International Journal of Physics and Mathematics
www.physicsjournal.net
Online ISSN: 2664-8644, Print ISSN: 2664-8636
Received: 26-05-2021; Accepted: 12-06-2021; Published: 27-06-2021
Volume 3, Issue 1, 2021, Page No. 31-34

Solving some special classes of standard congruence of prime modulus of higher degree

B M Roy[1], A A Qureshi[2*]
[1] Head, Department of Mathematics, Jagat Arts, Commerce & I. H. P. Science College, Goregaon, Maharashtra, India
[2] Head, Department of Mathematics, D R B Sindhu Mahavidyalaya, Nagpur, Maharashtra, India

Abstract
In this paper, some special classes of standard congruence of prime modulus of higher degree are considered for study. The main aim was to find a method of finding their solutions. After the rigorous study, it is found that each of the first two congruence have unique solution while the second two have exactly three solutions each. The formula/method for solutions obtained is tested by citing numerical examples and verified true. Now it is possible to solve the said congruence very easily in the least time.

Keywords: congruence of higher degree, fermat's theorem, inverse-modulo a prime, prime modulus

Introduction

A congruence of the type: $x^n \equiv a\ (mod\ p), p\ an\ odd\ prime,$ is called a standard congruence of (higher) degree n. The congruence is called solvable if a is nth power residue of p [1].

Many more congruence is solved by a number of mathematicians establishing formulae or algorithmic methods. Even then many more congruence are yet remain to formulate. The authors have successfully formulated many such congruence [5], [6], [7], [8], [9]. Here, four such congruence are considered for solutions. No method or formula is found for their solutions in the literature of mathematics. Without using any formula, such congruence become more complicated to find solutions. In [2], Problem-7, page-115, a problem is found: If $(a,p) = 1$, and p is prime such that $p \equiv 2\ (mod\ 3)$, then the congruence: $x^3 \equiv a\ (mod\ p)$, has the unique solution given by $x \equiv a^{\frac{2p-1}{3}} (mod\ p)$. Abruptly, an idea of these congruence under consideration come in the authors' mind. Such type of congruence are:

$x^7 \equiv 3\ (mod\ 11)$; $x^{11} \equiv 11\ (mod\ 17)$; $x^{15} \equiv 7\ (mod\ 23); x^{19} \equiv 2\ (mod\ 29)$;

And $4x^3 \equiv 3\ (mod\ 5)$; $x^9 \equiv 5\ (mod\ 13); x^{13} \equiv 3\ (mod\ 19), etc.$

These are of the types: $x^{\frac{2p-1}{3}} \equiv b\ (mod\ p)\ and\ ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$;

$x^{\frac{2p+1}{3}} \equiv b\ (mod\ p)$; $ax^{\frac{2p+1}{3}} \equiv b\ (mod\ p)\ \ etc.$

The authors have tried their best to find the methods of solutions of these congruence and their efforts are presented here in this paper.

Problem-Statements

The problems are stated in the form of theorems as under

Theorem-1: The congruence: $x^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$, $p\ odd\ prime, p \equiv 2\ (mod\ 3)$, has a unique solution given by $x \equiv b^3 (mod\ p)$.

Theorem-2: The congruence: $ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$, $p\ odd\ prime, p \equiv 2\ (mod\ 3)$, has a unique solution given by $x \equiv \bar{a}^3 b^3 (mod\ p)$.

Theorem-3: The congruence: $x^{\frac{2p+1}{3}} \equiv b\ (mod\ p)$, $p\ odd\ prime\ and\ p \equiv 1\ (mod\ 3)$, can be reduced to a standard cubic congruence of prime modulus and has exactly three incongruent solutions.

Theorem-4: The congruence: $ax^{\frac{2p+1}{3}} \equiv b\ (mod\ p)$, $p\ odd\ prime\ and\ p \equiv 1\ (mod\ 3)$, can be reduced to a standard cubic congruence of prime modulus and hence has exactly three incongruent solutions.

Literature Review

Proof of Theorem-1

As $p \equiv 2\ (mod\ 3), hence\ p - 2 = 3k \Rightarrow \frac{2p-1}{3} = 2k + 1,$ odd an integer.

If $x \equiv r\ (mod\ p)$ is a solution of the congruence: $x^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$**,** then

$r^{(2p-1)/3} \equiv b\ (mod\ p)\ giving\ \ r^{2p-1} \equiv b^3 (mod\ p)$.

It can also be written as $r^{p-1}.r^{p-1}.r \equiv b^3 (mod\ p)$ which gives

$r \equiv b^3 (mod\ p),\ \ by\ Fermat's\ Little\ Theorem.$

Thus, the congruence has unique solution $x \equiv b^3\ (mod\ p)$.

Proof of theorem-2

Consider the second congruence: $ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$.

If $x \equiv r\ (mod\ p)$ is a solution of the congruence: $ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p)$**,** then

$ar^{\frac{2p-1}{3}} \equiv b\ (mod\ p)\ giving\ a\bar{a}\, r^{\frac{2p-1}{3}} \equiv \bar{a}b (mod\ p)$

$i.e.\, r^{2p-1} \equiv (\bar{a}b)^3 (mod\ p)$; where $\bar{a}$ is the *inverse modulo prime p*
$i.e.\, \bar{a}a \equiv 1\ (mod\ p)$[3].

It can also be written as $r^{p-1}.r^{p-1}.r \equiv \bar{a}^3 b^3 (mod\ p)$ which gives: $r \equiv \bar{a}^3 b^3\ (mod\ p)$
$by\ Fermat's\ Little\ Theorem.$
Thus, the congruence has unique solution $x \equiv \bar{a}^3 b^3 \equiv (\bar{a}b)^3\ (mod\ p)$.

Proof of theorem-3

As $p \equiv 1\ (mod\ 3), hence\ p - 1 = 3k \Rightarrow \frac{2p+1}{3} = 2k + 1,$ odd an integer.
Consider the second congruence $x^{\frac{2p+1}{3}} \equiv b\ (mod\ p)$.
If $x \equiv r\ (mod\ p)$ is a solution of the congruence, then

$r^{(2p+1)/3} \equiv b\ (mod\ p)\ giving\ r^{2p+1} \equiv b^3$.

Then, $r^{p-1}.r^{p-1}r^3 \equiv b^3\ (mod\ p), so, r^3 \equiv b^3\ (mod\ p)$.
Therefore, r is a solution of the congruence $x^3 \equiv b^3\ (mod\ p), by\ Fermat's\ Theorem.$
But $p \equiv 1\ (mod\ 3), hence\ the$ congruence has exactly three solutions modulo p and the solutions can be obtained by author's method [4].

Proof of theorem-4

Consider the second congruence $ax^{\frac{2p+1}{3}} \equiv b\ (mod\ p)$.

If $x \equiv r\ (mod\ p)$ is a solution of the congruence, then

$ar^{(2p+1)/3} \equiv b\ (mod\ p)\ giving a\bar{a}\, r^{(2p+1)/3} \equiv \bar{a}b\ (mod\ p) i.e.\, r^{2p+1} \equiv (\bar{a}b)^3\ (mod\ p)$.

Then, $r^{p-1}.r^{p-1}r^3 \equiv (\bar{a}b)^3\ (mod\ p), so, r^3 \equiv (\bar{a}b)^3\ (mod\ p)$.
Therefore, r is a solution of the congruence $x^3 \equiv (\bar{a}b)^3\ (mod\ p), by\ Fermat's\ Theorem.$
But $p \equiv 1\ (mod\ 3), hence\ the$ congruence has exactly three solutions modulo p and the solutions can be obtained by author's method [4].

Illustrations

Illustration of theorem-1 by example

Consider $x^7 \equiv 3\ (mod\ 11)\ \ with\ b = 3, p = 11\ giving\ 7 = \frac{2.11-1}{3}$.

Therefore, given congruence is of the type $x^{(2p-1)/3} \equiv b\ (mod\ p)\ and\ p \equiv 2\ (mod\ 3)$.
It has a unique solution given by: $x \equiv b^3 (mod\ p)$.
Hence the solution of given congruence is: $x \equiv 3^3 = 27 \equiv 5\ (mod\ 11)$.

Verification

Substituting $x \equiv 5 \pmod{11}$ in the given congruence, we get

$$5^7 = 5^3.5^3.5 = 125.125.5 \equiv 4.4.5 = 80 \equiv 3 \ (mod\ 11).$$

Thus $x \equiv 5 \ (mod\ 11)$ satisfies the given congruence and so it is the unique solution of the said congruence which is proved as before. Hence the solution is verified true.

Illustration of theorem-2 by example

Consider the congruence $4x^3 \equiv 3 \ (mod\ 5)\ with\ p = 5, b = 3, a = 4$ giving $3 = \frac{2.5-1}{3}$.

So, the congruence is of the type: $ax^{\frac{2p-1}{3}} \equiv b \ (mod\ p)$.
Then its solution is given by $x \equiv \bar{a}^3 b^3 \ (mod\ p\ )$.
Therefore, for this congruence the solution is: $x \equiv \bar{4}^3 3^3 \ (mod\ p\ )$.
As we know that $4.4 \equiv 1 \ (mod\ 5)$, hence $\bar{a} = 4$,
and solution is $x \equiv 4^3 3^3 \equiv 12^3 \equiv 3 \ (mod\ 5)$.

Verification

Substituting $x \equiv 3 \pmod 5$ in the above congruence, we get

$$4.3^3 = 4.3.3.3 = 108 \equiv 3 \ (mod\ 11).$$

Thus $x \equiv 3 \ (mod\ 5)$ satisfies the given congruence and so it is the unique solution of the congruence which is proved as before. Hence the solution is verified true.

Illustration of theorem-3 by example:

Consider the congruence $x^9 \equiv 2 \ (mod\ 13)\ with$

$$p = 13, b = 2, \text{Giving: } 9 = \frac{2.13+1}{3}.$$

So, the congruence is of the type $x^{\frac{2p+1}{3}} \equiv b \ (mod\ p)\ and\ p \equiv 1 \ (mod\ 3)$.
It can be reduced to a cubic congruence: $x^3 \equiv b^3 \ (mod\ 13)\ i.e. x^3 \equiv 8 \ (mod\ 13)$.
It has three solutions which are the members of the residues of 13.
The residues of 13 are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.
Their cubes congruent to 13 are:
1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12
Therefore, $x \equiv 2, 5, 6 \ (mod\ 13)$ are the three solutions of the congruence.

Verification:

Substituting $x \equiv 2, 5, 6 \pmod{13}$ in the above congruence, we get

$$2^3 \equiv 8, 5^3 \equiv 8, 6^3 \equiv 8 \ (mod\ 13).$$

Thus $x \equiv 2, 5, 6 \ (mod\ 13)$ satisfies the given congruence and so these are the three solution of the congruence which are proved as before. Hence the solutions are verified true.

Illustration of theorem-4 by example

Consider the congruence $3x^9 \equiv 5 \ (mod\ 13)\ with$

$$p = 13, a = 3, b = 5, \text{Giving: } 9 = \frac{2.13+1}{3}.$$

So, the congruence is of the type $ax^{\frac{2p+1}{3}} \equiv b \ (mod\ p)\ with\ p \equiv 1 \ (mod\ 13)$.
It can be reduced to a cubic congruence: $x^3 \equiv \bar{a}^3 b^3 \ (mod\ 13) i.e. x^3 \equiv 9.8 \equiv 7 \ (mod\ 13)$.
It has solutions which are the members of the residues of 13.
The residues of 13 are: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12.
Their cubes congruent to 13 are:

1, 8, 1, 12, 8, 8, 5, 5, 1, 12, 5, 12 But 7 is not a cubic residue of 13.
Therefore, the congruence is not solvable.

Conclusion

In this paper, four congruence are studied and solved. The formulae/methods are tested true by solving suitable examples.

It is found that the congruence: $x^{\frac{2p-1}{3}} \equiv a\ (mod\ p), p\ odd\ prime, p \equiv 2\ (mod\ 3)$ has exactly one solution. It is given by $x \equiv a^3 (mod\ p)$.

Also, the congruence $ax^{\frac{2p-1}{3}} \equiv b\ (mod\ p), p\ odd\ prime,\ p \equiv 2\ (mod\ 3)$ has exactly one solution. It is also given by: $x \equiv \bar{a}^3 b^3 (mod\ p)$.

Also, the congruence $x^{\frac{2p+1}{3}} \equiv b\ (mod\ p), p\ odd\ prime,\ p \equiv 1\ (mod\ 3)$ can be reduced to a standard cubic congruence of prime modulus and has exactly three incongruent solutions and can be solved by author's method.

Also, the congruence $ax^{\frac{2p+1}{3}} \equiv b\ (mod\ p), p\ odd\ prime,\ p \equiv 1\ (mod\ 3)$ can be reduced to a standard cubic congruence of prime modulus; and has exactly three incongruent solutions and can be solved by author's method.

Acknowledgement

The first two theorems are studied and formulated by the first author (B M Roy) and the next two theorems are studied by the second author (A A Qureshi). Efforts of both the authors are presented here in the same paper as a single paper.

Reference

1. Koshy Thomas, *Elementary Number Theory with Applications*, Academic Press, Second Edition, Indian print, New Dehli, India, ISBN,2009:978-81-3:12:1859-4.
2. Zuckerman *et al*, *An Introduction to The Theory of Numbers*, fifth edition, Wiley India (P) Ltd, 2008.
3. Burton David M., *Elementary Number Theory*, seventh edition, Mc Graw Hill education (India), 2017.
4. Roy BM. *A Review of Finding Solutions of Standard Cubic Congruence of Prime Modulus*, (IJTSRD), ISSN: 2456-6470, 4(3).
5. Roy BM. *Formulation of solutions of of a special type of standard congruence of prime modulus of higher degree*, (IJARIIT), ISSN: 2454-132X, 4(2).
6. Roy BM, *Formulation of Two Special Classes of Standard Congruence of Prime Modulus of Higher Degree*, (IJTSRD), ISSN: 2456-6470, 3(3).
7. Roy BM, *Solutions of a special standard congruence of prime modulus of higher degree*, (IJRTI) 2456-3315, 5(2).
8. Roy B M & Qureshi A A., *Formulation of Some Classes of Solvable Standard Quadratic Congruence modulo a Prime Integer - Multiple of Three & Ten*, (IJSRED),ISSN: 2581-7175, 2(2).
9. Roy BM, Qureshi AA, *Solving Standard Cubic Congruence of composite modulus modulo a product of powered odd prime and powered three*, Proceedings (special issue: International Research journal of Science and Technology) National Conference on Emerging Trends In Science and Technology, 10 th Jun-21, Bharsingi, M. S., India.