DEMOCRATIC REPUBLIC OF ALGERIA AND POPULAR
MINISTRY OF HIGHER EDUCATION AND SCIENTIFIC RESEARCH

University Mohamed Boudiaf of M'sila
Faculty of Mathematics and Computer Science
Department of Mathematics

Master Memory

Speciality : Mathematics
Option : Algebra & Discrete Mathmatics

Title

Polynomial Congruence

Presented by :
M^iss Amroune Abir

Publicly defended on : 30/6/2019.

Before the jury composed of :

President :	M^r *D* MIHOUBI	Prof, University of Msila
Framer :	M^r *A* BOUDAOUD	Prof, University of Msila
Examiner :	M^r *S* MILLES	M.C.B, University of Msila

Academic Year 2018/2019

Acknowledgements

First of all, I thank «**Allah**» most merciful for giving me power and capacity to completel this work .

At the second stage I would like to thank my parents for thier support and encouragement throughout all the stage of my life.

Moreover I would like to express my sincere gratitide to my supervisor **Mr. Abdelmadjid Boudaoud** for his guidance and help he gave me.

Finally, I would like to thank my sister Chahra and my friend Zahra. and all the student friends of Mathematics and Computer Science faculty.

Contents

General introduction

This work is placed within the framework of the elementary number theory. Recall that, in general, the number theory is concerned with properties of the natural numbers 1, 2, 3, 4, ... , also called the positive integers. These numbers, together with the negative integers and zero, form the set of integers. Among the great mathematicians who introduce this specialty are: ***Karl Friedrich Gauss*** $(1777-1855)$, ***Pierre de Fermat*** $(1601-1665)$, ***Leonhard Euler***$(1707-1783)$ ***and Adrien-Marie Legendre*** $(1752-1833)$.

Among the most important topics in this specialty is the congruence which was introduced by ***Gauss*** as follows: If a number a divides the difference of the numbers b and c, b and c are said to be congruent relative to a; if not, b and c are incongruent. The number a is called the modulus. Gauss and Legendre were the first to consider the problem of finding solutions to polynomial congruences with prime and nonprime modulus.

Our object is exactly how to solve a given polynomial congruence $f(x) \equiv 0 \pmod{m}$. Our work is divided into three chaptres.

In the first chapter, we introduce some basic concepts. we also recall congruence concept and its properties.

In the second chapter, we recall the polynomial congruence concept, and discuss three main problems. Firstly, when do solutions exist, secondly, how many solutions are there, and thirdly, how to find them.

In the last chapter, we consider one type of congruence, namely quadratic congruence, we tackle the quadratic residue concept.

CHAPTER 1

DIVISIBILITY AND CONGRUENCES

1.1 Divisibility and Euclidean Division

The ideas that we will develop in this section are based on the notion of divisibility. Division of an integer by a positive integer produces a quotient and a remainder. Working with these remainders leads to modular arithmetic, which plays an important role in mathematics.

The essential references used in this section are the following: [3] and [5].

Definition 1.1 (Integer Divisibility)**.** If a and b are integers such that $a \neq 0$, then we say a divides b if there exists an integer k such that $b = ka$ and write $a \mid b$. Otherwise we write $a \nmid b$.

If a divides b we also say "a is a factor (divisor) of b" or "b is a multiple of a".

Theorem 1.1. *Let a, b, and c be an integers, such that $a \neq 0$. Then*

(i) If $a \mid b$ and $b \mid a$, then $a = \pm b$;

(ii) if $a \mid b$ and $b \mid c$, then $a \mid c$;

(iii) if $a \mid b$ and $a \mid c$, then $a \mid (sb + tc)$ for any integers s and t;

(iv) $a \mid b$ if and only if $ka \mid kb$ for any nonzero integer k.

Theorem 1.2 (Euclidean Division)**.** *If a and b are integers such that $b > 0$, then there exist unique integers q and r such that $a = bq + r$ where $0 \leqslant r < b$.*

Example 1.1. If $a = 35$ and $b = 15$, then $35 = 15 \cdot 2 + 5$. Here $q = 2$ and $r = 5$.

Definition 1.2 (Greatest Common Divisor)**.** The greatest common divisor of two integers a and b is the greatest integer that divides both a and b, denoted by (a, b). We also define $(0, 0) = 0$.

Example 1.2. Note that the greatest common divisor of 32 and 12 is 4. In other words $(32, 12) = 4$.

Theorem 1.3. *Let $a, b, b_1, \ldots,$ and b_n be integers, then*

(1) $(ca, cb) = c(a, b)$ *for any positive integer* c;

(2) $(a, 0) = a$ *for any interger* a;

(3) if $c \mid a$ *and* $c \mid b$, *then* $c \mid (a, b)$;

(4) $(|a|, |b|) = (a, b)$;

(5) If $(a, b_i) = 1$, $i = 1, 2, \ldots, n$, *then* $(a, b_1 b_2 \cdots b_n) = 1$.

Definition 1.3. Two integers a and b are relatively prime if $(a, b) = 1$.

Theorem 1.4. *Let a and b be an integers, let d be a positive integer. If $(a, b) = d$ then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. Assume that k is a positive common divisor such that $k \mid a/d$ and $k \mid b/d$. As a result, there are two positive integers m and n such that

$$a = d = km \ \ and \ \ b = d = kn;$$

thus we get that

$$a = kmd \ \ and \ \ b = knd.$$

Hence kd is a common divisor of both a and b. Also, $kd \geqslant d$. However, d is the greatest common divisor of a and b. As a result, we get that $k = 1$. □

The next theorem shows that the greatest common divisor of two integers does not change when we add a multiple of one of the two integers to the other.

Theorem 1.5. *Let a, b and c be an integers. Then $(a, b) = (a + cb, b)$.*

Example 1.3. Notice that $(6, 20) = (6, 20 - 3 \cdot 6) = (6, 2) = 2$.

Theorem 1.6. *The greatest common divisor of two integers a and b, not both 0 is the least positive integer d such that $ma + nb = d$ for some integers m and n.*

Definition 1.4. Let $a_1, a_2, \ldots, a_n$ be integers, not all 0. The greatest common divisor of these integers is the largest integer that divides all of the integers in the set, denoted by $(a_1, a_2, \ldots, a_n)$.

Definition 1.5. The integers $a_1, a_2, \ldots, a_n$ are said to be mutually relatively prime if

$$(a_1, a_2, \ldots, a_n) = 1.$$

Example 1.4. The integers $4, 7, 8$ are mutually relatively prime since $(4, 7, 8) = 1$ although $(4, 8) = 4$.

Definition 1.6. The integers $a_1, a_2, \ldots, a_n$ are called pairwise prime if for each $i \neq j$, we have $(a_i, a_j) = 1$.

Example 1.5. The integers $5, 16, 27$ are pairwise relatively prime. Notice also that these integers are mutually relatively prime.

Notice that if $a_1, a_2, \ldots, a_n$ are pairwise relatively prime then they are mutually relatively prime.

Lemma 1.1. *If a and b are two integers and $a = bq + r$ where also q and r are integers, then $(a, b) = (r, b)$.*

We now present the Euclidean algorithm in its general form. It states that the greatest common divisor of two integers is the last non zero remainder of the successive division.

Theorem 1.7 (Euclidean Algorithm)**.** *Let $a = r_0$ and $b = r_1$ be two positive integers where $a \geqslant b$. If we apply the Euclidean Division successively to obtain that*

$$r_j = r_{j+1}q_{j+1} + r_{j+2} \quad \textit{where } 0 \leqslant r_{j+2} < r_{j+1}$$

for all $j = 0, 1, \ldots, n-2$ and

$$r_{n+1} = 0,$$

then $(a, b) = r_n$.

Example 1.6. Finding greatest common divisor of 522 and 1236:
Note that

$$\begin{aligned} 1236 &= 522 \cdot 2 + 192 \\ 522 &= 190 \cdot 2 + 138 \\ 190 &= 138 \cdot 1 + 54 \\ 142 &= 54 \cdot 2 + 30 \\ 54 &= 30 \cdot 1 + 24 \\ 30 &= 24 \cdot 1 + 6 \\ 24 &= 6 \cdot 4 \end{aligned}$$

hence $(522; 1236) = 6$.

Extended Euclidean Algorithm We now use the steps in the Euclidean algorithm to write the greatest common divisor of two integers as a linear combination of the two integers. The following example will actually determine the variables m and n described in Theorem1.6. The following algorithm can be described by a general form but for the sake of simplicity of expressions we will present an example that shows the steps for obtaining the greatest common divisor of two integers as a linear combination of the two integers.

Example 1.7. Express 6 as a linear combination of 522 and 1236 :

$$\begin{aligned} 6 &= 30 - 1 \cdot 24 \\ &= 30 - 1(54 - 1 \cdot 30) \\ &= 2 \cdot 30 - 54 \\ &= 2 \cdot (138 - 54 \cdot 2) - 54 \\ &= 2 \cdot 138 - 5 \cdot 54, \\ &= 2 \cdot 138 - 5(192 - 138 \cdot 1) \\ &= 7 \cdot 138 - 5 \cdot 192 \\ &= 7 \cdot (522 - 19 \cdot 192 \\ &= 7 \cdot 522 - 19(1236 - 522 \cdot 2) \\ &= 45 \cdot 522 - 19 \cdot 123. \end{aligned}$$

As a result, we see that $6 = 45 \cdot 522 - 19 \cdot 1236$.

1.2 Prime Number

Definition 1.7. A prime is an integer greater than 1 that is only divisible by 1 and itself.

Example 1.8. The integers $2, 3, 5, 7, 11$ are prime numbers.

Note that any integer greater than 1 that is not prime is said to be a composite number.

Theorem 1.8. *There are infinitely many primes.*

Proof. Let $p_1, p_2, \ldots, p_n$ be any finite set of prime numbers. Consider the integer

$$N = p_1 p_2 \cdots p_n + 1$$

Since $N > 1$, N is divisible by some prime p. If $p = p_i$ for some $i = 1, \ldots., n$, then p divides $N - p_1 \cdots p_n + 1$, which is absurd. Therefore, $p \neq p_i$ for all $i = 1, \ldots, n$.

This means that, for any finite set of primes, there always exists a prime that does not belong to the set, and so the number of primes is infinite. □

Theorem 1.9. *If a, b, and c are positive integers such that $(a, b) = 1$ and $a \mid bc$, then $a \mid c$.*

We can generalize the above theorem as such: If $(a, n_i) = 1$ for every $i = 1, 2, \ldots, n$ and $a \mid n_1 n_2 \cdots n_{k+1}$, then $a \mid n_{k+1}$. arithmetic.

Theorem 1.10. *If p divides $n_1 n_2 \cdots n_k$, where p is a prime and $n_i > 0$ for all $1 \leqslant i \leqslant k$, then there is an integer j with $1 \leqslant j \leqslant k$ such that $p \mid n_j$.*

Theorem 1.11 (The Fundamental Theorem of Arithmetic)**.** *Every positive integer greater than 1 has a factorization into product of primes. The representation is unique, except for the order of the factors.*

Example 1.9. The prime factorization of 120 is given by $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^2 \cdot 3^2 \cdot 5$

Definition 1.8 (Least Common Multiple)**.** Let $a_1, a_2, \ldots, a_n$ be positive integers. The least common multiple (or lcm) of these integers is the smallest positive integer that is a multiples of them, denoted by $[a_1, a_2, \ldots, a_n]$.

Theorem 1.12. *Let a and b be two positive integers. Then*

(1) $[a, b] \geqslant 0$;

(2) $[a, b] = ab/(a, b)$;

(3) If $a \mid m$ and $b \mid m$, then $[a, b] \mid m$.

1.3 Linear Diophantine Equations

Definition 1.9. A linear equation of the form $ax + by = c$ where a, b and c are integers is known as a linear diophantine equation.

Note that a solution to the linear diophantine equation (x_0, y_0) requires x_0 and y_0 to be integers. The following theorem describes the case in which the diophantine equation has a solution and what are the solutions of such equations.

Theorem 1.13. *The equation $ax + by = c$ has integer solutions if and only if $d \mid c$ where $d = (a, b)$. If the equation has one solution $x = x_0, y = y_0$, then there are infinitely many solutions and the solutions are given by*

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

where t is an arbitrary integer.

Example 1.10. There are infinitely many integer solutions for the equation $15x + 7y = 9$ because $(15, 7) = 1 \mid 9$. We use the Euclidean algorithm to determine m and n where $15m + 7n = 1$. It turns out that $15(1) + 7(-2) = 1$. And also $9 = 1 \cdot 9$. Thus $x_0 = 9(1) = 9$ and $y_0 = 9(-2) = -18$ is a particular solution. The solutions are given by

$$x = 9 + 7t, \quad y = -18 - 15t$$

for all integers t.

1.4 Congruences

A congruence is nothing more than a statement about divisibility. The theory of congruences was introduced by Karl Friedreich Gauss. Gauss contributed to the basic ideas of congruences and proved several theorems related to this theory. We start by introducing congruences and their properties. We proceed to prove theorems about the residue system in connection with the Euler ϕ-function. We then present solutions to linear congruences which will serve as an introduction to the Chinese remainder theorem. We present finally important congruence theorems derived by Wilson, Fermat and Euler.

The essential references used in this section are the following: [1], [3], [5].

Definition 1.10. Let m be a positive integer. We say that a is congruent to b modulo m if $m \mid (a-b)$ where a and b are integers, e.g. if $a = b + km$ where $k \in \mathbf{Z}$.

If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$ and b is called residue of a modulo m. Otherwise we write $a \not\equiv b \pmod{m}$. The integer m is called the modulus.

Example 1.11. $17 \equiv 2 \pmod{3}$. Similarly $2k + 1 \equiv 1 \pmod{2}$ which means every odd number is congruent to 1 modulo 2.

Remark 1.1. Suppose m is positive, and a is any integer. By the Division Algorithm, there exist integers q and r with $0 \leqslant r < m$ such that $a = mq + r$. Hence $mq = a - r$ or $m \mid (a - r)$ or $a \equiv r \pmod{m}$ Accordingly:

(1) Any integer a is congruent modulo m to a unique integer in the set $\{0, 1, 2, ..., m-1\}$ The uniqueness comes from the fact that m cannot divide the difference of two such integers.

(2) Any two integers a and b are congruent modulo m if and only if they have the same remainder when divided by m.

There are many common properties between equations and congruences. Some properties are listed in the following theorem.

Theorem 1.14. *Let $m_1, m_2, \ldots, m_r$, m be a positive integer, and suppose a, b, c, and d are arbitrary integers.*

(1) $a \equiv a \pmod{m}$;

(2) If $a \equiv b \pmod{m}$, *then* $b \equiv a \pmod{m}$;

(3) If $a \equiv b \pmod{m}$ *and* $b \equiv c \pmod{m}$, *then* $a \equiv c \pmod{m}$;

(4) If $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $a \pm c \equiv b \pm d \pmod{m}$;

(5) If $a \equiv b \pmod{m}$ *and* $c \equiv d \pmod{m}$, *then* $ac \equiv bd \pmod{m}$;

(6) If $a \equiv b \pmod{m}$, *then* $ca \equiv cb \pmod{m}$ *for any integer* c;

(7) If $ca \equiv cb \pmod{m}$, *then* $a \equiv b \pmod{m/(c, m)}$. *In particular, if* $(c, m) = 1$, *then* $ca \equiv cb \pmod{m}$ *implies* $a \equiv b \pmod{m}$;

(8) If f(x) is an integral polynomial and $a \equiv b \pmod{m}$*, then* $f(a) \equiv f(b) \pmod{m}$.

Proposition 1.1. *Let* $m_1, m_2, \ldots, m_r$ *be positive integers. The following two statements are then equivalent:*

(i) $a \equiv b \pmod{m_i}$ *for* $i = 1, 2, \ldots, r$.

(ii) $a \equiv b \pmod{[m_1, m_2, \ldots, m_r]}$.

Proof. Suppose $a \equiv b \pmod{m_i}$ for all i. Then $(a - b)$ is a common multiple of all the m_i, and therefore $[m_1, m_2, \ldots, m_r] \mid (a - b)$. This means that $a \equiv b(mod[m_1, m_2, \ldots, m_r])$.

Conversely, if $a \equiv b \pmod{[m_1, m_2, \ldots, m_r]}$, then $a \equiv b \pmod{m_i}$ for each i, since $m_i \mid [m_1, m_2, \ldots, m_r]$. □

Theorem 1.15. *If* $a \equiv b \pmod{m}$*, then* $(a, m) = (b, m)$.

1.4.1 Residue Systems

Definition 1.11. A complete residue system modulo m is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.

Example 1.12. The easiest complete residue system modulo m is the set of integers $0, 1, 2, \ldots, m - 1$. Every integer is congruent to one of these integers modulo m.

Definition 1.12. A reduced residue system modulo m is a set of integers r_i such that:

(i) $(r_i, m) = 1$ for all i;

(ii) $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$;

(iii) For every integer a, if $(a, m) = 1$ then there exists r_i such that $a \equiv r_i \pmod{m}$.

A reduced residue system modulo m can be obtained by deleting all the elements of the complete residue system set that are not relatively prime to m.

Lemma 1.2. *A set of* m *incongruent integers modulo* m *forms a complete residue system modulo* m.

Proof. We will prove this lemma by contradiction. Suppose that the set of m integers does not form a complete residue system modulo m. Then we can find at least one integer a that is not congruent to any element in this set. Hence non of the elements of this set is actually congruent to the remainder when a is divided by m. Thus dividing by m yields to at most $m-1$ remainders. Therefore by the pigeonhole principle, at least two integers in the set that have the same remainder modulo m. This is a contradiction since the set of integers is formed of m integers that are incongruent modulo m. □

Theorem 1.16. *If $\{a_1, a_2, \ldots, a_n\}$ is a complete residue system modulo m, and if k is a positive integer with $(k, m) = 1$, then*

$$\{ka_1 + b, ka_2 + b, \ldots, ka_n + b\}$$

is another complete residue system modulo m for any integer b.

Proof. First we prove that no two elements of the set $\{ka_1 + b, ka_2 + b, \ldots, ka_n + b\}$ are congruent modulo m. Suppose there exists i and j such that

$$ka_i + b \equiv ka_j + b \pmod{m}.$$

Thus we get that

$$ka_i \equiv ka_j \pmod{m}.$$

Now since $(k, m) = 1$, we get

$$a_i \equiv a_j \pmod{m}$$

But for $i \neq j$, a_i is inequivalent to a_j modulo m. Thus $i = j$. Now notice that there are m inequivalent integers modulo m and thus by Lemma 1.2, the set form a complete residue system modulo m. □

1.4.2 Euler's ϕ-Function

Definition 1.13. The Euler ϕ-function of a positive integer n, denoted by $\phi(n)$ counts the number of positive integers less than n that are relatively prime to n.

Example 1.13. Since 1 and 3 are the only two integers that are relatively prime to 4 and less than 4, then $\phi(4) = 2$. Also, $1, 2, \ldots, 6$ are the integers that are relatively prime to 7 that are less than 7, thus $\phi(7) = 6$.

Now we can say that the number of elements in a reduced residue system modulo n is $\phi(n)$.

Theorem 1.17. *If $a_1, a_2, \ldots, a_{\phi(m)}$ is a reduced residue system modulo m and $(k, m) = 1$, then $ka_1, ka_2, \ldots, ka_{\phi(m)}$ is a reduced residue system modulo m.*

1.4.3 Linear Congruences

Because congruences are analogous to equations, it is natural to ask about solutions of linear equations. In this section, we will be discussing linear congruences of one variable and their solutions. We start by defining linear congruences.

Definition 1.14. A congruence of the form $ax \equiv b \pmod{m}$ where x is an unknown integer is called a linear congruence in one variable.

An integer s is called a solution of the linear congruence if $as \equiv b \pmod{m}$

Theorem 1.18. *Let a, b and m be integers such that $m > 0$ and let $d = (a, m)$. If $d \nmid b$, then the congruence $ax \equiv b \pmod{m}$ has no solutions. If $d \mid b$, then*

$$ax \equiv b \pmod{m}$$

has exactly d incongruent solutions modulo m. given by:

$$x \equiv x^* + \frac{m}{d}t \ (mod\, m)\ ;\ t = 0, 1, ..., d-1$$

where x^* is any solution of the congruence $(\frac{a}{d})x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$.

Remark 1.2. Notice that if $d = (a, m) = 1$, then there is a unique solution modulo m for the equation $ax \equiv b \pmod{m}$.

Example 1.14. Let us find all the solutions of the congruence $9x \equiv 3 \pmod{12}$. Notice that $(9, 12) = 3$ and $3 \mid 3$. Thus there are three incongruent solutions modulo 12. Hence we solve the congruence $3x \equiv 1 \pmod{4}$. We use the Euclidean algorithm to find the solution of the equation $3x - 4y = 1$. Thus the three incongruent solutions are given by $x = 3, 7, 11 \pmod{12}$.

Definition 1.15 (Modular Inverses)**.** A solution for the congruence $ax \equiv 1 \pmod{m}$ for $(a, m) = 1$ is called the modular inverse of a modulo m. We denote such a solution by a'.

Example 1.15. The modular inverse of 7 modulo 48 is 7. Notice that a solution for $7x \equiv 1 \pmod{48}$ is $x \equiv 7 \pmod{48}$.

Theorem 1.19. *If a and m are relatively prime integers with $m > 1$, then an inverse of a modulo m exists. Furthermore, this inverse is unique modulo m.*

Proof. By Theorem 1.6, since $(a, m) = 1$, there exists s and t such that

$$sa + tm = 1.$$

This implies $sa + tm \equiv 1 \pmod{m}$. Since $tm \equiv 0 \pmod{m}$, so $sa \equiv 1 \pmod{m}$, which implies s is an inverse of a modulo m. It remains to show that this inverse is unique modulo m. Suppose s and s' are inverses of a modulo m. Then,

$$sa \equiv 1 \equiv s'a \pmod{m}.$$

Since $(a, m) = 1$, by Theorem 1.14, we can divide both sides of the congruence by a, obtaining $s \equiv s' \pmod{m}$. □

Example 1.16. Computing the inverse of 24 modulo 7

Applying the Extended Euclidean Algorithm:

$$\begin{aligned} 24 &= 3 \cdot 7 + 3 \\ 7 &= 2 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

Using backward substitution:

$$\begin{aligned} 1 &= 7 - 2 \cdot 3 \\ &= 7 - 2 \cdot (24 - 3 \cdot 7) \\ &= -2 \cdot 24 + 7 \cdot 7 \end{aligned}$$

So $s = -2$ and $t = 7$, $-2 \cdot 24 \equiv 1 \pmod{7}$.

You can use as an inverse of 24 modulo 7, any integer equivalent to -2 modulo 7, such as: $\ldots, -9, -2, 5, 12, 19, \ldots$

Solving Linear Congruences

Let the linear congruence

$$ax \equiv b \pmod{m}. \tag{1.1}$$

One possible method to solve (1.1) is to multiply both sides of the congruence by an inverse a' of a modulo m.

Example 1.17. 3 is an inverse of 4 modulo 11, since $3 \cdot 4 \equiv 12 \equiv 1 \pmod{11}$. Using this we can solve:

$$\begin{aligned} 4x &\equiv 5 \pmod{11} \\ 3 \cdot 4x &\equiv 3 \cdot 5 \pmod{11} \\ 1 \cdot x &\equiv 15 \pmod{11} \\ x &\equiv 4 \pmod{11} \end{aligned}$$

1.4.4 Chinese Remainder Theorem (CRT)

A Chinese Mathematician asked in the first century: There are certain things whose number is unknown. When divided by 3, the remainder is 2; when divided by 5 the remainder is 3; and when divided by 7, the remainder is 2. What will be the number of things? This puzzle is asking for the solution of the following system of linear congruences:

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

The Chinese Remainder Theorem establishes that when the modulus are pairwise relatively prime, we can solve such as system of linear congruences uniquely module the product of the moduli.
The CRT allows us to solve a system of linear congruences whenever the modulus are pairewise coprime.

Theorem 1.20 (chinese Remainder Theorem)**.** *Let $m_1, m_2, ..., m_n$ be pairwise relatively prime positive integers and $a_1, a_2, ..., a_n$ be arbitrary integers. Then the system:*

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_2}, \\ \quad . \qquad . \\ \quad . \qquad . \\ \quad . \qquad . \\ x \equiv a_n \pmod{m_n}, \end{cases}$$

has a unique solution modulo $m = m_1 m_2 \cdots m_n$ *given by*

$$x_0 = \sum_{i=1}^{n} M_i b_i a_i,$$

where $M_i = \frac{m}{m_i}$ *and where each* b_i *is the solution of the congruence* $(\frac{m}{m_i})b_i \equiv 1 \pmod{m_i}$

Proof. Let $m_1 m_2 \cdots m_n$; then $\frac{m}{m_i}$ is integer $(\frac{m}{m_i}, m_i) = 1$. Thus by Remark 1.2, there exist integer b_i such that $(\frac{m}{m_i})b_i \equiv 1 \pmod{m_i}$; clearly, for $j \neq i$, we have $(\frac{m}{m_i})b_i \equiv 0 \pmod{m_j}$. Define

$$x = (\frac{m}{m_1})b_1 a_1 + (\frac{m}{m_2})b_2 a_2 + \cdots + (\frac{m}{m_n})b_n a_n.$$

Then

$$x \equiv (\frac{m}{m_i})b_i a_i \equiv a_i \pmod{m_i}, i = 1, 2, ...n.$$

Therefore x is a common solution of the given congruences.

If both x^* and y^* are common solutions, then

$$x \equiv y \pmod{m_i}, i = 1, 2, ..., n.$$

Hence by Proposition 1.1

$$x \equiv y \pmod{m},$$

□

Example 1.18. Solving the original old question, that asks for a solution to

$$\begin{cases} x \equiv 2 \pmod{3}, \\ x \equiv 3 \pmod{5}, \\ x \equiv 2 \pmod{7}. \end{cases}$$

We have

$$\begin{aligned} 35b_1 \equiv 1 \pmod{3} &\implies b_1 \equiv 2 \pmod{3}; \\ 21b_2 \equiv 1 \pmod{5} &\implies b_2 \equiv 1 \pmod{3}; \\ 15b_3 \equiv 1 \pmod{3} &\implies b_3 \equiv 1 \pmod{3}; \end{aligned}$$

so the solution $x_0 \equiv 35 \cdot 2 \cdot 2 + 21 \cdot 1 \cdot 3 + 15 \cdot 1 \cdot 2 \equiv 23(mod 105)$.

1.4.5 Theorems of Fermat, Euler, and Wilson

In this section we present three applications of congruences. The first theorem is Wilson's next, we present Fermat's theorem, also known as Fermat's little theorem Finally we present Euler's theorem which is a generalization of Fermat's theorem.

Theorem 1.21. *Let p be a prime. A positive integer m is its own inverse modulo p if and only if p divides $m+1$ or p divides $m-1$.*

Theorem 1.22 (Wilson's Theorem)**.** *If p is a prime number, then $(p-1)! \equiv -1 \pmod{p}$.*

The converse of Wilson's theorem tells us whether an integer is prime or not.

Theorem 1.23. *If m is a positive integer with $m \geqslant 2$ such that*

$$(m-1)! + 1 \equiv 0 \pmod{m}$$

then m is prime.

Theorem 1.24 (Euler's Theorem)**.** *If m is a positive integer and a is an integer such that $(a, m) = 1$, then*

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Example 1.19. Note that $34 = 81 \equiv 1 \pmod{5}$. Also, $2^{\phi(9)} = 26 = 64 \equiv 1 \pmod{9}$.

Corollary 1.1 (Fermat's Little Theorem)**.** *If p is a prime and a is a positive integer with $p \nmid a$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Theorem 1.25. *If p is a prime number and a is a positive integer, then $a^p \equiv a \pmod{p}$.*

Theorem 1.26. *If p is a prime number and a is an integer such that $p \nmid a$, then a^{p-2} is the inverse of a modulo p.*

CHAPTER 2

POLYNOMIAL CONGRUENCES

In this chapter, we investigate the general polynomial congruence $f(a) \equiv 0 \pmod{m}$, where $f(x)$ is an integrl polynomial.

The essential references used in this chapter are the following: [1] and [2].

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

$$f(x) \equiv 0 \pmod{m};$$

is called a *polynomial congruence* (or textitcongruence equation) in one unknown. An integer a is called a solution or a root modulo m of the polynomial congruence if

$$f(a) \equiv 0 \pmod{m}.$$

If a is a solution of the polynomial congruence and if $b \equiv a \pmod{m}$, then by Theorem 1.14.(8), b is also a solution. Therefore, in order to solve the polynomial cogruence it is enough to find all roots that belong to a given complete residue system modulo m, e.g. to find all solutions among the numbers $0, 1, 2, ..., m-1$. By the number of solutions of a polynomial congruence we will mean the number of such incongruent solutions.

Theorem 2.1. *Let $m = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ be the unique prime factorization of m, If c is a solution of $f(x) \equiv 0 \pmod{m}$, then c is a solution of $f(x) \equiv 0 \pmod{p_i^{a_i}}$ for $i = 1, 2, \ldots, n$. Conversely, If c_i is a solution of $f(x) \equiv 0 \pmod{p_i^{a_i}}$ for each i, then there is exactly one solution c of $f(x) \equiv 0 \pmod{m}$ such that $c \equiv c_i \pmod{p_i^{a_i}}$ for $i = 1, 2, \ldots, n$.*

Proof. Since $p_i^{a_i}$ divise m for each i, it is clear that any root of $f(x)$ modulo m is also a root of $f(x)$ modulo $p_i^{a_i}$ for $i = 1, 2, ..., n$. Suppose that $f(c_i) \equiv 0 \pmod{p_i^{a_i}}$ for each i. Since the $p_i^{a_i}$ relatively prime in pairs, we can use the Chinese Remainder Theorem to find an integer c, which is unique modulo m, such that $c \equiv c_i \pmod{p_i^{a_i}}$ for each i, thus $f(c) \equiv 0 \pmod{m}$. □

It follows that in order to solve a polynomial congruence modulo m it is sufficient to know how to solve congruences with prime power modulus.

Theorem 2.2. *Let $p_1, p_2, ..., p_n$ be prime numbers and $m = p_1^{a_1} p_2^{a2} \cdots p_n^{a_n}$. If t_i denotes the number of incongruent solutions of $f(x) \equiv 0 \pmod{p_i^{a_i}}$, then the number of solutions of $f(x) \equiv 0 \pmod{m}$ is precisely $t_1 t_2 \cdots t_n$.*

Proof. Suppose that, for each i, there are t_i incongruent solutions of $f(x) \equiv 0 \pmod{p_i^{a_i}}$. Since for every distinct set of solutions of the polynomial congruences $f(x) \equiv 0 \pmod{p_i^{a_i}}$ there is a single solution of $f(x) \equiv 0 \pmod{m}$, there are then t_1 choices for c_1, t_2 choices for c_2, and so forth. Hence there will be exactly $t_1 t_2 \cdots t_n$ roots of the polynomial congruence $f(x) \equiv 0 \pmod{m}$.

Clearly, if even one of the congruences $f(x) \equiv 0 \pmod{p_i^{a_i}}$ has no solution (whence $t_i = 0$), then there cannot be any roots of $f(x)$ modulo m. □

2.1 Polynomial Congruences with Prime Modulus

Theorem 2.3 (Division Algorithm for Integral Polynomials)**.** *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 $deg\ r(x) < deg\ g(x)$.*

Proof. Let n be the degree of the polynomial $f(x)$, let ax^n be the leading term of $f(x)$, and let k be the degree of $g(x)$. If $k = 0$, then $g(x)$ is the constant 1 and there is nothing to prove, so assume $k \geqslant 1$. The proof of existence is by induction on n. If $n < k$, we take $q(x)$ to be the zero polynomial and $r(x) = f(x)$. Assume now that $n \geqslant k$ and that we have proved the existence of $q(x)$ and $r(x)$ for all polynomials $f(x)$ of degree less than n. Consider the polynomial polynomial $f(x) - ax^{n-k}g(x)$; it is a polynomial of degree $n_1 < n$, since the leading term of $f(x)$ is cancelled out, and by our induction hypothesis there exist polynomials $q_1(x)$ and $r(x)$, such that $f(x) - ax^{n-k}g(x) = q_1(x)g(x) + r(x)$ and $deg\ r(x) < k$. Obviously, the polynomials $q(x) = ax^{n-k} + q_1(x)$ and $r(x)$ fulfill the requirements, and this completes the induction step.
Now we prove the uniqueness by the absurd. Assum that there are an integral polyno-

mials $q_1(x)$, $q_2(x)$, $r_1(x)$ and $r_2(x)$ such that:

$$f(x) = q_1(x)g(x) + r_1(x) \quad \text{and } f(x) = q_2(x)g(x) + r_2(x);$$

with

$$q_1(x) \neq q_2(x),\ r_1(x) \neq r_2(x),\ deg\ r_1(x) < g(x) \quad \text{and } deg\ r_2 < g(x).$$

Hence

$$g(x)(q_1(x) - q_2(x)) = r_2(x) - r_1(x);$$

since $deg\ (r_2(x) - r_1(x)) < deg\ g(x)$, the polynomial $q_1(x) - q_2(x)$ must equal to 0 (the zero polynomial) that implies $q_1(x) = q_2(x)$, it follows that $r_2(x) = r_1(x)$. □

Example 2.1. $f(x) = 3x^5 + 2x + 5$, $g(x) = x^2 + 1$.

$$\begin{aligned} f(x) &= 3x^3 g(x) + (f(x) - 3x^3 g(x)) \\ &= 3x^3 g(x) + (-3x^3 + 2x + 5) \\ &= 3x^3 g(x) + (-3xg(x) + f(x) + 3xg(x)) \\ &= (3x^3 - 3x)g(x) + (5x + 5) \end{aligned}$$

Theorem 2.4. *Assume $f(x)$ is an integral polynomial. Then, the integer a is a solution of the congruence $f(x) \equiv 0 \pmod{m}$ if and only if there exist an integral polynomial $q(x)$ and an integer b such that*

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

Proof. Use the division algorithm to write $f(x) = (x-a)q(x) + c$, where the quotient $q(x)$ is an integral polynomial and the remainder c is a constant polynomial, e.g. an integer. Now, $f(a) = c$ and hence a is a root of the congruence if and only if $c \equiv 0 \pmod{m}$, e.g. if and only if $c = mb$ for some integer b. We now turn to polynomial congruences

$$f(x) \equiv 0 \pmod{p}$$

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, $a^p - a \equiv 0 \pmod{p}$, and hence $f(a) \equiv r(a) \pmod{p}$ for all integers a. □

Example 2.2. $p = 5$, $f(x) = x^3 + 2x - 3$. Since $f(3) = 30 \equiv 0 \pmod 5$:
$f(x) = (x - 3)(x^2 + 3x + 11) + 30$

Theorem 2.5. *If p is a prime, then every polynomial congruence $f(x) \equiv 0 \pmod p$ is equivalent to a polynomial congruence $r(x) \equiv 0 \pmod p$, where $r(x)$ is a polynomial with degree less than p.*

Another way to obtain the polynomial $r(x)$ in Theorem 2.5 is to use the following lemma.

Lemma 2.1. *Assume $n \geqslant p$ and $n \equiv r(mod(p-1))$, where $1 \leqslant r \leqslant p-1$. Then $x^n \equiv x^r \pmod p$ for all x.*

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

Using Lemma 2.1 we can replace all terms of degree $\geqslant p$ in an integral polynomial $f(x)$ by equivalent terms of degree less than p, and this will lead to an integral polynomial $r(x)$ of degree less than p having the same roots modulo p as $f(x)$.

Example 2.3. Consider the congruence $f(x) = x^{11} + 2x^8 + x^5 + 3x^4 + 4x^3 + 1 \equiv 0 \pmod 5$. Division by $x^5 - x$ yields

$f(x) = (x^6 + 2x^3 + x^2 + 1)(x^5 - x) + 5x^4 + 5x^3 + x + 1$. Hence, the given congruence is equivalent to the congruence $f(x) = 5x^4 + 5x^3 + x + 1 \equiv x + 1 \pmod 5$.

Definition 2.1. Let $f(x) = a_n x_n + a_{n-1} x_{n-1} + \cdots + a_0$ be an integral polynomial. If l be the largest integer with $m \nmid a_l$, then l is called the degree of f modulo m. If $m \mid a_i$ for every i, then the degree of f is undefined.

Theorem 2.6. *Let p be a prime. The incongruent numbers $a_1, a_2, \ldots, a_k$are roots of the polynomial congruence $f(x) \equiv 0 \pmod p$ if and only if there exist two integral polynomials $q(x)$ and $r(x)$ such that*

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

and deg $r(x) < k$.

Proof. If such polynomials exist, then $f(a_j) = pr(a_j) \equiv 0 \pmod{p}$. The 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 Theorem 2.4. 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

$$f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)q_1(x) + pr_1(x). \tag{2.1}$$

From this, since $f(a_k) \equiv 0 \pmod{p}$, we obtain

$$(x-a_1)(x-a_2)\cdots(x-a_k)q_1(x) \equiv 0 \pmod{p}.$$

Since $(a_k - a_j, p) = 1$ for $j = 1, 2, \ldots, k-1$, we can cancel the factors $(a_k - a_j)$ in the above congruence to obtain $q_1(a_k) \equiv 0 \pmod{p}$. Hence by Theorem 2.4, there is a polynomial $q(x)$ and an integer b such that $q1(x) = (x-a_k)q(x) + pb$, and by substituting this into (2.1) we find that the polynomials $q(x)$ and $r(x) = b(x-a_1)(x-a_2)\cdots(x-a_{k-1}) + r_1(x)$ satisfy all the requirements. □

Theorem 2.7 (Lagrange)**.** *Let p be a prime and let $f(x)$ be an integral polynomial of degree n not all of whose coefficients are divisible by p. Then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n solutions.*

Proof. Assume the congruence has k solutions $a_1, a_2, \ldots, a_k$, and use Theorem 2.6 to write $f(x) = (x-a_1)(x-a_2)\cdots(x-a_k)q_1(x) + pr_1(x)$. Here, the quotient $q_1(x)$ must be nonzero, because we have assumed that not all coefficients of $f(x)$ are divisible by p. Consequently, $n = deg\ f(x) = k + deg\ q_1(x) \geqslant k$. □

Application

By Lagrange's Theorem, the congruence

$$x^{p-1} \equiv 1 \pmod{p}$$

has at most $p-1$ solutions modulo p, and it follows from Fermat's Little Theorem that these are $x = 1, 2, \ldots, p-1$. It follows from the proof of Lagrange's Theorem that we have the relation

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \pmod{p}$$

Comparing coefficients of powers of x, we find from the constant coefficient in this relation that $(-1)^{p-1}(p-1)! \equiv -1 \pmod{p}$, If p is an odd prime, we conclude that $(p-1)! \equiv -1$

$(\mathrm{mod}\ p)$, and for $p = 2$ we get the same result since $1 \equiv -1\ (\mathrm{mod}\ 2)$. which is a proof of Wilson's theorem.

Theorem 2.8 (Chebyshev, 1849)**.** *Let p be a prime, and let $f(x)$ be integral polynomial of degree $n \leqslant p$ 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 $f(x) \equiv 0\ (\mathrm{mod}\ p)$ has exactly n solutions if and only if every coefficient of $r(x)$ is divisible by p.*

Remark 2.1. 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 $(a, p) = 1$. By choosing a' such that $a'a \equiv 1\ (\mathrm{mod}\ p)$ and replacing $f(x)$ by the polynomial $a'f(x) - (a'a - 1)x^n$ we obtain a new polynomial with leading coefficient 1 and with the same roots 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 Fermats's theorem $q(a)f(a) \equiv a^p - a \equiv 0\ (\mathrm{mod}\ )p$ for each integer a. Since p is a prime, it follows that $q(a) \equiv 0\ (\mathrm{mod}\ p)$ or $f(a) \equiv 0\ (\mathrm{mod}\ p)$, e.g. every integer is a solution of either $q(x) \equiv 0(modp)$ or $f(x) \equiv 0\ (\mathrm{mod}\ p)$. Now, by Theorem 2.4, the first congruence has at most m solutions and the second has at most n solutions, so together there are at most $m + n = p$ roots. Since there are p roots, we conclude that the congruence $f(x) \equiv 0\ (\mathrm{mod}\ p)$ must have precisely n solutions. Conversely, since $r(x) = x^p - x - q(x)f(x)$ it follows from Fermat's theorem that every root of $f(x)$ modulo p is a root of $r(x)$ modulo p. Hence, if $f(x)$ has n roots, then $r(x)$ has at least n roots. Since the degree of $r(x)$ is less than n, this is, however, impossible unless every coefficient of $r(x)$ is divisible by p. □

Corollary 2.1. *Assume p is a prime and that $d \mid (p - 1)$. Then the congruence $x^d - 1 \equiv 0\ (\mathrm{mod}\ p)$ has exactly d solution.*

Proof. Write $p - 1 = nd$. Use the identity $y^n - 1 = (y - 1)(y^{n-1} + y^{n-2} + \cdots + y + 1)$ and replace y by x^d. We obtain $x^p - x = (x^{p-1} - 1)x = (x^d - 1)q(x)$, where $q(x) = \sum_{j=0}^{n-1} x^{jd}$. Theorem 2.8 now applies. □

Solutions of Poynomial congruence with prime modulus

The solutions of a polynomial congruence with prime modulus can always be found by testing, that is, by substituting each of the p numbers into the polynomial congruence to see if it does indeed satisfy the equation.

Example 2.4. Consider the solutions of the congruence.

$$f(x) = x^2 + 2x + 46 \equiv 0 \pmod 7.$$

Notice that

$$f(x) \equiv x^2 + 2x + 4 \pmod 7,$$

substitute numbers 0 to 6 (numbers below the modulo until zero).

$$\begin{aligned} 0^2 + 2 \cdot 0 + 4 &\not\equiv 0 \quad 4^2 + 2 \cdot 4 + 4 \equiv 0 \\ 1^2 + 2 \cdot 1 + 4 &\equiv 0 \quad 5^2 + 2 \cdot 5 + 4 \not\equiv 0 \\ 2^2 + 2 \cdot 2 + 4 &\not\equiv 0 \quad 6^2 + 2 \cdot 6 + 4 \not\equiv 0 \\ 3^2 + 2 \cdot 3 + 4 &\not\equiv 0 \end{aligned}$$

so the solutions are $x = 1$ and $x = 4$.

2.2 Polynomial Congruences with Prime Power Modulus

The general procedure for solving the polynomial congruence $f(x) \equiv 0 \pmod m$ when m is a prime power 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.

Definition 2.2. Let the function f be n times differentiable at a. Then the polynomial $T_n(x) = \sum_{j=0}^{n} \frac{f(a)^{(j)}}{j!}(x-a)^j$ is called the nth Taylor polynomial of f at a.

Lemma 2.2. *Let p be a prime and k a positive integer. Then for every choice of x and t,*

$$f(x + p^k t) \equiv f(x) + f'(x)p^k t \pmod{p^{k+1}}.$$

Proof. In the case of a polynomial $f(x)$ of degree n, the nth Taylor polynomial of $f(x)$ at $x + tp^k$ gives:

$$f(x + tp^k) = f(x) + tp^k f'(x) + t^2 p^{2k} f''(x)/2! + \ldots t^n p^{2n} f^{(n)}(x)/n!.$$

where $f', f'', \ldots, f^{(n)}$ denote the successive derivatives of f. the coefficients in the above nth Taylor polynomial are necessarily integral, since if $f(x) = x^m$ then $f^{(k)}(a)/k! =$

$\binom{m}{k}a^{m-k} \in Z$, and it follows for general $f(x)$ by linearity. Hence, $f(a + tp^k) = f(a) + tp^k j f'(a) \pmod{p^{k+1}}$. □

Theorem 2.9. *Let p be a prime and let k be an arbitrary positive integer, and suppose that a is a solution of $f(x) \equiv 0 \pmod{p^k}$.*

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

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

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

Proof. Let b be a solution of $f(x) \equiv 0 \pmod{p^{k+1}}$ that is congruent to a modulo p^k, then $b = a + p^k t$ for some integer t. By Lemma 2.2 we have

$$0 \equiv f(b) = f(a) + f'(a)p^k t \equiv \pmod{p^{k+1}},$$

Since $f(a) \equiv 0 \pmod{p^k}$, it follows that $f(a)/pk$ is integer, and we can divide the congruence above by pk to obtain

$$f'(a)t \equiv -f(a)/p^k \pmod{p}.$$

The latter congruence has a unique solution if $(f'(a), p) = 1$, i.e. if $p \nmid f'(a)$. If $p \mid f'(a)$, then we must have $f(a)/p^k \equiv 0 \pmod{p}$, that is $p^{k+1} \mid f(a)$, in which case any value of t in a complete residue system will be a solution. Finally, if $p \mid f'(a)$ but $p^{k+1} \nmid f(a)$, there will be no t that solves the congruence. □

Corollary 2.2. *Let p be a prime and k an arbitrary positive integer. If a is a solution of $f(x) \equiv 0 \pmod{p}$ and $p \nmid f'(a)$, then there exists precisely one solution b of $f(x) \equiv 0 \pmod{p^k}$ such that $b \equiv a \pmod{p}$.*

Proof. By Theorem2.9 (i) there exists a unique solution b_2 of f(x) $f(x) \equiv 0 \pmod{p^2}$ such that $b_2 \equiv a \pmod{p}$. It follows that $f'(b_2) \equiv f'(a) \pmod{p}$, and hence $p \nmid f'(b_2)$. Therefore,

by the same theorem there exists a unique solution b_3 of $f(x) \equiv 0 \pmod{p^3}$ such that $b_3 \equiv b_2 \equiv a \pmod{p}$. Proceeding like this we will finally obtain the unique solution $b = b_k$ that is congruent to a modulo p of the congruence $f(x) \equiv 0 \pmod{p^k}$. □

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

1. First find all solutions of the congruence $f(x) \equiv 0 \pmod{p}$.

2. Select one, say a_1, then there are either 0, 1 or p solutions of $f(x) \equiv 0 \pmod{p^2}$ congruent to a_1 modulo p, if solutions exist, they are found by solving the linear congruence $f'(a_1)t \equiv -f(a_1)/p \pmod{p}$. If there are no solutions, start again with a different a_1.

3. If there are solutions of $f(x) \equiv 0 \pmod{p^2}$, select one, say a_2, and find the corresponding roots of $f(x) \equiv 0 \pmod{p^3}$ by solving the congruence $f'(a_2)t \equiv -f(a_2)/p^2 \pmod{p}$. Do this for each root of $f(x) \equiv 0 \pmod{p^2}$.

   Note that since $a_2 \equiv a_1 \pmod{p}$, $f'(a_2) \equiv f'(a_1) \pmod{p}$, so we do not need to calculate $f'(a_2)$.

4. Proceeding in this fashion, we will eventually determine all solutions of $f(x) \equiv 0 \pmod{p^k}$.

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 $f(x) \equiv 0 \pmod{p}$.

Example 2.5. Solving the polynomial congruence

$$f(x) = 4x^5 + 15x + 331 \equiv 0 \pmod{200}. \tag{2.2}$$

Solution: Notice that $f'(x) = 20x^4 + 15$. Since $200 = 2^3 \cdot 5^2$ the given congruence may be replaced by the system

$$\begin{cases} f(x) \equiv 0 \pmod{8} \\ f(x) \equiv 0 \pmod{25} \end{cases}$$

We start with the congruence

$$f(x) \equiv 0 \pmod 8;$$

by inspection we solve the following congruence, and we have

$$f(x) \equiv 0 \pmod 2 \Longrightarrow x \equiv 1 \pmod 2$$

Lift the solution to the case for $2^2 = 4$:

Since $2 \nmid f'(1) = 35$, there is a unique solution to $f(x) \equiv 0 \pmod 4$

$$\begin{aligned} f'(1)t \equiv -f(1)/2 \pmod 2 &\Rightarrow 35t \equiv -350/2 \pmod 2 \\ &\Rightarrow t \equiv -1 \pmod 2 \\ &\Rightarrow t \equiv 1 \pmod 2 \end{aligned}$$

Then we find the solution $x = 1 + 1 \cdot 2 = 3$

Lift the solution to the case for $2^3 = 8$:

$$\begin{aligned} 1635t \equiv -1348/4 \pmod 2 &\Rightarrow 1 \cdot t \equiv -337 \pmod 2 \\ &\Rightarrow t \equiv -1 \pmod 2 \\ &\Rightarrow t \equiv 1 \pmod 2 \end{aligned}$$

So the solution is $x = 3 + 1 \cdot 4 = 7$.

by inspection we solve the following congruence, and we have

$$f(x) \equiv 0 \pmod 5 \Longrightarrow x \equiv 1 \pmod 5$$

Lift the solution to the case for $5^2 = 25$: Since $5 \mid f'(1) = 35$, and $25 \mid f(1) = 350$ there is 5 solution given by $x = 1 + t \cdot 5, t = 0, 2, \ldots, 4$ Thus there are a total of $1 \cdot 5 = 5$ solutions to (2.2), for example to find one of them we solve the system

$$\begin{aligned} x &\equiv 7 \pmod 8 \\ x &\equiv 4 \pmod{25} \end{aligned}$$

Uising the Chinese Remainder Theorem we obtain the solution $x = 151 \pmod{200}$

The other 4 solutions will be:

$$\begin{aligned} x &= 31 \pmod{200} \\ x &= 11 \pmod{200} \\ x &= 191 \pmod{200} \\ x &= 71 \pmod{200} \end{aligned}$$

2.3 The Congruence $x^2 \equiv a \pmod{p^k}$

By decomposing a modulus m into a product of primes and using Theorems 2.1 and 2.2, we reduce the study of the congruence $x^2 \equiv a \pmod{m}$ to a study of congruences of the forme

$$x^2 \equiv a \pmod{p^k}$$

where the modulus is a prime power. Now, the techniques in section 2 apply. However, since the derivative of x^2 is $2x$, and $2x \equiv 0 \pmod{2}$ we have to distinguish between the cases $p = 2$ and p odd prime.

Theorem 2.10. *Let p be an odd prime and suppose $k \geqslant 1$. If $(a, p) = 1$, then $x^2 \equiv a \pmod{p^k}$ has either no solutions or exactly two solutions, according as $x^2 \equiv a \pmod{p}$ is or is not solvable.*

Proof. If the congruence $x^2 \equiv a \pmod{p}$ has no solutions, then there are no solutions of $x^2 \equiv a \pmod{p^{k+1}}$. Now suppose there is a solution of $x^2 \equiv a \pmod{p}$, say s; then $-s$ is also a solution. Since s and $-s$ are incongruent modulo p, they are the only solutions of $x^2 \equiv a \pmod{p}$, by Theorem(2.7). Clearly, s is not divisible by p, since $(a, p) = 1$. Thus if $f(x) = x^2 - a$, then $f'(s) = 2s$ is not divisible by p, and so the result follows from Theorem(2.9.(i)). (In particular, the roots s and $-s$ modulo p each produce exactly one root modulo p^k for any $k \geqslant 1$.) □

Theorem 2.11. *Suppose that a is an odd integer. Then*

(i) $x^2 \equiv a \pmod{2}$ *is always solvable and has exactly one solution;*

(ii) $x^2 \equiv a \pmod{4}$ *is solvable if and only if* $a \equiv 1 \pmod{4}$, *in which case there are precisely two solutions;*

(iii) $x^2 \equiv a \pmod{2^k}$, *with* $k \geqslant 3$, *is solvable if and only if* $a \equiv 1 \pmod{8}$, *in which case there are exactly four solutions. In particular, if s is any solution, then all of the solutions are given by* $\pm s$ *and* $\pm s + 2^{k-1}$.

Proof. Parts (i) and (ii) are obvious. Now suppose $k \geqslant 3$. If we square the 2^{k-3} odd numbers from 1 to 2^{k-2}, no two of the squares are congruent modulo 2^k . For if $a^2 \equiv b^2 \pmod{2^k}$, with $a > b$ and a and b odd, then $2^k \mid (a - b)(a + b)$. But exactly one of $a - b$

and $a + b$ is congruent to 2 modulo 4 and hence has only one factor of 2. Thus the other must be divisible by 2^{k-1}, which is impossible since $a - b$ and $a + b$ are both less than 2^{k-1}. The square of an odd number is congruent to 1 modulo 8, and there are exactly 2^{k-3} positive integers less than 2^k that are congruent to 1 modulo 8. It follows that the squares of the 2^{k-3} odd numbers from 1 to 2^{k-2} are congruent modulo 2^k, in some order, to the positive integers less than 2^k that are congruent to 1 modulo 8. Thus if $a \equiv 1 \pmod{8}$, the congruence $x^2 \equiv a \pmod{2^k}$ clearly has a solution s, with $1 \leqslant s < 2^{k-2}$. It is obvious that there cannot be a solution if a is odd and $a \not\equiv 1 \pmod{8}$. If s is a solution of $x^2 \equiv a \pmod{2^k}$, then squaring $-s$ and $\pm s + 2^{k-1}$ modulo 2^k shows that these are also solutions; by taking least positive residues, we may suppose that all of the solutions are positive and less than 2^k . It is easily checked that no two of these numbers are congruent modulo 2^k. Thus the congruence $x^2 \equiv a \pmod{2^k}$ has at least four solutions whenever $a \equiv 1 \pmod{8}$. There are 2^{k-3} such a and at least four solutions for each a; this accounts for $4 \cdot 2^{k-3} = 2^{k-1}$ odd numbers less than 2^k , namely, all of them. It follows that if $a \equiv 1 \pmod{8}$, the congruence $x^2 \equiv a \pmod{2^k}$ has exactly four solutions. □

CHAPTER 3

QUADRATIC CONGRUENCE

In this Chapter, we consider a special type of polynomial congruence, namely, the quadratic congruence $x^2 \equiv a \pmod{p^k}$, where p is a prime. As indicated in Chapter 3, The cases $p = 2$ and p odd will be considered separately. (This is necessary because we are considering quadratic congruences. The prime 5, for example, must be treated differently for polynomial congruences of degree 5.)

Now we talk about the general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

3.1 General Quadratic Congrunece

If p is odd, The study of quadratic congruences modulo p^m reduces to the case where the modulus is simply prime p. We therefore consider the general quadratic congruence

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

Theorem 3.1. *Let p be an odd prime and suppose $(a, p) = 1$. Then all solutions of $ax^2+bx+c \equiv 0 \pmod{p}$ can be found by solving the chain of congruences:*

$$y^2 \equiv b^2 - 4ac \pmod{p}, \quad 2ax \equiv y - b \pmod{p}.$$

Thus, to solve a general quadratic congruence modulo p when p is an odd prime, it suffices to solve a congruence of the form $x^2 \equiv a \pmod{p}$

Proof. Let p be an odd prime and consider the general quadratic congruence $ax^2+bx+c \equiv 0 \pmod{p}$ such that $p \nmid a$. Since $(a, p) = 1$ implies $(4a, p) = 1$, we multiply the congruence by $4a$ to get the equivalent congruence

$$(2ax)^2 + 4abx + 4ac \equiv 0 \pmod{p},$$

that is,

$$(2ax + b)^2 \equiv b2 - 4ac \pmod{p}.$$

This last congruence has exactly the same solutions as the original. □

Example 3.1. Solving the general quadratic congruence

$$f(x) = x^2 + 3x + 2 \equiv 0 \pmod{7}.$$

Solution: Since 7 is odd and $(1, 7) = 1$ the solution is given by

$$y^2 \equiv 3^2 - 4 \cdot 1 \cdot 2 \pmod{7} \quad \text{and } 2 \cdot x \equiv y - 2 \pmod{7}.$$

We obtain $y \equiv \pm 1 \pmod{7}$.

solving $y \equiv 1 \pmod{7}$ gives $x = 6$, and $y \equiv -1 \pmod{7}$ yields $x = 5$.

We now consider $ax^2 + bx + c \equiv 0 \pmod{2^m}$. Since 4 is not relatively prime to 2, the preceding argument must be modified somewhat. We can still multiply by $4a$, but to obtain a congruence with the same solutions, the modulus now must be multiplied by an appropriate power of 2.

Theorem 3.2. *Let $a = 2^r s$, with s odd. Then all solutions of the congruence $ax^2 + bx + c \equiv 0 \pmod{2^m}$ can be found by solving the chain of congruences*

$$y^2 \equiv b^2 - 4ac \pmod{2^{m+r+2}}, \quad 2ax \equiv y - b \pmod{2^{m+r+2}}.$$

Proof. Multiply the original congruence by s to get the equivalent congruence $s(ax^2+bx+c) \equiv 0 \pmod{2^m}$. The modulus need not be changed, since $(s, 2^m) = 1$. Now multiply by $4 \cdot 2r$; this time, to get an equivalent congruence, we must also multiply the modulus by $4 \cdot 2r$. The net effect is to multiply by $4a$, and we obtain the equivalent congruence

$$(2ax + b)^2 \equiv b2 - 4ac \pmod{2^{m+r+2}}.$$

This is obviously equivalent to the chain of congruences given in the statement of the theorem. □

The Congruence $x^2 \equiv a \pmod{m}$

the analysis of a general quadratic congruence $ax^2 + bx + c \equiv 0 \pmod{m}$, reduces to an investigation of

$$x^2 \equiv a \pmod{2^k} \quad \text{and } x^2 \equiv a \pmod{p} \ (p \text{ an odd prime}).$$

Theorem 3.3. *(i) If $(a, p) = 1$, then $x^2 \equiv a \pmod{p^k}$ has no solutions if $x^2 \equiv a \pmod{p}$ is not solvable and exactly two solutions if $x^2 \equiv a \pmod{p}$ is solvable.*

(ii) Suppose a is odd. If the congruence $x^2 \equiv a \pmod{2^k}$ is solvable, then it has $1, 2$, or 4 solutions according as $k = 1$, $k = 2$, or $k \geqslant 3$.

Theorem 3.4. *Let $m = 2^k p_1^{k_1} \cdots p_r^{k_r}$, and suppose $(a, m) = 1$. Then the congruence $x^2 \equiv a \pmod{m}$ is solvable if and only if $x^2 \equiv a \pmod{2^k}$ and $x^2 \equiv a \pmod{p_i^{k_i}}$ $(i = 1, 2, \ldots, r)$ are solvable. If $x^2 \equiv a \pmod{m}$ is solvable, there are 2^r solutions if $k = 0$ or $k = 1$, 2^{r+1} solutions if $k = 2$, and 2^{r+2} solutions if $k \geqslant 3$.*

3.2 Quadratic Residues

Definition 3.1. Let m be an integer greater than 1, and suppose $(a, m) = 1$. If $x^2 \equiv a \pmod{m}$ has a solution, then a is called a quadratic residue of m. Otherwise a is called a quadratic nonresidue of m.

If $a \equiv b \pmod{m}$, then clearly, a is a quadratic residue of m if and only if b is a quadratic residue of m. Thus all of the quadratic residues of m can be found by squaring the elements of a reduced residue system modulo m. Since any solution of $x^2 \equiv a \pmod{m}$ must be relatively prime to m if a is relatively prime to m.

Example 3.2. Notice that $1^2 = 6^2 \equiv 1 \pmod{7}$, $3^2 = 4^2 \equiv 2 \pmod{7}$ and $2^2 = 5^2 \equiv 4 \pmod{7}$. Thus $1, 2, 4$ are quadratic residues modulo 7 while $3, 5, 6$ are quadratic nonresidues modulo 7.

The following theorem determines the number of integers that are quadratic residues modulo an odd prime.

Theorem 3.5. *If p is an odd prime, then there are precisely $(p-1)/2$ incongruent quadratic residues of p given by*

$$1^2, 2^2, \ldots, ((p-1)/2)^2$$

Proof. Let p be an odd prime. We wish to determine the values for a, $1 \leqslant a \leqslant p-1$, for wich the equation $x^2 \equiv a \pmod{p}$ is solvable. Since $x^2 \equiv (p-x)^2 \pmod{p}$ squares of numbers in the sets $\{1, 2, .., (p-1)/2\}$ and $\{(p-1)/2+1, \ldots, p-1\}$ are congruent in pairs.

Thus, we need only consider values of x for which $1 \leqslant x \leqslant (p-1)/2$. But the squares $1^2, 2^2, \ldots, ((p-1)/2)^2$ are all incongruent modulo p, otherwise $x^2 \equiv a \pmod{p}$ would have four incongruent solutions, contradicting Lagrange s theorem.Thus, the $(p-1)/2$ quadratic residues of p are precisely the integers

$$1^2, 2^2, ..., ((p-1)/2)^2$$

□

Theorem 3.6 (Euler's Criterion)**.** *Let p be an odd prime and suppose $(a,p) = 1$. Then a is a quadratic residue or nonresidue of p according as $a^{(p-1)/2} \equiv 1 \pmod{p}$ or $a^{(p-1)/2} \equiv -1 \pmod{p}$.*

The following important result follows immediately from Euler's criterion.

Theorem 3.7. *Let p be a prime.Then -1 is a quadratic residue of p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$*

Let us finally address the question of finding a solution to the congruence $x^2 \equiv a \pmod{p}$ assuming that a is a quadratic residue of p. In the case $p \equiv 3 \pmod{4}$ we have the following answer.

Theorem 3.8. *Let p be a prime and assume that $p \equiv 3 \pmod{4}$. If a is a quadratic residue of p, then the congruence $x^2 \equiv a \pmod{p}$ has the two solutions $\pm a^{(p+1)/4}$.*

Theorem 3.9. *Let p be an odd prime. Then*

(i) *-2 is a quadratic residue of p if and only if $p \equiv 1, 3 \pmod{8}$;*

(ii) *3 is a quadratic residue of p if and only if $p \equiv \pm 1 \pmod{12}$;*

(iii) *-3 is a quadratic residue of p if and only if $p \equiv 1 \pmod{6}$;*

(iv) *5 is a quadratic residue of p if and only if $p \equiv \pm 1 \pmod{5}$.*

3.3 Legendre Symbol

Definition 3.2. Let p be an odd prime and a be an integer such that $(a, p) = 1$.**The Legendre symbol** $\left(\frac{a}{p}\right)$ is defined by

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{if } a \text{ is a quadratic residue of } p \\ -1, & \text{if } a \text{ is a quadratic nonresidue of } p \end{cases}$$

Example 3.3.

$$\begin{aligned} \left(\tfrac{1}{7}\right) &= \left(\tfrac{2}{7}\right) = \left(\tfrac{4}{7}\right) = 1 \\ \left(\tfrac{3}{7}\right) &= \left(\tfrac{5}{7}\right) = \left(\tfrac{6}{7}\right) = -1 \end{aligned}$$

Theorem 3.10. *Suppose that p is an odd prime. Then*

(i) $a \equiv b \pmod{p}$ *implies* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$;

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(iii) $\left(\frac{a^2}{p}\right) = 1$;

(iv) $\left(\frac{a^2b}{p}\right) = \left(\frac{b}{p}\right)$.

We now show when is -1 a quadratic residue of a prime p.

Corollary 3.1. *Let p be an odd prime. Then* $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 (mod 4), \\ -1, & \text{if } p \equiv -1 (mod 4). \end{cases}$

Theorem 3.11 (Euler's Criterion)**.** *Let p be an odd prime, and let a be a positive integer such that $(a, p) = 1$. Then*

$$\left(\frac{a}{p}\right) \equiv a^{\phi(p)/2} \pmod{p}.$$

Proof. Assume that $\left(\frac{a}{p}\right) = 1$. Then the congruence $x^2 \equiv a \pmod{p}$ has a solution say $x = x'$. According to Fermat's theorem, we see that

$$a^{\phi(p)/2} = ((x')^2)^{\varphi(p)/2} \equiv 1 \pmod{p}.$$

Now if $\left(\frac{a}{p}\right) = -1$, then $x^2 \equiv a \pmod{p}$ is not solvable. we have that for each integer k with $(k, p) = 1$ there is an integer h such that $kh \equiv a \pmod{p}$. Notice that $i \neq j$ since

$x^2 \equiv a \pmod{p}$ has no solutions. Thus we can couple the integers $1, 2, \ldots, p-1$ into $(p-1)/2$ pairs, each has product a. Multiplying these pairs together, we find out that

$$(p-1)! \equiv a^{\phi(p)/2} \pmod{p}.$$

Using Wilson's Theorem, we get

$$\left(\frac{a}{p}\right) = -1 \equiv a^{\phi(p)/2} \pmod{p}.$$

□

Example 3.4. Let $a = 4$ and $p = 31$. We have $(4, 31) = 1$ then:

$$\begin{aligned}\left(\tfrac{4}{31}\right) &\equiv 4^{4/2} \pmod{31} \\ &\equiv 16 \pmod{31} \\ &\equiv 1 \pmod{31}.\end{aligned}$$

Indeed, the congruence $x^2 \equiv 4 \pmod{31}$ hase two solutions modulo 31: 2 and 29.

We now determine when 2 is a quadratic residue of a prime p.

Theorem 3.12. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) = (-1)^{p^2-1/8} = \begin{cases} 1, & \text{if } p \equiv \pm 1 \pmod{8}; \\ -1, & \text{if } p \equiv \pm 3 \pmod{8}. \end{cases}$$

General conclusion

In this work, we are interested in the study of polynomial congruences. This goal forced us to begin with preliminaries of the elementary number theory. After this we started solving the polynomial congruences, where the illustration with practical examples was always present.

We have understood and concluded that, concerning a polynomial congruence, we can always decide whether congruence has a solution or not, where we can calculate the solutions if they exist.

Bibliography

[1] Andrew Adler et John E. Coury, The Theory of Numbers, Jones and Bartlett Publishers.Inc, 1995.

[2] Lars-Ake Lindahl, Lectures on Number Theory Uppsala Universitet Mathematiska Institutions, 2002.

[3] Lucia Moura, Introduction to Number Theory and its Applications, https://WW.coursehero.com/sitemap/schools/47201-Baltimore-City-College/CSI2101 Discrete Structures Winter 2010 Into to Number Theory Lucia Moura The form MAT 202 at Baltimore City College.

[4] Bernd S. W. Schröder, Mathematical Analysis A Concise Introduction, John Wiley and Sons.Inc, New Jersey, 2008.

[5] Wissam Raji, An Introductory Course in Elementary Number Theory, Saylor Foundation, 2013.

[6] Melvyn B. Nathanson, Elementary Methods in Number Theory, Springer-Verlag, New York, 2000.

[7] Song Y.Yan, Elementary Number Theory, Springer, Berlin, 2002.

[8] K. Rosen, Elementary Number Theory and its Applications, 4th Edition, Addison Wesley, 2000.

[9] W.Edwin Clark, Elementary Number Theory, Departement of Mathematics, University of South Florida USA, 2003.

[10] W.D. Wallis A Beginnerâ€™s Guide to Discrete Mathematics, 2nd Edition, Southern Illinois University Carbondale,Springer Science+Business Media, 2012.

ملخص:

في هذا العمل المتواضع، نحن مهتمون بدراسة التوافقات متعددة الحدود (Polynomial Congruences). لهذا السبب درسنا المفاهيم الأساسية لنظرية الأعداد الأولية في المقام الأول؛ ثم بدأنا حل التطابقات متعددة الحدود. طوال العمل، كانت النظرية مصحوبة دائمًا بأمثلة عملية للحساب.

لقد فهمنا أنه فيما يتعلق بالتوافق متعدد الحدود (Polynomial Congruence)، يمكننا دائمًا أن نقرر ما إذا كان التطابق يحتوي على حل أم لا، حيث يمكننا حساب الحلول إذا كانت موجودة.

الكلمات المفتاحية: العدد الأولي، ترديد، توافق متعدد الحدود.

Résumé:

Nous nous sommes, dans ce modeste travail, intéressé à l'étude des congruences polynomiales. Pour cette raison nous avons étudié les notions fondamentales de la théorie élémentaire des nombres en premier lieu ; puis on a entamé la résolution des congruences polynomiales. Tout au long du travail, la théorie était toujours accompagnée avec des exemples pratiques de calcule. Nous nous sommes arrivé à comprendre que concernant une congruence polynomiale on peut toujours trancher si la congruence possède une solution ou non où nous pouvons calculer les solutions s'ils existent.

Mots-Clés: Nomber premier, Modulo, Congruence polynomial.

Abstract:

We have, in this modest work, interested in the study of polynomial congruences. For this reason we have studied the fundamental notions of the elementary theory of numbers in the first place; then we started the resolution of the polynomial congruences. Throughout the work, the theory was always accompanied by practical examples of calculation. We have understand that concerning a polynomial congruence we can always decide if the congruence has a solution or not, where we can calculate the solutions if they exist.

Keywords: Prime number, Modulus, Polynomial Congruence.