References:

[1] Carl Ludwig Siegel-Advanced Analytic Number Theory- Bombay 1980

[2] DavidGoodwin-Congruences WITH A Prime-Power Modulus (DECEMBRE 2011)

[3] Deniz Yesilyurt-Solving Linear Diophantine Equations and Linear Congruential Equations-Linnaeus University (thesis 01-06-2012)

[4] Hiram Paley/Paul M. Weicsel-a first course in ABSTRACT ALGEBRA-USA (1966).

[5] Hungerford- ABSTRACT ALGEBRA an introduction- saunders college publishing (1990)

[6] JAMES J. TATTERSALL-Elementary number theory in nine Chapters-Cambridge University Press (1999)

[7] Kenneth H.Rosen-Elementary Number Theory and its application

[8] Lars-Ake Lindahl-Lectures on Number Theory-Upssala (2002)

[9] Lucia Moura-Introduction to Number Theory and its Applications-Winter (2010)

[10] THOMAS A. WHITELAW-AN INTRODUTION TO ABSTRACT ALGEBRA-First published (1978)

[11] THOMAS W. HUNGERFORD-ABSTRACT ALGEBRA an Introduction

[12] الزكي، فوزي أحمد وعبد الرحمن، معروف ،مقدمة في نظرية الأعداد ، دار الخريجين للنشر الطبعة الثانية 1422ه\2002م

[13] الخطيب، روحي إبراهيم ، مقدمة في الجبر المجرد، دار المسيرة الطبعة الأولى 1437ه\2016م

[14] الدوسري، فالح بن عمران بن محمد، مقدمة في نظرية الأعداد، الطبعة الأولى 1428ه\2007م

$f'(0) = 3$ and $f(0) = 9$

Hence there are three solutions for

$$f(x) \equiv 0 \ (mod\ 9)$$

Corresponding to the solution $x = 0$ from

$$f(x) \equiv 0 \ (mod\ 3)$$

These are $x = 0,3$ and 6

We now have four solutions for

$$f(x) \equiv 0 \ (mod\ 3^2)$$

We check that $f(0) = 9$ and $f'(0) = 3$ and so

$$f(x) \equiv 0 \ (mod\ 27)$$

Has no solution arising from $x = 0$.

Next, $f(3) = 27$ and $f'(3) = 18$ and so, there are three solutions arising from $x = 3$.

These are $x = 3, 12$ and 21.

For $x = 6$ we have $f(6) = 171$ and $f'(6) = 81$. But $3 \nmid (179/9)$ and hence, there are no solutions arising from $x = 6$.

For $x = 5$ we find that $f(5) = 99$ and $f'(5) = 58$ and we need to solve the congruence

$$58t \equiv 11 \ (mod\ 3).$$

The solutions is $t = 1$ and so 14 is the solution for the congruence .

In conclusion the solutions to the congruence

$$f(x) \equiv 0 \ (mod\ 27)$$

Are 3,12,14 and 21.

This example shows that solutions modulo p in general may not lift to solutions modulo some higher powers of p, but not necessarily to solutions modulo arbitrarily high powers of p. Moreover, lifts of the solutions are not unique.

Example(8) : Consider the polynomial $f(x) = x^2 + x + 233$. We observe that $f(4) = 3^5$ and $f'(4) = 3^2$. So $f(4) \equiv 0\ (mod\ 3^5)$. Searching for solutions of $f(x) \equiv 0\ (mod 3^6)$ of the form $4 + 27t$, we find that

$$f(4 + 27t) \equiv 3^5 + 3^{5t} (mod\ 3^6),$$

And unique $t = 2$ gives such a solutions $f(58) \equiv 0\ (mod\ 3^6)$ Moreover, for any $t = 0,1, \dots ,8,$

$$f(58 + 81t) \equiv 0\ (mod\ 3^6).$$

Example : Solve $x^3 - 2x^2 + 3x + 9 \equiv 0\ (mod\ 3^3)$.

Solution:

The solution to the congruence

$$f(x) \equiv 0\ (mod\ 3)$$

Are $x = 0$ and 2

Now,

$$f'(x) = 3x^2 - 4x + 3.$$

Since $f'(2) \not\equiv 0\ (mod\ 3)$, we see that there is a unique solution arising for $x = 2$.

We need to solve

$$7t \equiv -15/3\ \ (mod\ 3)$$

And it turn out that $t = 1$. The solution for the congruence $f(x) \equiv 0\ (mod\ p)$ arising from $x = 2$ is therefore $2 + 3 = 5$.

Now,

$f'(x_1) = 2x_1 \equiv -1 \ (mod\ 5)$. If follows that $5 \nmid f'(x_1)$,and since $f(x_1) = 5 \equiv 0 \ (mod\ 5)$, we may apply Hensel's iteration to find integers x_n $(n \geq 1)$ with $f(x_n) \equiv 0 \ (mod\ 5^n)$. We obtain

$$x_2 \equiv x_1 - \frac{f(x_1)}{f'(x_2)} \equiv 2 - \frac{5}{-1} \equiv 7 \ (mod\ 5^2),$$

$$x_3 \equiv 7 - \frac{50}{14} \equiv 7 - \frac{50}{-1} \equiv 57 \ (mod\ 5^3)$$

$$x_4 \equiv 57 - \frac{3250}{114} \equiv 57 - \frac{3250}{-1} \equiv 3307 \equiv 182 \ (mod\ 5^4).$$

Thus $x = 182$ provides a solution of the congruence $x^2 + 1 \equiv 0 \ (mod\ 5^4)$. Pro-ceding similarly, one may lift the alternate solution $x \equiv -2$ to the congruence $x^2 + 1 \equiv 0 \ (mod\ 5)$ to obtain the solution $x \equiv -182 \ (mod\ 5^4)$. Note that in each instance, the lifting process provided by Hensel's lemma led a unique residue modulo 5^4 corresponding to each starting solution modulo 5.

Example(7) : Let $f(x) = x^2 - 4x + 13$. Find all of the solutions when

$f'(a) \equiv 0 \ (mod\ 3^4)$.

Notice that

$$x^2 - 4x + 13 \equiv x^2 + 2x + 1 \equiv (x + 1)^2 (mod\ 3),$$

and hence $x \equiv -1 \ (mod\ 3)$ is only solution of the congruence $f(x) \equiv 0 \ (mod\ 3)$. Next, since $f'(x) = 2x - 4$, we find that $3/f'(-1)$, we proceed systematically:

i) Observe first that all solutions satisfy $x \equiv 2 \ (mod\ 3)$, and so any solution x must satisfy $x \equiv 25$ or 8 modulo 9. One may verify that all three residue classes satisfy $f(x) \equiv 0 \ (mod\ 9)$.

ii) Next we consider all residues modulo 27 satisfying $x \equiv 2,\ 5$ or 8 modulo 9, and find that none of these (there are 9 such residues) provide solutions of $f(x) \equiv 0 \ (mod\ 27)$.

So there are no solutions to the congruence $x^2 - 4x + 3 \equiv 0 \ (mod\ 3^3)$.

[4] General procedure for finding all roots of $f(x) \equiv 0\ (mod\ p^k)$

The General procedure for finding all roots of $f(x) \equiv 0\ (mod\ p^k)$ can be summarized as follows.

1. First find all solutions of the congruence $f(x) \equiv 0\ (mod\ p)$.
2. Select one, say a_1; then there are either 0,1, or p solutions of $f(x) \equiv 0\ (mod\ p^2)$ congruent to a_1 modulo p; if solutions exist, they are found by solving the linear congruence $f'(a_1)t \equiv -\frac{f(a_1)}{p}\ (mod\ p)$. If there are no solutions, start again with a different a_1.
3. If there are solutions of $f(x) \equiv 0\ (mod\ p^2)$, select one, say a_2, and find the corresponding roots $f(x) \equiv 0\ (mod\ p^3)$ by solving the congruence $f'(a_2)t \equiv -\frac{f(a_2)}{p}\ (mod\ p)$. Do this for each root of $f(x) \equiv 0\ (mod\ p^2)$. Note that since $a_2 \equiv a_1\ (mod\ p)$, $f'(a_2) \equiv f'(a_1)\ (mod\ p)$, so we do not need to calculate $f'(a_2)$.
4. Proceeding in this fashion, we will eventually determine all solutions of $f(x) \equiv 0\ (mod\ p^k)$.

It is worth emphasizing that if at any step in this procedure we obtain multiple solutions, then we must apply the above process to each solution.

Unfortunately, there is no general procedure for starting the above algorithm, that is for finding all solutions of $f(x) \equiv 0\ (mod\ p)$. In the next section, we will discuss what can be said about the number of solutions, and in later sections we will treat some especial cases.

Example(6) : Let $f(x) = x^2 - 1$. Find the solutions of the congruence

$f(x) \equiv 0\ (mod\ 5^4)$.

Observe that the congruence $x^2 + 1 \equiv 0\ (mod\ 5)$ has the solutions$x \equiv \pm 2\ (mod\ 5)$ (not that there are at most 2 solutions modulo 5 by Lagrange's theorem). Consider first the solutions $x_1 = 2$ of the latter congruence. One finds that

$t \equiv -\overline{f'(a)}\frac{f(a)}{p^{k-1}} \ (mod\ p)$, where $\overline{f'(a)}$ is a multiplicative inverse of $f'(a)$ modulo p.

2) If $f'(a) \equiv 0\ (mod\ p)$ and $f(a) \equiv 0\ (mod\ p^k)$, $f(a + tp^{k-1}) \equiv 0\ (mod\ p^k)$for all integers t.

3) If $f'(a) \equiv 0\ (mod\ p)$ and $f(a) \not\equiv 0\ (mod\ p^k)$, then $f(x) \equiv 0\ (mod\ p^k)$ has no solutions that are equivalent to a modulo p^{k-1}.

Proof**:** (condition on t).

Suppose $S = a + tp^{k-1}$ solves $\overline{f'(a)} \equiv 0\ (mod\ p^k)$. Then S solves $f(x) \equiv 0\ (mod\ p^{k-1})$.

Then

$$0 \equiv f(S) = f(a + tp^{k-1})$$

$$= f(a) + \frac{f'(a)}{1!}(tp^{k-1})^1 + \frac{f''(a)}{2!}(tp^{k-1})^2 + \cdots + \frac{f^{(n)}(a)}{n!}(tp^{k-1})^n$$

$$\equiv f(a) + f'(a)tp^{k-1}(mod\ p^k)$$

$$f'(a)tp^{k-1} \equiv -f(a)(mod\ p^k)$$

$$f'(a)t \equiv -\frac{f(a)}{p^{k-1}}\ (mod\ p)$$

For all t that satisfy the congruence above, $S = a + tp^{k-1}$ solve $f(x) \equiv 0\ (mod\ p^k)$.

[3:5] **Corollary :** Let a be a solution of the polynomial congruence $f(x) \equiv 0\ (mod\ p)$, where p is prime. If $f'(a) \not\equiv 0\ (mod\ p)$, then for every k there is a unique solution a_k of $f(x) \equiv 0\ (mod\ p^k)$ that was obtained from a. We have $a_1 = a$ and

$$a_k = a_{k-1} - f(a_{k-1})\overline{f'(a)}$$

where $\overline{f'(a)}$ is a multiplicative inverse of $f'(a)$ modulo p.

$$f(x) \equiv 0 \ (mod\ p) \qquad (3)$$

Conversely, assume a is a solution of (3), and let us look for solutions b of (2) such that $b \equiv a \ (mod\ p)$, that is such that $b = a + pt$ for some integer by (1),

$$f(a + pt) = f(a) + f'(a)pt + p^2t^2g(pt) \equiv f(a) + f'(a)t \ (mod\ p^2),$$

And hence $a + pt$ solves the congruence (2) if and only if

$f(a) + pf'(a)t \equiv 0 \ (mod\ p^2)$, that is if and only if

$$tf'(a) \equiv -\frac{f(a)}{p} (mod\ p) \qquad (4)$$

If $(f'(a), p) = 1$, then (4) has a unique solution $t = t_0 (mod\ p)$, and it follows that $x \equiv a + pt_0 (mod\ p^2)$ is a solution of the congruence (2) and that it is the only solution satisfy $x \equiv a \ (mod\ p)$.

If $p/f'(a)$, then (4) is solvable if and only if $p^2/f(a)$, and in this case any number t solves (4). Hence $x \equiv a + pj \ (mod\ p^2)$ solve (2) for $g = 0,1, \dots, p-1$. In this case, the congruence (2) has p solutions that are congruent to a modulo p.

If $p/f'(a)$ and $p^2 \nmid f(a)$, then (2) has no solution that is congruent to a.

The step leading from p^k to p^{k+1} is analogous. Thus we have the following theorem.

[3:4] **Theorem** : (Hensel lemma)Let f be a polynomial with integer coefficients, let p be prime, let $k \geq 2$ be an integer and let a be a solution of the congruence

$$f(x) \equiv 0 \ (mod\ p^{k-1}).$$

Then

1) If $f'(a) \not\equiv 0 \ (mod\ p)$, then there is a unique integer $t \in \{0,1, \dots, p-1\}$ so that $f(a + tp^{k-1}) \equiv 0 \ (mod\ p^k)$. It is given by

Proof:

We use the binomial theorem

$$f(a+t) = \sum_{j=0}^{n} c(a+t)^j$$

$$= \sum_{j=o}^{n} c_j \sum_{k=0}^{j} \binom{j}{k} a^{j-k} t^k$$

$$= \sum_{k=0}^{n} \sum_{j=k}^{n} c_j \frac{j!}{(j-k)!\,k!} a^{j-k} t^k$$

$$= \sum_{k=0}^{n} t^k \frac{1}{k!} \sum_{j=k}^{n} c_j \frac{j!}{(j-k)!} a^{j-k}$$

$$= \sum_{k=0}^{n} t^k \frac{1}{k!} f^{(k)}(a)$$

Let use start by noting that if $f(x)$ is an integral polynomial and a is an integer, then there in an integral polynomial $g(t)$ such that

$$f(a+t) = f(a) + f'(a)t + t^2 g(t) \qquad (1)$$

This is a special case of Taylor's. To prove it, we note that $f(a+t)$ is obviously a polynomial in t with integral coefficients, and hence $f(a+t) = A + Bt + t^2 g(t)$, where $g(t)$ is an integral polynomial. The coefficient A is obtained by putting $t = 0$, and to determine B we first differentiate and then take $t = 0$.

Let us now consider the congruence

$$f(x) \equiv 0 \ (mod\ p^2) \qquad (2)$$

Where p is prime. Any solution a of this congruence must also be a solution of the congruence

Proof:

"$\Longrightarrow$" is trivial, because if m divides $f(x)$, then so do any of its factors.

For "$\Longleftarrow$" note that if, for all j, x solves the equation $f(x) \equiv 0\ (mod\ p_j^{aj})$, then for all j, p_j^{aj} is a factor of $f(x)$. Because the p_j are pairwise distinct. The product of the p_j^{aj} is contained in the prime factorization of $f(x)$. Hence m divides $f(x)$, that is, $f(x) \equiv 0\ (mod\ m)$.

Example(5): Find the solution of congruence

$$x^2 + 2x + 46 \equiv 0\ (mod\ 7)$$

$$x^2 + 2x + 4 \equiv 0\ (mod\ 7)$$

$0^2 + 2.0 + 4 \not\equiv 0,\ 1^2 + 2.1 + 4 \equiv 0,\ 2^2 + 2.2 + 4 \not\equiv 0,\ 3^2 + 2.3 + 4 \not\equiv 0,$

$4^2 + 2.4 + 4 \equiv 0,\ 5^2 + 2.5 + 4 \not\equiv 0, 6^2 + 2.6 + 4 \not\equiv 0,$ so the solutions are $x = 1$ and $x = 4$.

[3:2] Definition **:** Let $f(x) = \sum_{j=o}^{n} a_j x^j$. Then the derivative of f is

$$\acute{f}(x) = \sum_{j=1}^{n} a_j j x^{j-1}.$$

[3:3] Theorem : (Taylor's Theorem) If f is a polynomial of degree n and a, t are real numbers, then

$$f(a+t) = \sum_{k=o}^{n} \frac{f^{(k)}(a)}{k!} t^k$$

$$= f(a) + tf'(a) + t^2 \frac{f''(a)}{2!} + \cdots + t^n f^{(n)}(a)/n!$$

Where all terms $\frac{f^k(a)}{k!}$ Are polynomial in a with integer coefficients.

Note that the above theorem is Taylor's theorem applied to polynomials, where we chose the degree of the Taylor polynomial so that the Taylor polynomial is equal to the original polynomial.

[2:15] **Theorem :** Let f be a homogeneous polynomial in n variables and $1 \leq \deg(f) < n$. Then the congruence

$$f(x_1, \dots, x_n) \equiv 0 \ (mod\ p)$$

Has at least one non-zero solution.

Proof:

Suppose that in contrary this congruence has only zero solution. We consider the polynomial

$$h(x_1, \dots, x_n) = 1 - f(x_1, \dots, x_n)^{p-1}.$$

We have $h(x_1, \dots, x_n) \equiv 1 \ (mod\ p)$ if $x_1 \equiv \cdots \equiv x_n \equiv 0 \ (mod\ p)$, and by Fermat's theorem, $h(x_1, \dots, x_n) \equiv 1 \ (mod\ p)$ for all the other residues. Let $\tilde{h}$ be a reduced polynomial equivalent to h with $\deg(\widetilde{h}) \leq \deg(h)$. We also consider the reduced polynomial

$$g(x_1, \dots, x_n) = \prod_{i=1}^{n} \left(1 - x_i^{p-1}\right).$$

It take exactly the same values as h and $\tilde{h}$. So $g \equiv \tilde{h}$, and by the previous theorem, $g \sim h$. However, $\deg(g) = n(p-1)$, but $\deg(\widetilde{h}) < n(p-1)$. This gives a contradiction.

[3] Polynomial Congruence with Prime Power Moduli

Solving the polynomial congruence $f(x) \equiv 0 \ (mod\ m)$ when m is a prime power p^k, is to start with a solution for the modulus p and use it to generate a solution (or in some cases several solutions) modulo p^2. Using the same technique, we produce solutions modulus p^3, p^4, and so on, until we finally obtain solutions for the original modulus p^k. The details will be given below.

[3:1] **Lemma :** If the prime power factorization of m is $m = \prod_{j=1}^{k} p_j^{a_j}$ with pairwise distinct prime p_j, then x solves the equation $f(x) \equiv 0 \ (mod\ m)$ if and only if, for all j, x solve the equation $f(x) \equiv 0 \ (mod\ p_j^{a_j})$.

[2:13] Definition : Let f and g be polynomial in n variables.

i) f is equivalent to g modulo p, $f \equiv g$, if for all $(a_1, a_2, \dots, a_n) \in Z^n$,

$$f(a_1, a_2, \dots, a_n) \equiv g(a_1, a_2, \dots, a_n) \ (mod\ p)$$

ii) f is congruent to g, $f \sim g$, if all the coefficients of corresponding monomials of f and g are congruent modulo p.

iii) f is reduced if it has degree less that p in each of the variables.

It is clear that if $f \sim g$, then $f \equiv g$. It follows from Fermat's theorem that every polynomial f is equivalent to a reduced polynomial $\tilde{f}$ such that $\deg(\tilde{f}) \leq \deg(f)$.

The following theorem is an extension of Lagrange's theorem.

[2:14] **Theorem** : If f and g are educed polynomials and $f \equiv g$, then $f \sim g$.

Proof:

Without loss of generality, we may assume that g is zero polynomial. let n be the number of variables in f. The proof goes by induction on n. The case $n = 1$ follows immediately from Lagrange's theorem because $\deg(f) \leq p - 1$. In the general case, we write

$$f(x_1, \dots, x_n) = f_{p-1}(x_1, \dots, x_{n-1})x_n^{p-1} + \cdots + f_0(x_1, \dots, x_{n-1}).$$

Given $a_1, \dots, a_{n-1} \in \mathbb{Z}$, the equation

$$f_{p-1}(a_1, \dots, a_{n-1})x_n^{p-1} + \cdots + f_0(a_1, \dots, a_{n-1}) \equiv 0 \ (mod\ p)$$

Has p solutions. Hence, by Lagrange's theorem again, $f_i(a_1, \dots, a_{n-1}) \equiv 0 \ (mod\ p)$. This shows that $g_i \equiv 0$, and by induction, $g_i \sim 0$. This completes the proof.

We say that a polynomials $f(x_1, \dots, x_n)$ is homogeneous if all of its monomial have the some degree.

by the polynomial $áf(x) - (áa - 1)x^n$ we obtain a new polynomial with leading coefficient 1 and with the same solutions modulo p as the original one.

Proof:

Let m denote the degree of $q(x)$; then obviously $m + n = p$, and the leading coefficient of $q(x)$ is 1, too. If every coefficient of $r(x)$ is divisible by p, then by Fermat's theorem $q(a)f(a) \equiv a^p - a \equiv 0\ (mod\ p)$ for each integer a. Since p is a prime, it follows that $q(a) \equiv 0\ (mod\ p)$ or $f(a) \equiv 0\ (mod\ p)$, i.e. every integer is a solution of either $q(x) \equiv 0\ (mod\ p)$ or $f(x) \equiv 0\ (mod\ p)$. Now by (theorem 3.1.5), the first congruence has most m solutions and the second has at most n solutions, so together there are at most $m + n = p$ solutions. Since there are p solutions, we conclude that the congruence $f(x) \equiv 0\ (mod\ p)$ must have precisely n solutions.

Conversely, since $r(x) = x^p - x - q(x)f(x)$ it follows from Fermat's theorem that every solutions of $f(x)\ modulo\ p$ is a solution of $r(x)$ modulo p. Hence, if $f(x)$ has n solutions, then $r(x)$ has at least n solutions. Since the degree of $r(x)$ is less than n, this is, however, impossible unless every coefficient of $r(x)$ is divisible by p.

[2:12] **Corollary** : Assume p is a prime and that $d/(p-1)$. Then the congruence $x^d - 1 \equiv 0\ (mod\ p)$ has precisely d solutions modulo p.

Proof**:**

Suppose that $d/(p-1)$. Then there exists a polynomial integral $g(x)$ with $x^{p-1} - 1 = (x^d)^{(p-1)/d} - 1 = (x^d - 1)g(x)$. But the degree of g is $p - 1 - d$, and so by Lagrange's theorem the congruence $g(x) \equiv 0\ (mod\ p)$ has a most $p - 1 - d$ solutions modulo p. Then since $x^{p-1} - 1$ has precisely $p - 1$ zeros modulo p, we see from the above relation thar $x^d - 1$ has at least d zeros modulo p. But Lagrange's theorem shows that the latter polynomial has at most d zeros modulo p, and thus we see that it has precisely d zeros modulo p.

$x\ (mod\ p)$ for all x, whence $x^p - x + 1 \not\equiv 1\ (mod\ p)$ for every residue x.

[2:10] **Theorem**: (Wilson's theorem) The natural number n is prime if and only if $(n-1)! \equiv -1\ (mod\ n)$.

Proof:

Suppose that p is prime. By Fermat's Little theorem solutions to $g(x) = x^{p-1} - 1 \equiv 0\ (mod\ p)$ are precisely $1,2,\dots,p-1$. Consider $h(x) = (x-1)(x-2)\dots\big(x-(p-1)\big) \equiv 0\ (mod\ p)$, whose solutions by construction are the integer$1,2,\dots,p-1$. Since $g(x)$ and $h(x)$ both have degree $p-1$ and the same leading term $f(x) = g(x) - h(x) \equiv 0\ (mod\ p)$ is a congruence of degree at most $p-2$ having $p-1$ incongruent solutions, contradicting Lagrange's theorem hence, every coefficient of $f(x)$ must be a multiple of p, and thus $\deg\big(f(x)\big) = 0$. However, since $f(x)$ has no constant term, $f(x) \equiv 0\ (modp)$ is also satisfied by $x \equiv 0\ (mod\ p)$. Therefore, $0 \equiv f(0) = g(0) - h(0) = -1 - (-1)^{p-1}(p-1)!\ (mod\ p)$. If p is an odd prime, then $(-1)^{p-1} \equiv 1\ (mod\ p)$, and if $p = 2$, then $(-1)^{p-1} \equiv -1 \equiv 1\ (mod\ 2)$. Hence, for any prime p we have $(p-1)! \equiv 1\ (mod\ p)$. Conversely, if n is composite, then there exist an integer d, $1 < d < n$, such that d/n. Hence, $d/(n-1)!$, and$(n-1)! \equiv 0\ (mod\ d)$implying that $(n-1)! \not\equiv -1\ (mod\ n)$..

Example(4) : The congruence $x^2 - 1 \equiv 0\ (mod\ 8)$ has the four solutions 1,3,5 and 7. If however the modulus is prime, then the number of solution can not exceed the degree unless all coefficients of the polynomial are divisible by p.

[2:11] **Theorem :** Let p be a prime, and suppose that the polynomial $f(x)$ has degree $n \le p$ and leading coefficient 1. Use the division algorithm to write $x^p - x = q(x)f(x) + r(x)$, where $\deg r(x) < \deg f(x)$. Then $f(x) \equiv 0\ (mod\ p)$ has exactly n solutions if and only if every coefficient of $r(x)$ is divisible by p.

Remark. The assumption that the leading coefficient of $f(x)$ be 1 is really no restriction. If the leading coefficient is a, we may assume that $(a,b) = 1$. By choosing $\acute{a}$ such that $\acute{a}a \equiv 1\ (mod\ p)$ and replacing $f(x)$

$$f(x) = (x - a_1)(x - a_2) \dots (x - a_k)q(x) + pr(x)$$

And $\deg r(x) < k$.

Proof:

If such polynomials exist, then $f(a_j) = pr(a_j) \equiv 0 \ (mod\ p)$. Then converse is proved by induction on the number k of roots. For $k = 1$, the existence of $q(x)$ and r(x) was proved in (theorem3.1.2**).** Assume the theorem is true for $k - 1$ roots. Then there are two polynomials $q_1(x)$ and $r_1(x)$, with $\deg r_1(x) < k - 1$, such that

$$f(x) = (x - a_1)(x - a_2) \dots (x - a_{k-1})q_1(x) + pr_1(x) \qquad (1)$$

From this, since $f(a_k) \equiv 0 \ (mod\ p)$, we obtain

$$(a_k - a_1)(a_k - a_2) \dots (a_k - a_{k-1})q_1(a_k) \equiv 0 \ (mod\ p).$$

Since $(a_k - a_j) = 1$ for $j = 1,2, \dots, k - 1$, we can cancel the factor $(a_k - a_j)$ in the above congruence to obtain $q_1(x) \equiv 0 \ (mod\ p)$. There is a polynomial $q(x)$ and an integer b such that $q_1(x) = (x - a_k)q(x) + pb$, and by substituting this into (1) we find that the polynomials $q(x)$ and $r(x) = b$.

[2:9] **Theorem** : (Lagrange)Let p be a prime and let $f(x)$ be an integral polynomial of degree n (modulo p), with $n \geq 1$. Then the congruence $f(x) \equiv 0 \ (mod\ p)$ has at most n solutions.

Example(3) : It follows from Lagrange's theorem that the congruence's

- **i)** $x^2 + 1 \equiv 0 \ (mod\ p)$ has at most 2 solutions for any prime p, we have shown that this congruence has precisely 2 solutions when $p \equiv 1 \ (mod\ 4)$, and 0 solutions when $p \equiv 3 \ (mod\ 4)$.
- **ii)** The congruence $x^2 - 2 \equiv 0 \ (mod\ 3)$ has no solution
- **iii)** The congruence $x^p - x + 1 \equiv 0 \ (mod\ p)$ has at most p solutions modulo p. In fact this congruence has no solutions for any prime p because Fermat's little theorem shows that $x^p \equiv$

Where the modulus p is a prime number. If the degree of $f(x)$ is greater than or equal to p, we can reduce the degree in the following way: Divide the polynomial $f(x)$ by $x^p - x$; according to the division algorithm there are two integral polynomials $q(x)$ and $r(x)$ such that$f(x) = (x^p - x)q(x) + r(x)$ and $\deg r(x) < p$. By Fermat's theorem $a^p - a \equiv 0 \ (mod\ p)$, and hence $f(a) \equiv r(a) \ (mod\ p)$ for all integers a. This proves the following result.

[2:6] **Theorem** : If p is a prime, then every polynomial congruence $f(x) \equiv 0 \ (mod\ p)$ is equivalent to a polynomial congruence $r(x) \equiv 0 \ (mod\ p)$, where $r(x)$ is a polynomial with degree less than p.

[2:7] **Lemma**: Assume $n \geq p$ and $n \equiv r \ (mod\ (p-1))$, where $1 \leq r \leq p-1$. Then $x^n \equiv x^r \ (mod\ p)$ for all x.

Proof:

Write $n = q(p-1) + r$. By Fermat's theorem $x^{p-1} \equiv 1 \ (mod\ p)$ if $x \not\equiv 0 \ (mod\ p)$, and hence $x^n = (x^{p-1})^q . x^r \equiv 1^q . x^r = x^r \ (mod\ p)$ holds for all $x \not\equiv 0 \ (mod\ p)$, and for $x \equiv 0 \ (mod\ p)$ the congruence is trivially true.

Example(2) : Consider the congruence $x^{11} + 2x^8 + 3x^4 + 4x^3 + 1 \equiv 0 \ (mod\ 5)$. Division by $x^5 - x$ yields

$x^{11} + 2x^8 + 3x^4 + 4x^3 + 1 = (x^6 + 2x^3 + x^2 + 1)(x^5 - x) + 5x^4 + 5x^3 + x + 1.$

Hence the given congruence is equivalent to the congruence $5x^4 + 5x^3 + x + 1 \equiv 0 \ (mod\ 5)$.

Instead, we could have used (lemma 3.1.1). since $11 \equiv 3, 8 \equiv 4$, and $5 \equiv 1$ modulo 4, we replace the terms $x^{11}, 2x^8$, and x^5 by $x^3, 2x^4$, and x, respectively. This result in the polynomial $x^3 + 2x^4 + x + 3x^4 + 4x^3 + 1 = 5x^4 + 5x^3 + x + 1 \equiv x + 1 \ (mod\ 5)$.

[2:8] **Theorem** : Let p be a prime. The non-congruence number $a_1, a_2, \dots, a_k$ are roots of the polynomial congruence $f(x) \equiv 0 \ (mod\ p)$ if and only if there exist two integral polynomials $q(x)$ and $r(x)$ such that

the degree of the polynomial, abbreviated $deg\, f(x)$, and the corresponding coefficient a_k is called the leading term of the polynomial. This leaves the $degf(x)$ undefined when $f(x)$ is the zero polynomial, i.e., when all coefficients a_i are zero. To have the degree defined in that case, too, we define the degree of the zero polynomial to be the symbol $-\infty$, which we consider to be less then all integers.

Those, a phrase like "$f(x)$ is a polynomial of degree$< n$" means that $f(x)$ is a nonzero polynomial of (ordinary) degree$< n$or the zero polynomial.

If $f(x) = \sum_{i=0}^{n} a_i x^i$, $a_i \equiv b_i \ (mod\ m)$ and $g(x) = \sum_{i=0}^{n} b_i x^i$, then clearly $f(x) \equiv g(x) \ (mod\ m)$ for all x. Hence, in a congruence $f(x) \equiv 0 \ (mod\ m)$ we may reduce the coefficients modulo m, and in particular we may delete terms $a_i x^i$ with $a_i \equiv 0 \ (mod\ m)$ without changing the solution set.

Example(1) :The congruence

$$20x^5 + 17x^4 + 12x^2 + 11 \equiv 0 \ \ (mod\ 4)$$

Is equivalent to the congruence

$$x^4 + 3 \equiv 0 \ (mod\ 4)$$

And by trying $-1, 0, 1, 2$ we find the solution $x \equiv \pm 1 \ (mod\ 4)$.

[2:4] **Theorem** : (the division algorithm for integral polynomial)

Let $f(x)$ and $g(x)$ be two integral polynomials, and assume the leading coefficient of $g(x)$ is equal to 1. Then there exist two unique integral polynomials $q(x)$ and $r(x)$ such that $f(x) = q(x)g(x) + r(x)$ and deg $r(x)$ <deg $g(x)$.

[2:5] **Theorem** : Assume $f(x)$ is an integral polynomial . Then, the integer a is a root of the congruence $f(x) \equiv 0(mod\ m)$ if and only if there exist an integral polynomial $q(x)$ and an integer b such that

$$f(x) = (x - a)q(x) + mb.$$

We now turn to polynomial congruence's

$$f(x) \equiv 0 \ (mod\ p)$$

[2:1] **Theorem :** Let

$$\begin{cases} f_1(x) \equiv 0 \ (mod m_1) \\ f_2(x) \equiv 0 \ (mod m_2) \\ \quad \vdots \\ f_r(x) \equiv 0 \ (mod \ m_r) \end{cases}$$

be a system of polynomial congruence's, and assume that the moduli $m_1, m_2, \dots, m_r$ are pairwise relatively prime. Let X_j be a complete set of incongruent solutions modulo $m_j$of the $j\ th$congruence, and let $n_j$denote the number of solutions. The number of solutions of the system then equals $n_1, n_2, \dots, n_r$, and each solution of the system is obtained as the solution of the system

$$\begin{cases} x \equiv a_1 \ (mod m_1) \\ x \equiv a_2 \ (mod m_2) \\ \quad \vdots \\ x \equiv a_r \ (mod \ m_r) \end{cases}$$

With $(a_1, a_2, \dots, a_r)$ ranging over the set $X_1 . X_2 . \dots . X_r$.

of course, a set X_j night by empty in which case $n_j = 0$.

[2:2] **Theorem** : let $f(x)$ be an integral polynomial. For each positive integer m, let $X(m)$ denote a completes set of roots modulo m of the polynomial congruence

$$f(x) \equiv 0 \ (mod \ m).$$

and let $N(m)$ denote the number of roots.

Assume $m = m_1 m_2 \dots m_r$, where the numbers $m_1, m_2, \dots, m_r$ are pairwise relatively prime; then

$$N(m) = N(m_1) N(m_2) \dots N(m_r).$$

Moreover, to each r-tuple $(a_1, a_2, \dots a_r) \in X_1(m_1) \times X_2(m_2) \times \dots \times X_r(m_r)$ there corresponds a unique solution $a \in X(m)$ such that $a \equiv a_j \ (mod \ m_j)$ for each j.

[2:3] polynomial congruence with prime modulo

Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ or $f(x) = \sum_{i=0}^{n} a_i x^i$ be an integral polynomial. The largest integer k such that $a_k \neq 0$ is called

Remark:

Every congruence's $ax \equiv b\ (mod\ m)$ equivalent Diophatine equation $ax + my = b$, but the Diophantine equation has infinite solutions

$$x = x_0 + \frac{m}{d}t, \qquad y = y_0 - \frac{a}{d}t, \qquad t \in Z$$

While congruence $ax \equiv b$ has exactly d incongruent solution modulo m is

$$x = x_0 + \frac{m}{d}t, \qquad 0 \le t \le d - 1$$

[1:12] **Corollary** : When we have an inverse of modulo m, we can use it to solve any convergence of the form $ax \equiv b\ (mod\ m) \Rightarrow x \equiv \bar{a}b(mod\ m)$, $\bar{a}$ is inverse of a.

[1:13] **Theorem**: The linear congruence $a_1x_1 + a_2x_2 + \cdots + a_nx_n \equiv b\ (mod\ m)$ has solution if and only if $d = (a_{1,} \dots, a_n, m)/b$

[2] Polynomial congruence

A Polynomial $f(x) = \sum_{i=0}^{n} a_i x^i$with coefficients $a_i \in z$ is called an integral polynomial, and the congruence

$$f(x) \equiv 0\ (mod\ m)$$

is called polynomial congruence.

Next, consider a system

$$\begin{aligned} f_1(x) &\equiv 0\ (modm_1) \\ f_2(x) &\equiv 0\ (modm_2) \\ &\vdots \\ f_r(x) &\equiv 0\ (modm_r) \end{aligned}$$

of polynomial congruence's where the moduli $m_1, m_2, \dots, m_r$ are assumed to be pairwise relatively prime. By a solution of such a system we mean, of course, an integer which solve simultaneously all the congruence's of the system. If a is a solution of the system, and if $b \equiv a\ (mod\ m_1m_2 \dots m_r)$, then b is also a solution of the system, since for each j we have $b \equiv a\ (modm_j)$. Hence, to find all solutions of the system it suffices to consider solutions belonging to a system we will mean the number of such incongruent solutions.

[1:4] **Corollary** : Let n be a positive integer and let $a_1, a_2, \dots, a_n$ be integers such that $p/(a_1, a_2, \dots, a_n)$, p a prime. Then p/a_i, for some I such that $1 \leq i \leq n$

[1:5] Definition : Let n be a positive integer that is either itself a prime number or that can be expressed as a product of prime numbers. Then we say that n has a factorization into prime number, or that n has a prime factorization. If $n = P_1 P_2 \dots P_s$, $s \geq 1$, and each P_i is a prime, we call this expression a prime factorization for n.

[1:6] **Corollary:** If $n > 1$ is a positive integer, then n has a unique representation in the form

$$n = {P_1}^{e_1} {P_1}^{e_2} \dots {P_1}^{e_r}$$

Where P_i is prime, $i = 1,2, \dots, r$, $P_i < P_j$, for $i < j$ and $e_i > 0$, all i.

[1:7] Definition : let a and n be positive integers. If $(a, n) = 1$ and $a^{n-1} \equiv 1 \ (mod\ n)$, then n is called a probable prime to the base a. A composite probable prime is called a pseudo prime.

[1:8] **Lemma:** (pseudo prime) let P be a prime. Then $x^2 \equiv 1 \ (mod\ P)$ if and only of $x \equiv \pm 1 \ (mod\ P)$.

[1:9] **Proposition** : Let $m_1, m_2, \dots, m_r$ be positive integers. The following two statements are then equivalent:

i) $a \equiv b \ (mod\ m_i)$ for $i = 1,2, \dots, r$.
ii) $a \equiv b \ (mod\ [m_1, m_2, \dots, m_p])$.

[1:10] Definition : A congruence of form ax ≡ b (mod m)

Where x is an unknown integer is called a linear congruence in one variable.

[1:11] Theorem: Let a, b and m be integers with $m > 0$ and $\gcd(a, m) = d$, if d/b, then $ax \equiv b \ (mod\ m)$ has exactly d incongruent solution modulo m

$$x = x_0 + \frac{m}{d}t, \quad 0 \leq t \leq d - 1$$

Introduction

Polynomial Congruence's with a prime and prime power modulo, this theme is part of the congruence's of integers; so assigned to define congruence's and its most important types and important theories e.g define congruence of two integers, linear congruence, system of linear congruence and polynomial congruence modulo m; either the includes Polynomial Congruences with a prime and Polynomial Congruences with a prime power moduli; finally we get the results, recommendations, conclusions.

[1] Preliminaries :-

[1:1] Diophantine equation is an equation in one or more variables which can be solved in integers the most basic Diophantine equation is the linear Diophantine equation in two variables x, y can write $ax + by = c$, where $a, b, c \in Z$.

[1:2] **Theorem:** Let a, b and c be integers with a and b not both zero. The linear diophatine equation

$$ax + by = c$$

Has a solution

i) If and only if a/b where $d = \gcd(a, b)$

ii) If x_0, y_0 in a particular solution then all other solution are given by

$x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ for integer t.

[1:3] Definition: An integer greater than 1(> 1) is called a prime number or a prime if it has only positive divisor are 1 and p. an integer > 1 which is not a prime is called composite.

[1:4] **Theorem** : Let p be a prime number and let p/ab,$a, b \in Z$. Then p/a or p/b.

ملخـــــص

هدفت الورقة العلمية إلى مناقشة تطابقات كثيرات الحدود بمقياس الأعداد الأولية والأعداد الأولية الأسية. التي لها أهمية كبيرة في الحياة العلمية الحديثة خاصة علم التشفير. استخدمت الورقة العلمية المنهج الوصفي الاستقرائي، وتوصل الباحث إلى عدة نتائج منها الطريقة العامة لحل تطابقات كثيرات الحدود بمقياس الأعداد الأولية الأسية (Hensel's lemma) ووضحت الورقة الطريقة العامة لإيجاد كل جذور $f(x)\equiv 0 \pmod{p^k}$.

Abstract

This scientific paper aims to discuss deals with Polynomials Congruence with a Prime and Prime Power Moduli. Interference in many applications in modern times in particular cryptography. the scientific paper is based on the descriptive approach, the search yielded several result the most important is the general method of solutions for Polynomial Congruence>s with a Prime Power Moduli f(x)≡0 (mod p^k) is by Hensel's lemma, the paper explained the general method for finding all roots of f(x)≡0 (mod p^k).

Polynomial Congruence`s with A Prime and Prime-Power Modulus

تطابقات كثيرات الحدود بمقياس الأعداد الأولية والأعداد الأولية الأسية

DR. ALTAYEB. A/ ELGADIR A/ ELMAGID*

* University of Holly Quran-Wad Medani-Sudan .