INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 5, Issue 5)
Available online at: www.ijariit.com

Rp-122: Formulation of solutions of a special standard quadratic congruence of composite modulus- An even multiple of a power of an odd positive integer

B. M. Roy
roybm62@gmail.com
Jagat Arts, Commerce and Indiraben Hariharbhai Patel Science College,
Goregaon, Maharashtra

ABSTRACT

In this study, a special standard quadratic congruence of composite modulus-an even multiple of Power of an odd positive integer is studied rigorously and a very simple formula for the solutions of the congruence is established. It is found that congruence has many incongruent solutions. The solutions can be obtained without any pen & Paper. It can be calculated orally. The congruence was not formulated earlier. This is the first time a formulation of the solutions of the said congruence is made available by the author. This is the merit of the paper.

Keywords— *Composite modulus, Formulation, Quadratic congruence.*

1. INTRODUCTION

The author already formulated many standard quadratic, cubic, biquadratic and congruence of higher degree of prime and composite modulus. All are published in different international science journals successfully [1], [2], [3], [4], [5], [6], [7]. Even many more are remained to formulate. Here is one such a very special type of standard quadratic congruence of a very special composite modulus is considered for formulation. It is of the type:

$$x^2 \equiv a^2 \ (mod\ 2^m a^n);\ m \geq 3.$$

2. LITERATURE REVIEW

The congruence under consideration is

$$x^2 \equiv a^2 \ (mod\ 2^m a^n);\ m \geq 3.$$

It was not formulated by earlier mathematicians. No formulation for its solutions are found in the literature of mathematics. First time the author is going to present its formulation. Such types of congruence are generally solved using Chinese Remainder Theorem (C R T) [8]. It takes a long time for solutions. Sometimes the problems seems to be solved impossible. This is the demerit of the C-R -T method.

3. NEED OF RESRARCH

The demerits of the CRT method is the main problem to the students. To eliminate the demerits, formulation is very necessary. The author wished to formulate the congruence and to wants to present his research in this paper. This is the need of this paper.

4. PROBLEM STATEMENT

“To formulate a standard quadratic congruence of composite modulus of the type:

$$x^2 \equiv a^2 \ (mod\ 2^m a^n)"$$

5. ANALYSIS AND RESULTS

Consider the congruence to be formulated: $x^2 \equiv a^2 \ (mod\ 2^m a^n)$; a an odd positive integer.

For solutions, consider

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

Then,

$$x^2 \equiv (a^{n-1}.2^{m-1}k \pm a)^2 \text{ (mod } a^n.2^m)$$

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

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

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

$$\equiv\ a^2 \ (mod\ a^n.2^m),$$

by binomial expansion formula.

Thus, $x \equiv a^{n-1}.2^{m-1}k \pm a\ \ (mod\ a^n.2^m)$ is a solution of the said congruence

$$x^2 \equiv a^2 \ (mod\ a^n.2^m).$$

But, if we consider $k = 2a$,

Then

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

$$\equiv a^n2^m \pm a\ \ (mod\ a^n.2^m)$$

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

Which is the same solution as for $k = 0$.

Similarly, for higher values of k, the solutions repeats as for $k = 1, 2, 3, \dots ..$

Therefore, all the required solutions are given by

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

These are $2(2a) = 4a$ incongruent solutions for all values of k. The congruence has two solutions for every value of k and k has different values.

6. ILLUSTRATIONS

Consider the congruence

$$x^2 \equiv 9 \ (mod\ 432).$$

It can be written as

$$x^2 \equiv 9 \ (mod\ 27.16)\ i.e.\ \ x^2 \equiv 3^2 \ (mod\ 3^3.2^4)$$

with

$$a = 3\ , and\ m = 4, \qquad n = 3.$$

Such congruence always has $4a = 4.3 = 12$ solutions.
Those solutions are given by

$$x \equiv a^{n-1}.2^{m-1}k \pm a \ (mod\ a^n.2^m); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 3^{3-1}.2^{4-1}k \pm 3\ \ \equiv 72k \pm 3 \ (mod\ 3^3.2^4); k = 0, 1, 2,3, 4, 5.$$

$$i.e.\ x \equiv 72k \pm 3 \ (mod\ 432); k = 0, 1, 2, 3, 4, 5.$$

$$i.e.\ x \equiv 0 \pm 3; 72 \pm 3; 144 \pm 3; 216 \pm 3; 288 \pm 3; 360 \pm 3 (mod\ 432)$$

$$i.e. x \equiv 3, 429; 69, 75; 141, 147; 213, 219; 285, 291; 357, 363\ \ (mod\ 432).$$

$$i.e. x \equiv 3, 69, 75, 141, 147, 213, 219, 285, 291, 357, 363, 429 \ (mod\ 432).$$

These are the twelve solutions of the congruence under consideration.

Consider the congruence

$$x^2 \equiv 225 \ (mod\ 27000).$$

It can be written as

$$x^2 \equiv 15^2 (mod\ 15^3.2^3)$$

with

$$a = 15, \qquad m = 3, \qquad n = 3.$$

Such congruence always has $4a = 4.15 = 60$ solutions.

Those solutions are given by

$$x \equiv a^{n-1}.2^{m-1}k \pm a \ (mod\ a^n.2^m); k = 0, 1, 2, 3, 4, \dots \dots .., (2.15 - 1)$$

$$i.e.\ x \equiv 15^{3-1}.2^{3-1}k \pm 15 \ \equiv 900k \pm 15 \ (mod\ 5^3.2^3); k = 0, 1, 2, 3, 4, \dots \dots \dots 29 .$$

$$i.e.\ x \equiv 0 \pm 15; 900 \pm 15; 1800 \pm 15; 2700 \pm 15; \dots \dots; 24300 \pm 15;$$

$$25200 \pm 15; 26100 \pm 15 \ (mod\ 27000)$$

$$i.e. x \equiv 15, 26985; 885, 915; 1785, 1815; 2685, 2715; \dots \dots ..$$

$$\dots\dots\dots\ 24285, 24315; 25185, 25215; 26085, 26115 \ (mod\ 27000).$$

These are the **sixty** solutions of the congruence under consideration.

Consider the congruence

$$x^2 \equiv 25 \ (mod\ 4000).$$

It can be written as

$$x^2 \equiv 5^2 (mod\ 5^3.2^5)$$

With

$$a = 5, \qquad m = 5, \qquad n = 3.$$

Such congruence always has $4a = 4.5 = 20$ solutions.

Those solutions are given by

$$x \equiv a^{n-1}.2^{m-1}k \pm a \ (mod\ a^n.2^m); k = 0, 1, 2, 3, 4.$$

$$i.e.\ x \equiv 5^{3-1}.2^{5-1}k \pm 5 \ \equiv 400k \pm 5 \ (mod\ 5^3.2^5); k = 0, 1, 2, 3, 4.$$

$$i.e.\ x \equiv 0 \pm 5; 400 \pm 5; 800 \pm 5; 1200 \pm 5; 1600 \pm 5; 2000 \pm 5; 2400 \pm 5;$$

$$2800 \pm 5; 3200 \pm 5; 3600 \pm 5 \ (mod\ 4000)$$

$$i.e. x \equiv 5, 3995; 395, 405; 795, 805; 1195, 1205; 1595, 1605; 1995, 2005;$$

$$2395, 2405; 2795, 2805; 3195, 3205; 3595, 3605 \ (mod\ 4000).$$

These are the **twenty** solutions of the congruence under consideration.

7. CONCLUSION

Thus, it can be concluded that the congruence under consideration $x^2 \equiv a^2 \ (mod\ a^n.2^m)$, is formulated successfully for an odd positive integer a and has $4a$ solutions which can be given by $x \equiv a^{n-1}.2^{m-1}\ k \pm a \ (mod\ a^n.2^m); k = 0, 1, 2, \dots \dots \dots (2a - 1)$.

8. MERIT OF THE PAPER

Formulation is the merit of this paper. A special type of standard quadratic congruence of composite modulus is formulated, which was not formulated earlier. The formulation is time-saving and very simple. Sometimes the solutions can be obtained orally.

9. REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[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] H S Zuckerman at el, 2008, An Introduction to The Theory of Numbers, fifth edition, Wiley student edition, INDIA, ISBN: 978-81-265-1811-1.