International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 3, March-April 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

RP-163: Solving a Special Standard Quadratic Congruence Modulo an Even Multiple of an Odd Positive Integer

Prof B M Roy

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

ABSTRACT

The author, here in this paper, presented a formulation for solving a special standard quadratic congruence modulo an even multiple of an odd positive integer. 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 positive integer, Quadratic Congruence*

How to cite this paper: Prof B M Roy "RP-163: Solving a Special Standard Quadratic Congruence Modulo an Even Multiple of an Odd Positive Integer" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-3, April 2021, pp.1144-1146, URL: www.ijtsrd.com/papers/ijtsrd41116.pdf

IJTSRD41116

INTRODUCTION

Every reader of mathematics knows the mathematical statement of division algorithm. It states that if a is divided by $m \neq 0$,the quotient q and the remainder r are obtained and these four integers -a, m, q, r - are written as: $a = mq + r; 0 \leq r < m.$ This is the mathematical statement of Division Algorithm.

It can be written as: $a - r = mq; 0 \leq r < m.$

It can further be writtenin modular form 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 called the congruence of composite modulus.

Here the author wishes to formulate of solutions ofthe 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.

PROBLEM-STATEMENT

To establish a formula forthe solutions of the congruence:

$x^2 \equiv 2^{2m} (mod\ 2^n.b);$ $b\ being\ odd\ positive\ integer,$

$n\ is\ always\ even\ with\ n = 2m, b\ an\ odd\ positive\ integer.$

LITERATURE REVIEW

The said congruence is not found in the literature of mathematics. Also, no method or no formulation is seen in the literature to find the solutions of

$x^2 \equiv 2^{2m} (mod\ 2^n.b);\ b\ being\ odd\ positive\ integer, n\ is\ always\ even.$ But readers can use Chinese Remainder Theorem (CRT) [1].

The congruence can be split into two separate congruence:

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

$x^2 \equiv 2^{2m} (mod\ b) \dots\dots\dots\dots\dots (2)$

Solving (1) & (2), then using CRT, all the solutions can be obtained easily.

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: $x^2 \equiv 2^{2m} (mod\ 2^n.b);\ \ b\ odd\ positive\ integer.$

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

Then, $x^2 \equiv (2^{n-m}.bk \pm 2^m)^2\ (mod\ 2^n.b)$

$\equiv (2^{n-m}.bk)^2 \pm 2.2^{n-m}.bk.2^m + (2^m)^2\ \ (mod\ 2^n.b)$

$\equiv (2^{n-m}.bk)^2 \pm 2.2^n.bk + (2^m)^2\ \ (mod\ 2^n.b)$

$\equiv 2^n.bk[2^{n-2m}.bk \pm 2] + 2^{2m} (mod\ 2^n.b); 2m = n, an\ even\ integer.$

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

Therefore, it is seen that $x \equiv 2^{n-m}.bk \pm 2^m\ (mod\ 2^n.b)$ satisfies the said congruence and it gives solutions of the congruence for different values of k.

But if $if\ k = 2^m, the\ solutions\ reduces\ to\ the\ form$

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

$\equiv 2^n.b \pm 2^m\ \ (mod\ 2^n.b)$

$\equiv 0 \pm 2^m\ (mod\ 2^n.b)$

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

Also for $k = 2^m + 1,, the\ solutions\ reduces\ to\ the\ form$

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

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

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

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

Therefore, all the solutions are given by

$x \equiv 2^{n-m}.bk \pm 2^m (mod\ 2^m.b); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (2^m - 1).$

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

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 16\ (mod\ 144).$

It can be written as: $x^2 \equiv 2^{2.2} (mod\ 2^4.9)\ \ with\ m = 2, n = 4, b = 9.$

It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.b)\ \ with\ m = 2, n = 4, b = 9.$

It has exactly 2^{m+1} in congruent solutions given by

$x \equiv 2^{n-m}.bk \pm 2^m (mod\ 2^n.b); k = 0, 1, 2, 3, \ldots\ldots\ldots\ldots, (2^2 - 1).$

$\equiv 2^{4-2}.9k \pm 2^2 (mod\ 2^4.9); k = 0, 1, 2, 3.$

$\equiv 36k \pm 4\ (mod\ 144); k = 0, 1, 2, 3.$

$\equiv 0 \pm 4; 36 \pm 4; 72 \pm 4; 108 \pm 4\ (mod\ 144)$

$\equiv 4, 140; 32, 40; 68, 76; 104, 112\ (mod\ 144).$

Example-2: Consider the congruence: $x^2 \equiv 2^{2.2}\ (mod\ 2^4.7)$

It is of the type: $x^2 \equiv 2^{2m} (mod\ 2^n.p)\ \ with\ m = 2, n = 4, p = 7.$

It has exactly 2^{m+1} in congruent solutions given by

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

$\equiv 2^{4-2}.7k \pm 2^2 (mod\ 2^4.7); k = 0, 1, 2, 3\ \ldots\ldots\ldots, (2^3 - 1)$

$\equiv 28k \pm 4\ (mod\ 112)\ ; k = 0, 1, 2, 3.$

$\equiv 0 \pm 4;\ 28 \pm 4;\ 56 \pm 4;\ 84 \pm 4\ (mod\ 112)$

$\equiv 4, 108;\ 24, 32;\ 52, 60;\ 80, 88\ (mod\ 112).$

Example-3: Consider the congruence: $x^2 \equiv 2^4\ (mod\ 2^4.125)$

It is of the type: $x^2 \equiv 2^{2m}(mod\ 2^n.p^3)\ with\ m = 2, n = 4, p = 5.$

It has exactly 2^{m+1} incongruent solutions given by

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

$\equiv 2^{4-2}.125k \pm 2^2(mod\ 2^4.125); k = 0, 1, 2, 3\ \dots \dots \dots \dots, (2^2 - 1)$

$\equiv 500k \pm 4\ (mod\ 2000); k = 0, 1, 2, 3.$

$\equiv 0 \pm 4;\ 500 \pm 4;\ 1000 \pm 4;\ 1500 \pm 4\ (mod\ 2000)$

$\equiv 4, 1996; 496, 504; 996, 1004; 1496, 1504\ (mod\ 2000).$

Example-4: Consider the congruence: $x^2 \equiv 2^6\ (mod\ 2^6.15)$

It is of the type: $x^2 \equiv 2^{2m}(mod\ 2^n.p)\ \ with\ m = 3, n = 6, b = 15.$

It has exactly 2^{m+1} incongruent solutions given by

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

$\equiv 2^{6-3}.15k \pm 2^3(mod\ 2^6.15); k = 0, 1, 2, 3\ \dots \dots \dots, (2^3 - 1)$

$\equiv 120k \pm 8\ (mod\ 960); k = 0, 1, 2, 3, \dots \dots \dots \dots, 7.$

$\equiv 0 \pm 8;\ 120 \pm 8;\ 240 \pm 8; 360 \pm 8;\ 480 \pm 8;\ 600 \pm 8;\ 720 \pm 8;\ 840 \pm 8\ (mod\ 960$

$\equiv 8, 952;\ 112, 128;\ 232, 248;\ 352, 368;\ 472, 488;$

$592, 608;\ 712, 728;\ 832, 848\ (mod\ 960).$

These are sixteen incongruent solutions of the congruence.

Example-5: Consider the congruence: $x^2 \equiv 2^6\ (mod\ 2^6.3)$

It is of the type: $x^2 \equiv 2^{2m}(mod\ 2^n.b)\ \ with\ m = 3, n = 6, b = 3.$

It has exactly 2^{m+1} incongruent solutions given by

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

$\equiv 2^{6-3}.3k \pm 2^3\ (mod\ 2^6.3); k = 0, 1, 2, 3\ \dots \dots \dots, (2^3 - 1)$

$\equiv 24k \pm 8\ (mod\ 192)\ ; k = 0, 1, 2, 3, \dots \dots \dots \dots, 7.$

$\equiv 0 \pm 8;\ 24 \pm 8;\ 48 \pm 8;\ 72 \pm 8; 96 \pm 8;\ 120 \pm 8;\ 144 \pm 8;\ 168 \pm 8 (mod\ 192)$

=8, 184; 16, 32; 40, 56; 64, 80; 88, 104; 112, 128; 136, 152; 160,176$(mod\ 192)$.

These are sixteen incongruent solutions of the congruence.

CONCLUSION

Therefore, here in this case, it can now be concluded that the congruence under consideration: $x^2 \equiv 2^{2m}(mod\ 2^n.b)$ has 2^{m+1} incongruent solutions given by

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

The truth and correctness of the formula established is verified solving some suitable examples.

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.