Formulation of solutions of two special standard congruence of prime modulus of higher degree.

Prof. B. M. Roy

Head, Department of Mathematics
Jagat Arts, commerce & I. H.P. Science College, Goregaon (Gondia), M. S., India.
(Affiliated to RTM Nagpur University, Nagpur)
Pin-441801

***ABSTRACT*: In this paper, two congruence of higher degree of prime modulus are considered and a successful attempt has been made to formulate their solutions. Without the formulation, the solutions of the congruence are very difficult. The formulae are established and tested true.**

***Keywords*: Congruence of higher degree; Modular Inverse element; Fermat's Theorem.**

INTRODUCTION

A congruence of the type $x^n \equiv a \pmod p$, with an odd prime integer p, is called a standard congruence of higher degree if $n \geq 3$, a positive integer.

But a congruence of the type $ax \equiv b \pmod m$ is called a linear congruence. It has unique solution if $(a, m) = 1$.

Modular inverse of an element is associated to a linear congruence. So, let us define modular inverse of an integer.

"An integer b is called a modular inverse of another integer a modulo an integer m,

if $ab \equiv 1 \pmod m$". Modular inverse of a is denoted by $\bar{a}$.

Here, b is denoted by $\bar{a}$ i.e. $b = \bar{a}$. So, the ab≡1 (mod m) becomes $a\bar{a} \equiv 1 \pmod m$.

Such an integer is unique if $(a, m) = 1$.

Here, also we want to mention Fermat's theorem:

"If p is an odd prime integer such that $(a, p) = 1$, then, $a^{p-1} \equiv 1 \pmod p$."

Many mathematicians viz. Lagrange, Fermat, worked on congruence of higher degree.

Even there is hope to do more. In this context, this paper is prepared.

PROBLEM STATEMENT

The congruence $x^{p-2} \equiv a \pmod p$ where p is a positive prime integer and $1 \leq a \leq p-1$, has a unique solution $x \equiv \bar{a} \pmod p$, $\bar{a}$ being the inverse element of a modulo p.

Also, the congruence $ax^{p-2} \equiv b \pmod p$ with p an odd prime integer, $(a, b, p) = 1$,has a unique solution $x \equiv a\bar{b} \pmod p$, $\bar{b}$ being the inverse element of b modulo p. Formulation of these solutions is the problem here.

Proof of the statements:

Here proof of the statements made above are given.

Proof of the first statement:

Consider the congruence in the 1st statement: $x^{p-2} \equiv a \pmod p$, p an odd positive prime integer and $1 \leq a \leq p-1$. So, $(a, p) = 1$.

Let r be a solution of the congruence considered.

Then, $r^{p-2} \equiv a \pmod p$ giving $r^{p-1} \equiv ar \pmod p$ with $(r, p) = 1$.

Therefore, by Fermat's Theorem, we have from above congruence that $1 \equiv ar \pmod p$.

This gives $ar \equiv 1 \pmod p$ ....………………………………………………………..(1)

Then by definition of inverse element, we get $r \equiv \bar{a}(\text{mod } p) \ldots\ldots\ldots\ldots\ldots\ldots(2)$

Thus, the solution of the congruence considered is $x \equiv \bar{a}(\text{mod } p)$.

Uniqueness of proof:

As we know that every residue of prime positive integer p has exactly one inverse element, hence the residue r has a unique inverse element. Therefore, $\bar{a}$ is the only inverse element ofa.

Let r_1 be another solution. Then from (1): $ar_1 \equiv 1 \ (\text{mod } p)$ giving $r_1 \equiv \bar{a}(\text{mod } p)$ ….…………(3).

From (2) & (3): $r - r_1 \equiv o \ (\text{mod } p)$ giving $r \equiv r_1(\text{mod } p)$ and so $r = r_1$.

Therefore, solution is unique.

proof of second statement:

Consider the congruence as in the statement (B) above: $ax^{p-2} \equiv b \ (\text{mod } p)$, p being odd prime integer, $(a, b, p) = 1$.

Let r be a solution of the congruence.

Then $(r, p) = 1$ and hence, $ar^{p-2} \equiv b \ (\text{mod } p)$ giving $ar^{p-1} \equiv rb \ (\text{mod } p)$.

By Fermat's Theorem, we have $a.1 \equiv rb \ (\text{mod } p)$ giving $a \equiv rb \ (\text{mod } p)$

i. e. $br \equiv a \ (\text{mod } p)$ …………………………………………………………………..(4)

So, $r \equiv a\bar{b}(\text{mod } p)$ ….……………………………………………………………(5)

Therefore, the solution of the congruence considered is $x \equiv a\bar{b}(\text{mod } p)$.

Uniqueness of proof:

As $\bar{b}$ is always unique and a is given, hence $a\bar{b}$ is unique.

Relation (4) is equivalent to the linear congruence $bx \equiv a \ (\text{mod } p)$.

As $(a, b, p) = 1$, hence the congruence has unique solution.

Therefore the congruence in consideration has a unique solution.

Illustration by examples

Let us consider the congruence $x^9 \equiv 3 \ (\text{mod } 11)$. Here $p = 11, a = 3; 9 = 11 - 2 = p - 2$.

Then the congruence is of the type $x^{p-2} \equiv a \ (\text{mod } p)$.

Hence the solution is $x \equiv \bar{a}(\text{mod } p)$

$$\text{i. e. } x \equiv \bar{3} = 4 \ (\text{mod } 11) \text{ as } 3.4 = 12 \equiv 1 \ (\text{mod } 11).$$

Verification:

If $x \equiv 4 \ (\text{mod } 11)$, then

$4^9 = 4^3.4^3.4^3 = 64.64.64 \equiv (-2).(-2).(-2) = -8 \equiv 3 \ (\text{mod } 11)$.

Therefore, $x \equiv 4 \ (\text{mod } 11)$satisfies the congruence $x^9 \equiv 3 \ (\text{mod } 11)$.

Hence $x \equiv 4 \ (\text{mod } 11)$ is the required unique solution.

Let us consider the congruence $3x^5 \equiv 2 \ (\text{mod } 7)$.

Here $p = 7, a = 3, b = 2, 5 = 7 - 2 = p - 2$.

Then the congruence is of the type $ax^{p-2} \equiv b \ (\text{mod } p)$.

Hence the solution is $x \equiv a\bar{b}(\text{mod } p)$

$$\text{i. e. } x \equiv 3.\bar{2} = 3.4 = 12 \equiv 5 \ (\text{mod } 7) \text{ as } 2.4 = 8 \equiv 1 \ (\text{mod } 7).$$

i. e. $x \equiv 5 \ (\text{mod } 7)$is the solution.

Verification:

If $x \equiv 5 \pmod 7$, then

$3.5^5 = 3.25.25.5 \equiv 3.4.4.5 \equiv (15).(16) \equiv 1.2 = 2 \pmod 7$.

Therefore, $x \equiv 5 \pmod 7$ satisfies the congruence $3.x^5 \equiv 2 \pmod 7$.

Hence $x \equiv 5 \pmod 7$ is the required unique solution.

CONCLUSION

Thus, the conclusion now can be made that the congruence $x^{p-2} \equiv a \pmod p, 1 \leq a \leq p-1$, p an odd prime integer, has a unique solution $x \equiv \bar{a} \pmod p$.

Also, the congruence $ax^{p-2} \equiv b \pmod p, (a, b, p) = 1$, p odd prime integer, has a unique solution $x \equiv a\bar{b} \pmod p$.

MERIT OF THE PAPER

As seen in above examples, such congrence can be solved very easily using estsblied formulae but by no other method such easily.This is the merit of the paper.

REFERENCE

[1] Thomas Koshy, Elementary Number Theory with Applications, 2/e, Academic press, 2009 (India)
[2] Roy B. M., Discrete Mathematics and Number Theory, Das Ganu Prakashan, Nagpur(India), Jan. 2016
[3] Niven I., Zuckermann H. S., Montgomery H. L., (1960), Reprint 2008), An Introduction to Theory of Numbers, 5/e, Wiley India (Pvt.) Ltd.