 0 \leq r < m$. This is the mathematical statement of Division Algorithm. If it can be written as: $a - r \equiv mq; 0 \leq r < m$. It can be written 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

The problem is- "Formulation of solutions of the congruence: $x^2 \equiv 2^{2m} (mod\ 2^n.p)$;
$p\ being\ odd\ prime; m < n;\ n\ is\ always\ even.$"

LITERATURE REVIEW

There existed no method or no formulation in the literature of mathematics to find the solutions of the said congruence: $x^2 \equiv 2^{2m} (mod\ 2^n.p)$; $p\ being\ odd\ prime$; $m < n$; $n\ is\ always\ even$. But readers can use Chinese Remainder Theorem [1].

The congruence can be split into two separate congruence:

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

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

Solving (1) & (2), then CRT 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: $x^2 \equiv a\ (mod\ 2^n)$[5].

It is seen that 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 & error method. It is time consuming and complicated. The author wants to overcome this difficulties and wishes to find a direct formulation of the solutions of the congruence.

ANALYSIS & RESULTS

Consider the congruence: $x^2 \equiv 2^{2m} (mod\ 2^n.p);\ p\ odd\ prime.$

For its solutions, consider $x \equiv 2^{n-m-1}.pk \pm 2^m\ (mod\ 2^m.p)$

Then, $x^2 \equiv (2^{n-m-1}.pk \pm 2^m)^2\ (mod 2^m.p)$

$\equiv (2^{n-m-1}.pk)^2 \pm 2.2^{n-m-1}.pk.2^m + (2^m)^2\ (mod\ 2^n.p)$

$\equiv (2^{n-m-1}.pk)^2 \pm 2^n.pk + (2^m)^2\ (mod\ 2^n.p)$

$\equiv 2^n.pk[2^{n-2m-2}.pk\ \pm 1] + 2^{2m} (mod\ 2^n.p); n \geq 2m + 2, n\ even.$

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

Therefore, it is seen that $x \equiv 2^{n-m-1}.pk \pm 2^m\ (mod\ 2^m.p)$ 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 $k = 2^{m+1} + 1,, the\ solutions\ reduces\ to\ the\ form$

$x \equiv 2^{n-m-1}.p.(2^{m+1} + 1) \pm 2^m\ (mod\ 2^n.p)$

$\equiv 2^n.p + 2^{n-m-1}.p \pm 2^m\ (mod\ 2^n.p)$

$\equiv 2^{n-m-1} \pm 2^m\ (mod\ 2^n.p)$

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

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

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

ILLUSTRATIONS

Example-1: Consider the congruence: $x^2 \equiv 2^4\ (mod\ 2^6.7)$

It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)\ with\ m = 2, n = 6, p = 7.$

It has exactly 2^{m+2} $incongruent$ solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (mod\ 2^n.p); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots, (2^{m+1} - 1).$

$\equiv 2^{6-2-1}.7k \pm 2^2 (mod\ 2^6.7); k = 0, 1, 2, 3\ \ldots \ldots \ldots, (2^3 - 1)$

$\equiv 56k \pm 4\ (mod\ 448); k = 0, 1, 2, 3, 4, 5, 6, 7.$

$\equiv 0 \pm 4; 56 \pm 4; 112 \pm 4; 168 \pm 4; 224 \pm 4; 280 \pm 4; 336 \pm 4; 392 \pm 4\ (mod\ 448)$

$\equiv 4, 444; 52, 60; 108, 116;\ 164, 172; 220, 228; 276, 284; 332, 340; 388, 396\ (mod\ 448).$

Example-2: Consider the congruence: $x^2 \equiv 2^4\ (mod\ 2^6.5)$

It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)\ with\ m = 2, n = 6, p = 5.$

It has exactly 2^{m+2} $incongruent$ solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (mod\ 2^n.p); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots, (2^{m+1} - 1).$

$\equiv 2^{6-2-1}.5k \pm 2^2 (mod\ 2^6.5); k = 0, 1, 2, 3\ \ldots \ldots \ldots, (2^{2+2} - 1)$

$\equiv 40k \pm 4\ (mod\ 320); k = 0, 1, 2, 3, 4, 5, 6, 7$

$\equiv 0 \pm 4; 40k \pm 4; 80 \pm 4; 120k \pm 4;\ 160 \pm 4; 200k \pm 4; 240 \pm 4; 280 \pm 4\ (mod\ 320)$

$\equiv 4, 316; 36, 44; 76, 84; 116, 124; 156, 164\ 196, 204; 236, 244; 276, 284\ (mod\ 320).$

Example-3: Consider the congruence: $x^2 \equiv 2^6\ (mod\ 2^{10}.3)$

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

$\equiv 2^{10-3-1}.3k \pm 2^3 (mod\ 2^{10}.3); k = 0, 1, 2, 3\ \ldots \ldots \ldots, (2^4 - 1)$

$\equiv 192k \pm 8\ (mod\ 3072); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots \ldots, 15.$

$\equiv 0 \pm 8; 192 \pm 8; 384 \pm 8; 576 \pm 8; 768 \pm 8; 960 \pm 8; 1152 \pm 8; 1344 \pm 8; 1536 \pm 8;$

$1728 \pm 8; 1920 \pm 8; 2112 \pm 8; 2304 \pm 8; 2496 \pm 8; 2688 \pm 8; 2880 \pm 8\ (mod\ 3072)$

$\equiv 8, 3064; 184, 200; 376, 392; 568, 584; 760, 776; 952, 968; 1144, 1160;\ 1336,\ 1352;\ 1528,\ 1544;\ 1720,\ 1736;\ 1912, 1928;\ 2104,\ 2120;\ 2296,\ 2312;\ 2488,\ 2504;\ 2680,\ 2696; 2872, 2888\ (mod\ 3072).$

These are thirty two incongruent solutions of the congruence.

Example-4: Consider the congruence: $x^2 \equiv 2^6\ (mod\ 2^8.3)$
It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)\ with\ m = 3, n = 8, p = 3.$

It has exactly 2^{m+2} $incongruent$ solutions given by
$x \equiv 2^{n-m-1}.pk \pm 2^m (mod\ 2^n.p); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots, (2^{m+1} - 1).$

$\equiv 2^{8-3-1}.3k \pm 2^3 (mod\ 2^8.3); k = 0, 1, 2, 3\ \ldots \ldots \ldots, (2^4 - 1)$

$\equiv 48k \pm 8\ (mod\ 768); k = 0, 1, 2, 3, \ldots \ldots \ldots \ldots \ldots, 15.$

$\equiv 0 \pm 8; 48 \pm 8; 96 \pm 8; 144 \pm 8; 192 \pm 8; 240 \pm 8; 288 \pm 8; 336 \pm 8; 384 \pm 8;$

$432 \pm 8; 480 \pm 8; 528 \pm 8; 576 \pm 8; 624 \pm 8; 672 \pm 8; 720 \pm 8\ (mod\ 768)$

$\equiv 8, 760; 40, 56; 88, 104;\ 138, 152; 184, 200; 232, 248; 280, 296; 328, 344; 376, 392; 424, 440; 472, 488;\ 520, 536; 568, 584; 616, 632; 664, 680; 712, 728\ (mod\ 768).$

These are thirty two incongruent solutions of the congruence.

CONCLUSION

Therefore it can now be concluded that the congruence under consideration:

$x^2 \equiv 2^{2m} \ (mod \ 2^n.p)$ has 2^{m+2} incongruent solutions given by

$$x \equiv 2^{n-m-1}.pk \pm 2^m (mod \ 2^m.p); k = 0, 1, 2, 3, \dots \dots \dots \dots, (2^{m+1} - 1).$$

REFERENCE

[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, page-64; page-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, 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 (IJRTI), ISSN: 2456-3315, Vol-05, Issue-12, Dec-20.

[5] Roy B M, Reformulation of a special standard quadratic congruence of even composite modulus, Research Journal of Mathematical and Statistical Science (IJMRSS), ISSN: 2394-6407, Vol-07, Issue-02, Mar-20.