Research Journal of Mathematical and Statistical Sciences ISSN 2320-6047
Vol. **7(2),** 30-32, May **(2019)** *Res. J. Mathematical and Statistical Sci.*

Short Communication

Formulation of solutions of a class of standard cubic congruence of even composite modulus-a power of an odd positive integer multiple of a power of three

B.M. Roy
Department of Mathematics, Jagat Arts, Commerce and I.H.P. Science College, Goregaon, Dist. Gondia, MS-441801, India
roybm62@gmail.com

Available online at: www.iscamaths.com , www.isca.in , www.isca.me
Received 24th January 2019, revised 3rd April 2019, accepted 2nd May 2019

Abstract

In this paper, a special class of standard cubic congruence of even composite modulus- a power of an odd positive integer multiple of power of three- is formulated. The established-formula is tested true. First time, a formula is developed for the solutions of the standard cubic congruence of the said type. Without formulation, it was very difficult to find the solutions of such cubic congruence. Formulation makes it possible to do so. Here lies the merit of the paper.

Keywords: Cubic congruence, composite number, Chinese remainder theorem, power modulus.

Introduction

A cubic congruence of prime modulus is a congruence of the type: $x^3 \equiv a \ (mod\ p); p$ being an odd positive integer. If p is replaced by a composite integer, then it is called a cubic congruence of composite modulus. It is found that some cubic congruence has exactly one solution; some other has exactly three solutions and some has no solutions. e.g. The congruence: i. $x^3 \equiv 5\ (mod\ 11)$ has exactly one solution $x \equiv 3\ (mod\ 11)$; ii. $X^3 \equiv 6\ (\text{mod } 7)$ has exactly three solutions $x \equiv 3, 5, 6\ (\text{mod } 7)$; $x^3 \equiv 2\ (\text{mod } 7)$ has no solution.

Author has formulated some standard cubic congruence of composite modulus. Here is the generalization of his previous paper on standard cubic congruence of composite modulus. It is said that the standard cubic congruence: $x^3 \equiv a\ (mod\ p)$ is solvable if a is cubic residue of p[1].

Literature Review

Some discussion is found about the general cubic congruence on internet, also the cubic reciprocity law is discussed. The standard cubic congruence has not been considered and discussed systematically in the literature of mathematics. Much had been written on standard quadratic congruence. A detailed study is found in the literature. Not more literature on cubic congruence is found but only a definition of it[2].

The author already formulated a class of standard cubic congruence of the type $x^3 \equiv b^3\ (mod\ 3^n)$ with solutions $x \equiv 3^{n-1}k + b\ (mod\ 3^n) for\ k = 0, 1, 2$, with exactly three solutions and it is published in *IJRULA, Vol. 1, Issue-8, Nov. 2018*[3].

Also, the cubic congruence of the type $x^3 \equiv a^3\ (mod\ 3^n.b)$, for an integer $b \neq 3l$ with three solutions: $x \equiv 3^{n-1}bk + a\ (mod\ 3^n.b) for\ k = 0, 1, 2,$ is published in *IJRULA, Vol.1, Issue-9,* Dec. *2018*[4].

Also the cubic congruence of the type: $x^3 \equiv a^3 (\text{mod } 3^n.b^r)$ $b \neq 3l$ with three solutions

$x \equiv 3^{n-1}.b^r.k + a\ (\text{mod } 3^n.b^r)$; $k = 0, 1, 2$ is Published in IJRIAR, Vol.03, Issue -1, Jan. 2019, ISSN: 2659-1561[5].

One more research paper on standard cubic congruence of even composite modulus of the type:

$x^3 \equiv a^3\ (mod\ 2^m.3^n)$; m, n $> 1, a$ any positive integer with three solutions given by

$x \equiv 3^{n-1}2^m k + a\ (mod\ 2^m.3^n); k = 0, 1, 2$ and is published in IJARIIT, Vol-5, Issue-1, Jan-Feb. 2019[6].

Here the congruence under consideration is the generalisation of the above papers and also have exactly three solutions.

Need of research: Finding the standard cubic congruence a neglected chapter in Number Theory, the author willingly has gone through the chapter and found much material for the research work. He (the author) tried his best to formulate the generalization of cubic congruence previously formulated and wish to present his effort in this paper. This is the need of this study.

Problem-statement: Here, the problem is "To establish a formulation for the solutions of a class of standard cubic congruence $x^3 \equiv a^3\ (mod\ 2^m.3^n.b^r)$; b being an odd positive integer$b \neq 3l;\ m, n, r\ are\ positive\ integers$.

Results and discussion

Consider the congruence under consideration: $x^3 \equiv a^3(mod\ 2^m 3^n.b^r); b \neq 3l,$ is any odd prime integer.

For its solutions, let
$x = 2^m.3^{n-1}.b^r k + a;\ \ k = 0, 1, 2, 3, 4, 5 \dots \dots \dots$

Then, $x^3 = (2^m.3^{n-1}.b^r.k + a)^3$
$= (2^m.3^{n-1}.b^r.k)^3 + 3.(2^m.3^{n-1}.b^r.k)^2.a + 3.2^m.3^{n-1}.b^r k.a^2 + a^3$
$= a^3 + 2^m.3^n.b^r(2^{2m}.3^{2n-3}b^{2r}k^3 + 2^m.3^{n-2}b^r k^2.a + ka^2)$
$\equiv a^3\ (mod\ 2^m.3^n.b^r)$

Thus, it is a solution of the said congruence.

But for $k = 3$, it can be seen easily that $x \equiv a\ (mod\ 2^m.3^n.b^r)$ which gives the same result as for $k = 0$. Similar results are for other higher values of k.

Therefore, it is concluded that the said congruence has only three solutions for $k = 0, 1, 2$.

These are: $x \equiv 2^m.3^{n-1}.p^r k + a\ \ (mod\ 2^m.3^n.b^r)\ with\ k = 0, 1, 2.$

Sometimes said congruence can be written as:
$x^3 \equiv c\ (mod 2^m.3^n.b^r)$.

In this case, it can be written as
$x^3 \equiv c + k.2^m.3^n.b^r\ (mod\ 2^m.3^n.b^r)^7$

$\equiv a^3\ (mod\ 2^m.3^n.b^r), \qquad if\ \ c + 2^m.3^n.b^r = a^3.$

The solutions are given by as before.

Illustration: Consider the congruence:

$$x^3 \equiv 27\ (mod\ 254016)$$

It can be written as $x^3 \equiv 27\ (mod\ 64.81.49)$.
$i.e.\ x^3 \equiv 3^3\ (mod\ 2^6.3^4.7^2)$.

It is of the type: $x^3 \equiv a^3\ (mod\ 2^m.3^n.b^r)\ with\ a = 3, n = 4, b = 7, m = 6,\ \ r = 2.$

Such congruence has three solutions.

The solutions are given by
$x \equiv 2^m.3^{n-1}.b^r k + a\ (mod\ 2^m.3^n.b^r)$
$\equiv 2^6.3^3.7^2 k + 3\ (mod\ 2^6.3^4.7^2)$
$\equiv 84672k + 3\ (mod\ 254016)\ with\ k = 0, 1, 2.$
$\equiv 0 + 3, 84672 + 3, 169344 + 3\ (mod\ 254016)$
$\equiv 3, 84675, 169347\ (mod\ 250164).$

Consider the congruence: $x^3 \equiv 216\ (mod\ 54000)$.
$i.e.\ x^3 \equiv 6^3\ (mod\ 16.27.125)$

It can also be written as: $x^3 \equiv 6^3\ (mod 2^4.3^3.5^3)$.

It is of the type: $x^3 \equiv a^3\ (mod\ 2^m.3^n.b^r)\ with\ a = 6, n = 4, b = 5, m = 4,\ \ r = 3.$

Such congruence always has three solutions.

The solutions are given by
$x \equiv 2^m.3^{n-1}.b^r k + a\ (mod\ 2^m.3^n.b^r)$
$\equiv 2^4.3^2.5^3 k + 6\ \ (mod\ 2^4.3^3.5^3)$
$\equiv 18000k + 6\ (mod 16.27.125)\ with\ k = 0, 1, 2.$
$\equiv 0 + 6, 18000 + 6, 36000 + 6\ (mod\ 54000)$
$\equiv 6, 18006, 36006\ (mod\ 54000).$

Consider the congruence $x^3 \equiv 2456\ (mod\ 7560)$.

It can be written as $x^3 \equiv 2456 + 2.7560 = 17576 = 26^3\ (mod\ 2^3.3^3.35)$
It is of the type $x^3 \equiv a^3\ (mod\ 2^m.3^n.b^r)\ \ with\ a = 26, m = 3, n = 3, b = 35,\ \ r = 1.$

It has three solutions given by $x \equiv 2^m.3^{n-1}.b^r k + a\ \ (mod\ 2^m.3^n.b^r),\ k = 0, 1, 2.$
$\equiv 2^3.3^2.35\ k + 26\ (mod\ 2^3.3^3.5)$
$\equiv 2520k + 26\ (mod\ 7560)$
$\equiv 26, 2546, 5066\ (mod\ 7560).$

Conclusion

Therefore, it can be concluded that the standard cubic congruence of the type $x^3 \equiv a^3\ (mod\ 2^m.3^n.b^r); b$ being any odd integer, has exactly three solutions given by
$x \equiv 2^m.3^{n-1}.b^r k + a\ (mod\ 2^m.3^n.b^r)\ with\ k = 0, 1, 2.$

Merit of the paper: First time, a cubic congruence of the said type is considered for study and a formula is established to find all the solutions. Such type of standard cubic congruence is not yet formulated. Formulation is the merit of the paper.

References

1. Thomas Koshy (2009). Elementary Number Theory with Applications. 2/e (Indian print, 2009), Academic Press, Page No. 548, supplementary Exercises No.4, ISBN: 978-81-312-1859-4.
2. Zuckerman H.S., Niven I. and Montgomery H.L. (1960). An Introduction to The Theory of Numbers. 5/e, Wiley India (Pvt) Ltd, Page No. 136-136, Exercise-18, ISBN: 978-81-265-1811-1.
3. Roy B.M. (2018). Formulation of solutions of a class of standard cubic congruence modulo nth power of three.

International Journal for Research Under Literal Access (IJRULA), 1(8), 254-257. www.ijrula.com /ARCHIVES.

4. Roy B.M. (2018). Formulation of solutions of a class of standard cubic congruence modulo an integer multiple of nth power of three. *International Journal for Research Under Literal Access* (IJRULA), 1(9), 297-300. www.ijrula.com / ARCHIVES

5. Roy B.M. (2019). Formulation of solutions of a class of standard cubic congruence modulo rth power of an integer multiple of nth power of three, International Journal of Recent Innovations In Academic research (IJRIAR). 3(1). https://www.ijriar.com/docs, ISSN(online): 2635-3040, ISSN(print): 2659-1561.

6. Roy B.M. (2019). Formulation of a class of standard cubic congruence of even composite modulus. *International Journal of Advance Research, Ideas and Innovations in Technology(IJARIIT),* 5(1). *https://www.ijariit.com, ISSN:2454-132X.*

7. Roy B.M. (2016). Discrete Mathematics & Number Theory. 1/e, Das Ganu Prakashan, Nagpur, India, 88. ISBN: 978-93-84336-12-7.