JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

RP-187: Solving special standard quadratic congruence of composite modulus modulo an odd prime multiple of powered even prime

Prof B M Roy

Head, Department of Mathematics

Jagat Arts, Commerce & I H P Science College, Goregaon

Dist - Gondia, M. S., India. Pin: 441801.

ABSTRACT

Here in this study, the author has considered two very special types of standard quadratic congruence of even composite modulus modulo an odd prime multiple of powered even prime integer for formulation of its solutions. A simple formula is established and formulated for each congruence under consideration. These formulae find the solutions very easily with less effort. The method proved time-saving. Formulation is the merit of the paper.

KEY- WORDS

Composite modulus, Even prime, Formulation, Prime multiple, Quadratic congruence.

INTRODUCTION

The solutions of a standard quadratic congruence of the type: $x^2 \equiv a \ (mod\ K)$ are the values of x that satisfies the congruence means to find those values of x whose square when divided by K gives the remainder a. Here in this study, the author has selected the values of a and m are: $a = 2^{2m}, K = 2^{2m},\ 2^{2m+1}$.

Then the congruence under consideration for study become: $x^2 \equiv 2^{2m}\ (mod\ 2^{2m}.p)$ and $x^2 \equiv 2^{2m}\ (mod\ 2^{2m+1}.p)$.

PROBLEM-STATEMENT

Here the problem of study is:

To find the solutions of the congruence:

(1) $x^2 \equiv 2^{2m}\ (mod\ 2^{2m+1}.p); p\ an\ odd\ prime.$

(2) $x^2 \equiv 2^{2m}\ (mod\ 2^{2m}.p); p\ an\ odd\ prime.$

LITERATURE REVIEW

The two special standard quadratic congruence of composite modulus considered for formulation are neither be formulated nor discussed in the literature of mathematics. Thomas Koshy [1], David M Burton [2], Zuckerman et el [3] all have discussed the linear and standard quadratic congruence of prime and composite modulus but nothing is found reported for the present problem. The author has already formulated many such standard quadratic congruence of composite modulus [4], [5], [6], [7]. To continue the research, the author has consider the problem under consideration for formulation of solutions.

ANALYSIS & RESULTS

PROBLEM-01:

Consider the congruence: $x^2 \equiv 2^{2m} \ (mod\ 2^{2m+1}.p); p\ an\ odd\ prime; m\ is\ positive\ integer.$

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

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

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

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

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

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

$$\equiv 0 + 2^{2m} \ (mod\ 2^{2m+1}.p)$$

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

Therefore, the formulation satisfies the congruence and hence it can be considered as solutions of the said congruence for different values of positive integer k.

But for $k = 2^m$, **the solutions formula reduces to the form:**

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

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

$$\equiv 0 \pm 2^m \ (mod\ 2^{2m+1}.p)$$

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

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

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

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

$$\equiv 0 + 2^{m+1}.p \pm 2^m(mod\ 2^{2m+1}.p)$$

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

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

Therefore, all the solutions are given by

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

This gives $2.2^m = 2^{m+1}$ incongruent solutions as for each value of k gives exactly two solutions.

PROBLEM-02:

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

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

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

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

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

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

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

$$\equiv 0 + 2^{2m} \ (mod\ 2^{2m}.p)$$

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

Therefore, the formulation satisfies the congruence and hence it can be considered as solutions of the said congruence for different values of positive integer k.

But for $k = 2^m$, the solutions formula reduces to the form:

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

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

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

$$\equiv 0 \pm 2^m \ (mod\ 2^{2m}.p)$$

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

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

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

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

$$\equiv 0 + 2^m.p \pm 2^m (mod\ 2^{2m}.p)$$

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

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

Therefore, all the solutions are given by

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

This gives $2.2^m = 2^{m+1}$ incongruent solutions as for each value of k gives exactly two solutions.

ILLUSTRATIONS

EX-1: Consider the congruence $x^2 \equiv 64 (mod\ 384)$

It can be written as: $x^2 \equiv 2^6 \ (mod\ 2^7.3)$ $i.e.$ $x^2 \equiv 2^{2.3} \ (mod\ 2^{2.3+1}.3)$

It is of the type $x^2 \equiv 2^{2m} \ (mod\ 2^{2m+1}.p)$ $with\ m = 3, p = 3$.

Its solutions are

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

$\equiv 2^{3+1}.3k \pm 2^3\ (mod\ 2^{2.3+1}.3)$

$\equiv 2^4.3k \pm 2^3\ (mod\ 2^{2.3+1}.3)$

$\equiv 48k \pm 8\ (mod\ 384); k = 0, 1, 2, 3, 4, 5, 6, 7$.

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

≡8, 376; 48, 56; 88, 104; 136, 152; 184, 200; 232, 248; 272, 296; 328, 344 (mod 384)

These are the sixteen solutions.

EX-2: Consider the congruence $x^2 \equiv 64 (mod\ 640)$

It can be written as: $x^2 \equiv 2^6\ (mod\ 2^7.5)\ \ i.e.\ \ x^2 \equiv 2^{2.3}\ (mod\ 2^{2.3+1}.5)$

It is of the type $x^2 \equiv 2^{2m}\ (mod\ 2^{2m+1}.p)\ with\ m = 3, p = 5$.

Its solutions are

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

$\equiv 2^{3+1}.5k \pm 2^3\ (mod\ 2^{2.3+1}.5)$

$\equiv 2^4.5k \pm 2^3\ (mod\ 2^{2.3+1}.5)$

$\equiv 80k \pm 8\ (mod\ 640); k = 0, 1, 2, 3, 4, 5, 6, 7$.

$\equiv 0 \pm 8; 80 \pm 8; 160 \pm 8; 240 \pm 8; 320 \pm 8; 400 \pm 8; 480 \pm 8; 560 \pm 8\ (mod\ 640)$

≡8, 632; 72, 88; 152, 168; 232, 248; 312, 328; 392, 408; 472, 488; 552, 568 (mod 640)

These are the sixteen solutions.

Example-3: Consider the congruence $x^2 \equiv 2^6\ (mod\ 2^6.5)$

It can be written as: $x^2 \equiv 2^{2.3}\ (mod\ 2^{2.3}.5)$

It is of the type $x^2 \equiv 2^{2m}\ (mod\ 2^{2m}.p)\ with\ m = 3,\ \ n = 6, p = 5$.

Its solutions are

$x \equiv 2^m.pk \pm 2^m (mod\ 2^{2m}.p)$

$\equiv 2^3.5k \pm 2^3\ (mod\ 2^{2.3}.5)$

$\equiv 2^3.5k \pm 2^3\ (mod\ 2^{2.3}.5)$

$\equiv 40k \pm 8\ (mod\ 320); k = 0, 1, 2, 3, 4, 5, 6, 7$.

$\equiv 0 \pm 8; 40 \pm 8; 80 \pm 8; 120 \pm 8; 160 \pm 8; 200 \pm 8; 240 \pm 8; 280 \pm 8\ (mod\ 320)$

≡8, 312; 32, 48; 72, 88; 112, 128; 152. 168; 192, 208; 232, 248; 272, 288 (mod 320)

These are the sixteen solutions.

Example-4: Consider the congruence $x^2 \equiv 2^8\ (mod\ 2^8.3)$

It can be written as: $x^2 \equiv 2^{2.4}\ (mod\ 2^{2.4}.3)$

It is of the type $x^2 \equiv 2^{2m}\ (mod\ 2^{2m}.p)\ with\ m = 4, n = 8, p = 3$.

Its solutions are

$x \equiv 2^m.pk \pm 2^m (mod\ 2^{2m}.p)$

$\equiv 2^4.3k \pm 2^4\ (mod\ 2^{2.4}.3)$

$\equiv 2^4.3k \pm 2^4\ (mod\ 2^{2.4}.3)$

$\equiv 48k \pm 16\ (mod\ 1280); k = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.$

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

$384 \pm 16; 432 \pm 16; 480 \pm 16; 528 \pm 16; 576 \pm 16; 624 \pm 16;\ (mod\ 1280)$

≡8, 312; 32, 48; 72, 88; 112, 128; 152. 168; 192, 208; 232, 248; 272, 288 (mod 1280)

These are the thirty two solutions.

CONCLUSION

Therefore, it is concluded that the first congruence under consideration has incongruent solutions given by $x \equiv 2^{m+1}.pk \pm 2^m (mod\ 2^{2m+1}.p); k =, 1, 2, \dots \dots 2^m$.

Also, the second congruence under consideration has sixteen incongruent solutions given by $x \equiv 2^m.pk \pm 2^m (mod\ 2^{2m}.p); k =, 1, 2, \dots \dots 2^m$.

Merit of the paper

The quadratic congruence considered for formulation are successfully formulated and the formulation help the authors to find the solutions very easily. It made the study of congruence easy. These are the merit of the paper.

REFERENCES

[1] Thomas Koshy, 2009, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN: 978-81-312-1859-4.

[2] Burton David M., *Elementary Number Theory*, seventh edition, Mc Graw Hill education (India), 2017. ISBN: 978-1-25-902576-1.

[3] Zuckerman at el, *An Introduction to The Theory of Numbers*, fifth edition, Wiley India (P) Ltd, 2008, ISBN: 978-81-265-1811-1.

[4] B M Roy, *A Study on Standard Quadratic Congruence of Prime Modulus having Solutions Consecutive- Integers*, (JETIR),ISSN: 2349-5162, Vol-08, Issue-07, July-21.

[5] B M Roy, *Formulation of Solutions of a Special Standard Quadratic Congruence modulo an Even Prime Integer raised to the power n*, International Journal of Physics and Mathematics (IJPM), ISSN: 2664-8644, Vol-03, Issue-02, Aug-21.

[6] B M Roy, *Formulation of Standard Quadratic Congruence of Even Composite Modulus modulo an even prime raised to the power n*, International Journal of Research in Applied Science & Engineering Technology (IJRASET), ISSN: 2321-9653, Vol-09, Issue-09, Aug-21.