Received Date: April 2024 Revised: May 2024 Accepted: June 2024

A Study on the Solution of Modular Polynomial

Yogendra Prasad Shah
Department of Mathematics, Patan Multiple Campus
yog.9841@gmail.com.

Uday Kumar Karn
Department of Mathematics, Patan Multiple Campus
Uday.karn@pmc.tu.edu.np
doi: https://doi.org/10.3126/ppj.v4i01.70279

Abstract

This study deals with the analysis of modular solutions with their suitable conditions for existence or non-existence of solutions to modular equations with the lifting of solutions and their structure to the equations like $f(x)\equiv 0(mod p^k)$.where p is prime and whose co-efficient are divisible by p has at most n solutions. If the coefficients are not divisible, then their solutions becomes less than or greater than n depending upon the modulus and the solutionof lifting to the equation is tree stem like structures studied.

Key Words: Congruence, modular polynomial, modular solutions, co-primes.

Introduction

The theory of congruence was introduced by Carl Friedrich Gauss (1777-1855) one of the greatest Mathematician of all time. Gauss. Contributed to the theory of numbers in many outstanding ways including the system of arithmetic's of integers and their properties. Although pierre-de Fermat (1601-1665) had earlier studied number theory in a somewhat systematic way. Gauss was the first to develop the subject as a branch of Mathematics rather than just a scattered collection of interesting problems. In his book Disquisitiones Arithemeticae (1801), written at age 24, Gauss introduced the theory of congruences which gained ready acceptance as a fundamental tool for the study of number theory and this congruency concept is known as the modular arithmetic. This is a topic residing under number theory which highlights the power of remainders when solving the problems. According to Gauss let 'm' be an integer for a, b $\in$ Z we write a≡b (mod m) and say "a is congruent to b" modulo m" if m/a-b or a and b leave the same remainder when divided by m, or b is a remainder dividing 'a' by m. Some fundamental ideas of congruences such as rule of addition, multiplication, multiplicative inverse and residue class modulo established as [1]. The theorems of Fermat and Euler are especially noteworthy providing powerful techniques for analyzing the multiplicative aspect of congruences. These two pioneers in number theory worked in widely contrasting ways. Mathematics was avocation for Fermat who was a layer by profession. He communicated his Mathematical ideas by correspondence with other giving very few details of proofs of his assertions. "One of his

claim is known as Fermat's last theorem" although it is not a theorem at all as yet having never been proved. This is discussed in [1].

This study mainly focuses on the nature of the solutions of congruence equations and their relations to the degree of the congruence polynomial of degree ≥1. Further analyze the roots if the algebraic polynomial with the congruence polynomials. More over every algebraic polynomial of degree n has n roots in the real field as well as in complex field. But in the modular, arithmetic's taking modulus to the polynomial it has not necessary to have n roots such type of congruency equations may have no solutions, single solutions or many solutions not necessary to have n solutions. Therefore, we establish the appropriate conditions due to which we can determine the actual nature of solutions depending up on the features of congruence equations: i.e. under which condition does solution exist or not. If exists then what is the number of solutions and how these roots related with the degree of congruence polynomials.

Therefore, this study focuses on a clear and concise suggestions for the conditions of determinations of the number of solutions of depending on the degree of polynomial modulo m and finding their solutions it exists.

This study is a key tool which is useful for as aspect of number theory well as solving Diophantine equation refers to finding an integral solution to a polynomial equation in more than one variable. Such equations have attracted researcher through a long history. This study also helpful for modular arithmetic hardware algorithms for public key cryptosystem and used in having pseudo-random number generation and data cyber security. So, the findings to this study become a fundamental and important tool for the further study in the number theory.

Objective

For solving the congruence polynomial equations of degree n, provided methods and rule cannot suggest the exact idea about the nature of solution, i.e. when the congruence equations have solutions or when it have no solutions, if the solutions exists then what is the number of solutions. Therefore, to find the appropriate conditions for existence, non-existence and number of existing solutions depending upon the features of modular equations. Further to study the different conditions for existence of the solution to the polynomial congruence like $f(x) \equiv 0 (mod\ p^k)$ and lifting of the solutions to the p^{k+1}, p^{k+2} ... with their structure details.

Preliminaries

Divisibility; Suppose that a and b be the two integers with $a \neq 0$ and if there exist an integer x such that $b = ax$ .Then the integer b is called divisible by an integer a and is denoted by $a|b$. We also say that b is multiple of a and that a is called the divisor of b.If $a|b$ and $0 < a < b$ then a is a proper divisor of b

Definition 1. Let the complete residue system modulo m is $r_1, r_2 \dots \dots r_n$,then number of solutions of $f(x) \equiv 0(mod\ m)$ is the number of the r_i such that $f(r_i) \equiv 0(mod\ m)$.

Some examples - $x^2 + 1 \equiv 0\ (mod\ 7)$has no solution.

$x^2 + 1 \equiv 0\ (mod\ 5)$ has two solutions

$x^2 - 1 \equiv 0\ (mod\ 8)$ has four solutions

Definition 2. Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_h$ be the polynomial of degree n .If $a_n \not\equiv 0(mod\ m)$ then the degree of congruence $f(x) \equiv 0(mod\ m)$ is n and if $a_n \equiv 0(mod\ m)$, let j be the largest integer such that $a_j \not\equiv 0(mod\ m)$,then the degree of the congruence is j .If there is no such integer j ,that is if all coefficients of $f(x)$ are multiple of m, no degree is assigned to the congruence.

Example 2: $f(x) = 6x^3 + 3x^2 + 2x + 9$ then $f(x) \equiv 0(mod\ 5)$ is of degree 3 and $f(x) \equiv 0(mod\ 2)$ is of degree 2. where as $f(x)$ is of degree 3

Definition 3:(congruence and incongruence solution) The Integer which satisfy a given linear congruence modulo m and belonging to the same residue class are called congruent solutions. If they belong to different modulo class are called incongruent solution.

Definition 4 - Let $(q, n) = 1$ then an integer q is called quadratic residue modulo n ,if it is congruent to perfect square ($mod\ n$) that is there exist an integer x such that $x^2 \equiv q\ (mod\ n)$ otherwise q is called a quadratic non residue $(mod\ n)$

Definition-5 If $f(a) \equiv 0(mod\ p^j)$, $f(b) \equiv 0(mod\ p^k), j < k$, and $a \equiv b(mod\ p^j)$, then we say that b lies above a or a lifts to b.

Definition-6 If $f(a) \equiv 0(mod\ p^j)$, then the root a is called nonsingular if $f'(a) \neq 0(mod\ p)$. Otherwise, it is called singular.

Solutions of Congruences

Suppose $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$. denote a polynomial of degree n having integral coefficients. If an integer u such that $f(u) \equiv 0(mod\ m)$,then u is called a solution of the congruence $(x) \equiv 0(mod\ m)$. An integer is a solution of congruence or not which depends up on the modulus m as well as on the polynomial $f(x)$.If v is another integer such that $u \equiv v(mod\ m)$,$and\ f(v) \equiv 0(mod\ m)$ then v, is also a solution of $f(x) \equiv 0(mod\ m)$. So we shall say that $x \equiv u(mod\ m)$ is a solution of $f(x) \equiv 0(mod\ m)$, meaning that every integer congruent to u modulo m satisfies $f(x) \equiv 0(mod\ m)$.But in counting the number of solution of a congruence restrict attention to a complete residue system belonging to the modulus

Example 1.-The congruence $x^2 - x + 4 \equiv 0(mod\ 10)$ has solutions $x = 3$ and $x = 8$. Except this, all-other solutions are of the from $3 \pm 10t, 8 \pm 10t$ where t is a non zero integer. In counting the number of solutions of a congruence, we restrict to a complete residue system belonging the modulus. So, there are only two solutions that is x = 3, and 8, that are the only numbers belonging to complete residue 0, 1, 2, · · ·, 9 of ($mod\ 10$).

The congruence $x^2 - 7x + 2 \equiv 0(mod10)$has exactly four solutions they are x =3, 4, 8, 9. Thus if, $f(x) \equiv 0(mod10)$ as a solution $x = a$ then all integers x satisfying $f(x) \equiv 0(mod10)$ are also solutions, so this entire congruence class is counted as a single solution.

Linear congruences

The congruence of the form $ax \equiv b(mod\ m)$where $a,\ b$ are given integer and m is given positive integer, is called linear congruence.

Which is equivalent to the equation $ax + my = b$ where we of course only consider integral solutions $x\ and\ y$. We know from linear Diophantine equation this equation is solvable if and only if $d = (a, m)$ divides b and if $x_o, y_0$is a solution then the complete set of solution is given by

$$x = x_0 + \frac{m}{d}n, y = y_0 + \frac{a}{d}n$$

We get d pairwise incongruent x-values modulo m by taking $n = 0,1,2 \ldots\ldots d - 1$, and any solution x is congruent to one of these. This proves the following theorem.

Theorem 1. The solvability of linear congruence $ax \equiv b(mod\ m)$ can easily be described by following

(a) If $(a, m) = 1$ that is $a\ and\ m$ are relatively prime then
There is exactly one incongruent solution modulo m.

(b) If $(a, m) \nmid b$ then the linear congruence has no solution.

(c) If $(a, m)|b$ then there are exactly (a, m) distinct incongruent solution modulo m

If the linear congruence $ax \equiv b(mod\ m)$ has exactly one incongruent solution let it be x_0 then there are infinitely many congruent solutions as
$x_0 + km$,$k \in Z$=.{….−2,−1,0,1,2 ….} ….(1) if this congruence equation has more than one incongruent solution and let x_0 be the first incongruent solution then all other incongruent solutions are given by $x_0 + \frac{m}{d}p(mod\ m)$, $0 \le p \le d - 1$, and infinitely many congruence solutions are calculated by (1)

Example 2. Solve the congruence $17x \equiv 9(mod276)$

Solutions: we have

$$17x \equiv 9(mod\ 276) \ldots (1)$$

$$a = 17, \quad b = 9, \quad m = 276$$

$d = (a, m) = (17,276) = 1 \ \ and \ 1|9$ so the (1) has exactly one incongruent solution modulo 276.

By Euclidean Algorithms 276=17.16+4

17=4.4+1

4=4.1+0

Now, 1=17-4.4

1=17-4(276-17.16)

1=17-4.276+64.17

1=65.17-4.276

65.17=1+4.276 taking mod 276 we have

17(65)≡1+4.276 (mod 276)

17(65)≡1+0 (mod 276)

17(65)≡1 (mod 276)

Multiplying by 9 we get.

17(65.9)≡9 (mod276)

Comparing to (1) we have

$x \equiv 65.9(mod\ 276)$

$x \equiv 585(mod\ 276)$

$x \equiv 33(mod\ 276)$ is only the incongruent solution of (1) so the congruent solutions are

Let $x_0 = 33\ then\ x = 33 + k276 \ \ k \in Z$

That is {…….-243….33, 309……} ans.

Corollary 1. The congruence $ax \equiv 1(mod\ m)$is solvable if and only if $(a, m) = 1$ and in this case any two solutions are congruent modulo m.

Corollary 2. If$(a, m) = 1$, then the congruence $ax \equiv b(mod\ m)$ is solvable for any b and any two solutions are congruent modulo m.

The Congruence $x^2 \equiv a\ (mod\ m)$

Consider the congruence $x^2 \equiv a(mod\ m)$ … (1) We discuss when do the solutions exist, how many solutions are there and how to find them [5].

We will first show that we can always reduce a congruence of the form (1) to a congruence of the same form with $(a, m) = 1$

Assume therefore that$(a, m) > 1$, and let p be a prime dividing (a, m) that is $p|a\ and\ p|m$ Suppose x is a solution of (1). Then $p|x^2$and hence $p|x$. Write $x = py$ then (1) is equivalent to $p^2y^2 \equiv a(mod\ m)$ .Divide by p to obtain
(2) $py^2 \equiv a|p\ (mod\ m|p)$… (2)

There are three cases

(i) If $p^2|m\ and\ p^2|a$ then (2) is equivalent to the congruence $y^2 \equiv a|p^2(mod\ m|p^2)$, and for each solution y_0 of this congruence (if there are any), there are p incongruent solutions modulo m of the original congruence (1). These are $x \equiv py_0(mod\ m|p)$. If $(a|p^2, m|p^2) > 1$, we repeat the whole procedure.

(ii) If $p^2|m\ \ but\ p^2 \nmid a$ then (2) is a contradiction. Hence, (1) has no solutions in this case.

(iii) If $p^2 \nmid m\ then\ (p, m|p) = 1$, and hence there is a number c such that $cp \equiv 1\ (mod\ m|p)$. It follows that (2) is equivalent to the congruence $y^2 \equiv ca|p\ (mod\ m|p)$, Any solution y_0 of this congruence yields a unique solution $x \equiv py_0(mod\ m)\ of$ (1). If $ca|p, m|p) > 1$ we can repeat the whole procedure.

Note that if $p^2|a$, then $ca|p = cp.a|p^2 \equiv 1.a|p^2 \equiv\ a|p^2(mod\ m|p)$, i.e. (2) is equivalent to the congruence $y^2 \equiv a|p^2\ (mod\ m|p)$in that case [5].

Example 3. Solve the four congruences:

$(i)\ x^2 \equiv 36\ (mod\ 45)$

Solution: Here (36, 45) = 9 and writing $x = 3y$ we obtain the equivalent congruence $y^2 \equiv 4\ (mod\ 5)$ with the solutions $y \equiv \pm 2(mod\ 5)$ which can be written as $y \equiv 2(mod\ 5) and\ y \equiv -2(mod\ 5)$ incongruent solutions so the congruent solutions are $2 + 5t\ and - 2 + 5t\ \ \ where\ t \in Z$.

(ii) $x^2 \equiv 15\ (mod\ 45)$

Since 9|45 but $9 \nmid 45$ so there is no solution.

$(iii)\ x^2 \equiv 18\ (mod\ 21)$

Since $18,21) = 3$ and write $x = 3y$ and obtain the following sequence of equivalent congruences $9y^2 \equiv 18\ (mod\ 21), 3y^2 \equiv 6(mod\ 7), y^2 \equiv 2(mod\ 7)$ having solutions $y \equiv \pm 3\ (mod\ 7)$. Therefore (iii) has the solution $\equiv \pm 9\ (mod\ 21)$

Euler's criteria: - let p be an odd prime number and a be a positive integer that is relative prime to p then equation

$x^2 \equiv a(mod\ p)$ has solutions if and only if $a^{\frac{p-1}{2}} \equiv 1(mod\ p)$.Equivalently the equation $x^2 \equiv a(mod\ p)$ has no solutions if and only if $a^{\frac{p-1}{2}} \equiv -1(mod\ p)$

Example 4: Solve $x^2 \equiv 899(mod\ 50261)$

Solution- Since, by the above theorem it can be written as
$899^{25130} \equiv 1(mod\ 50261)$ has solutions

To find the solutions we keep adding the modulus $a = 899$ until we get a perfect square

$x^2 \equiv 899 \equiv 899 + 50261 \equiv 899 + 2(50261) \equiv \cdots \ldots \ldots \ldots$

899+4297(50261) =215972416 $\equiv 14696^2(mod\ 50261)$

That is $x^2 \equiv 14696^2(mod\ 50261)$

Which gives $x \equiv 14696(mod\ 50261)$
$x \equiv -14696(mod\ 50261)$
i.e. $x \equiv 35565\ (mod\ 50261)$

Example $\mathbf{5.3x^2 \equiv 13961(mod\ 50261)}$since

$1369^{25130} \equiv -1(mod\ 50261)$ has no solutions.

Theorem 2. Let p be an odd prime and a be an integer that is not divisible by p then the equation

$x^2 \equiv a(mod\ p)$...(1) has no solutions or exactly two solutions

Corollary 3: -Let $p$be an odd prime number. The equation $x^2 \equiv a(mod\ p)$ has exactly two solutions for $\frac{p-1}{2}$ and many numbers $a \in \{1,2,3 \ldots p-1\}$ and has no solutions for the other $\frac{p-1}{2}$ numbers $a \in \{1,2,3 \ldots p-1\}$.

Remark 1: -For even prime $p = 2$ the equation $x^2 \equiv a(mod\ 2)$has the solutions for $x^2 \equiv 0(mod\ 2), x = 0$ is only solutions.

For $x^2 \equiv 1(mod\ 2), x = 1$ is the only solution.

Example 6: - consider the equation $x^2 \equiv a(mod\ 11)$has $a = 1,3,4,5,9$ are the quadratic residue and therefore each quadratic residue has exactly two solutions. That is

(1) $x^2 \equiv 5(mod\ 11)$ have solutions $x = 4\ and\ x = 7$

(2) $x^2 \equiv 9(mod\ 11)$ have solutions $x = 3\ and\ x = 8$

(3) $x^2 \equiv 4(mod\ 11)$ have solutions $x = 2\ and\ x = 9$

Example 7: - The equations $x^2 \equiv b(mod\ 11)$ has $b = 2,6,7,8,10$ are non -quadratic residue so it has no solutions.

Remark 2: - For the composite moduli the quadratic equations $x^2 \equiv a(mod\ m)$can have more than two solutions.

Example 8: - $x^2 \equiv 1(mod\ 8)$has four solutions.

Lemma1. If p is an odd prime, $(a,p) = 1$ and a is a quadratic residue of p, then the congruence $x^2 \equiv a(mod\ p)$has exactly two roots.

Proof: - In [5]

Theorem 3. If p is an odd prime and $(a,p) = 1$ then $x^2 \equiv a\ (mod\ p^k)$ has exactly two solutions if a is a quadratic residue of p, and no solutions if a is a quadratic nonresidue of p.

Proof- As in [5]

Lemma 2: --Assume p is a prime and that $d|(p-1)$ .Then the congruence $x^d - 1 \equiv 0\ (mod\ p)$ has exactly d solutions.

Proof-Write $p - 1 = nd$ .Use the identity $y^n - 1 = (y-1)(y^{n-1} + y^{n-2} + \cdots + y + 1)$ and on taking $y = x^d$. We obtain

$$x(x^d - 1)\left(1 + x^d + \cdots + y^{d(e-1)}\right) = x^p - x.$$

Lemma 3: -If $x^k \equiv 1\ (mod\ 11)$,where p is prime then the number of solutions is $\gcd\ (k, p-1)$ [2].

Example-The congruence $x^5 \equiv 1(mod\ 11)$

Solution. The $\gcd(5,10) = 5$ so the given congruence has 5 solutions. That is $x = 1,3,4,9.$

Theorem 4. Suppose a is odd. Then

(i) The congruence $x^2 \equiv a(mod\ 2)$ is always solvable and has exactly one solution;

(ii) The congruence $x^2 \equiv a\ (mod\ 4)$is solvable if and only if $a \equiv 1\ (mod\ 4)$in which case there are precisely two solutions.

Polynomial Congruences with Prime Power Moduli

The general procedure for solving the polynomial congruence $f(x) \equiv 0\ (mod\ p^k)$, is to start with a root for the modulus p and use it to generate a root (or in some cases several roots) modulo p^2.Using the same technique, we produce roots modulo $p^3, p^4,$ and so on, until we finally obtain roots for the original modulus p^k . Thus let $x = a$ is a solution of the polynomial congruence $f(x) \equiv 0(mod\ p^j)$ and use it to get a solution modulo p^{j+1}.This idea is to try to get a solution $x = a + tp^j$ of the congruence $f(x) \equiv 0\ (mod\ p^{j+1})$,where t is to be determined. The details will be given by the Hensel's Lemma.

Lemma 4: - Let p be a prime and let k be an arbitrary positive integer, and suppose that a is a solution of $f(x) \equiv 0 \ (mod\ p^k)$

(i) If $p \nmid f'(a)$, then there is precisely one solution b of $f(x) \equiv 0 \ (mod\ p^{k+1})$ such that $b \equiv a \ (mod\ p^k)$. The solution is given by $b = a + p^k t$, where t is the unique solution of $f'(a)t \equiv -\frac{f(a)}{p^k} \ (mod\ p)$.

(ii) If $p|$ f'(a) and $p^{k+1}|f(a)$, then there are p solutions of the congruence $f(x) \equiv o(mod\ p^{k+1})$that are congruent to a modulo p^k ; these solutions are $a + p^k j$ for $j = 0,1,2 \ldots p-1$.

(iii) If $p|f'(a)$ and $p^{k+1} \nmid f(a)$, then there are no solutions of the congruence $f(x) \equiv 0(mod\ p^{k+1}$ that are congruent to a modulo p^k.

Example 9 - Discuss the solutions of $x^2 + x + 223 \equiv 0(mod\ 3^j)$

Solutions- the solution of $x^2 + x + 223 \equiv 0(mod 3)$ is only $x = 1$

And $f(1) \equiv 0(mod\ 9)$ has solutions that is

$x_1 = 1 + 0.3 = 1$

$x_2 = 1 + 1.3 = 4$

$x_3 = 1 + 2.3 = 7$

Thus $x = 1, x = 4, x = 7 \equiv 0(mod\ 9)$

And $f(1) = 225 \not\equiv 0(mod\ 27)$

$f(4) = 243 \equiv 0(mod\ 27)$

$f(7) = 279 \not\equiv 0(mod\ 27)$

From $f(1) and\ f(7)$ has no solutions $f(4) \equiv 0(mod\ 27)$ has solutions that is

$x_1 = 4 + 0.9 = 4$

$x_2 = 4 + 1.9 = 13$

$x_3 = 4 + 2.9 = 22$

$f(4) = 243 \equiv 0\ (mod\ 81),\ f(13) = 405 \equiv 0(mod\ 81)$ and $f(22) = 729 \equiv 0\ (mod\ 81)$ and each has three solutions.

$f(4) \equiv 0\ (mod\ 81)$ has three solutions

$x_1 = 4 + 0.27 = 4$

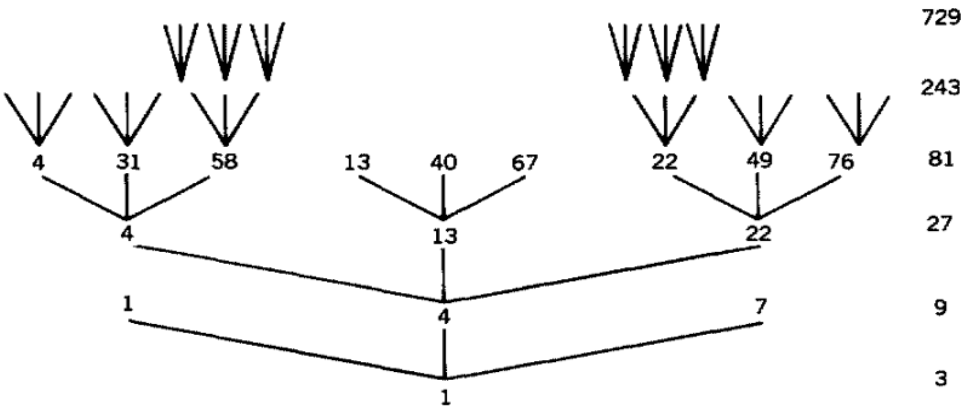
$x_2 = 4 + 1.27 = 31$

$$x_3 = 4 + 2.27 = 58$$

That is three solutions $4, 31, 58 (mod\ 81)$. Similarly, $f(13) \equiv 0 (mod\ 81)$ has three solutions say $13, 40, 67\ (mod\ 81)$ and $f(22) \equiv 0 (mod\ 81)$ has $22, 49, 76\ (mod\ 81)$ therefore we have exactly nine solutions (mod 81).

In fact it is noted that $f(4) \equiv 0 (mod\ 3^5), 3^2 | f'(4)$ then the solution $4 (mod\ 243)$ is one of the nine solutions of the form $4 + 27z (mod\ 243)$,which can be verified precisely one value of $z\ (mod\ 3)$ name $z = 2$ for which $f(4 + 27z) \equiv 0 (mod\ 3^6)$ which implies nine solution of the form $58 + 81z\ (mod\ 3^6)$. Similarly $f(22) \equiv 0 (mod\ 3^5), 3^2 | f'(22)$ and $22\ (mod 243)$ is one of nine solution of the form $22 + 27z (mod\ 243)$ that can be verified one value of $z\ (mod\ 3), z = 0$ for which $22 + 27z$ is a solution $(mod\ 3^6)$ that is nine solutions $mod\ 3^6)$ of the form $22 + 81z$.On the other hand $f'(13) \equiv 0 (mod\ 27)$ so that $f(13 + 27z) \equiv f(13) (mod\ 3^6)$. As $3^4 | f(13)$, therefore no three solutions $13 + 27z\ (mod\ 81)$ lifts to a solution $mod (243)$.Hence from this discussion for each $j \geq 5$ there precisely 18 solutions $(mod\ 3^j)$ of which 12 do not lifts to 3^{j+1},While each of remaining six lifts to three solutions $(mod\ 3^{j+1})$.

Table 1 Solutions of $x^2 + x + 223 \equiv 0 \pmod{3^j}$.



Summary and Conclusion

Introducing the degree of polynomial congruence with different modulus and integral coefficient, the appropriate conditions for existence and non-existence of solutions and the number of solutions, if exists are discussed with suitable examples. As in linear cases the solvability of the congruence $ax \equiv b\ (mod\ p)$ and the number of solutions exist which is given in the theorem (2). and the examples (4) and (5). Also finding other incongruent solutions with one solution using it to find the infinitely many congruent solutions. The conditions that the congruence $x^2 \equiv a\ (mod\ m)$ has different number of solution or no

solutions and examples (6),(7),and (8) and theorem (6).The solvability of the congruence like $x^2 \equiv a(mod\ 2)$ and $x^2 \equiv a(mod\ 2^k)$ with $k > 3$ and a is odd the exact number of solutions are described in theorem[8].The existence of solution of general quadratic congruence $ax^2 + bx + c \equiv 0(mod\ m)$ can be determined by its discriminants being quadratic residue modulo m has solution and has no solution if discriminant be quadratic non residue modulo m. The existence or non- existence and the number of solutions depends upon the prime modulus in theorem[3.6].The general polynomial congruence $f(x) \equiv 0(mod\ p)$ of degree n has at most n roots or less than n roots under the certain conditions, are discussed in theorem(17)and(18) .Similarly n^{th} polynomial like $x^d - 1 \equiv 0(mod\ p)$ and $x^k \equiv 1\ (mod\ p)$ where p is prime and the exact number of solution is discussed in Lemma[2] and [3].

Findings and Recommendations'

The integral polynomial congruence of degree $nf(x) \equiv 0(mod\ p)$ where p is prime and whose co-efficient are divisible by p has at most n solutions. If the coefficients are not divisible, then by using Division algorithms for polynomial reduces it in the degree$\leq f(x)$ and their solutions becomes less than or greater than n depending upon the modulus. Primitive roots also determine the solution, if m has primitive roots and $n/\emptyset(m)$then the congruence $x^n - 1 \equiv 0(mod\ m)\ has$ n roots. But in the linear polynomial congruence $ax \equiv b(mod\ m)$ is solvable if a and b are co-prime and the number of incongruent solutions is equal to the GCD of a and b. The discriminant of the quadratic congruence, and their modulus by taking Legendre symbol or Jacobi symbol that determines the existence or non-existence of the solution of congruence but the number of solutions depends upon modulus. The prime power moduli congruence $f(x) \equiv 0(mod\ p^k)$ has lifting the solutions to modulus as p^k, p^{k+1}…and it forms tree like structure of solutions. There is not necessary to every congruence polynomial has solutions if it has, then there exist two types of solutions one is incongruent solutions which is finite and other is congruent solution which is infinitely many but these solutions are always integers. Where as in case of general polynomial equations of degree n has exactly n roots these are real, complex number and repeated. The solutions of the congruence polynomial with composite modulus using the Jacobi symbols are the area of the further study.

Reference

Borevich, Z.I. &Shafarevich, I.R. (1966). *Congruences: Number theory*, New York: San Francisco.

Broder A.Z. and Dolev D. (1984) Flipping coins in many pockets proceeding of 25th *Annual IEE. Symposium Foundation of Computer Science pp.(157-170)*

Carlitz. L (1956). Note on quartic congruence, *Amir Math monthly -63 pp. (569-573).*

Carlitz. L. (1956). A special quartic congruence. *Amir Math Scand Vol.4pp. (243-246*).

Cassels, J.W.S. (1971). An introduction to the geometry of numbers" *Springer verlag, meidelberg*

Cohen. H. (1993). A course in computational Algebraic number theory, *Graduate text in Mathematics vol.138 Springer berlin pp. (198-299)*

Daileda. R.C. (2001). Quadratic congruences, the quadratic formula and Euler's criterion. *Number theory pp. (1-17). http// ramanujan.math.trinity.edu.*

David. A. Smith. (2019). Polynomial congruences with Hensel's Lifting theorem (*University of Texas at Arlington). https//uta academicwork.com*

Dickson L. (1919). Numbers: *History of the theory of numbers Carnegie inst. Of Washington vol.3 pp.(486)*

Hastad J. (1989) Solving simultaneous modular equations of low degree" *(published in SIAM)*

Kenneth I. & Rosen. M. (1993). A classical introduction to modern number theory *New York Springer*

Leonard P.A. (1969). on factoring quartics (mod p), *Journal of . Number theory 1 pp. 113-115.*

Lindahl Lars-Ake (2002). *Lectures on Number theory Uppsala university. http//zbook.org.*

Montgory. P.l. (1985). Modular multiplication without trivial division, *Mathematics of computation*

Muller M. & Seidt H. (2004). Intraprocedural analysis of modular Arithmetic, *Technical report 789.*

Niven I. Zukerman HS., Montgomery HL. (1991). Congruences. *An introduction to theory of numbers. pp. (47-128) by John Wiley and Sons Inc.*

K.S. (2001). The cubic congruence $x^3 + Ax^2 + Bx + C \equiv 0(mod\ p)$ and binary quadratic forms. *Journal of London Math Society 64* (1)pp 273-275.

Stewart A. & Zima. E.V. (2006). Base-2 Cunningham Numbers in modular Arithmetic, *Technical report pp.(85-91) Redrived from* Shipman. J. (2007). Improving the fundamental theorem of algebra. *math intelligencer 29 [4] pp. (9-14).*

Skolem. T. (1952) The congruence of 4^{th} degree modulo p. a prime., *Norsk Mat. Tidsskr -34 pp.(73-80)* Spearman, B.K. & Williams *http//www.wlu.ca*

Sun Zhi-Hong (2003). Cubic and Quartic congruences modulo a prime. *Journal of number theory, vol.102, pp 41-89.htttp//www.MATHEMATICSWEB.org*